European Commission

JRC SCIENCE FOR POLICY REPORT

Testing and certification of automated vehicles (AV) including cybersecurity and artificial intelligence aspects

A review on testing and certification of AV with specific focus on cybersecurity and artificial intelligence aspects

Baldini, G.

2020

Joint Research Centre

EUR 30472 EN

Contact information
Name: Gianmarco Baldini
Address: European Commission, Joint Research Centre, Via Enrico Fermi 2749
Email: gianmarco.baldini@ec.europa.eu
Tel.: +39 0332 78 6618

EU Science Hub
https://ec.europa.eu/jrc

JRC121631

EUR 30472 EN

PDF ISBN 978-92-76-26818-5 ISSN 1831-9424 doi:10.2760/86907

Luxembourg: Publications Office of the European Union, 2020

How to cite this report: Baldini, G., Testing and certification of automated vehicles including cybersecurity and artificial intelligence aspects, EUR 30472 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-26818-5, doi:10.2760/86907, JRC121631.

Contents

Foreword

Autonomous/Automated vehicles (AVs) are becoming a reality. Prototyping and testing of autonomous vehicles technologies is increasingly happening around the world. The safe deployment of autonomous vehicles includes many different technologies, competences and processes, which must be tested and evaluated with a high degree of accuracy because the safety in road transportation may be at risk. At the same time, machine learning and artificial intelligence is becoming increasingly important in the digital world and this is an essential element of autonomous vehicles. The robustness of machine learning and artificial intelligence must be tested both against unintentional and intentional adversarial events. The latter may be due to cybersecurity threats, which can become present in the evolution of the road transport including the future deployment of AVs. Before AVs are actually deployed in the road infrastructure, all these aspects must be evaluated and tested with a rigorous process, which can be quite cumbersome due to the complexity of AVs as cyber physical system and the road infrastructure context where AVs have to operate. To gain a better understanding of these aspects and how they are linked among them, DG.JRC.E3 has started a study on testing and certification of autonomous vehicles with a focus on artificial intelligence and cybersecurity, whose output is this report.

Acknowledgements

I acknowledge the colleagues of DG JRC E.3 (in particular Jose Luis Ramos Hernandez), DG JRC C.4 (in particular Maria Cristina Galassi and Biagio Ciuffo) and DG GROW.C.4 for their valuable input to the report, for reviewing it and for providing relevant references used in this report.

Authors

Gianmarco Baldini

Executive summary

This report focuses on the testing and certification of autonomous vehicles (AV) and the technologies and components used in their implementation. Autonomous vehicles are very complex cyber physical systems composed by many inter-connected components like sensors, actuators and artificial intelligence processors. They are supposed to operate with high accuracy and safety with limited presence of human drivers or completely in their absence (i.e., driverless cars). In addition, they are supposed to be robust against unintentional or intentional malfunctions, which can be caused by cybersecurity threats as vehicles will be increasingly connected, which can be exploited by cybersecurity attackers.

The report reviews the existing activities at global and European level for testing and certification of autonomous vehicles with a particular focus on the current revision of the UNECE regulatory framework.

Then, the report focuses on three separate elements of testing of automated vehicles: a) definition of processes for cybersecurity testing and mitigation of cybersecurity threats, b) testing and evaluation of artificial intelligence components of the automated vehicles and c) definition of database scenarios and languages for testing of automated vehicles. These areas have been selected because they address gaps in the policy support analysis needed by DG GROW C.4.

On each of these areas, the report identifies key recommendations at regulatory and standardization level.

Policy context

Type approval of vehicles is a specific concept of Type Approval applied to the automotive sector. The current regulatory framework for Type Approval of motor vehicles is centered on the United Nation's World Forum for Harmonization of Vehicle Regulations, which is charged with creating unified automotive standards and regulations to facilitate international trade.

The revision of the UNECE regulations for automated vehicles has been the focus of the work of Working Party 29 (WP29), which is a unique worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee. In particular, Working Party on Automated/Autonomous and Connected Vehicles (GRVA) was created on June 2018 to revise the Type approval regulation for the future automated/autonomous and connected vehicles with a list of priorities, which included definition of Functional Requirements ("FRAV"), Validation Method for Automated Driving ("VMAD"), Cyber security (and software updates), ADAS and Braking Systems.

Key conclusions

Type approval (including testing and certification) of automated vehicles may be a very complex task where there are still many open questions at regulatory, industry and research level. This report proposes a set of recommendations for policy makers, standardization bodies, industry and research communities to foster an adequate testing of automated vehicles before they are deployed in the market.

Main findings

This report provides a set of recommendations in the different different areas of cybersecurity, artificial intelligence, software update in AV and scenarios defintion for Type Approval of AVs.

Regarding **cybersecurity aspects**, the report recommends a review of existing accreditation schemes in Europe to verify if they are adequate to support the auditing of the Cyber Security Management System (CSMS) of AV manufacturers. In addition, the report recommends the set-up of a *vulnerability database* and an associated process for the reporting of threats and vulnerabilities in AV (for all levels of automation) at European level.

Regarding **Artificial Intelligence in** AV this report recommends the definition of harmonized metrics to evaluate the test coverage of artificial intelligence algorithms and to improve research efforts to make the AI components in AVs more robust against adversary machine learning.

Regarding the design and implementation of **software update in AV**, this report recommends an increase in research and standardization efforts to improve the efficiency and coverage of of software testing in particular for the software update. Efficiency is needed to support a rapid assessment and deployment of

software updates in the AVs present in the field. Coverage is needed to ensure that sotware updates are tested in the widest set of scenarios and contexts.

Regarding the **Type approval of AV**, various recommendations are put forward. One recommendation requires the definition of a common scenario database based on a common language at European level and the definition of common processes with a clear definition of roles for the main stakeholders in the AV domain. Another recommendation is to support the definition of adequate metrics for the selection and filtering of scenarios. In addition, this report recommends the definition of a process to collect information from the market, which can be used to improve the scenario definition and the scenario database.

Related and future JRC work

This report is related to other reports produced by the JRC in the area of road transportation, artificial intelligence, cybersecurity and type approval. In particular, it is related to the 'The future of road transport – Implications of automated, connected, low-carbon and shared mobility' (EC 2019c) for the aspects or road transportation. This report is related to the JRC report investigating the robustness of Artificial Intelligence in the digital domain (Robustness and Explainability of Artificial Intelligence (EC 2020b)). Regarding Cybersecurity aspects in the digital society, this report is related to the report 'Cybersecurity, our digital anchor' (EC 2020c). Regarding the aspects of type approval of automotive vehicles, this report is related to (Galassi 2020a).

The JRC will continue to support DG GROW and DG MOVE in the evolution of road transport with a particular focus on the Type Approval of AV, cybersecurity aspects and the application of Artificial Intelligence in AV.

1 Introduction

Autonomous or automated driving (in the rest of this report the two terms are used in the same meaning) is a new technology, which has the promise to change dramatically our life. One of the main current references on automated driving (SAE 2016a) defines 6 levels of automated driving starting from level 0 with no automation to level 6, which is the fully automated vehicles. There are already in the market Autonomous Vehicles (AV) up to level 3 and level 4 are expected to be in the market in the next 3-4 years (Bhutani 2018).

At the same time, the automotive industry is changing rapidly in different dimensions: the increasing shift to electric vehicles, the application of different forms of connectivity to modern vehicles (DSRC and cellular connectivity), the greater sensitivity to cybersecurity and privacy concerns. All these changes will integrate each other in ways yet to be seen.

Regulators are facing this evolving scenario and they have the challenge to formulate adequate policies which (on one side) ensure the safety of citizens and (on another side) foster the development and deployment the market and innovation in AVs industry. One important aspect, which is addressed in this report, is the testing of AVs (i.e., Type Approval or homologation), which is expected to be evolve and/or be integrated in the current regulatory framework of Type Approval (UN 1958), (EC 2019b).

The validation and verification of AVs poses interesting challenges: in particular the testing of the Artificial Intelligence (AI) components, which is supposed to replace the human driver component. Testing of cybersecurity aspects is also quite important because a cybersecurity threat to AVs may produce significant safety hazards.

Regulators, standardization bodies and industry have already started to look at testing of AVs (see Section 2.2 for a review of the current activities). The aim of this report is to investigate and summarize the current activities in this area and analyze in detail specific testing aspects including the assessment of the AI component of the AVs, testing of cybersecurity, definition of AV testing scenarios and related scenario database.

Note: a definition of the concepts identified in this report is provided in the List of Definitions at the end of this report.

1.1 Problem statement

Autonomous driving systems will be one of the most complex systems ever implemented and they aim to replicate the driving capabilities of human beings. AVs are arguably going to be heavily based on artificial intelligence algorithms in a cyber-physical system. Even if AI has achieved remarkable capabilities in many areas, their application to a domain where safety aspects are relevant requires additional care. In particular, AV needs to be carefully evaluated before their deployment in the market. This is a novel area of work and it presents many challenges. The main challenge is to guarantee a complete coverage of testing for all the possible driving situations. This is a slow and costly process, which could hamper the market deployment of these technologies. Moreover, we cannot allow untested vehicles to be deployed on the road. This trade-off is one of the most significant challenge for testing and certification of AVs.

Another significant challenge is that, AVs may be based on updatable software which may subject to another testing and certification phase. From this point of view, a fine balance must be reached between the need to deliver software updates to the AVs in time to support their operational needs and the need to properly test the software update before distribution to AVs. This aspect is particularly important for the software update and testing of AI algorithms, which implement the cognitive capabilities of the AV and which are directly related to safety hazards on the road.

Finally, the potential of cybersecurity attacks should also be addressed as cybersecurity can generate significant safety hazards when the driver is absent or not full in control. Even if government, industry and research communities have increased their attention to cybersecurity aspects of AVs (e.g., identification of threats and vulnerabilities), cybersecurity testing of AVs is a novel area, which still requires further developments.

1.2 Scope of the report

The scope of this report is to analyze in detail the challenges identified in the problem statement above. In particular, the report identifies and analyzes the most significant challenges in the testing and certification of AVs at the technical level for three specific aspects: cybersecurity testing, testing of the artificial intelligence component in AV and definition of the database scenarios to drive the Type Approval process of AVs. The report focuses on these specific aspects because they are considered the highest priorities for the testing of automated vehicles (see Section 2) and because they address gaps in the policy support analysis for the upcoming Type Approval regulations in Europe for AVs.

The scope of this report is not to provide a comprehensive view on the evolution of the Type Approval for AVs. This aspect is addressed in other JRC reports. See for example (Galassi 2020a).

This report does not address specific organizational aspects related to the assessment of AV manufacturers or other stakeholders involved in the Type Approval process.

This report has been produced to support DG GROW.C.4 for the drafting of policies for the Type Approval of automated vehicles in Europe.

1.3 Structure of the report

- Section 2 describes the overall framework for testing and validation of autonomous vehicles and a description of the main components. This section also provides a review on the current regulatory, industry and standardization activities on testing and validation of AVs.
- Section 3 This section focuses on the risk assessment process, cybersecurity certification and secure software update processes, which may part of the future Type Approval framework.
- Section 4. This section focuses on the specific aspect of testing and certification of the artificial intelligence (AI) component in the AV. In particular, it deals on the aspects related to robustness of the artificial intelligence algorithms against intentional and unintentional malfunctions.
- Section 5. This section focuses on the definition of scenarios for AVs focuses on the definition of scenario for the testing of AVs including cybersecurity and AI aspects. Coverage of testing scenarios, the ratio of real and simulated scenarios and metrics for scenario evaluation are the aspects addressed in this section.
- Section 6 provides recommendations to policy makers and standardization bodies based on the results of the analysis.
- Section 7 provides the conclusions and future developments.

2 Testing and certification of autonomous vehicles: a multidisciplinary approach

Testing and certification of AVs may require a multidisciplinary approach which includes a variety of disciplines. AVs are still essentially machines, represented in their simplest form as a combination of a vehicle body, wheels, tires and some method (e.g., electric or fuel based) of propulsion. The absence of the human driver component makes the verification and validation of AVs before market deployment a complex task. Testing of AVs should include assessment of cyber physical design of the AVs, testing of the AI components, cybersecurity assessment, evaluation of the quality of the sensors and certification of the methods to update the AVs functions (e.g., software update). This is not an exhaustive list as all the human driving functions must be assessed.

To replicate the human driving functions, the AVs must implement a set of functions, which are pictorially described in the following Figure 1.

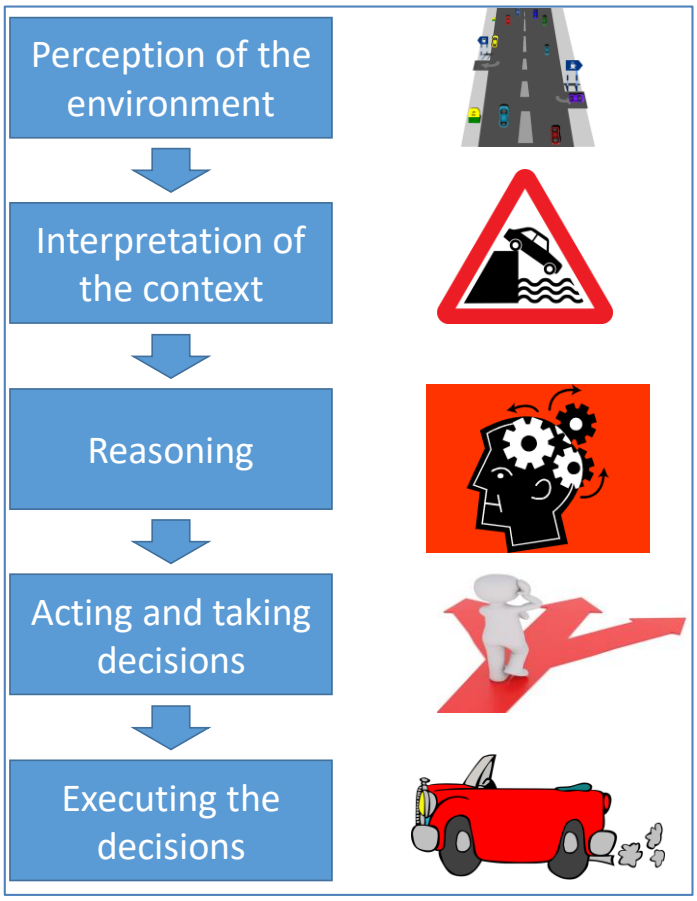

Figure 1 The different functions of Automated Vehicles

A brief description of the different functions of automated vehicles is shown below:

- *Perception of the environment*. This function is responsible to collect information from the road infrastructure using the sensors, which are installed in the vehicle: cameras, LIDARs, Inertial Measurement Units (IMU) and so on. This may include also messages received from the road infrastructure or other vehicles through wireless communication means.
- *Interpretation of the context*. This function is responsible to interpret the data received from the sensors and prepare it for the reasoning process. For example, the interpretation of a sign is part of this function.
- *Reasoning*. This function includes all the Artificial Intelligence (AI) subtasks, which must create a cohesive understanding from the interpretations created by the function below. For example, the interpretation of the image of a pedestrian crossing the road must be correlated with the current speed information received from the odometer to understand if a decision must be taken.

- *Acting and taking decision*. This function is responsible to make a decision from the output of the reasoning function. Taking the example of the reasoning function, this function may decide to turn the vehicle left or right, braking or both actions.
- *Executing the decisions*. This function is responsible to execute the decision taken in the previous function above. For example, the AV may decide to brake.

Theoretically all these functions must be tested in the Type Approval/homologation phase of the AV. There are a number of challenges to achieve this objective as discussed in following subsection 2.3. For example, the decision of an AV in a specific scenario must not only be correct (e.g., the pedestrian is avoided) but also executed in a timely fashion (e.g., change of collision course with another vehicle is executed in a specific time). It is also difficult to anticipate a priori all the potential situations where an AV can be involved.

Each of these functions mentioned above can also be the target for a cybersecurity attack, which may hamper the behavior of the AVs in the road, with the risk of safety hazards or non-conformance to regulations.

2.1 Testing framework

To introduce some of the concepts, which are described more in detail in the rest of this report, we provide a high-level overview of what could be the main components of a testing framework in the Figure 2 below. Some of the testing activities will be described more in detail in the rest of the report.

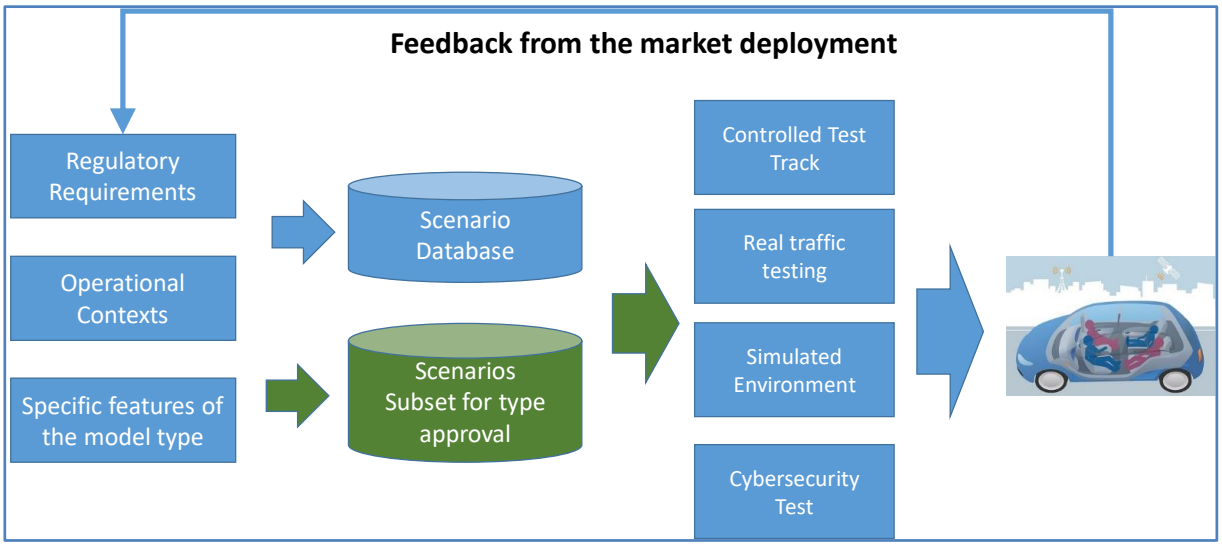

Figure 2 Potential Type Approval phases

A brief description of each phase is reported below. Some of the phases will be further described in the rest of this report:

- *Requirements definition*. The requirements from regulations at international level (UNECE 2020a), (UNECE 2020b) (see subsection 2.2.1) can be used to drive the definition of scenarios together with other sources of information including the operational contexts (urban environment, highways) where the AVs must operate.
- *Database of scenarios*. A database scenario is created either at government level or for the specific manufacturer. Depending on the specific model type of AV (commercial vehicle or passenger vehicle), specific scenarios should/could be selected from the overall set of scenarios.
- *Testing*. Each scenario can be used in a different testing environment: a controlled test track environment, real traffic testing in a normal traffic environment or a simulated environment.

Some scenarios are specific for cybersecurity testing to assess the robustness of the AV against cybersecurity threats.

- *Feedback from the market deployment*. After the deployment phase, information from the performance of the AV in the field can be used as a feedback to the definition of high level requirements for the creation or update of existing testing scenarios.

2.2 Review of the state of art

This subsection aims to review the state of art in different areas: regulatory and policy frameworks, report from industry and industry association and from the research community. A subsection on the current standardization activities in this sector (e.g., SAE) is also included.

2.2.1 Regulatory/Policy frameworks

Type Approval of vehicles is a specific concept of Type Approval applied to the automotive sector. The current regulatory framework for Type Approval of motor vehicles is centered on the United Nation's World Forum for Harmonization of Vehicle Regulations, which is in the charge of creating unified automotive standards and regulations to facilitate international trade. Currently, under the auspices of the Forum, more than 100 separate regulations applicable to passenger vehicles have been developed. Three UN Agreements, adopted in 1958, 1997 and 1998, provide the legal framework allowing Contracting Parties (member countries) attending the WP.29 sessions to establish regulatory instruments concerning motor vehicles and motor vehicle equipment.

The revision of the UNECE regulations for automated vehicles has been the focus of the work of Working Party 29[1] . As described in the WP29 web site: "The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) is a unique worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee".

In particular, Working Party on Automated/Autonomous and Connected Vehicles (GRVA) was created on June 2018 to revise the Type approval regulation for the future automated/autonomous and connected vehicles with a list of priorities (the following test is extracted from (UNECE 2020c)), which included definition of Functional Requirements ("FRAV"), Validation Method for Automated Driving ("VMAD"), Cyber security (and software updates), ADAS and braking Systems. This report focuses only on specific aspects of the revision of automated vehicles. Recently (June 2020) the regulations for cybersecurity (UNECE 2020a) and Over The Air (OTA) software update in automated vehicles (UNECE 2020b) have been approved by the GRVA steering board and they are discussed in this report in Section 2.2.1.

In the European Union, Type Approval is regulated by ECE Regulations and by Decision 97/836/EC (EC 1997). As described in (EC 2007), "when the Community has decided to apply on a compulsory basis a UNECE Regulation for the purpose of EC vehicle type-approval in accordance with Article 4(4) of Decision 97/836/EC, the annexes to the Frame Directive shall be amended as appropriate in accordance with the regulatory procedure with scrutiny referred to in Article 40(2) .The UNECE Regulations listed in Part II of Annex IV are recognised as being equivalent to the corresponding separate directives or regulations in as much as they share the same scope and subject matter. Where the Community has decided to apply a new UNECE Regulation or a UNECE Regulation as amended, Part II of Annex IV shall be amended as appropriate".

We also note that automotive EC Directives and ECE Regulations require third party approval - testing, certification and production conformity assessment by an independent body. Each member state is required to appoint an Approval Authority to issue the approvals, and a Technical Service to carry out the testing to the Directives and Regulations.

The testing of essential operational and safety systems in automobiles is also the focus of national new car assessment programs (NCAPs). The NCAPs have been established in the late 1970s by the U.S. National Highway Traffic Safety Administration (NHTSA), NCAPs have been subsequently adopted by the

[1] https://www.unece.org/trans/main/wp29/introduction.html

automotive industry in other parts of the world, including the European New Car Assessment Program (Euro NCAP)[2].

Even if it is not a regulation, the US report "Preparing for the Future of Transportation: Automated Vehicles 3.0" (USDOT 2018) provides important recommendations on potential regulatory actions by the US Department of Transportation. In particular, the report claims that it is important to have federal regulations for AV, even if in general the U.S.A. does not have any unique federal regulations and only provides guidelines to the state governments. The primary focus of (USDOT 2018) is on safety and the integration of AVs with the existing road infrastructure and other modes of transportation. State, local, and tribal jurisdictions are identified as responsible for "licensing human drivers, registering motor vehicles, enacting and enforcing traffic laws, conducting safety inspections, and regulating motor vehicle insurance and liability" as well as "planning, building, managing and operating transit and the roadway infrastructure".

In Europe, (EC 2016) described the overall strategy for cooperative, connected and automated mobility, thus supporting the integration of connectivity and automated vehicles technologies. A list of specific actions are identified in the communications to foster the definition of compliance assessment process, support for hybrid connectivity, ensuring safety and security in the operation of cooperative, connected and automated technologies and so on. The actions are linked to on-going European projects like C-ROADS (CROADS 2020).

The European Commission(EC) also launched GEAR 2030 in 2016 to explore solutions to AV-related issues, and in February 2017 the group made recommendations for using Event Data Recording (EDR) devices. In May 2016, the European Parliament recommended that the EC should create a mandatory insurance scheme to safeguard full compensation for victims of AV accidents and a legal status should be created for all robots to determine liability in accidents.

Since 2018, the JRC Sustainable Transport Unit in DG JRC supports the Commission (DG GROW) in the evaluation of different innovative approaches to be introduced in the new AVs type-approval legislation for the safety certification of automated vehicles. The JRC SAFE-TYPE project was setup in this framework and defines the objectives in terms of desktop and experimental research activities, as well as outreaching activities and collaboration in internationals working groups, including contribution to UNECE GRVA activities. See (Galassi 2020a) and (Galassi 2020b) for further details.

2.2.2 Standardization activities

Standardization bodies have started to investigate the development and testing of automated vehicles and their activities are reported here.

ISO 26262, "Road vehicles – Functional safety." (ISO 26262) was originally published by the International Organization for Standardization (ISO) in 2011 and represents an adaptation of IEC 61508, "Functional safety of electrical/ electronic/programmable electronic safety-related systems." The safety requirements in ISO 26262 are based on a qualitative assessment of specific risks linked to the malfunction of electrical and electronic systems under anticipated operating scenarios.

SAE has been also particularly active in the area of automated vehicles and cybersecurity. SAE J3016 (SAE 2016) has defined the levels of automated vehicles, which are commonly used in literature. SAE J3061 (SAE 2016a) establishes a set of high-level guiding principles for Cybersecurity as it relates to cyber-physical vehicle systems like automated vehicles. At the time of writing this report (August 2020), the standard is still under development but it should be finalized soon.

The ISO/SAE DIS 21434 "Road vehicles — Cybersecurity engineering", which is also under development at the time of writing this report (October 2020) defines requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces. While the standard is for modern automotive vehicles in general, it can also be applied to automated vehicles (UNECE 2020a).

Note that a more extensive study of the mapping of standards applicable to cybersecurity in automated vehicles in provided in Section 3 of this report.

[2] https://www.euroncap.com/

2.2.3 Industry activities

Industry has been obviously involved in the development and production of AVs in recent years with levels 2 and 3 of automation already deployed in the road that provides significant competitiveness advantages to the AV manufacturers.

In this subsection, we briefly report on positions papers produced by industry representatives or industry associations in relation to regulatory aspects and more precisely on testing/certification of AVs.

ACEA produced a position paper in 2019 (ACEA 2019) "Roadmap for the deployment of automated driving in the European Union", which identifies a time plan and key regulations, which should be defined for the deployment of AVs in the market. Some of the regulations are already in place (Cybersecurity Act) but others should be created ex-novo. The proposed set of regulations are identified within their context (international or European) and a for a wide range of aspects: safety, cybersecurity and so on.

The author in (TUV 2020) focuses on the regulatory aspects for the homologation of AV. The position paper reviews the current regulatory status and claims that there are still significant regulatory gaps to be fulfilled. Then, the position paper proposes a six-point approach for developing future homologation and approval regulations for automated vehicles, which is based on:

1. Establish scenario-based testing approach as state of the art.
2. Establish a comprehensive and globally-accessible database for testing scenarios.
3. Determine the criticality metrics essential to safe automated operation.
4. Integrate simulation into the homologation process and recognize the validity of virtual methods in regulatory approval schemes.
5. Enforce the assessment of functional safety in the certification or homologation process.
6. Use real-world driving as a final validation of operational safety.

BMW e-book on autonomous vehicles (BWM 2020) also gives some indications on the potential regulations actions. One key recommendation is that manual, automated, and self-driving modes each need their own regulation because humans and machines are too different in their reaction times and in how they perceive and analyze traffic situations for the application of the same set of regulations. In addition, automated vehicles and humans learn about traffic regulations in different way. In particular, AV must be able to learn traffic regulations using machine interpretable language, which should not leave space to ambiguities. There are also interoperability issues on traffic regulations definitions across different jurisdictions, which can be relatively easy to interpret by human beings through signs, but AVs may also receive the rules in a digital format (see also (Baldini 2020) for a discussion on machine interpretable traffic regulations and a potential deployment approach).

The PEGASUS project was promoted by German Federal Ministry for Economic Affairs and Energy (BMWi) for the establishment of generally accepted quality criteria, tools and methods as well as scenarios and situations for the release of highly-automated driving functions. Its objective is to develop and demonstrate methods, criteria, tools and guidelines to safeguard highly automated driving functions (Level 3), in order to facilitate the rapid implementation of automated driving into practice (PEGASUS, 2020). In particular, the PEGASUS project has defined a comprehensive framework for the verification and validation of automated vehicles like the one shown in Figure 3 below, which describes the overall flows and key components of the framework.

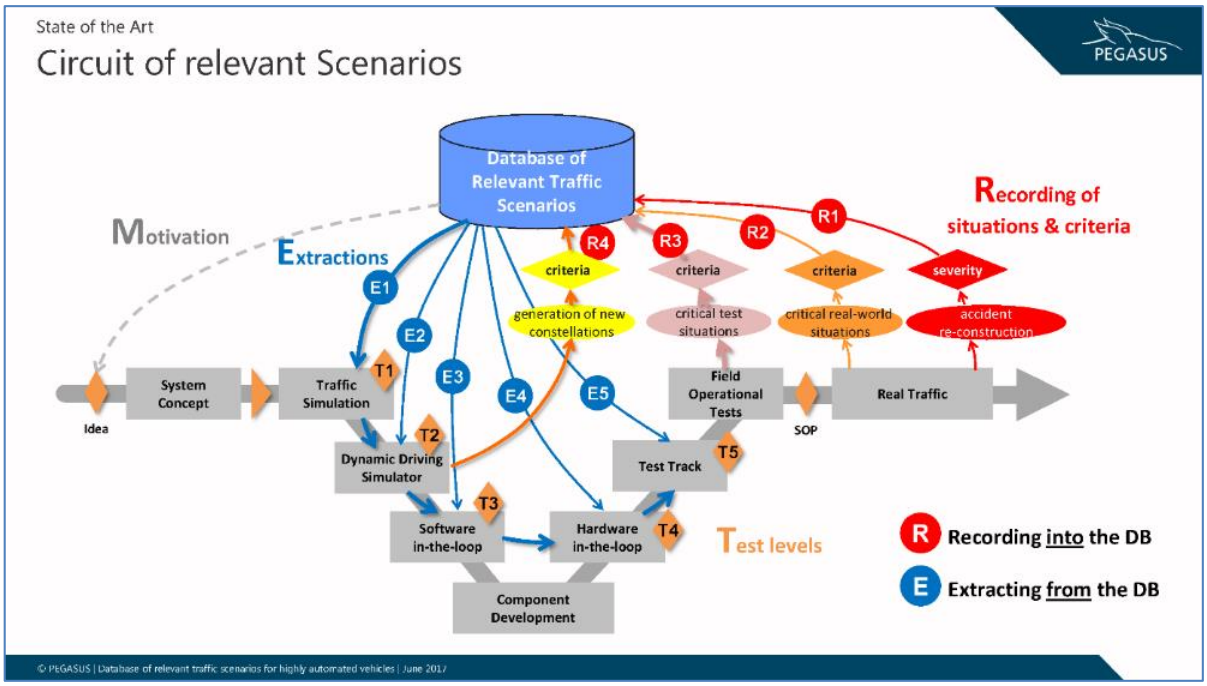

Figure 3 PEGASUS framework for verification and validation of automated vehicles (From (PEGAGUS 2020))

2.2.4 Research studies

In this section, we report on recent studies on the comparison of regulatory frameworks for automated vehicles. Because automated vehicles technologies and related regulations activities are quite recent, only studies in the period 2018-2020 are evaluated.

The conclusions of the references study are reported. This does not imply the acceptance of the conclusions by the author of this report and/or the European Commission.

(Taeihagh 2019) have conducted an extensive review of the regulatory activities (or lack of them) in various parts of the world with specific focus on liability, cybersecurity, privacy and societal impact. The conclusions by the authors of the study show that a number of regulatory challenges must still be resolved. In particular, the liability scheme is not clear on who/which entity should take the liability in case of an AV accident. The societal impact on the job destruction (e.g., commercial vehicle drivers and taxi drivers) due to the introduction of AVs was also pointed out as a priority for government. The study highlighted the risk for cybersecurity and privacy and pointed out to various initiatives to mitigate related threats through a combination of regulations, best practices and standards to be adopted.

A study and comparison among regulatory frameworks for automated vehicles is also available in (Lee 2020), The report compares existing government activities and recent regulatory actions around the world. In particular, the study examines in detail the regulatory activities by USA (with a focus on California), Europe (with a focus on Germany) and Australia. The study highlighted some potential challenges not only related to safety and liability aspects due to malfunctions of AVs, but also issues in the public acceptance of AV technologies in the field. Then, the study reports various best practices, which could be adopted (and which are also related to testing, which is the scope of this report) including:

- On-road testing of vehicles should have at least one human safety driver who is ready to take control to maximize safety until the on-road testing of AVs is more advanced.
- The requirement of a black box for safety investigations, which is already implemented in some countries, would help to improve knowledge and to determine liability in the event of an accident.
- Test drivers of AV and remote monitors should be able to deactivate the system easily and at any time.
- Test drivers of AV should receive a specific training.

(Shladover 2019) reports on the experiences and lessons learnt from the initial regulation activities and testing of AV in the state of California in USA. The authors of the study identified some specific certification challenges (which are also discussed in the rest of this report):

- It is important and difficult to distinguish between the capabilities or competency and the functional safety of the automated driving system because these are developed and deployed in a different way. Competency describes how well the automation behaves when dealing with hazards in the normal external driving environment, while functional safety describes how well the system deals with internal faults and failures".
- It is not clear if the certification should be performed by an independent third party, by the manufacturer itself through a self-certification or by the government as a specific type of independent third party. Each of these approaches has advantage and disadvantages.
- It is difficult to ascertain if an automated vehicle system is sufficiently safe that it should be permitted to use public roads on a regular basis.

Some of the challenges identified by the authors are summarized in the following subsection 2.3.

2.3 Summary of the challenges for testing and certification

We summarize the challenges for testing and certification identified in the previous sections:

- Regulations for testing of automated vehicles should be harmonized at international level (this challenge is currently addressed by UNECE WP29 GRVA)
- Testing in real traffic conditions requires special conditions and training for the test drivers and manufacturers because the AV is not yet Type Approved in the testing phase and software failures may create safety hazards.
- Testing of AVs is a very complex task, which should be addressed using different testing phases and environments.
- Testing coverage is difficult to determine a-priori in comparison to the Type Approval of conventional vehicles as the space of potential scenarios could be unlimited.
- Cybersecurity testing is particularly important in the testing of AV because of the safety hazards and the potential absence or limited presence of a human controller.
- Because AV can be dependent on software updates to improve the AI components of the AV, periodic testing and calibration should be performed during the lifecycle of the AV. This is also needed because AI algorithms are dependent on the quality of the data originating by the sensors which could degrade in time.

Some of these challenges will be further discussed in the rest of this report in relation to cybersecurity testing, testing of artificial intelligence and scenario database.

3 Assessment of cybersecurity aspects for testing of autonomous vehicles

Assessment of cybersecurity aspects for autonomous vehicle is a wide area, which can involve different processes and roles. It is also an emerging discipline because AV are still mostly in a prototype phase regarding the highest levels of automation (level 5 of SAE automated vehicles levels) but lower levels of automation are already deployed and there is an increasing awareness of cybersecurity threats of AVs, also because of the parallel introductions of different forms of connectivity in modern vehicles, which can extend the surface attack. The reason is that cybersecurity attackers do not need to physically access the vehicle to implement the attack, but they can connect remotely through the connectivity link. One example of this possibility was shown by (Miller 2015), where researchers were able to perform a remote attack against an unaltered 2014 Jeep Cherokee which resulted in physical control of some components of the vehicle.

Then, the aim of this section is firstly to provide a high level view of the cybersecurity aspects in AVs and what types of processes should be set up including risk assessment and vulnerability analysis. In many cases, existing standards in the cybersecurity domain can be customized and tailored to the AV context to support the implementation of these processes. In other cases, standards, which were started specifically for the AV context, are still under development at the time of writing this report.

Then, the section discusses specific aspects like the secure development and engineering process (which must be evaluated in the audit process), the aspects related to software and hardware integrity, how the lifecycle of autonomous vehicles is related to cybersecurity aspects (when an update must be performed and how the cybersecurity certification is affected). Deployment aspects are also considered: definition of organization and capabilities needed by specific elements of the AV operational framework. Related standards are also identified.

Three main sets of processes are identified:

1. A set of processes for the cybersecurity testing and certification of the AV type focuses on the identification of the main risks, threat scenarios and testing of the potential mitigation techniques and solutions, which are adopted by the manufacturer.
2. A set of processes for the cybersecurity assessment of the manufacturer is needed to ensure that specific standards for the design and development of AVs are met. The validation of these sets of processes is part of the audit process.
3. Regarding the lifecycle of the AVs, a set of processes should also be set in place to support a trusted environment, which is robust against cybersecurity threats. These processes include security checks for third party providers, workshops, passengers and drivers (at levels of automation less than 5) when they interact with AVs.

Figure 4 shows the overall schema of the different processes, which can participate in the overall assessment of the AVs and the other parties involved in the AV context.

To summarize, the structure of this section is following:

- Section 3.1 identifies the key processes and roles involved in the cybersecurity aspects of automated vehicles.
- Section 3.2 provides the potential applicability of key processes to the identified roles and entities (e.g., AVs).
- Section 3.3 describes more in detail how the cybersecurity testing process of AVs (including verification and validations aspects) can be implemented.
- Section 3.4 describes more in detail the assessment of organizations including the audit process.
- Section 3.5 describes the processes involved in the monitoring of cybersecurity threats and vulnerabilities including market surveillance of AVs for cybersecurity aspects.

3.1 Identification of the key processes and roles

Figure 4 identifies the main processes to be established to address cybersecurity aspects of AVs.

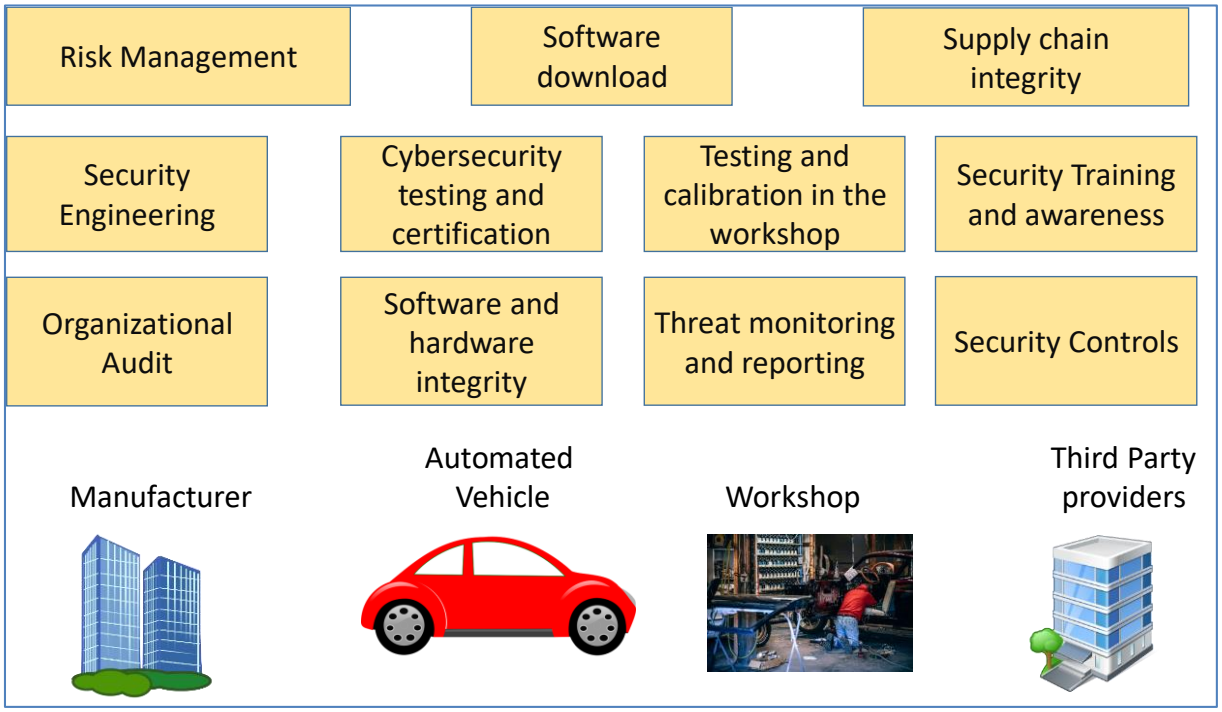

Figure 4 Main processes, roles and entities for cybersecurity aspects of AVs

The following main roles and entities are identified:

- *Manufacturer*. It is the manufacturer of the AVs.
- *Automated Vehicle*. It is the AV, whose type must be submitted to Type Approval (including cybersecurity testing).
- *Third party providers* are application providers which can have telematics interfaces to the AVs. They can include insurance companies or other commercial companies.
- *Workshop*. It is the workshop where the maintenance and periodic checks of the AVs is performed. It can be a vehicle manufacturer workshop or a certified workshop.

Additional roles/entities, which can be involved are:

- *Law enforcement*, which can also be involved in cybersecurity accidents when they are related to the infringement of regulations or when such accidents can jeopardize the conformance of AVs to such regulations.
- *Automated vehicles components manufacturer and suppliers*, which are responsible to provide components to the AVs manufacturers and they may satisfy specific security requirements defined by the manufacturers. In other words, they are the suppliers in the AV supply chain.
- *Passengers/drivers*, which may be involved in cybersecurity and privacy aspects and who may be victim or cause of a cybersecurity threat to the AVs.

The following Table 1 shows the main processes and entities and a potential proposal on how the processes can be allocated among them. It also describes how relevant standards can be associated to the processes.

The following key processes are identified and described in the following Table 1.

Note: the listing of specific relevant standards does not imply that the cited standard should be part of the identified process. The column **Relevant Standards** is only used to list standards, which could potentially be applied to the process described in the same row of Table 1.

Table 1 Main processes and relevant standards

Process	Description	Relevant Standards
Risk Management	Risk Management is the process to identify, evaluate and prioritize risks (in this case related to cybersecurity threats) followed by the application of processes and resources to minimize, monitor, control the probability of impact of adversary events on the entity (organization, system), which is the object of the risk assessment. Risk is an effect of uncertainty on objectives and it can be measured as a combination of the impact of an event with the associated probability of an occurrence.	ISO 31000
Security Engineering	Security Engineering is concerned with building systems, which are deployed to be secure and remain secure. Security engineering is used to achieve system assurance. Security engineering includes a number of techniques including computer security, cryptography, hardware and software integrity and so on.	ISO 21827, SAE J3061, ISO 21434 (under development)
Cybersecurity Testing and Certification	The processes required to test, verify and validate the cybersecurity requirements for an automated vehicle. This process also includes the definition of cybersecurity testing scenarios.	ISO 26262 (for the aspects of cybersecurity related to functional safety), SAE J3061 (for cybersecurity best practices), UN Regulation on Cybersecurity and Cyber Security Management systems published by UNECE WG29, Common Criteria ISO 15408, EU Cybersecurity Act Regulation(EU) 2019/881, IEC 62443.
Security Controls	Security controls are safeguards or countermeasures to avoid, detect, counteract or minimize cyber-security risks to a AV.	ISO 27001, NIST SP 800-12
Threat Monitoring and reporting	This is the process to report the appearance of a vulnerability or a cybersecurity threat to one or more AV types.	EU Cybersecurity Act Regulation(EU) 2019/881.

Software and hardware integrity	This is the process to guarantee the integrity of the functions of the software and hardware. Regarding software integrity, it is related to the software update process.	UN Regulation on Cybersecurity and Cyber Security Management systems published by UNECE WG29 (UNECE 2020a) and (UNECE 2020b)
Supply chain integrity	This is a set of processes, policies and technologies used to provide transparency and products traceability on the supply chain to minimize the risk of the introduction of products and components, which are not secure, faulty or with suboptimal performance.	ISO 28000
Organizational Audit	The set of processes required to perform the compliance of an organization regarding cybersecurity aspects.	ISO 27001, ISO/IEC 17011
Security Training and Awareness	This is the set of processes to guarantee and maintain an adequate (i.e., adequate to the defined requirements) level of cybersecurity training of the human personnel involved in the operation and usage of automated vehicles.	NIST 800-50.
Testing and calibration in the workshop.	This is the set of processes, which a laboratory/workshop may (depending on the specific regulatory framework) have the obligation to fulfil.	ISO 17020:2012, ISO 17025:2017.
Secure software download	This is the process to ensure the download of new software versions in the AV.	(UNECE 2020b), ISO 21434 (under development)

3.2 Identification of the key processes and allocation to roles

This subsection describes in detail the specific processes, which should be adopted to implement the needed cybersecurity processes for testing and certification of autonomous vehicles

Table 2 Potential applicability of processes for roles/entities in the context of cybersecurity of AVs

Processes	***Manufacturer***	***Workshop***	***Third Party providers***	***Law Enforcement***	***Automated vehicles components manufacturer***	***Passengers /drivers***
Risk Management	X	X	X	X	X	
Security Engineering	X		X		X	

Cybersecurity Testing and Certification	X		X		X	
Security Controls	X	X	X			
Threat Monitoring and reporting	X	X	X	X	X	X
Software and Hardware integrity			X		X	
Supply chain integrity	X				X	
Organizational Audit	X	X	X			
Security Training and Awareness	X	X	X	X	X	X
Testing and calibration in the workshop.	X	X				

Notes on Table 1:

- Risk Management processes may be applicable to any organization involved in the development, production and deployment of automated vehicles including the market surveillance (which is the reason why law enforcement is involved).
- Security engineering process may be applicable to any organization involved in development; in particular vehicle manufacturers.
- Cybersecurity testing and certification is applicable to the automated vehicles because they are the object of the testing, but other entities (workshop) may be involved as well.
- In this specific context, security controls are applicable to entities involved in the product and maintenance of automated vehicles.
- Threat monitoring and reporting involves all the identified roles/entities because each role can report on identified vulnerabilities of an AV. Law enforcement is also involved because, law enforcers can find out in the field about cybersecurity threats, which impact conformance to regulations.
- Software and hardware integrity mostly involves manufacturers but also the automated vehicle itself because techniques could be implemented in the vehicle to make it more robust against cybersecurity threat affecting the integrity of its components (e.g., monitoring the integrity of the software modules in the ECU).
- Supply chain integrity mostly affects the AV manufacturer and the supplier of components.
- Organizational audit mostly impacts organizations involved in the development of the AV, its maintenance (workshop) or the applications interfacing with it.
- Security training and awareness may impact organizations involved in the maintenance of the AV (manufacturer, components suppliers or workshop), which may interface to AVs for the provision of services (third party providers), to monitor its compliance to road regulations (law enforcement) or even drivers/passengers because misuse of the AVs functions can lead to cybersecurity vulnerabilities.
- The process to ensure the testing and calibration capabilities, including the competence of the human personnel, is related to workshops. Manufacturers are also included here because manufacturers workshops may be present as well.
- Software download involves the secure (in terms of integrity) download of the software from the manufacturer backend systems to the AV. It may also include download of third party software if approved by the AV manufacturer (UNECE 2020b).

There are dependencies among the different processes, which are described in the following bulleted list:

- Risk Management is directly linked to most of the other processes:
    - The identification and definition of risks drives the definition of the tests used for verification and validation. It also drives the certification of the AV from the cybersecurity point of view.
    - It drives the definition of requirements for the supply chain integrity. For example, it drives the definition of the tracking and tracing requirements along the supply chain since such requirements are used to mitigate risks that the components of the AV are not secure.
    - It drives the definition of the security controls to mitigate risks related to vulnerabilities.
    - It drives the definition of requirements for secure software download in relation to risks due to cybersecurity threats impacting the integrity of the download software.
    - It can be used to define the competence of workshops for accurate and complete periodic testing and calibration.
    - It shapes requirements for cybersecurity engineering.
    - It drives the definition of requirements for software and hardware integrity to mitigate risks related to tampering of software and hardware components in the vehicle.
    - It can impose specifications for the training of personnel to mitigate cybersecurity risks.
    - Risk management is directly linked to organizational audit because the organization must prove to an auditor that risks are properly managed.
- Threat monitoring and reporting
    - This process collects information on new vulnerabilities and threats as a feedback to the risk management process.
    - Information of executed threats can be collected by workshops and reported by them if they have adequate competence.
    - The collection of information may require vehicle forensics capability which should be part of the cybersecurity engineering design.
- Software and hardware integrity
    - The integrity of software is directly related to the software download process because the entire chain of software download and activation must be made secure.
    - The integrity of the hardware is directly related to the supply chain integrity process not only from the suppliers to the manufacturer but also to the workshops for parts replacement.
- Organizational audit
    - The audit of the organization can also include the assessment of the security engineering processes, supply chain integrity and security training.
- Testing and calibration in the workshop
    - Testing and calibration in the workshop requires capabilities, which can be obtained with adequate training. This is particularly important for cybersecurity aspects, which is a new competence area for workshop personnel.

The development of each of the identified processes implies that these dependencies should be addressed, thus the following recommendation:

Recommendation 1: The design and implementation of the processes required for cybersecurity aspects in automated vehicles must take in consideration the dependencies among the processes themselves.

3.3 Cybersecurity testing of AVs

Testing and certification of autonomous vehicles for cybersecurity aspects is a research area, which can include many different elements from other disciplines because AV are in essence cyber physical systems where computing platforms (e.g., ECU) can be subject to cybersecurity attacks. Then, the existing techniques and research literature in computer security can be adapted to this context as well. On the other side, AVs are cyber-physical systems where the output of the algorithms executing in the computing platforms hosting the AI algorithms, are used to control a physical object (the AV), which must navigate in the road infrastructure without causing harm to its occupants, other vehicles in the road and pedestrians. In comparison to conventional computer security, testing for cybersecurity of AV must take in consideration the safety hazards, which may derive from cyber physical threats.

Even if the task of cybersecurity testing and certification of AVs can benefit from techniques and approaches from other domains, it still remains a complex task where rigorous processes must be set in place not only for the initial deployment of the AV but also during its lifetime as operational conditions may change: AVs can benefit from software updates, which can enhance its functions and robustness but also sensors and actuators may degrade in time.

Government, industry and research communities have started to investigate testing and certification of cybersecurity requirements in parallel to functional testing of AVs, which is also a very complex task. Ideally, cybersecurity testing on AVs should not be performed separately from functional testing but it is also true that cybersecurity testing may require a different set of tools and procedures. In many cases, cybersecurity testing of AVs has been considered as an evolution of cybersecurity testing of modern vehicles, which have already implemented lower levels of automation for specific functions (ENISA 2019).

At regulatory level, an important milestone has been reached in June 25, 2020 with the formal approval in UNECE GRVA WG29, of two new regulations (UNECE 2020a) and (UNECE 2020b) on automotive cybersecurity. In the press release[3], UNECE stated that "The two new UN Regulations, adopted yesterday by UNECE's World Forum for Harmonization of Vehicle Regulations, require that measures should be implemented across 4 distinct disciplines: Managing vehicle cyber risks; Securing vehicles by design to mitigate risks along the value chain; Detecting and responding to security incidents across vehicle fleet; Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to on-board vehicle software". In fact, the two new regulations were based on two specific technical reports: the first on testing the cybersecurity of automated vehicles and the second on the integrity of the software download function. The regulations are expected to be finalized and published in early 2021 and apply to the 54 contracting parties (states/countries, which do not include US or Canada). Once the regulations enter into force, OEMs in the member states will be required to implement specific cybersecurity and software-update practices and capabilities for Vehicle Type approvals.

We note that DG.JRC.E.3 substantially contributed to the drafting of these regulations by providing contributions, comments and corrections to the draft version of the regulations during the drafting meetings.

Because of the importance of these two new regulations, the following paragraphs describe more in detail some of the processes identified in the regulations (they include most of the processes identified in Section 3.1).

[3] http://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html

The following subsection 3.3.1 analyzes UNECE GRVA WG29 regulations on cybersecurity aspects (UNECE 2020a) and subsection 3.3.2 analyzes UNECE GRVA WG29 regulation on Software Updates and Software Updates Management Systems (UNECE 2020b).

3.3.1 Analysis of UNECE GRVA WG29 regulation on Cybersecurity and Cyber Security Management System

One key aspect of the regulation (UNECE 2020a) is that it does not describe specific technical details (e.g., a specific cryptographic algorithm) but it identifies and defines high level processes to which manufacturers and other entities must be compliant. In some specific cases, where additional technical details are needed, the regulation delegates their definition to standards (e.g., ISO/SAE 21434). This approach is probably based on two main considerations. The first consideration is that cybersecurity aspects in AV deal mostly with processes and roles definition rather than the specific technology. The second consideration is that technological advancements in AV may trigger regulation obsolescence or the need to revise periodically the regulations, which could become a challenging task. Because of the dynamic nature of the automotive cyber environment, detailed technical measures could be counterproductive.

The regulation adopts a similar approach to the separation in different process areas described in Section 3 of this report:

a) Type Approval of AVs,

b) set up of processes and audit of the manufacturer.

The area related to monitoring/market surveillance is described in a limited way in the regulation and it mostly focused on the problem to provide software update (in the software OTA regulation) in a secure way (i.e., to support the integrity of the software, authentication of the software provider and confidentiality of the transmitted data).

Point a) (Type approval of the AVs) involves actually testing the vehicle and certifying that the design of vehicle architecture, the risk assessment procedures, and the implementation of cybersecurity controls were executed correctly. In this approval process, an authority tests an individual type of vehicle to check if the cybersecurity measures were actually implemented.

Annex 5 of the regulation provides a list of vulnerabilities or attack methods related to the threats and potential mitigation techniques, which shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers. The words “shall be considered” mean that content of Annex 5 is not binding but it can be useful for the implementation of the risk assessment.

Point b) focuses on definition and description of Cyber Security Management Systems (CSMS, the namesake of the regulation) and includes cybersecurity requirements for an OEM’s organizational structure, processes, and governance. CSMS certification demands evidence (i.e., audit) from the OEM, including test reports and threat modeling, in order to prove that due diligence was done in ensuring cybersecurity measures throughout the lifecycle of the vehicle.

Point a) is discussed more in detail in this subsection.

Point b) is discussed in detail in Section 3.4

As mentioned before, the support for monitoring and reporting of cybersecurity vulnerabilities and attacks is somewhat limited but it is anyway discussed in Section 3.5. of the regulation (UNECE 2020a).

Vehicle Type requirements detail the various steps a manufacturer must take for Type Approval and then, in Sections 8-10 of (UNECE 2020a), the regulation explains that the Vehicle Type approval must be maintained throughout the entire lifecycle of the vehicle including the potential modification of vehicles and the extension of a vehicle if it impacts the vehicle’s technical performance with respect to cybersecurity aspects. It is important to note that in order for an OEM to receive Vehicle Type approval, it must first complete the CSMS approval.

The regulation does not identify a list of binding technical specifications, which must be fulfilled for Type Approval, but Section 5 of cybersecurity regulation states that: “Approval Authorities shall grant, as appropriate, Type Approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation” and then the requirements areas are specified, which include

"Implement appropriate cyber security measures in the design of the vehicle type" and "Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyber-attacks". The manufacturer must perform a risk assessment process: "(clause 7.3.3. of [1]. The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately" and "clause 7.3.4. of (UNECE 2020a). the vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment".

As described before, Annex 5 of the regulation (UNECE 2020a) identifies key vulnerabilities, which should be used by the manufacturer in their risk assessment process.

The reported vulnerabilities are similar to vulnerabilities reported in other sources, which analyzed cybersecurity threats in modern vehicles (ENISA 2019), (Petit 2014). The list of specific vulnerabilities can be classified in the specific following categories:

- Threats to vehicles regarding their communication channels
- Threats to vehicles regarding their update procedure
- Threats to vehicles regarding unintended human actions facilitating a cyber-attack.
- Threats to vehicles regarding their external connectivity and connections
- Threats to vehicle data/code

Vulnerabilities are also listed for the back end servers, which can be used to collect the data from the vehicles.

Mitigation solutions are also proposed to address these threats and vulnerabilities, but it is up to the manufacturer to adopt them or not.

As written before, the regulation does not mandate a specific testing solution. Subsection 3.6 will elaborate on the potential testing techniques, which could be implemented.

3.3.2 Analysis of UNECE GRVA WG29 regulations on Software Updates and Software Updates Management Systems

Regulation (UNECE 2020b) provides a framework for the automotive sector to put in place the necessary processes for (the following text is extracted from the UNECE web site):

- Identifying the hardware and software versions, which are legitimate for a vehicle type;
- Identifying software relevant for Type Approval;
- Verifying that the software on a vehicle component (e.g., ECU) is what it should be;
- Identifying interdependencies, especially with regards to software updates;
- Identifying vehicle targets and verifying their compatibility with a software update;
- Assessing if a software update affects the Type Approval or legally defined parameters (including adding or removing a function). In this context, parameters (e.g., the hyper-parameters of the machine learning algorithm used in the visual analysis) are part of the software;
- Assessing if an update affects safety or safe driving;
- Informing vehicle owners of updates;
- Documenting all the above.

All of these will be audited by national technical services or homologation authorities.

Software update in (UNECE 2020b) is generally meant as the complete set of operations of software download, integrity checking, software activation and reporting on the software update status.

The Type Approval principles under the 1958 Agreement (UN 1958) mean that manufacturers will need to demonstrate, prior to putting vehicles on the market, that they fulfil the following requirements:

- The Software Update Management System (SUMS) is in place and its application to vehicles on the road is available;
- Protect Software Update (SU) delivery mechanism and ensure integrity and authenticity;
- Software identification numbers must be protected;
- Software identification number is readable from the vehicle;

For OTA software updates:

- Restore function if the software update fails for whatever reason;
- Execute software update only if there is sufficient electric power in the vehicle;
- Ensure safe execution of the new software version;
- Inform users (e.g., drivers, passengers) about each software update and about their completion status and time;
- Ensure that the vehicle is in general capable of conducting software updates (e.g., the ECU is malfunctioning and it is not able to activate the new software version);
- Inform user (e.g., drivers, passengers) when a mechanic is needed. Then, a workshop may be required to complete successfully the software update.

As in the case of the regulation on cybersecurity (UNECE 2020b), this regulation provides high level requirements and does not specify how the actual tests must be defined. Subsection 3.6 will elaborate on the potential testing techniques,

One key aspect of the software update which has been extensively discussed in other domains beyond transportation (see the Cybersecurity Act (EC 2019a)) is the need to implement an efficient software testing and certification process to enable the software update of certified software. The main trade-off is between the need to fix in the shortest time possible an identified vulnerability in the AVs with the need to follow a rigorous process for software testing and update because safety aspects are present in AV. For example, a software failure due to a faulty software update in functions related to braking may generate critical safety risks. Then, it is important that any software update is subject to an extensive regression testing to ensure that the update does not compromise AV functions and in particular AV safety functions. Software testing to reach a high level of reliability is not a new research area and the aeronautical, defense and space industries have developed sophisticated techniques to implement and test software updates (Loyall 1997). On the other hand, these domains have different time scales for software deployment and distribution and in many contexts, designers and software developers do not have to deal with the complexity of traffic scenarios where a multitude of vehicles are present. This means that the testing scenarios in other domains can be considerable less complex than for automated vehicles. The software update of the Artificial Intelligence algorithms is particularly important because they take the decisions (almost in real-time) on the actions to take during the driving of the AVs (see also Section 4). Note that software updates include both the implementation of the operational functions of the AVs and the implementation of the cybersecurity functions (see also Section 3.6).

The specific context of AV and the challenge to conduct an efficient testing of software updates may require an advancement of software testing techniques with specific focus on the testing of artificial intelligent algorithms. Advancements in this area will enhance the competitive advantage of the European industry on one side and it will improve the safety on the road infrastructure on another side.

Then, the following recommendation is issued:

Recommendation 2: The function of software updates in automated vehicles will require the implementation of time efficient software testing processes while maintaining a wide testing coverage of the operational scenarios. This report recommends the increase of research in software testing for automated vehicles through research funding schemes (Horizon Europe) with a particular focus on testing of the artificial intelligence components of the automated vehicle.

3.4 Organizational Audit

One of the critical obligations described in the regulation (UNECE 2020) is that the manufacturer sets up a Cyber Security Management System (CSMS). As described in (UNECE 2020), "Cyber Security Management System (CSMS) means a systematic risk-based approach defining organizational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks". The evidence of the creation and continuous support for the CSMS must be proven by the AV manufacturer to the auditor (i.e., the Type Approval authority) to obtain the Certificate of Compliance (CoC).

One important aspect of the CSMS is the implementation of the secure supply chain with clause 7.2.2.5: "The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations".

In addition, while the regulation does not indicate the method by which a vehicle manufacturer must verify the cybersecurity of the Tier 1 and 2 components (Tier1 and Tier2 is related to supply chain terminology here. For example, Tier1 is the first level of supply to the manufacturer), it demands in Section 5.1.1 of (UNECE 2020a) that the vehicle manufacturer must "collect and verify the information required under this Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed".

This means that the vehicle manufacturer must define supply chain processes (e.g., tracking and tracing and/or due diligence) to ensure that the supplier provides secure components.

On the other side, the accreditation of vehicle manufacturers, which are going to implement a CSMS may require an update of existing accreditation schemes at European level. Thus the following recommendation is proposed.

Recommendation 3: This report recommends to revise the existing accreditation schemes in Europe to verify if they are adequate to support the auditing of the Cyber Security Management System (CSMS) of automated vehicle manufacturers for the cybersecurity aspects of Type Approval.

3.5 Cybersecurity Threat Monitoring and reporting

The regulation (UNECE 2020a) requires the manufacturer to implement monitoring processes (clause 7.2.2.2(g)). These processes are defined in (UNECE 2020a) with the following description. "The processes used to monitor, to detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified". The manufacturer must also demonstrate that the monitoring process is continual (clause 7.2.2.4): "The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual". It is also noted that the privacy rights must be respected "This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent".

One aspect that is not described in an exhaustive way is the implementation of the market surveillance and the reporting of vulnerabilities and cybersecurity threats. In this context, a process must be set in place according to the local regulations where similar approaches are already defined. For example, the Cybersecurity Act (EC 2019a) foresees and defines processes for the collection and reporting of cybersecurity vulnerabilities in different domains, which may include the automotive sector. Even if no decision has been taken to this regard, this report recommends the creation of a vulnerability database at European level to report on cybersecurity vulnerabilities in the automotive sector and more specifically for AVs.

One example in the cybersecurity sector is the National Vulnerability Database (NVD) https://nvd.nist.gov/ in USA, which performs a similar function in the USA.

Recommendation 4: This report recommends to set up a vulnerability database and an associated process for the reporting of threats and vulnerabilities in automated vehicles (for all levels of automation) at European level.

On the other side, the creation of such a database must take in consideration the challenge to share information among stakeholders (e.g., OEM and suppliers) where there is still considerable resistance as highlighted in (Morris 2020). Potential approaches based on blockchain may be considered because blockchain have been deployed for similar objectives of distributed data integrity and they can be implemented with confidentiality solutions in place (Neisse 2020).

3.6 Potential approaches/techniques for cybersecurity testing of automated vehicles

This subsection describes the potential approaches for testing, which can be adopted to fulfill the regulations (UNECE 2020a) and (UNECE 2020b) and additional regional regulations.

There are limited studies on the discipline of cybersecurity testing of automated vehicles including the testing of security of Over The Air (OTA) software download. In most cases, testing approaches are derived from existing approaches from the generic Information and Communication Technologies (ICT) domain but the characteristics of automated vehicles, require a specific effort of customization and tailoring.

We review in this section, contributions and analysis from the most significant resources identified through desktop research on cybersecurity testing for vehicles and AV in particular.

The authors in (Wooderson, 2017) have analyzed and identified the challenges of cybersecurity testing and how they are different from functional testing especially in the context of modern vehicles. The following main challenges were identified:

- While traditional forms of functional testing are typically suitable at revealing the differences between the intended behavior and implemented behavior, cybersecurity testing should also evaluate what the system should not do. For example, unintentional leakage of sensitive information via side channels such as transient power consumption or electromagnetic emanations from a microcontroller is a cybersecurity vulnerability even if the microcontroller fulfills the functional requirements as expected.
- It is almost impossible to reach 100% cybersecurity coverage testing because new threats, vulnerabilities and attack methods to exploit them are continually discovered and previous methods improved upon. Then, cybersecurity testing is a process or set of processes where the identification of vulnerabilities must be periodically executed.

Then, (Wooderson, 2017) identifies the range of activities, which should be part of cybersecurity testing:

- Vulnerability testing, which has the objective to identify cybersecurity vulnerabilities in the vehicle. The identification of the vulnerabilities often requires extensive testing to try different combinations of inputs and conditions. Attack trees can be used to implement a structured analysis text execution to improve coverage.
- Penetration testing can be used to address the cases mentioned before to evaluate what the system should not do (e.g., side channel information leakage or susceptibility to fault injection attacks). In this case, a skilled tester should be employed because the space of all the possible attacks is too large for a practical deployment of the product in a reasonable time and the attack space should be focused on more probable attacks and attacker can implement. In comparison to ICT, penetration testing in automated vehicles can be helped by a proper design of the AV where only specific interfaces (i.e., wireless connection) are available to digital world outside the vehicle. Penetration testing could be implemented as *black box testing* where the internal implementation of the system under test is not known by the tester or *white box testing* where the tester has some a-priori knowledge of the system, which can be exploited by the tester to anticipate vulnerabilities due to the attacker, who has similar knowledge of the system.

Vulnerability and Penetration Testing' process steps recommended by SAE J3061 (SAE 2016) can be used for this purpose.

Cybersecurity assessment and certification has a long history in ICT and a number of cybersecurity and evaluation schemes have been proposed as discussed in the Cybersecurity Act (EC 2019a) and other resources for the IoT domain (Matheu 2019). The Common Criteria certification based on the ISO 15408 is one of the most known cybersecurity evaluation processes. It is performed by an independent cybersecurity evaluator. While it is well known and mature from the development point of view, it has its weaknesses, primarily the high cost associated to the evaluation. We note that Common Criteria was not mentioned in the UNECE regulation (UNECE 2020a). On the other side, it has merits, which could not be ignored (SAFERTEC 2020). In the text of (UNECE 2020a), no clear standard has been identified and defined for this purpose; thus leaving the choice to the vehicle manufacturer.

Similar types of testing for the cybersecurity of automated vehicle are identified in (Chattopadhyay 2020) and they are listed below:

- Penetration Testing, which is commonly performed as part of a security audit and which can be performed as black box or white box as discussed previously in this section.
- Red Teaming: This is a process for detecting network and system vulnerabilities by assuming the role of an attacker, also alternatively termed as ethical hacking.
- Fuzz Testing, where a wide range of random data is provided as an input to the software/system to make it fail with the objective to anticipate attacks in the field
- Network Testing where the resilience of the in-vehicle network of the AV is evaluated in stress conditions to create conditions, which can show vulnerabilities.

In particular, Fuzz testing is also recommended in (Fowler 2018) as a valuable technique for testing the cybersecurity of AV.

Each of these techniques can be used in the cybersecurity testing but the choice is left to the vehicle manufacturers on which technique to use as indicated in (UNECE 2020a). Each testing technique can also be used in various phases of the lifecycle of the AV. For example, fuzz testing can be used not only in the initial testing and verification before market deployment but also when an update is performed on the AV.

Another relevant aspect in cybersecurity testing of AV is the definition of a testbed. The definition of such a testbed is discussed in (Appel 2020), where it is described the development of a testbed for the assurance of safety and security of components with all capabilities from Model-in-loop to Software-in-loop to Hardware-in-loop testing. The advantage of this testbed is to merge the testing of the safety aspects with the security aspects.

The authors in (Appel 2020) discuss the need to implement specific attack scenarios for the network interface both in the in-vehicle interfaces and the external Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). The test bed is composed by the CARLA simulator (CARLA 2020) with hardware and software components to support an extended test scenario where cybersecurity attacks together with functional testing is performed. The paper recognizes that cybersecurity testing is still in a growth/starting phase and a harmonized activity on the definition of test bed for cybersecurity testing of AVs would be needed.

We also support a similar conclusion in this report with the additional consideration that standards should be developed for the specific AVs domain or customized from other domains. For example, TTCN-3 has been used to test automotive software (TTCN 2020) and it could also be used for cybersecurity purposes.

Regardless of the choice of the test definition language, this report proposes the following recommendation:

Recommendation 5: Standardization efforts should be directed to the definition of test bed for cybersecurity testing of automated vehicles including the definition of appropriate testing languages.

Similar considerations can also be proposed for the testing of software download and integrity even if in that case the function is well defined and there is extensive knowledge on testing of software download security (e.g., automatic software download in ICT infrastructure or secure software download in smartphones).

In fact, because AVs will be more reliant on software components, the experience in software testing for cybersecurity purposes can be re-used for AVs testing and in particular for the OTA software update function. The bibliography on this topic is extensive (Wysopal 2006), (Felderer 2016) and it not reported here also because some of the techniques have been already identified before (e.g., fuzz testing, penetration testing).

4 Testing and certification of artificial intelligence in automated vehicles

This section is focused on the testing and certification of the artificial intelligence algorithms used in autonomous vehicles: in particular, the Machine Learning/Deep Learning (ML/DL) algorithms, which are used to collect and analyze the surrounding environment (e.g., other vehicles, signs on the road) and create the operational awareness, which is essential for the correct functioning of the AVs.

As described in (Fremont 2020), a defining characteristic of the growth in autonomous vehicles (AVs) and automated driving systems (ADS) is the expanding use of ML and other artificial intelligence (AI) based components in them. In particular, deep neural networks (DNN)s, have proved to be fairly effective at perceptual tasks, such as object detection (e.g., approaching vehicles), classification (e.g., recognition of the signs), and image segmentation (e.g., layout of the road infrastructure),

The main aspects considered in this section are:

- The role of ML/DL algorithms in autonomous vehicles and the challenge to design effective algorithms.
- Role of the virtual and real testing environment
- Robustness of ML/DL against adversarial effects.
- Testing and certification of the AV regarding artificial intelligence.
- Update of ML/DL algorithms after market deployment.

Each of these aspects is evaluated for its potential impact on the testing and certification of AVs. If challenges and weaknesses are described, each subsection tries to identify and describe potential countermeasures.

4.1 Role of ML/DL algorithm in AVs and ADS

This subsection focuses on the testing and certification of ML/DL algorithm in AVs and ADS and what solutions have been proposed by the government, standardization, industry and research communities.

One example of tool for the testing of ML/DL algorithms is proposed in (Dreossi 2019) and it is called Verifai.

As described in (Koopman 2016), the proper functioning of the AVs is only possible if the combination of perception of the environment and the execution of decisions on the basis of the perceived context awareness is done correctly. Without the presence of a driver (level 5 of automation) or even with the presence of a driver which is not active in specific situations (level 4 of automation) the objective of the ML/DP algorithm is to minimize the error function in determining the proper course of action (e.g. steer in one direction to avoid an obstacle). While there are different types of ML/DL algorithms (supervised, unsupervised), one common element among them is inductive learning where the ML/DL creates a model, which tries to represent the reality in a faithful way so that actions can be taken accordingly. The difference between the prediction of the ML/DL algorithm and the reality (e.g., the ground truth) is the error function of the model, which must be minimized.

There are significant challenges for the implementation of ML/DL in AVs, which must be overcome and where the research community is currently focused.

These challenges are described in the following numbered list and they are relevant to the testing of AVs.

1. In an ideal situation, the model should represent all the potential situations which an AV could face. This goal is almost impossible to achieve unless the AV drives in a controlled environment (selected tracks), which is also not realistic. Then, the great part of the research/industry community has focused on definition of means to design the model in the most comprehensive way possible. This goal has prompted the expansion of the basic controlled track test to simulated environments or testing in real traffic conditions with the assumption that full coverage of all situations is not possible. Simulated environments for the design and testing of ML/DL can be used for this purpose and these aspects are described more in detail in subsection 4.2.

2. ML/DL can also be the subject of attacks to the induction learning design if wrong data is fed to the system. This is called Adversarial Machine Learning (AML) where the objective is to inject false data to the ML/DL algorithm so that it creates the wrong model. While it can be assumed that the pre-deployment is a controlled environment where intentional adversarial machine learning is absent (but errors in the creation of the model are still possible), cybersecurity attacks including AML can be effective in the field to disrupt the update of the ML/DL algorithms described in the previous item 3. Additional details on this aspect are discussed in subsection 4.3.
3. In comparison to many domains where ML/AI is used, errors in the prediction of the ML/DL algorithm can cause safety hazards. Then it is extremely important that the error function is minimized, which is again related to the accuracy of the created model described in the previous point. The validation of the model is one of the critical aspects in the testing/certification of AVs, which is discussed more in detail in subsection 4.4.
4. Because the full coverage of the scenarios is impossible to achieve in the initial design/production phase of AVs, many researchers have proposed the possibility to augment the cognitive capabilities of the ML/AI algorithms after-market deployment. This is possible with specific ML/DL approaches like Reinforcement Learning (Zhou 2019), (Feng 2020a), (Feng 2020b) where the feedback from the field (while the AVs is driving on the road) is used to reinforce the initial design of the algorithm (e.g., the weights of the DL algorithm are recalibrated with an internal reward mechanism). Other means could be based on advances in the ML/DL design by the AV manufacturers, which proceed to perform software updates to the AVs. Then, the software update function must also be tested. Additional details on this aspect are discussed in subsection 4.5.

4.2 Role of the virtual and real testing environment for AI/ML algorithms

This subsection discusses the role of virtual and real testing environment, the trade-off and balance among them and how they can be used for the testing and certification of AVs.

Real-testing of AVs is a necessary step, which cannot be avoided. We can classify real-testing in two separate categories: real-testing in a controlled track and real-testing in a normal traffic environment.

In the first category (real-testing in a controlled track or track testing), the test environment can be controlled to the level that test scenarios can be reproduced with specific conditions including timing, position of the vehicle on the road, presence of obstacles and topology of the road.

The advantage of track testing is its controllability and reproducibility. The disadvantage is the cost of setting up the track environment and running the test scenarios. Another obvious disadvantage (derived from the previous one) is that not all the driving conditions can be executed. Track testing is not able to reproduce all the conditions an autonomous vehicle will face on the road.

To complement track testing, real testing in a normal traffic environment is often used to test AVs prototypes. It has shown its effectiveness to evaluate scenarios or conditions, that were not planned, which is its main advantage. The main disadvantage is the possibility to create hazards to other vehicles or humans in the road (e.g. pedestrians). Another disadvantage of real testing in a normal traffic environment is that it is not fully reproducible: depending on the traffic conditions, some traffic events may happen or not. The third disadvantage is that this type of testing is still not able to provide an extensive coverage of testing. As it has been reported in literature (Feng 2020a), AVs should run for hundreds of thousands of miles to achieve an almost full coverage of the traffic situations, which is obviously not practical.

Then, virtual testing is used to complement real-testing described above. Simulation testing can help to address the gaps in real-testing identified above. Obviously, simulation cannot be identical to the execution in a physical environment: there is always a gap between those two also called the reality gap (Jakobi 1995).

The advantage of the simulation environment is that it can reproduce in a cost effective way a large number of driving scenarios. Reproducibility is the key word as the simulation environment is a completely controlled environment. In particular, it can simulate different environment conditions (e.g., fog, rain), which can negatively impact the perceptiveness of the AVs. Another advantage is that it can be implemented in a full machine to machine (M2M) environment without the need of human involvement and

which can be easily ported from one simulation environment to another even if the problem of a common language must be still resolved in many cases. The main disadvantage is how faithful the simulation environment resembles the real environment. In particular, the simulation of the sensors and actuators in the vehicle is a key challenge as a model of the vehicle must be faithfully reproduced with all the connections and dependencies among the internal components (e.g., powertrain modules, braking systems and so on). On the other side, the simulation can be refined and validated by using real data from the vehicles.

From the point of view of the ML/DL design and testing, each of the testing environments described before can be used to evaluate the performance of the ML /DL algorithms as discussed in the following bulleted list:

1. *Real testing in a controlled environment*. The advantage of this type of testing is that the environment and the conditions can be controlled and measured. From the ML/DL point of view, this means that it is possible to compare the prediction of the ML/DL with the true reality (ground truth) during the test. Then, the error function can be measured in a precise way. The disadvantage of this type of testing is that only a limited number of scenarios can be tested, which means that the ML/DL model is limited and it may be not adapt to the real world conditions or to a hostile environment where AML is implemented. This can be mitigated by applying adverse conditions in the controlled environment (e.g., introducing adversarial environment conditions) but again there is still the problem that the space of adversarial attacks may be limited.

2. *Real testing in a normal traffic environment*. The advantage of this type of testing is that the ML/DL algorithm is tested in much larger space of contexts and the initial designed model can be widely evaluated so that corrections can be introduced. The main disadvantage is that the environment is not controlled. Then, it is not possible to reproduce testing conditions and different executions of the tests may reproduce different outcomes of the ML/DL algorithm. It is also more difficult than in a controlled environment to determine the ground truth as the conditions are not controlled even if information on the road conditions can be derived from the recording of the sensors installed in the AVs (e.g., camera, Lidar). AVs under test in this environment could be equipped with a larger set of sensors than the usual market deployment to collect more useful information to determine the ground truth. A final disadvantage of real testing in a normal traffic environment is that errors in the ML/DL algorithm prediction can cause safety hazards to pedestrian or humans in the AV or other vehicles in the road.

3. *Simulation environment.* The advantage of this type of testing is that an extensive set of scenarios and conditions can be simulated to evaluate the ML/DL algorithm and its model. This testing environment is also called vehicle in the loop. In addition, the ground truth is easy to determine (because it is controlled in the simulated environment) and the error functions between predictions and ground truth can be easily calculated. Furthermore, various adversarial ML/DL scenarios can be implemented by simulating difficult environmental conditions (e.g., fog, slippery roads) or obfuscating the signs to confuse the sign recognition system of the AV. The main disadvantage is that the definition and reproduction of all the scenarios including the simulation of the sensors/actuators of the vehicle is a massive amount of work, which requires significant effort even from large industries. A potential way to mitigate this problem would be to define the simulation scenarios with a collaborative effort between government and industry. The additional benefit of this approach is that the end-result would be a set of simulation testing scenarios, which could be used for Type Approval/certification of AVs and which could be defined in an impartial way because of the government involvement (see Recommendation 6 below).

   A disadvantage of this testing environment is that the real components like sensors and actuators must be simulated properly. In particular, their performance must be evaluated because the timing of the chain of decision->action between the ML/DL algorithm decision output and the execution of the identified action in the actuators of the AVs (i.e., brakes) must be faithful to the real AVs conditions. In this context, special considerations should be taken to simulate the potential physical degradations of the actuators components in the vehicle due to their usage and time. While a human driver may have an intuitive perception that the condition of the vehicle are not optimal (and the conditions of the vehicle are anyway usually checked in the periodic mandatory inspections), the advance in automotive sensors can provide an improvement and

feed the ML/DL with up-to-date information on the conditions of the sensors and actuators in the AV.

To summarize this analysis, each of the testing environments has its own advantages and disadvantages. Then, an initial recommendation is to include all the different environments for the Type Approval/certification of AVs.

Recommendation 6: Type approval/certification of the Artificial Intelligence components of the AV should include real testing in a controlled environment, real testing in a normal traffic environment and testing in a simulation environment. The simulation environment should be able to reproduce the realistic conditions of a vehicle including the possible degradation of its physical components (e.g., actuators, sensors).

In addition, while it is recommended that each type of testing should be based on a harmonized set of tests, this aspect is particularly important for the testing in the simulation environment because of the huge effort needed to set-up a comprehensive set of tests and the need to have the impartiality of these tests. Testing in a normal traffic environment cannot be controlled a priori which makes the harmonization difficult and real testing in a controlled environment could be executed in specialized AV manufacturer facilities. The definition of such comprehensive set of scenarios is also linked to the creation of the scenario database described in Section 5.

Thus the following recommendation.

Recommendation 7: A government/industry partnership should be set up for the definition of a simulated testing environment and a common set of simulated testing scenarios based on a common language and a defined set of outcomes.

4.3 Robustness of ML/DL against adversarial effects in autonomous vehicles

This subsection discusses a potential weakness of the ML/DL in its application to AVs. ML and more specifically DL, which has been demonstrated (Papernot 2016), (McDaniel 2016) to be vulnerable to adversarial effects, like the injection of false data to confuse the ML/DL trained algorithm. In the context of classification (which is one of the main tasks of ML/DL in AV as they need to classify and discriminate different objects in the road infrastructure), adversarial samples are crafted to force a target model to classify them in a class different from their legitimate class (McDaniel 2016). For example, a speed limit sign could be classified with a different speed limit.

The reason of this weakness has been demonstrated in various experiments (Huang 2011), in particular for Deep Learning (DL) and the processing of images (Papernot 2016), which is performed by a camera and it is an essential element of the AVs sensor equipment. This weakness is relevant for all the machine learning algorithms but in particular for deep learning. It consists in feeding the ML/DL algorithm with false or confusing information to create or update a model, which is altered and which could perform in a non-correct way while driving in the road infrastructure. There are numerous examples from literature. In (Biggio 2018) and (Arkar 2017), are mentioned examples of AML where the false image of a sign was captured by the camera of an AV.

An extensive review on AML in AVs and potential mitigation measures is provided in (Qayyum 2020) and the key findings are reported here:

- AML can affect all the main cognitive functions of an AV: perception, prediction, planning and decision making but attacks to some cognitive functions of AV like planning and decision require the access to in-vehicle components and systems, which may be difficult to implement. Then, most of the listed attacks in literature are related to perception of the environment and detection.
- Based on the adversarial knowledge available to the adversaries, attacks can be divided into three types; white-box, gray-box, and black-box attacks. White-box attacks assume a complete knowledge about the underlying ML/DL model, including parameters optimization, weights and so on gray box attacks assume some knowledge of the ML/DL model like the ML algorithm. A black box attack refers to the real-world knowledge where there is not much information available to the attacker about the targeted ML/DL scheme.
- It could be difficult to differentiate between intentional adversarial attacks (cybersecurity threats) and unintentional failures. For example, in 2016 a Tesla autopilot was not able to handle the image contrast between the bright sky and a white truck which resulted in the death of the human tester (Guardian 2016).

There is the need to make more robust the ML/DL algorithms in AVs. Various sources (Qayyum 2020), (Goodfellow 2018), (Brendel 2017) have identified approaches to make the ML/DL more robust against AML. Potential techniques are identified in the following list:

- Training with adversarial examples the ML/DL model can make it more robust against the specific examples inserted in the training. The problem is that it is usually not possible to foresee in advance what type of adversarial examples should be adopted.
- A mitigation technique can be based on the observation that input feature spaces are typically unnecessarily large and provide a vast room for an adversary to construct adversarial perturbations. Then, ML/DL algorithms can be made more robust by proposing feature squeezing as a defense strategy to adversarial examples (Xu 2018).
- A similar approach to the previous point is to select specific features, which are particularly robust against AML and use only these features in the classification either by inserting a selection filter or by using only a subset of features.
- The input data space can be transformed in a new space (e.g., using a manifold) to make the data model more robust against AML. Generative Adversarial Networks (GANs) can also be used for cleaning adversarial perturbations.

- Create additional and complementary models to enhance the robustness of the main model used by the AV. For example, the authors in (Goodfellow 2014) proposed an ensemble training that works by assembling multiple instances of the original DL models.
- The recent studies on federated learning can also improve the robustness of the models used in the ML/DL algorithms by collecting information from different ML/DL components from different vehicles. The application of federated learning to automated vehicles is still in its infancy, but it could be explored further (Pokhrel 2020).

To mitigate the criticality of AML to AV, it should be also noted that some AML attacks imply anyway the access to the data input to the AI components in the AV (e.g., data from sensors to AI components). Then, cybersecurity mitigation techniques focused on restricting the access to the interfaces or the in-vehicle network of the AV could also improve the robustness of the AV against AML.

To summarize, AML attacks in AVs are possible at different phases (e.g., detection, decision) of the cognitive engine of the AVs and AVs should be protected against this type of attacks or at least some of the mitigation techniques identified above should be included in the design and update of the ML/DL. Then the following recommendation is proposed:

Recommendation 8: Design of the Machine Learning/Deep Learning algorithms in automated vehicles should include mitigation techniques against adversary machine learning.

4.4 Testing and certification of the AV regarding Artificial Intelligence (AI)

The modern evolution of automotive vehicles to increasing levels of autonomy will also make them more dependent on the software, which is not only limited to the software implementation of AI functions (i.e., generally implemented by ML/DL algorithms) but it also includes the software of other computing platforms in the vehicle like the Electronic Control Units (ECU).

Testing and certification of the AI component in the AVs is part of the overall testing of the AV, which is extensively discussed in sections 2 and 5. In this subsection, we discuss the main aspects related to the AI component.

The following key points are identified:

- Testing of AI in AV has similar challenges to the testing of AI in other domains (e.g., image processing, cybersecurity). In particular, as discussed in (Koopman 2016), the creation of scenarios and labelled sets for the validation of the AI models can require significant effort considering the variety of scenarios an AV can face. The labelling effort usually requires human action but it could be automatized in some contexts. For example, the labelling could be part of the definition of a simulated environment scenario.
- As discussed in the previous subsection 4.3, the robustness of the ML/DL algorithms in the AI element of the AV must be tested. One potential approach is to augment the testing scenarios with variations of the basic data set as suggested in (Tian 2018), where the authors proposes a testing methodology based on two main elements. The first element is to increase the testing coverage with synthetic images, which are variation of the initial scenario where images are obfuscated with noise, scaled translated or rotated. The second element is specific to neural networks and it is targeted to implement extended neurons coverage and create testing inputs, which are able to stimulate as many neurons as possible of the neural networks implemented in the AI of the AV. The authors in (Tian 2018), show that many "corner cases" which can lead to safety hazards are discovered through their testing framework. The limitations of this approach is that neurons coverage is usually designed for specific DL algorithms like Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN) and its application requires anyway significant testing effort.

- As with the overall testing of AVs, an optimization algorithm can be implemented to identify the most relevant tests. An optimization algorithm is proposed in (Feng 2020a) and (Feng 2020b). In another study, the authors have used evolutionary algorithms to restrict the subset of specific testing scenarios (Klischat 2019). Even with these recent and promising results, the definition of the optimization algorithm can be quite complex and further research is needed in this area (see recommendation at the end of this subsection).
- Due to the complexity of AI and the width of the scenario space in AV, another approach is to perform tests in the different phases of the development cycle. In addition, specific functions of the ML/DL can be tested with appropriate testing scenarios. This "divide and impera" approach is proposed and described in detail in (Vishnukumar 2017).

To summarize, testing of the AI components in AV share many similarities to testing of AI in general but there are specific aspects related to the AVs scenarios and the development cycle of the AVs, which must be taken in consideration. Even if promising studies and results have been proposed, it is noticed that most of the studies are quite recent. In addition, testing for AML is still in the early phase and this would require more effort by the research and industry community. Thus the following recommendation is provided.

Recommendation 9: There is the need to expand the research efforts for the testing of Artificial Intelligence components (e.g., Machine Learning/Deep Learning) in automated vehicles with specific focus on the optimization of the test cases, application of testing activities in different phases of the development lifecycle and testing for Artificial Intelligence robustness against adversary machine learning. It is also recommended that research outputs should be standardized to support harmonized testing of AVs.

4.5 Lifecycle of AVs: update of ML/DL algorithms aftermarket deployment

Beyond the initial testing of the ML/DL algorithms in the AV as part of the Type Approval process or similar Validation and Verification processes, it is expected that AVs will have the capability to be updateable in software during their deployment lifecycle. This assumption is supported by various sources, in particular (UNECE 2020b), which describes the Over The Air (OTA) software update requirements and the related Type Approval process. The content of (UNECE 2020b) was already discussed in detail in subsection 3.3.2 and its analysis will not be repeated here.

(UNECE 2020b) and other sources (Halder 2020) discuss in details the operational requirements for OTA software update in AVs, but these studies are generic for all the software components in the AV, while this subsection discusses instead the impact on the testing of the AI component in the AVs when only the AI software is updated.

As in the previous sections, the key points are discussed in the bulleted list below. Then a summary of the key points is provided and a recommendation is issued.

- Software update in the case of ML/DL algorithms does include not only the update of the software (e.g., the software for a full new algorithm) but also the update of the hyper parameters of the ML/DL algorithms (e.g., C parameter in the SVM algorithm) or the weights in a neural network. In both cases, the integrity of the transmitted information should be preserved Over The Air (OTA), but the update design could be slightly different also because the size of the hyper parameters can be less than a full software package.
- It can be assumed (UNECE 2020a) that the computing platform hosting the ML/DL algorithms has specific requirements for protection (e.g., physical security) and anti-tampering because such algorithms implement the essential cognitive capabilities of an AV. Then, the secure OTA for the ML/DL algorithms should have an even higher level of security than the OTA for the AV.

- As in the case of general AV software updates, a critical aspect is the re-evaluation of the ML/DL algorithms before deployment. The re-evaluation should include a regression testing to evaluate not only the updated parts of the code and the new functions (e.g., image analysis) but all the existing functions. Because the ML/DL software is part of the overall AVs software, it should also be conformant to the Type Approval process defined in (UNECE 2020b) and/or current or future regional requirements (e.g., EU regulations on type approval).
- ML/DL algorithms are heavily dependent on the quality of the data, which is provided as an input. In the initial Type Approval phase, the ML/DL algorithms are tested against the data from the sensors (e.g., camera) installed in the vehicle. The operational status of these sensors in this initial Type Approval phase can be assumed to be quite high. Once the vehicle is deployed, the quality of the sensors and the related data may degrade, which may introduce errors in the cognitive functions of the ML/DL algorithms. Such degradation can be compensated by frequent calibration checks at the workshop or it can be mitigated by the ML/DL algorithm itself if the degradation factor is known. This function could be improved if the automated vehicle periodically sends information to the manufacturer systems (e.g., cloud or other backend systems) to inform them about the status of the AV and its sensors/actuators. This is called predictive maintenance, which is not a recent concept, but it should be adapted to AV. See (Machin 2019) for a recent analysis on predictive maintenance in the automotive sector. Then, the manufacturers can send back to the ML/DL algorithms a new set of calibration factors, which can mitigate the degradation of the sensors within certain limits. This is also a form of software update, which must be addressed.

To summarize: while the OTA software update in AV has received considerable attention in recent times and requirements and functions are being defined both in regulatory and standardization bodies, the software update of the ML/DL algorithms require specific measures, which must be defined and adopted. This aspect has not received enough attention by the research and industry community. Thus, the following recommendation is issued:

Recommendation 10: Specific measures must be defined and adopted for the Over The Air (OTA) software update of the Machine Learning/Deep Learning algorithms in Autonomous Vehicles. Software update in this context may also mean update of the Machine Learning/Deep Learning hyper-parameters.

5 Scenarios for testing and certification of automated vehicles

The aim of this section is to describe the processes to create the scenarios for testing and certification of automated vehicles. This set of scenarios may include both real and virtual test scenarios and do also include specific scenarios to test cybersecurity attacks or ML/DL as described in the previous sections.

The following subsections will be part of the analysis:

- Language to define the scenarios for testing and certification. Relationship between set of testing scenarios and Type Approval.
- Role of real and virtual testing.
- Metrics of evaluation related to the scenario definition.
- Definition of a potential scenario database.
- Scenario lifecycle and process to update the scenarios from real operational conditions including market surveillance.

In this report, we use the definition of scenario from (Ulbrich 2015).

"A scenario describes the temporal development between several scenes in a sequence of scenes. Every scenario starts with an initial scene. Actions & events as well as goals & values may be specified to characterize this temporal development in a scenario. Other than a scene, a scenario spans a certain amount of time."

5.1 Scenario language

This subsection discusses the language to define the scenarios for testing and certification. Because, testing and certification of AVs is going to be a complex process with many different variables, it is important to define a language, which is able to represent without ambiguities all the complex variables present in a testing scenario and be comprehensive enough to address all the potential scenarios. A major limitation of current tools is the lack of programmability of test environments.

As discussed in (Queiroz 2019), engineers working on the definition of testing scenarios need to learn tool-specific languages or program simulated traffic from scratch due to large variety of simulation tools for testing of AVs. Migrating scenarios between different simulation tools requires extra effort and impairs comparisons between different driving systems.

In the following paragraphs, we provide an overview of the main languages for the definition of testing scenarios for AVs.

Note that there are also testing toolkits to generate tests for AVs like the one described in (OAS 2020).

Table 3 Languages for testing scenarios of automated vehicles

Measurable Scenario Description Language (M-SDL)	The Measurable Scenario Description Language (M-SDL) is a recent higher-level DSL similar to SCENIC, which precedes its definition; while M-SDL is more specialized for AV testing, it has less support than SCENIC for probabilistic and geometric modeling and is not supported by open-source back-end tools for verification, debugging, and synthesis of autonomous AI/ML based systems. M-SDL is described in Foretellix, Inc. (2020) Measurable Scenario Description Language. [Online]. Available: https://www.foretellix.com/open-language/.
GeoScenario	GeoScenario is a somewhat higher-level domain specific language (DSL) for scenario representation, whose syntax also looks like XML. (Queiroz 2019)
SCENIC	SCENIC is a flexible high-level language that is complementary to OpenScenario. (Freemont 2019). SCENIC can be complemented by the opensource VERIFAI toolkit for Machine Learning/Artificial Intelligence. VERIFAI is described in (Dreossi 2019).

OpenScenario and Open Drive	https://www.asam.net/ Simulation standards: OpenDrive (https://www.asam.net/standards/detail/opendrive/), OpenScenario (https://www.asam.net/standards/detail/openscenario/) OpenScenario is of widespread use among stakeholders for the scenario description, and is also adopted by initiatives related to Database development (e.g. by France, UK) ASAM took over work done by PEGASUS on that: see also PEGAUS Project (PEGASUS 2020).
PARACOSM	Paracosm is a reactive language introduced by (Majumdar 2019) for writing test scenarios for AVs. Paracosm allows users to programmatically describe complex driving situations with specific visual features as well as reactive temporal behaviors of cars and pedestrians. Paracosm programs are executed on top of a game engine that provides realistic physics simulation and visual rendering. The infrastructure allows systematic exploration of the state space, both for visual features, environmental conditions (lighting, shadows, fog) and for reactive interactions with the environment (pedestrians, presence of approaching vehicles, etc).
CrisGen	The authors in (Nonnengart 2019) introduce a novel formal method-based approach CriSGen for an automated and complete generation of critical trac scenarios for virtual training of self-driving cars.

5.2 Real and virtual testing of AV

Testing of AVs can be implemented either in a real environment, a simulated/virtual environment or even a combination of both:

- Real environment testing is the one currently adopted in the automotive industry where vehicles are submitted to driving test conditions either in a specialized track environment which can be controlled by the testers (e.g., to introduce special conditions like obstacles) or in real traffic conditions, which can reproduce more faithfully the conditions when the vehicle is deployed in the market but which cannot be controlled by the tester.
- Simulated environment is where the computing platform of the AV is subject to a virtual simulation, to evaluate the response of the AVs processing functions and its sensors or actuators if they are also part of the simulated environment test. In comparison to the real environment testing, the simulated environment can widen the set of conditions defined by the testers but there is the risk that realistic conditions are not reproduced in a complete way.
- Mixed reality test drive (MRTD) is a combination of the two type of testing approaches described above. It uses real environmental conditions of real test drives and the accuracy and reproducibility of virtual test drive vehicle behavior descriptions (scenarios). An example of MRTD is described in (Heinz 2017) where OpenScenario is used as a scenario language.

5.3 Evaluation metrics for scenario language definition.

This subsection discusses the potential metrics for the evaluation of the scenario languages (to understand which language would be preferable and/or adopted),

A proposal for the evaluation of scenario languages is suggested in (Queiroz 2019), where the authors identify the following basic principles (the following text is extracted from (Queiroz 2019)):

1. *Reuse*: Leverage existing open formats to build a new language on top of well-known and used structures. With this approach, existing tools can be reused to support our new language with only minor adjustments.
2. *Simplicity*: The language is simple enough to be human readable when simple scenarios are modeled. Tools are encouraged to support complex scenarios.
3. *Coverage*: It is able to express the main components of a scenario.
4. *Extensibility*: It can be easily extended with new features and specializations of its standard components.
5. *System independence*: It supports test cases for different AV designs, operating on different levels of automation.
6. *Tool independence*: It can be interpreted and executed by alternative simulation and test environments.
7. *Executability*: It can express concrete scenarios that can run in simulation environment without the need of additional steps or software modules. For example, a scenario does not need the addition of a software module implementing a machine learning algorithm to execute.

Another important consideration can be derived from (SAE 2018) that states: "Some of the technologies used in autonomous vehicles are inherently statistical in nature. In general, they tend to be non-deterministic (non-repeatable), and may give answers that are only correct to some probability – if a probability can be assigned at all. Validating such systems presents challenges not typically found in more deterministic, conventional automotive control systems". One of the reasons is that the cognitive process to understand the context and take an action is implemented in the vehicle rather than by the human. Because the human driver response can vary in the human driver population when executing a specific driving scenario, the same consideration can be applied to an AV as the cognitive algorithms outcome may vary from model to model or from slight variations in the scenario (e.g., presence of varying degrees of visibility due to rain, fog or darkness).

One of the outcomes of the consideration above is that evaluation metrics for a scenario execution may not be an exact pass/fail criterion but it can also provide a statistical indicator on how a scenario was passed. For example, an AV may not always provide the same outcome in a test track testing scenario especially when all the conditions may not be fully reproducible. On the other side, the desired outcome of the testing and the AV deployment is to reach almost 100% or 100% statistical probability success especially when safety aspects are present (e.g., avoid a pedestrian). This aspect of testing of AV is discussed in detail in (ADAPTIVE 2015) where statistical tools, which can be applied to AV testing, are identified and described.

5.4 Definition of a potential scenario database

This subsection discusses the definition of a scenario database and describes the key components including the identification of relevant activities (i.e., creation of a database) in this domain.

5.4.1 Scenarios Filtering

One initial consideration for the definition of a database scenario is that highly automated systems and AVs in particular are typically highly-dimensional systems with continuous dynamics interacting with complex and unpredictable environments. Therefore, it is not possible to exhaustively cover this infinite state-space with a finite (and sufficiently small) number of tests (ENABLE 2019).

This means that we need a criterion to define and select relevant tests for the overall Type Approval/Certification of AV types (UoM 2020). If not all the available scenarios can be part of the Type Approval/Certification, a sub-selection of scenarios can be filtered from the overall set on the basis of specific metrics/criteria like:

1. *Consistency with reality*: A scenario could be consistent with real situations, so that its application to the Type Approval of automated vehicles is justified. For example, the test scenario parameters ideally should be selected based on naturalistic road user data (see (UoM 2020) for an extensive discussion on this aspect).

2. *Requirements traceability*. A scenario could be easy to trace to high level requirements for the functioning of the specific AV type. Then, a scenario could be preferable to another if it addresses a greater part of requirements or in a more complete way.
3. *Criticality*. This metric evaluates the scenario based on its relevance to critical situations like a vehicle accident or a near miss situation.
4. *Cost and complexity.* This metric evaluates the cost and the complexity of the scenario execution.
5. *Relation to the operational context of the AV.* This metric evaluates how relevant is the scenario to the operational context for which the AV has been designed. For example, the operational context of a commercial vehicle is different from a passenger vehicles or the operational context is different for vehicle with a level of automation equal to 4 instead of 5 (see (SAE 2016a) for a description of the levels of automation).

These are only examples of possible criteria/metrics. More work is needed to identify potential criteria and metrics, which can be used to filter and select scenarios for specific contexts, thus the following recommendation.

Recommendation 11: Because the number of possible scenarios for testing AVs can be unbounded and it can also vary depending on the operational context of the AV (e.g., commercial vehicle, passenger vehicle), it is important to define selection criteria to identify a limited but still suitable set of test scenarios. Additional research efforts are needed in this area.

5.4.2 Scenarios Classification

An important functionality of the database is the capability to classify scenarios along different dimensions. This is different from the definition of criteria/metrics for the selection of adequate scenarios discussed in the previous subsection but it is focused on how the scenarios should be stored in the scenario database and which categories or classification dimensions can be used for their classification. This would help the task of searching of scenarios from the scenario database.

The following categories are proposed at this stage:

1. *Virtual/Track/Real/Mixed Reality.* If the scenario must be executed in a virtual, track test site, real or mixed reality context.
2. *Autonomous Vehicle category*. To which category of autonomous vehicle the scenario should be applied. For example, a scenario could only be applied to commercial vehicles or passenger vehicles or both.
3. *Level of automation*. To which level of automation the scenario refers.
4. *Repeatability*. If a scenario must be executed a number of times rather than only one.
5. *Requirements area traceability*. This dimension indicates to which requirements area (or areas) the scenario refers.
6. *Regulation*. If a scenario is defined in relation to a specific regulation.
7. *Dependencies*. This dimension is used to describe the dependencies of one scenario on other scenarios.
8. *Criticality.* This dimension indicates if the scenario is related to a critical situation or a hazardous situation. This can also be related to the concept that scenario may be impossible to achieve because there is not time for the AV to reach (e.g., to avoid a pedestrian) or possible. See (UoM 2020) for further discussions on this aspect.
9. *Sensitivity.* If the test scenario contains sensitive information.

10. *Formal definition.* If the test scenario is defined in a formal way, semi-formal, or informal notation. Formal or semi-formal are preferable.

In addition, all scenarios shall include (ISO 26262) the parameter ranges of the state values used for scenario representation and scenarios shall provide a formal notation for the representation of the parameter ranges (for example a data format) to enable an automated processing

Additional information on scenarios definition and their attributes is available from ISO 26262 and some ambiguities in relation to this aspect are discussed in (Menzel 2018). To resolve such ambiguities, the authors have defined three different categories of scenario (extracted from (Menzel 2018)):

- Functional scenarios include operating scenarios on a semantic level. The entities of the domain and the relations of those entities are described via a linguistic scenario notation. The scenarios are consistent. The vocabulary used for the description of functional scenarios is specific for the use case and the domain and it can include different levels of detail.
- Logical scenarios include operating scenarios on a state space level. Logical scenarios represent the entities and the relations of those entities with the help of parameter ranges in the state space. The parameter ranges can optionally be specified with probability distributions. Additionally, the relations of the parameter ranges can optionally be specified with the help of correlations or numeric conditions. A logical scenario includes a formal notation of the scenario.
- Concrete scenarios distinctly depict operating scenarios on a state space level. Concrete scenarios represent entities and the relations of those entities with the help of concrete values for each parameter in the state space.

5.4.3 Desirable qualities for a Scenario Database

This subsection describes the desirable qualities and requirements for a scenario database. This is not to be confused with the criteria/metrics for the scenario selection and classification discussed in the previous sub-sections.

The following requirements are defined:

1. Access control with defined roles to limit the access of unauthorized users to sensitive content and scenarios.
2. Capability to store the scenario parameters range of values together with the scenario itself.
3. Capability to translate scenarios from other databases and other formats.
4. Preserve the integrity of scenarios records.
5. Support the traceability of requirements, scenarios and results.
6. Possibility to update the scenarios format and content.
7. Powerful searching capabilities to identify relevant scenarios based on metadata of the scenario.

5.4.4 A list of existing scenario databases

The scenario database is a data storage area (central or distributed) for storing the scenarios and their associated metadata including the range of the parameters, used in the scenario. There are already similar scenario databases in other contexts.

For example, in the aviation, maritime and railway sectors, the European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) database exists, developed by the JRC and already used within aviation, maritime and railway sectors worldwide (EC 2020a).

In the sector of testing of automated vehicles, we have various examples of projects, whose goal is to set up a scenario database.

In Germany, the project PEGASUS (Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations) has the goal to develop a generally accepted and standardized procedure, for the testing and approval of automated driving functions to facilitate the rapid

implementation of automated driving into practice. The description of the scenarios is based on the OpenDRIVE and OpenSCENARIO (PEGASUS 2020).

In UK, the MUSICC project (UK DoT 2020) has defined a Multi-User Scenario Catalogue for CAVs, which has the objective to:

- Create a standard language to describe scenarios
- Build an open and extensible library of scenarios for CAV certification
- Focus on simulation testing environment

A functional prototype system has been built and is undergoing user trials with interested stakeholders. The scenario database language is OPENSCENARIO. The timeframe is for a full deployment for the end of 2022.

In France, the MOSAR (Méthodes et Outils pour la conception et la validation de Systèmes Autonomes Robustes) defines scenarios libraries for AV design and validation.

In Sweden, the DRIVE SWEDEN project is a strategic Innovation Program (SIP) that focuses on creating a mobility system of the future for people and gods that are sustainable, safe and accessible for all. The program is funded by the Swedish Energy Agency, the Swedish Research Council Formas and Sweden's innovation agency VINNOVA. In the context of the DRIVE SWEDEN project, there is an activity of the creation of a scenario database for testing of automated vehicles.

The list is not exhaustive and a more detailed description is provided in (Galassi 2020a) and (Galassi 2020b).

As shown in the examples above, there are different database scenarios, which could generate a fragmentation of test scenarios across jurisdictions: national or regional. A public-private partnership could be set up to define a common scenario database to be used as a reference framework for Type Approval activities. The scenario database includes the processes to define a scenario language, the methodology to create and apply scenarios and to improve the scenarios on the basis of market surveillance.

Recommendation 12: A public-private partnership could be set-up to design, develop and deploy a scenario database for Type Approval of automated vehicles. The scenario database includes the processes to define a scenario language, methodology to create and apply scenarios and to improve the scenarios on the basis of market surveillance.

5.5 Processes for the scenario database

We can identify three main processes for the scenario databases:

1. Definition of the scenarios from the initial requirements
2. Application of scenarios definition to testing
3. Update of scenarios definition from feedback received from the field after market deployment (market surveillance).

For the first two processes, PEGASUS project has defined an extensive framework, which is described in Figure 3 and Figure 5. We refer to the PEGASUS project at https://www.pegasusprojekt.de/en/ (PEGASUS 2020) for an additional description of these processes.

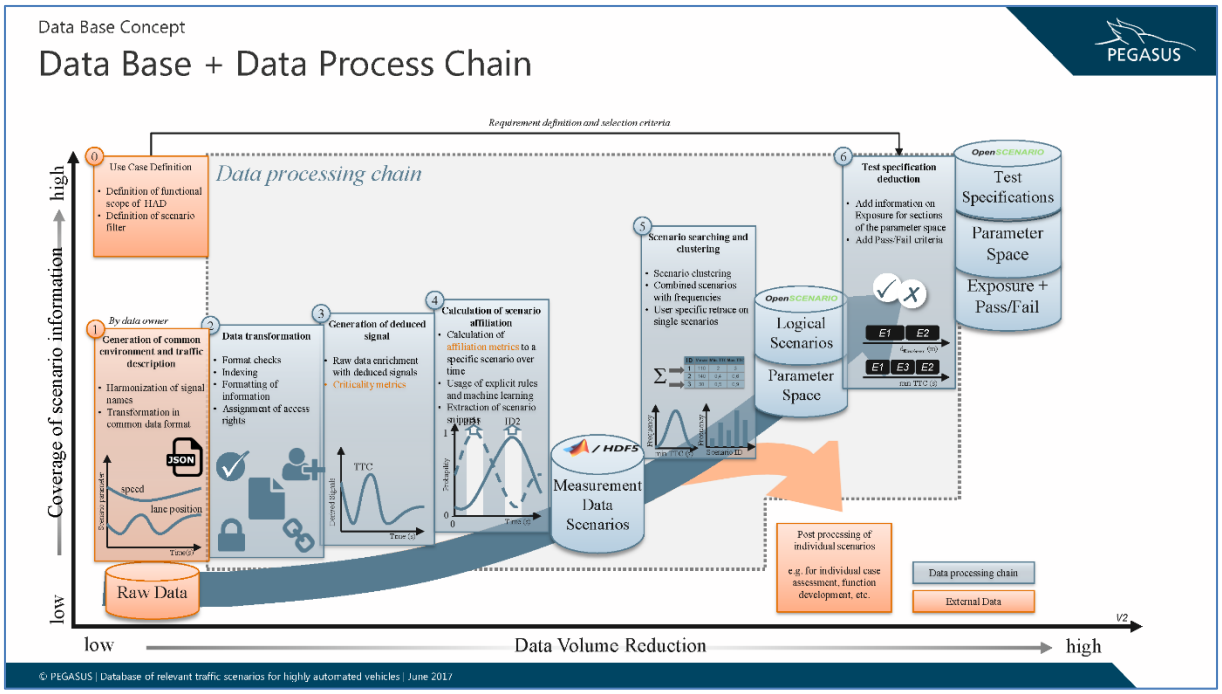

Figure 5 Database data process chain (from PEGASUS project (PEGASUS 2020))

Even if it is acknowledged that the PEGASUS project has performed an admirable effort in the definition of processes for the creation of a scenario database, the results from the PEGASUS project must be further assessed with similar initiatives to create a harmonized set of processes for the creation and maintenance of the database scenario for testing of AVs. Thus, the following recommendation is provided, which is linked to Recommendations 12 and 14.

Recommendation 13: The results from the PEGAGUS project must be evaluated by an impartial committee to decide which elements can be included in a European wide scenario database framework for the testing of AVs.

The third process must be defined but the following considerations can be put forward:

1. It must be decided which parties are responsible to collect the data from market surveillance which can be used an input and feedback to the scenario generation process and update.
2. The format to collect the data for market surveillance must be decided.
3. It is must be decided who is responsible to update the scenarios on the basis of the collected data. It could be assumed that the responsible are the same, who drafted the initial scenarios.
4. Because of different jurisdictions in Europe, the data may be collected by different entities. Interoperability and well defined channels to report information must be defined.
5. The role of vehicle manufacturers, law enforcers and consumers' associations must be defined. Each organization have different knowledge, rights and obligations in the automotive domain. Each of these stakeholders may have different access rights to access the scenario database.

Recommendation 14: A process for collection of data used to update existing scenarios must be defined with a clear definition of roles for the main stakeholders in the automated vehicle domain (e.g., manufacturers, law enforcers and consumers' associations).

6 Recommendations

The purpose of this section is to summarize the recommendations, which were initially presented in the previous sections of the report. Each recommendation is related to a specific area: update of regulatory framework, standardization activities, guideline for the industry or research opportunity.

6.1 Summary table of the recommendations

Table 4 Summary of the recommendations of this report

Identifier	Recommendation description	Area
1	The design and implementation of the processes required for cybersecurity aspects in automated vehicles must take in consideration the dependencies among the processes themselves.	Regulation, industry, research
2	The function of software update in automated vehicles will require the implementation of time efficient software testing processes while maintaining a wide testing coverage of the operational scenarios. This report recommends the increase of research efforts in software testing for automated vehicles through research funding schemes (Horizon Europe) with a particular focus on testing of the artificial intelligence components of the automated vehicle.	Standardization, research
3	This report recommends to revise the existing accreditation schemes in Europe to verify if they are adequate to support the auditing of the Cyber Security Management System (CSMS) of automated vehicle manufacturers for the cybersecurity aspects of Type Approval.	Regulation, standardization
4	This report recommends to set up a vulnerability database and an associated process for the reporting of threats and vulnerabilities in automated vehicles (for all levels of automation) at European level.	Regulation
5	Standardization efforts should be directed to the definition of test bed for cybersecurity testing of automated vehicles including the definition of appropriate testing languages.	Standardization
6	Type approval/certification of the Artificial Intelligence components of the AV should include real testing in a controlled environment, real testing in a normal traffic environment and testing in a simulation environment.	Regulation, standardization, research
7	A government/industry partnership should be set up for the definition of a simulated testing environment and a common set of simulated testing scenarios based on a common language and a defined set of outcomes.	Regulation, industry
8	**The** design of the Machine Learning/Deep Learning algorithms in automated vehicles should include mitigation techniques against adversary machine learning.	Industry, research

9	There is the need to expand the research efforts for the testing of Artificial Intelligence components (e.g., ML/DL) in automated vehicles with specific focus on the optimization of the test cases, application of testing activities in different phases of the development lifecycle and testing for AI robustness against adversary machine learning. It is also recommended that research outputs should be standardized to support harmonized testing of AVs.	Industry, research
10	Specific measures must be defined and adopted for the Over The Air (OTA) software update of the Machine Learning/Deep Learning algorithms in Autonomous Vehicles. Software update in this context may also mean update of the ML/DL learning hyper-parameters and weights.	Industry, research
11	Because the number of possible scenarios for testing AVs can be unbounded and it can also vary depending on the operational context of the AV (e.g., commercial vehicle, passenger vehicle), it is important to define selection criteria to identify a limited but still suitable set of test scenarios. Additional research efforts are needed in this area.	Industry, research
12	A public-private partnership should be set-up to design, develop and deploy a scenario database for Type Approval of automated vehicles. The scenario database includes the processes to define a scenario language, methodology to create and apply scenarios and processes to improve the scenarios on the basis of market surveillance.	Regulation, industry
13	The results from the PEGAGUS project must be evaluated by an impartial committee to decide which elements can be included in a European wide scenario database framework for the testing of AVs	Regulation, industry
14	A process for the collection of data used to update existing scenarios must be defined with a clear definition of roles for the main stakeholders in the automated vehicle domain (e.g., manufacturers, law enforcers and consumers' associations.)	Regulation, industry

6.2 Discussion

The recommendations identified in the previous subsection address different aspects of Type Approval in AV with a number of recommendations focused on the artificial intelligence components in the AV since it is a largely unexplored area where the complexity of the problem faces severe time requirements for safety reasons.

There is some overlapping and dependencies among the different recommendations. Recommendation 2 on efficient software testing for software update overlaps with recommendation 10, which is focused on the update and testing of the artificial intelligence (AI) components (ML/DL algorithms). Even if there is overlapping, the distinction between the recommendations should be maintained because the testing and update process for AI components can be quite different from the general software update. For example, the AI update may be only limited to the update of the ML/DL hyper parameters defined in the algorithms. Recommendation 14 on the collection of information from the field to enhance and update existing testing scenarios has also some overlap with Recommendation 4 in regards to the cybersecurity aspects, where a vulnerability database is created for vulnerabilities/threats identified in the field. On the other side, the

recommendations 4 and 14 should be kept distinct because they may be implemented by different stakeholders (cybersecurity agencies and experts for 4 and transportation experts for 14).

Recommendation 2 on the definition of efficient software testing to support a rapid testing and deployment of software updates may be dependent on Recommendation 11 for the definition of criteria/metrics for the proper selection of testing scenarios.

Recommendation 8 on the design of ML/DL algorithms to make them robust against AML is dependent on Recommendation 9 for the definition of specific tests for AI because such testing will also include robustness against AML.

Recommendation 12 on the definition of a public/private partnership to create a scenario database is dependent on recommendation 7 for the definition of public/private partnership to design a simulated test environment.

Such overlapping and dependencies are related to the consideration that each recommendation is focused on a function or set of functions but Type Approval is composed by many functions, which are all needed to guarantee the safety of the AV before AVs are deployed on the road. This is the reason why Recommendation 1 is proposed in this report.

7 Conclusions

This report has conducted an analysis on three main aspects of testing and certification of automated vehicles: cybersecurity testing, testing of the artificial intelligence algorithms and definition of the testing scenarios, which can be part of the Type Approval. These aspects are related among them because cybersecurity vulnerabilities can negatively impact the safety of the automated vehicle. Testing of the artificial intelligence (AI) algorithms is a significant part of the overall testing of automated vehicles because the AI algorithms are ultimately responsible for the driving actions at high levels of automation.

Testing and certification of automated vehicles is a new area where there are still many open questions at regulatory, industry and research levels. This report proposes a set of recommendations for policy makers, standardization bodies, industry and research communities to foster an adequate testing of automated vehicles before they are deployed in the market. The recommendations are focused on the most critical areas for the operation and deployment of automated vehicles, where further studies and experimental activities are required. In particular, this report recommends the creation of public/private partnerships to foster the definition of harmonized testing scenarios to support the Type Approval process. A fragmentation of scenarios and testing processes may introduce gaps in Type Approval, which negatively impact AV safety. A set of recommendations are defined to improve the cybersecurity aspects in AVs both to support specific efforts to improve cybersecurity testing of AV and to create a vulnerability database for AV, which can enhance the cybersecurity testing scenarios.

Another set of recommendations is focused on the definition of software update processes in AV which can benefit from efficient testing processes to support a safe and rapid deployment of new software releases in AVs in the field. The robustness of the machine learning/deep learning algorithms of the artificial intelligence components in the AV is also addressed in another set of recommendations. In particular, this report recommends the definitions of specific testing processes for machine learning/deep learning algorithms and further study to make them more robust against adversarial machine learning and cybersecurity threats.

Further developments of this report will investigate how the recommendations presented in this report can be discussed in consultations with the government, industry, research and user communities to be implemented in policies and standards.

References

(ACEA 2019)	ACEA. Roadmap for the Deployment of Automated Driving. https://www.acea.be/publications/article/roadmap-for-the-deployment-of-automated-driving-in-the-european-union. Last accessed 10 October 2020.
(Adaptive 2015)	Horizon 2020 Adaptive project Deliverable D7.1. Test and Evaluation Plan https://www.adaptive-ip.eu/index.php/AdaptIVe-SP7-v12-DL-D7.1-Test%20and%20Evaluation%20Plan-file=files-adaptive-content-downloads-Deliverables%20&%20papers-AdaptIVe-SP7-v12-DL-D7.1-Test%20and%20Evaluation%20Plan.pdf Last accessed 10 October 2020.
(Appel 2020)	Appel, M., Oruganti, P. S., Ahmed, Q., Wilkerson, J., & Sekar, R. (2020). A Safety and Security Testbed for Assured Autonomy in Vehicles (No. 2020-01-1291). SAE Technical Paper.
(Arcuri 2010)	A. Arcuri, M. Z. Iqbal, and L. Briand, "Black-box system testing of real-time embedded systems using random and search-based testing," inIFIPInternational Conference on Testing Software and Systems.Springer,2010, pp. 95–110.
(Arkar 2017)	Arkar Min Aung, Yousef Fadila, Radian Gondokaryono, and LuisGonzalez. Building robust deep neural networks for road sign detection. https://arxiv.org/abs/1712.09327 Last accessed 10 October 2020.
(ASAM 2020)	ASAM - Standardization for Automotive Development https://www.asam.net/ Last accessed 10 October 2020.
(Bhutani 2018)	Ankita Bhutani, Preeti Wadhwani , Autonomous Cars Market Size, By Level of Autonomy (Level-1, Level-2, Level-3, Level-4), By Type (Internal Combustion Engine (ICE), Hybrid Electric Vehicle (HEV), Battery Electric Vehicle (BEV)), Industry Analysis Report, Regional Outlook, Growth Potential, Competitive Market Share & Forecast, 2018 – 2024. Published Date: Oct 2018. Report ID: GMI1224 https://www.gminsights.com/industry-analysis/autonomous-car-market. Last accessed 10 October 2020.
(Biggio 2018)	Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331.
(BMW 2020)	Self-driving and cooperative cars https://www.bmw.com/content/dam/bmw/marketBMWCOM/bmw_com/categories/Innovation/ebook-self-driving-cars/pdf/e-book-self-driving-cars_en.pdf.asset.1578326516692.pdf.

	Last accessed 10 October 2020.
(Brendel 2017)	Brendel, W., Rauber, J., & Bethge, M. (2017). Decision-based adversarial attacks: Reliable attacks against black-box machine learning models. arXiv preprint arXiv:1712.04248. https://arxiv.org/abs/1712.04248 Last accessed 10 October 2020.
(CARLA 2020)	CARLA Simulator. https://carla.org/. Last accessed 10 October 2020.
(Chattopadhyay 2020)	Chattopadhyay, A., Lam, K. Y., & Tavva, Y. (2020). Autonomous vehicle: Security by design. IEEE Transactions on Intelligent Transportation Systems.
(CROADS 2020)	C-ROADS web site https://www.c-roads.eu/platform.html. Last accessed 10 October 2020.
(Dreossi 2019)	Dreossi, T., Fremont, D. J., Ghosh, S., Kim, E., Ravanbakhsh, H., Vazquez-Chanlatte, M., & Seshia, S. A. (2019, July). Verifai: A toolkit for the formal design and analysis of artificial intelligence-based systems. In International Conference on Computer Aided Verification (pp. 432-442). Springer, Cham
(EC 2007)	"Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive) Text with EEA relevance". eur-lex.europa.eu - Access to European Union law. publications.europa.eu - Publications Office of the European Union. 9 October 2007. Retrieved 27 September 2009. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32007L0046 Last accessed 10 October 2020.
(EC 2016)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility COM/2016/0766 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A766%3AFIN Last accessed 10 October 2020.
(EC 2018)	Regulation (EU) 2018/858 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 (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance.) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R0858. Last accessed 20 October 2020.

(EC 2019a)	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2019/881/oj. Last accessed 10 October 2020.
(EC 2019b)	Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2019/2144/oj. Last accessed 10 October 2020.
(EC 2019c)	Alonso Raposo, M. (Ed.), Ciuffo, B. (Ed.), Alves Dies, P., Ardente, F., Aurambout, J-P., Baldini, G., Baranzelli, C., Blagoeva, D., Bobba, S., Braun, R., Cassio, L., Chawdhry, P., Christidis, P., Christodoulou, A., Corrado, S., Duboz, A., Duch Brown, N., Felici, S., Fernández Macías, E., Ferragut, J., Fulli, G., Galassi, M-C., Georgakaki, A., Gkoumas , K., Grosso, M., Gómez Vilchez, J., Hajdu, M., Iglesias, M., Julea, A., Krause, J., Kriston, A., Lavalle, C., Lonza, L., Lucas, A., Makridis, M., Marinopoulos, A., Marmier, A., Marques dos Santos, F., Martens, B., Mattas, K., Mathieux, F., Menzel, G., Minarini, F., Mondello, S., Moretto, P., Mortara, B., Navajas Cawood, E., Paffumi, E., Pasimeni, F., Pavel, C., Pekár, F., Pisoni, E., Raileanu, I-C., Sala, S., Saveyn, B., Scholz, H., Serra, N., Tamba, M., Thiel, C., Trentadue, G., Tecchio, P., Tsakalidis, A., Uihlein, A., van Balen, M., Vandecasteele, I., The future of road transport - Implications of automated, connected, low-carbon and shared mobility, EUR 29748 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-14318-5, doi: 10.2760/668964, JRC116644.
(EC 2020a)	European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) https://ec.europa.eu/jrc/en/scientific-tool/eccairs-portal-european-coordination-centre-accident-and-incident-reporting-systems-web-portal. Last accessed 10 October 2020.
(EC 2020b)	Hamon, R., Junklewitz, H. and Sanchez Martin, J., *Robustness and Explainability of Artificial Intelligence*, EUR 30040 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-14660-5 (online), doi:10.2760/57493 (online), JRC119336.
(EC 2020c)	Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R., Nordvik, J., Papameletiou, D., Reina, V., Ruzzante, G., Sanchez Martin, J., Sportiello, L., Steri, G. and Tirendi, S., *Cybersecurity, our*

	digital anchor, Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., Kounelis, I., Mortara, B., Nordvik, J. and Sanchez Martin, J. editor(s), EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1 (online),978-92-76-19958-8 (print), doi:10.2760/352218 (online),10.2760/967437 (print), JRC121051.
(ENABLE 2019)	Enable s-3. Testing and Validation of highly automated systems. Summary of the results 2019. https://www.tugraz.at/fileadmin/user_upload/Institute/IHF/Projekte/ENABLE-S3_SummaryofResults_May2019.pdf Last accessed 10 October 2020.
(ENABLE 2020)	Enable s-3 project web site. https://www.enable-s3.eu/ . Last accessed 10 October 2020.
(ENISA 2019)	ENISA good practices for security of Smart Cars https://www.enisa.europa.eu/publications/smart-cars. Last accessed 10 October 2020.
(Felderer 2016)	Felderer, M., Büchler, M., Johns, M., Brucker, A. D., Breu, R., & Pretschner, A. (2016). Security testing: A survey. In Advances in Computers (Vol. 101, pp. 1-51). Elsevier.
(Feng 2020a)	S. Feng, Y. Feng, C. Yu, Y. Zhang and H. X. Liu, (2020) "Testing Scenario Library Generation for Connected and Automated Vehicles, Part I: Methodology," in *IEEE Transactions on Intelligent Transportation Systems*, doi: 10.1109/TITS.2020.2972211.
(Feng 2020b)	Feng, S., Feng, Y., Sun, H., Bao, S., Zhang, Y., & Liu, H. X. (2020). Testing scenario library generation for connected and automated vehicles, part II: Case studies. IEEE Transactions on Intelligent Transportation Systems.
(Foretellix 2020)	Measurable Scenario Description Language.[Online]. Available: https://www.foretellix.com/open-language/. Last accessed 10 October 2020.
(Fowler 2018)	D. S. Fowler, J. Bryans, S. A. Shaikh and P. Wooderson, "Fuzz Testing for Automotive Cyber-Security," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg City, 2018, pp. 239-246, doi: 10.1109/DSN-W.2018.00070.
(Fremont 2019)	D. J. Fremont et al., "Scenic: A language for scenario specification and scene generation," in Programming Language Design and Implementation (PLDI), 2019, pp. 63–78.
(Fremont 2020)	Fremont, D. J., Kim, E., Pant, Y. V., Seshia, S. A., Acharya, A., Bruso, X., ... & Mehta, S. (2020). Formal Scenario-Based Testing of Autonomous Vehicles: From Simulation to the Real World. arXiv preprint arXiv:2003.07739. https://arxiv.org/abs/2003.07739. Last accessed 10 October 2020.
(Galassi 2020a)	Galassi, M. and Lagrange, A., New approaches for automated vehicles certification, Tsakalidis, A. editor(s), EUR 30087 EN, Publications Office of the

	European Union, Luxembourg, 2020, ISBN 978-92-76-10720-0 (online), doi:10.2760/766068 (online), JRC119345. https://ec.europa.eu/jrc/en/publication/new-approaches-automated-vehicles-certification. Last accessed 10 October 2020.
(Galassi 2020b)	Galassi, M. and Lagrange, A., New approaches for automated vehicles certification, Part II. Editor Publications Office of the European Union, Luxembourg, 2020, JRC121507. To appear.
(Goodfellow 2014)	J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572,2014
(Goodfellow 2018)	Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making machine learning robust against adversarial inputs. Communications of the ACM, 61(7), 56-66.
(Guardian 2016)	Tesla driver dies in first fatal crash while using autopilot mod https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk. Last accessed 10 October 2020.
(Halder 2020)	Halder, S., Ghosal, A., & Conti, M. (2020). Secure Over-The-Air Software Updates in Connected Vehicles: A Survey. *Computer Networks*, 107343
(HEADSTART 2020)	HeadStart project https://www.headstart-project.eu/ Last accessed 10 October 2020.
(Heinz 2017)	Heinz, A., & Wolfram Remlinger, J. S. (2017). Track-/Scenario-based Trajectory Generation for Testing Automated Driving Functions. In 8. Tagung Fahrerassistenz.
(Huang 2011)	Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011, October). Adversarial machine learning. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (pp. 43-58).
(ISO 26262)	ISO 26262. "Road vehicles – Functional safety", Parts 1-12
(Jakobi 1995)	N. Jakobi, P. Husbands, and I. Harvey, \Noise and the Reality Gab: The Use of Simulation in Evolutionary Robotics," Lecture Notes in Computer Science, vol. 929, pp. 704, 720, 1995.
(Khastgir 2017)	S. Khastgir, G. Dhadyalla, S. Birrell, S. Redmond, R. Addinall, and P. Jennings, "Test scenario generation for driving simulators usingconstrained randomization technique," SAE Technical Paper, Tech. Rep.,2017
(Klischat 2019)	Klischat, M., & Althoff, M. (2019, June). Generating critical test scenarios for automated vehicles with evolutionary algorithms. In 2019 IEEE Intelligent Vehicles Symposium (IV) (pp. 2352-2358). IEEE.
(Lee 2020)	Lee, D., & Hess, D. J. (2020). Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization. Transportation Research Part A: Policy and Practice, 136, 85-98.

(Li 2016)	L. Li, W.-L. Huang, Y. Liu, N.-N. Zheng, and F.-Y. Wang, "Intelligencetesting for autonomous vehicles: a new approach,"IEEE Transactions on Intelligent Vehicles, vol. 1, no. 2, pp. 158–166, 2016.
(Loyall 1997)	Loyall, J. P., Mathisen, S. A., & Satterthwaite, C. P. (1997, July). Impact analysis and change management for avionics software. In Proceedings of the IEEE 1997 National Aerospace and Electronics Conference. NAECON 1997 (Vol. 2, pp. 740-747). IEEE.
(Machin 2019)	Machin, M., Garrido, P., Martinez, F. J., & Sanguesa, J. A. (2019, January). V-tracer: A vehicular trace generator for future predictive maintenance. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-2). IEEE.
(Majumdar 2019)	Majumdar, R., Mathur, A., Pirron, M., Stegner, L., & Zufferey, D. (2019). Paracosm: A Language and Tool for Testing Autonomous Driving Systems. arXiv preprint arXiv:1902.01084 https://arxiv.org/abs/1902.01084 Last accessed 10 October 2020.
(Matheu 2019)	Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, 64-83.
(McDaniel 2016)	McDaniel, P., Papernot, N., & Celik, Z. B. (2016). Machine learning in adversarial settings. IEEE Security & Privacy, 14(3), 68-72.
(Menzel 2018)	Menzel, T., Bagschik, G., & Maurer, M. (2018, June). Scenarios for development, test and validation of automated vehicles. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 1821-1827). IEEE.
(Miller 2015)	Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, *2015*, 91.
(Morris 2020)	Morris, D., Madzudzo, G., & Garcia-Perez, A. (2020). Cybersecurity threats in the auto industry: Tensions in the knowledge environment. Technological Forecasting and Social Change, 157, 120102
(MOSAR 2020)	Méthodes et Outils pour la conception et la validation de Systèmes Autonomes Robustes (includes scenarios library for AD design and validation) – France https://www.irt-systemx.fr/ Last accessed 10 October 2020.
(Mullins 2018)	E. Mullins, P. G. Stankiewicz, R. C. Hawthorne, and S. K. Gupta,"Adaptive generation of challenging scenarios for testing and evaluation of autonomous vehicles,"Journal of Systems and Software, vol. 137, pp.197–215, 2018
(Neisse 2020)	Neisse, R., Hernández-Ramos, J. L., Matheu-Garcia, S. N., Baldini, G., Skarmeta, A., Siris, V., ... & Nikander, P. (2020). An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information. IEEE Internet Computing, 24(3), 19-29.

(Nonnengart 2019)	Nonnengart, A., Klusch, M., & Müller, C. (2019). CriSGen: Constraint-based Generation of Critical Scenarios for Autonomous Vehicles. In Proc. of the Int. Workshop on Formal Methods for Autonomous Systems.
(OAS 2020)	The Open Autonomous Safety at https://oas.voyage.auto/ has produced a Testing Toolkit available at https://oas.voyage.auto/testing-toolkit/. The OAS Testing Toolkit is a Sketch library and asset collection designed to quickly and effectively communicate testing scenarios. https://oas.voyage.auto/testing-toolkit/. Last accessed 10 October 2020.
(Papernot 2016)	Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016, March). The limitations of deep learning in adversarial settings. In 2016 IEEE European symposium on security and privacy (EuroS&P) (pp. 372-387). IEEE.
(PEGASUS 2020)	PEGASUS project https://www.pegasusprojekt.de/en/about-PEGASUS. Last accessed 10 October 2020.
(Petit 2014)	Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent transportation systems, 16(2), 546-556.
(Pokhrel 2020)	Pokhrel, S. R., & Deakin Univeristy, G. (2020). Towards efficient and reliable federated learning using blockchain for autonomous vehicles. *Computer Networks*
(Qayyum 2020)	Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. IEEE Communications Surveys & Tutorials, 22(2), 998-1026.
(Queiroz 2019)	R. Queiroz et al., "GeoScenario: An open DSL for autonomous driving scenario representation," in Proc. 2019 IEEE Intelligent Vehicles Symposium, 2019, pp. 287–294.
(SAE 2015)	SAE International. (2015). Guidelines for Safe On-Road Testing of SAE Level 3, 4, and 5 Prototype Automated Driving Systems (ADS). Warrendale, PA: Author.
(SAE 2016)	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061. https://www.sae.org/standards/content/j3061/ Last accessed 10 October 2020.
(SAE 2016a)	SAE International. (2016). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Warrendale, PA: Author.
(SAE 2018)	Koopman, P., & Wagner, M. (2018). Toward a framework for highly automated vehicle safety validation (No. 2018-01-1071). SAE Technical Paper.
(SAFERTEC 2020)	SAFERTEC project https://www.safertec-project.eu/wp-content/uploads/2020/01/2019SecEvalCriteria.pdf. Last accessed 10 October 2020.

(Shladover 2019)	Shladover, S. E., & Nowakowski, C. (2019). Regulatory challenges for road vehicle automation: Lessons from the california experience. Transportation research part A: policy and practice, 122, 125-133.
(Taeihagh 2019)	Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Reviews, 39(1), 103-128
(Thorn 2018)	Thorn, E., Kimmel, S. C., Chaka, M., & Hamilton, B. A. (2018). A framework for automated driving system testable cases and scenarios (No. DOT HS 812 623). United States. Department of Transportation. National Highway Traffic Safety Administration.
(Tian 2018)	Yuchi Tian, Kexin Pei, Suman Jana, and Baishakhi Ray. 2018. DeepTest: Automated testing of deep-neural-network-driven autonomous cars. In Proceedings of the 40th International Conference on Software Engineering. ACM, 303–314
(TTCN 2020)	Testing and Test Control Notation v3 http://www.ttcn-3.org/index.php/about/references/applicatio-domains. Last accessed 10 October 2020.
(Tuncali 2020)	Cumhur Erkan Tuncali, Georgios E. Fainekos, Hisahiro Ito, and James Kapinski. 2018. Sim-ATAV: Simulation-Based Adversarial Testing Framework for Autonomous Vehicles. In Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week), HSCC 2018, Porto, Portugal, April 11-13, 2018. ACM, 283–284. https://doi.org/10.1145/3178126.3187004.
(TUV 2020)	Homologation of automated vehicles: The regulatory challenge. https://www.i-at.eu/bestanden/I-AT/Documenten/DOC_Homologation%20of_automated%20vehicles_The%20regulatory_challenge.pdf. Last accessed 20 August 2020.
(TUV 2020)	Cybersecurity Assessment for Connected and Automated Vehicles https://www.tuvsud.com/en/industries/mobility-and-automotive/automotive-and-oem/autonomous-driving/cybersecurity-assessment-for-connected-and-automated-vehicles. Last accessed 20 August 2020.
(UK DoT 2020)	Multi-User Scenario Catalogue for Connected and Autonomous Vehicles - United Kingdom https://ts.catapult.org.uk/innovation-centre/cav/cav-projects-at-the-tsc/musicc/ Last accessed 10 October 2020.
(Ulbrich 2015)	S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer. Defining and substantiating the terms scene, situation, and scenario for automated driving. In 2015 IEEE 18th International Conference on Intelligent Transportation Systems, pages 982–988, Sept 2015.

(UN 1958)	"1958 Agreement", formally titled "Agreement concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions". E/ECE/TRANS/505/Rev.2
(UNECE 2020a)	Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf. Last accessed 14 August 2020.
(UNECE 2020b)	Proposal for a new UN Regulation on Software Updates and Software Updates Management Systems. https://undocs.org/ECE/TRANS/WP.29/2020/80. Last accessed 10 August 2020.
(UNECE 2020c)	UNECE GRVA. https://www.unece.org/trans/main/wp29/meeting_docs_grva.html. Last accessed 10 October 2020.
(UoM 2020)	Conducting the Mcity ABC Test: A Testing Method for Highly Automated Vehicles. https://mcity.umich.edu/wp-content/uploads/2020/04/mcity-whitepaper-conducting-ABC-test.pdf. Last accessed 10 October 2020.
(USDOT 2018)	U.S. Department of Transportation, 2018. Preparing for the Future of Transportation: Automated Vehicles 3.0. National Highway Traffic Safety Administration October. https://www.transportation.gov/av/3. Last accessed 14 August 2020.
(Vishnukumar 2017)	H. J. Vishnukumar, B. Butting, C. Müller and E. Sax, "Machine learning and deep neural network — Artificial intelligence core for lab and real-world test and validation for ADAS and autonomous vehicles: AI for efficient and quality test and validation," 2017 Intelligent Systems Conference (IntelliSys), London, 2017, pp. 714-721, doi: 10.1109/IntelliSys.2017.8324372
(Wooderson, 2017)	Wooderson, P. and Ward, D., "Cybersecurity Testing and Validation," SAE Technical Paper 2017-01-1655, 2017, doi:10.4271/2017-01-1655.
(Wysopal 2006)	Wysopal, C., Nelson, L., Dustin, E., & Dai Zovi, D. (2006). The art of software security testing: identifying software security flaws. Pearson Education.
(Xu 2018)	Weilin Xu, David Evans, and Yanjun Qi. Feature squeezing: Detectingadversarial examples in deep neural networks. In25th Annual Networkand Distributed System Security Symposium, NDSS 2018, San Diego,California, USA, February 18-21, 2018, 2018
(Zhou 2019)	Zhou, M., Yu, Y., & Qu, X. (2019). Development of an efficient driving strategy for connected and automated vehicles at signalized intersections: A reinforcement

	learning approach. IEEE Transactions on Intelligent Transportation Systems, 21(1), 433-443.

List of abbreviations

AI	Artificial Intelligence
AML	Adversary Machine Learning
AV	Autonomous Vehicles
ADS	Automated Driving Systems
CNN	Convolutional Neural Networks
CSMS	Cyber Security Management System
DL	Deep Learning
DNN	Deep Neural Networks
DSRC	Dedicated Short Range Communications
EC	European Commission
ECU	Electronic Component Unit
EU	European Union
GAN	Generative Adversarial Networks
IMU	Inertial Measurements Units
ISO	International Standardization Organization
ML	Machine Learning
MRTD	Mixed Reality Test Drive
M-SDL	Measurable Scenario Description Language
NVD	National Vulnerability Database
OEM	Original Equipment Manufacturer
OTA	Over The Air
RNN	Recurrent Neural Networks
SU	Software Update
SAE	Society of Automotive Engineers
TTCN-3	Testing and Test Control Notation Version 3
UNECE	United Nations Economic Commission for Europe
VMAD	Validation Method for Automated Driving

List of definitions

Term	Definition	Reference
Approval Authority	'approval authority' means the authority or authorities of a Member State, notified to the Commission by that Member State, with competence for all aspects of the type-approval of a vehicle, system, component or separate technical unit, or of the individual vehicle approval, for the authorisation process for parts and equipment, for issuing and, if appropriate, for withdrawing or refusing approval certificates, for acting as the contact point for the approval authorities of the other Member States, for designating the technical services, and for ensuring that the manufacturer meets its obligations regarding the conformity of production;	(EC 2018)
Automated Vehicle	"automated vehicle" means a motor vehicle designed and constructed to move autonomously for certain periods of time without continuous driver supervision but in respect of which driver intervention is still expected or required	(EC 2019b)
Certificate of Conformity	'certificate of conformity' means the document issued by the manufacturer which certifies that a produced vehicle conforms to the approved type of vehicle and complies with all regulatory acts that were applicable at the time of its production;	(EC 2018)
Component	'component' means a device that is intended to be part of a vehicle, that can be type-approved independently of a vehicle and that is subject to the requirements of this Regulation (EC 2018) or any of the regulatory acts listed in Annex II of (EC 2018) where the specific regulatory act makes express provision to that effect;	(EC 2018)
Cybersecurity	'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.	(EC 2019a)
Cybersecurity Certification	Cybersecurity certification requires the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance; as such cybersecurity certification plays a key role role in increasing trust and security in products, services and processes. Cybersecurity certification in the EU serves the purpose of providing notice and assurance to users about the level of conformity against stated requirements. EU cybersecurity certification schemes serve as the vehicle to convey such requirements from the EU policy	ENISA[4]

[4] ENISA Web site on cybersecurity certification https://www.enisa.europa.eu/topics/standards/certification.

	level to the industry service provision level and further to the users and conformity assessment bodies.	
Cyber Threat	'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;	(EC 2019a)
EU type approval	'EU type-approval' means the procedure whereby an approval authority certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements of this Regulation;	(EC 2018)
ICT product	'ICT product' means an element or a group of elements of a network or information system;	(EC 2019a)
Manufacturer	'manufacturer' means a natural or legal person who is responsible for all aspects of the type-approval of a vehicle, system, component or separate technical unit, or the individual vehicle approval, or the authorisation process for parts and equipment, for ensuring conformity of production and for market surveillance matters regarding that vehicle, system, component, separate technical unit, part and equipment produced, irrespective of whether or not that person is directly involved in all stages of the design and construction of that vehicle, system, component or separate technical unit concerned;	(EC 2018)
Market surveillance	'market surveillance' means the activities carried out and measures taken by the market surveillance authorities to ensure that vehicles, systems, components and separate technical units as well as parts and equipment made available on the market comply with the requirements set out in the relevant Union harmonisation legislation and do not endanger health, safety, the environment or any other aspect of public interest protection.	(EC 2018)
Motor Vehicle	'motor vehicle' means any power-driven vehicle that is designed and constructed to be moved by its own means, that has at least four wheels, is complete, completed or incomplete, and has a maximum design speed exceeding 25 km/h;	(EC 2018)
National type approval	'national type-approval' means the procedure whereby an approval authority certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements laid down by the law of a Member State, the validity of such approval being restricted to the territory of that Member State;	(EC 2018)
Placing on the market	'placing on the market' means making available a vehicle, system, component, separate technical unit, part or equipment for the first time in the Union;	(EC 2018)

Technical Service	'technical service' means an organisation or body designated by the approval authority as a testing laboratory to carry out tests, or as a conformity assessment body to carry out the initial assessment and other tests or inspections;	(EC 2018)
Type Approval	Type-Approval means the procedure whereby an approval authority certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements.	(EC 2018)
Vehicle on-board diagnostic	'vehicle on-board diagnostic (OBD) information' means the information generated by a system that is on board a vehicle or that is connected to an engine, and that is capable of detecting a malfunction, and, where applicable, is capable of signalling its occurrence by means of an alert system, is capable of identifying the likely area of malfunction by means of information stored in a computer memory, and is capable of communicating that information off-board;	(EC 2018)
Virtual Testing method	'virtual testing method' means computer simulations, including calculations, to demonstrate that a vehicle, a system, a component or a separate technical unit fulfils the technical requirements of a regulatory act listed in Annex II without requiring the use of a physical vehicle, system, component or separate technical unit;	(EC 2018)

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-30472-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/86907

ISBN 978-92-76-26818-5