Position Paper on
Safety validation and roadworthiness testing

Authors: Álvaro Arrúe (Applus IDIADA), Sjef van Montfort (TNO), Jens Kotte (IKA), Julie Maes (BIVV), Gregory Dugernier (BIVV), Ben Rutten (TU/e), Martin Dirnwoeber (Austriatech)

Summary

Safety validation and roadworthiness testing involve the definition of a comprehensive set of methodologies and tools aiming to verify whether vehicles comply with the regulatory and technological requirements. This verification is one of the building blocks for the safe deployment of automated road transport on public roads. These methodologies and tools must take into account both regulatory and technological requirements and should address the whole vehicle lifecycle.

Strong challenges must be addressed to create complete, reliable and continuously evolving procedures which involve not only different types of testing (compliance, commercial up to type approval), but they should also include different levels of granularity, interactions with all road users and with the environment (large amount of highly dynamic and highly variable scenarios) during the whole development process and life cycle of the vehicle. Simulation and virtual testing will play an increasingly relevant role as it provides a very effective way to deal with the high number of scenarios Connected and Automated Driving (CAD) vehicles will encounter. Verification/validation is a very complex issue which is not solved for higher automation and full connectivity yet. No common methodology or process for the verification/validation of SAE level 4/5 systems is defined and with current knowledge verifiable. Further research in the area is fundamental starting from the existing regulatory framework and promoting harmonization throughout Europe.

Exhaustive (safety) validation and trustful roadworthiness testing of increasingly complex systems are key elements to both guarantee and promote the successful deployment of safe, socially accepted automated road transport on our roads.

For this purpose, Europe's future R&D agenda should take into account research on technical, regulatory and societal challenges, guaranteeing Europe's global competitiveness in CAD development and deployment.

Introduction

There is a need to go beyond current state-of-the-art, taking into account the automated vehicle as another element in a complex system that interacts with a highly dynamic and variable environment populated by heterogeneous road users. Cost-effective solutions are paramount as the CAD validation will grow exponentially due to the inherent complexity associated to an exponential growth of the scenarios that the vehicle will be involved. This CARTRE theme will cover both the completeness of the required testing during the development process and during the entire lifecycle of the vehicle, as well as the nature and timeline of the needed procedures. Vehicle type approval, as reference mandatory process in the European Union, should also reflect and cover the complexity that automation involves.

Challenges

There are many challenges that need to be addressed regarding road automation and its verification/validation. First of all, it is important to perform an initial validation for new systems to be introduced in the market. However, the safety validation must be observed during the whole vehicle lifecycle. These two approaches present different challenges:

- **Initial release validation**: With the current state-of-the art on validation/verification methodologies it is not feasible to physically test all the possible road situations. It is critical to find out a minimum set of tests that provide high enough confidence for public road release. A comprehensive, reliable, balanced and complementary combination of physical tests and simulated tests should be defined in order to guarantee the safety of a vehicle before its deployment to public roads.

- **Real world awareness**: Functional validation taking into account the **environment in which the vehicle will drive, including:** Testing in real life situations; (in advance) identification of key scenarios towards the description of a dynamic scenario database.

- **Development completeness:** Including validation testing of operational safety and functional safety as part of the development of a new function and/or a whole automation level. Include/adapt/improve existing development methodologies from other domains (i.e. software development).

- **Human interaction :** This topic (see related CARTRE Theme) must include the vehicle interaction with the driver as well as with the rest of road users and must be reflected in safety validation.

- **Granularity**: Testing should cover several levels of the whole system: component level, vehicle level, system level (including interaction with other road users and infrastructure) taking into account its specific characteristics, commonalities and differences (i.e. scenarios and/or raw data)

- **In-house verification/validation before type approval is updated**: The in-house validation/verification methodologies involved in the initial release of vehicles i.e. until submission for type approval must take into account the current state of type approval process while being flexible enough to adapt to new regulations as they are introduced.

- **Current state-of-the art**: Review of the existing safety validation procedures that might be directly affected by higher levels of automation i.e. passenger passive safety in an automated vehicle, and potentially be outdated. This review should include all the already existing types of testing: compliance, commercial testing (i.e. Euro NCAP), type approval/self-certification. An industry wide international consent is required in order to have a common state of the art.

- **Vehicle update**: If a vehicle hardware and/or software receives an update that modifies its functionalities, these changes and their impact on safety must be addressed. However, it is important to clearly understand when a new update should be considered different enough to start a new validation procedure or if new, whether different approaches able to deal with the update need to be developed.

- **Infrastructure functional updates:** Interaction between infrastructure and vehicles might be changed or improved i.e. with new communication standards or message sets that might have an impact on already deployed vehicles and as a result new tests might be required to make sure legacy vehicles maintain their original safety performance.

- **Vehicle lifecycle:** Maintenance of the CAD systems should be followed during the vehicle lifecycle and regular updates (Over the air (OTA) or through other means) have to be considered. The potential impact OTA might have during the vehicle lifecycle and re-certification schemes have to be defined. The Periodical Technical Inspection (PTI) procedure might also have to be reviewed in terms of periodicity and the tests carried out to check the correct functioning of the automation features (sensors, software, …) of the vehicle**.**

Input for research agenda

Verification/validation of SAE level 4/5 systems/functions can still not be fully achieved with current knowledge and further research in the area is fundamental.

- Development of verification/validation tools and methodologies capable to deal with the initial release of foreseen development of higher levels of automation but also throughout the vehicle lifecycle. These tools and methodologies could either be built from already existing (i.e. coming from the automotive or software development domain) or creating radically new ones.
- Foster the creation of a standardised and agreed methodology for validation of automated driving functions based on a common state of the art.
- Include human factors in the whole testing and potential certification scheme especially for those levels that still require a decisive involvement of the driver. Interaction with other (automated) road users should also be observed in the process.
- Research on new (and disruptive) technologies for CAD i.e. artificial Intelligence should always take into account its verification and validation and potentially certification throughout the vehicle lifecycle (see related CARTRE theme).
- Promote standardisation initiatives for new protocols, methodologies or tools where possible, taking into account the requirements of the target element (as part of the system) under test (component, vehicle level, etc…).
- Encourage the technical R&D efforts that technically support the creation/adoption of a European level certification scheme for automation.
- Investigations on what can be tested in simulation and what should be tested on real roads (test tracks, public roads) together with guidelines to validate the simulation models.

Impact

All technical developments are useless if a proper regulatory framework is not in place. Europe's leadership in the automotive sector can be compromised if a fair, trustworthy, harmonized and complete process for safety assessment is not developed. At higher levels of automation, the current approaches do not suffice anymore.

This we consider to be critical in order to reduce the number of road fatalities and to harvest the economic and environmental benefits of automation. For this purpose, it is necessary to promote the development of a European level certification/approval scheme that fosters the development and market introduction of AD by the Industry.

A European level approach would speed up the development process and reduce the time to market of new automated functions with a higher level of safety of the deployed systems. The enhancement of the safety level of new functions through a consolidated and trustworthy verification/validation methodology would increase the user acceptance of these technologies and contribute to its market adoption.

2040 vision

As already addressed, safety validation and roadworthiness testing have a long road ahead in terms of development, both in the short and mid-term. There are a lot of challenges that need to be addressed and questions to be answered in order to keep up the pace of technological development. Nevertheless, this discussion theme envisions a future in which the following goals should be achieved:

- Harmonized regulation based on a common state of the art and flexible enough to adapt to new technologies and realities (higher penetration of automation in the mixed environment). For instance, adaptation of safety regulations to the CAD reality i.e. crashless scenario
- Common methodology which is accepted worldwide enabling multi-stakeholder cooperation

- Validation methodology which is "affordable" by all manufacturers as well as other involved stakeholders (e.g. suppliers and AV technology companies) in terms of costs and timing and guarantees safety performance at user and societal level

Conclusions from breakout sessions

During the dedicated session that took place in the 1st European Conference on Connected and Automated Driving (April 2017, Brussels), the panellists had the chance to present to the audience some of the worldwide initiatives that are trying to give an answer to theme challenges. Some conclusions can be extracted from their presentations:

- Practical cases are important to truly understand the hidden problems of the challenge (as found in the EU Truck platoon challenge)
- Information for the end user regarding its vehicles characteristics is important. The way an AD function is developed has a great impact in their performance and safety
- Some initiatives like the German PEGASUS projects are starting to tackle scenario definition and sharing
- Japan highlighted that impact assessment and roadworthiness testing should be jointly considered as a way to identify benefits and risks

Cooperation between stakeholders was also encouraged by the speakers in different ways:

- (International) harmonization of regulation and its complementarity with commercial testing
- The potential to extend scenario databases to other AD functions, components, countries and stakeholders i.e. technical centres, traffic authorities, etc..
- Stakeholder cooperation to develop cost efficient, harmonised vehicle validation including RTOs, Industry, Member States and other

Further discussion was engaged during the panel session organised within the Symposium on Research & Innovation for Connected and Automated Driving (April 2018, Vienna). A number of conclusions could be achieved:

- There are several initiatives but we need to make progress to learn how can we provide full coverage validation
- Virtual Validation needs to be validated (in terms of reliability and completeness) and accepted by regulators (more used to physical testing approaches)
- Improving procedures to obtain scenarios, however data sharing (at international level) would certainly reduce costs but there is a challenge in terms of property and local differences
- It is not just about the safety of the function, but how the driver makes use of the vehicle and the evaluation of safety in relation to other road users/elements

Also some next steps were identified as a way to speed up the validation of CAD:

- Sharing of scenarios can hugely reduce costs but technical and organisational issues need to be solved: sharing costs in the definition of critical scenarios is favoured, but the mechanisms to share the scenarios between stakeholder in a fair, privacy driven and sustainable way still needs to be defined and agreed
- Stakeholders need FOTs / Pilots to obtain relevant, real world data that supports the improvement of physical/virtual validation tools and methodologies

During this session a number of questions were asked to the audience. Through the use of an interactive tool their answers were collected:
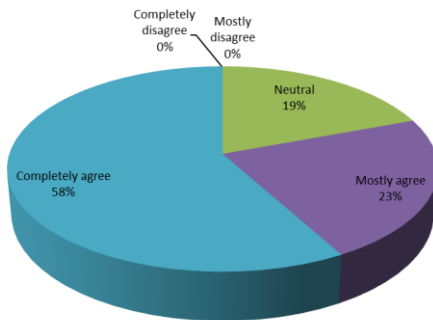
Automotive industry faces an enormous effort to realise the safety validation of AD. A coordinated approach on safety validation is needed

- Completely disagree 0%
- Mostly disagree 3%
- Neutral 5%
- Mostly agree 31%
- Completely agree 61%
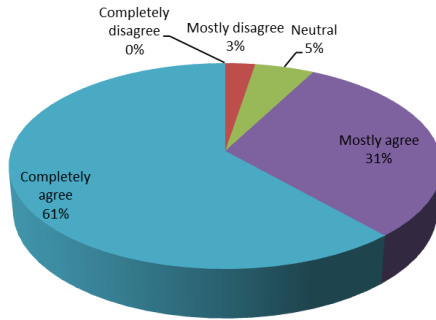
Without virtual testing, it is not possible to achieve safety validation. Virtual testing not sufficient : Testing in a real-life environment is necessary

- Completely disagree 0%
- Mostly disagree 6%
- Neutral 13%
- Mostly agree 28%
- Completely agree 53%
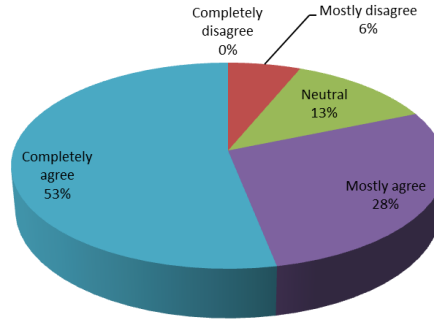
Sharing scenarios is critical for safety and cost reduction purposes

- Completely disagree 0%
- Mostly disagree 0%
- Neutral 19%
- Mostly agree 23%
- Completely agree 58%

Your test cases can never be complete. The scenarios will dynamically change with the increasing number of AD functions on the road

- Completely disagree 0%
- Mostly disagree 3%
- Neutral 27%
- Mostly agree 33%
- Completely agree 37%
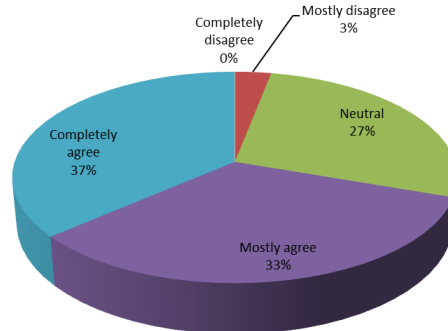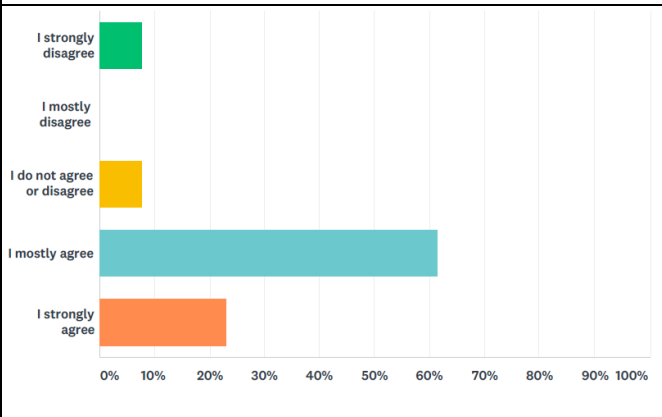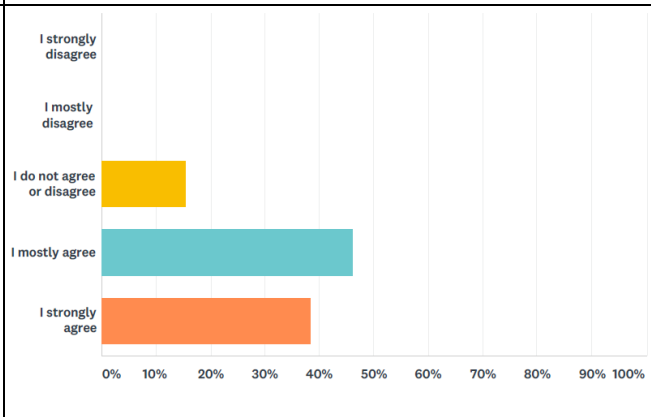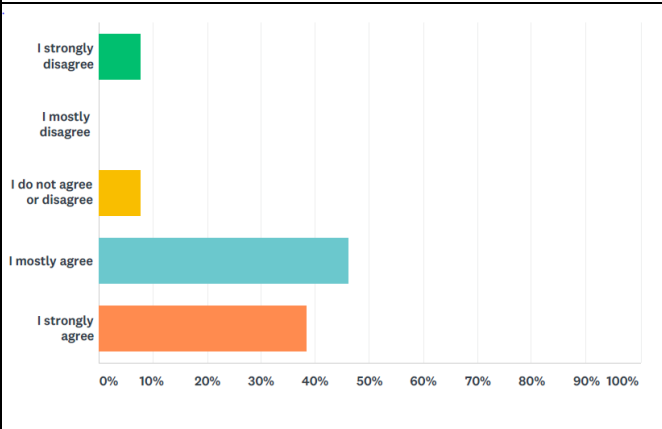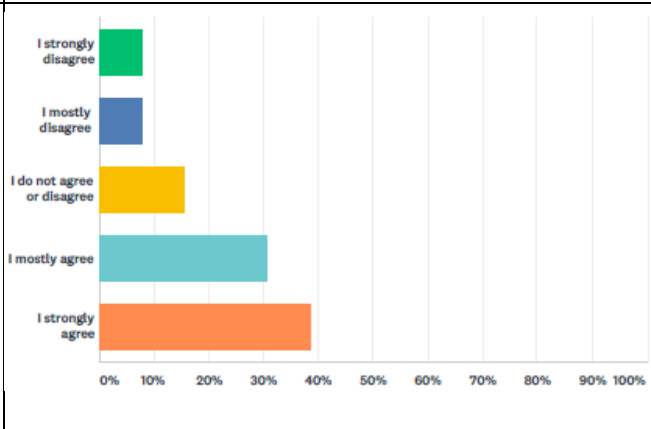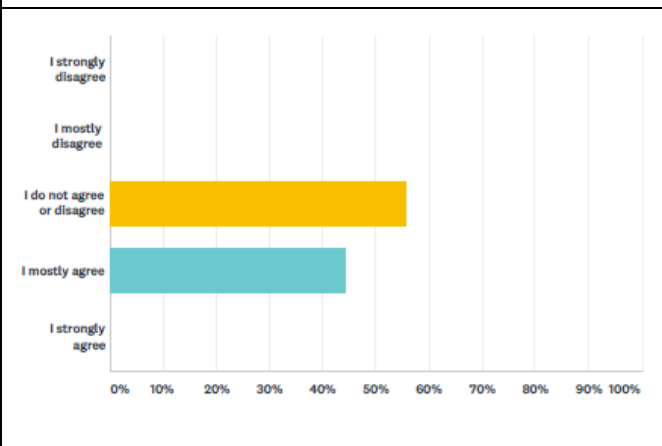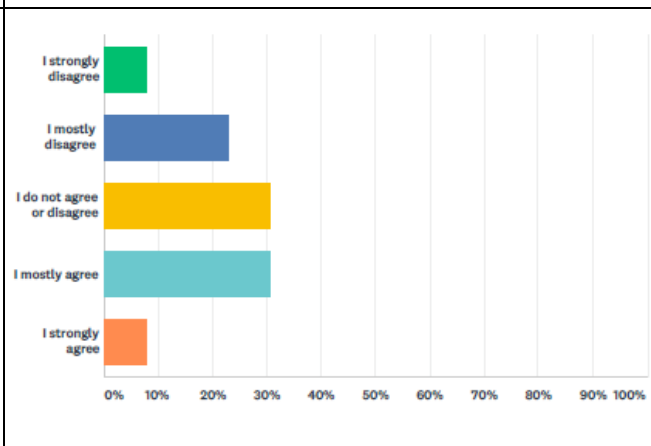
We need to define initial safety release procedures first before we can handle updates in the functionality

- Completely disagree 0%
- Mostly disagree 6%
- Neutral 22%
- Mostly agree 53%
- Completely agree 19%
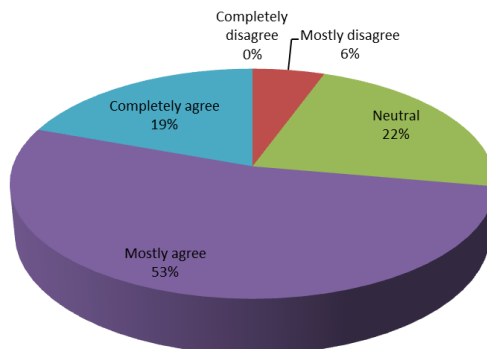
Survey on statements

The CARTRE project organised an online open survey in order to collect expert opinion on some of the statements discussed during the project. This survey allowed participants to vote their level of agreement with the proposed statements. These statements do not necessarily represent the opinion of the project but were used as a dynamizer for further discussions. The following results were achieved:

The test cases can never be complete

Automated vehicles need to deal with drivers that do whatever they want to do

A coordinated approach on safety validation is needed for global leadership

The current lack of regulation is an opportunity for development and testing of Automated Driving

Automotive industry faces an enormous effort to realise the safety validation of AD

Without virtual testing, it is not possible to achieve safety validation

Periodic re-certification is essential for automated driving functions

The scenarios will dynamically change with the increasing number of AD functions on the road

Virtual testing isn't sufficient for safety validation and roadworthiness testing. Testing in a real-life environment is absolutely necessary

A legislative framework for road safety validation and roadworthiness testing of automated vehicles must be developed

For ART, we need to define initial safety release procedures first before we can handle updates in the ART functionality

A fully automated car is not allowed to cause an accident in any situation

The periodicity of the periodical technical inspection will have to be reviewed taking into account key moments in an automated vehicle's lifecycle, such as software updates	Testing is important to generate public trust

Sharing scenarios between stakeholders is critical for safety and cost reduction purposes

Open Issues

Throughout the process of creation of this position paper, some challenges have already been identified through consensus. However, some topics were also identified and should also be tackled in the future:

- Cybersecurity: How do we introduce security in the validation process to be sure that safety is not affected?
- What (set of) scenarios have to be tested?
- What kind of software changes/updated need what kind of new testing? How do we identify that a software has been changed enough to require a new process and how this process should be?
- Impact on the scenarios as the mixed environment gets more and more automated. How do we update and with which criteria do we adapt the (commonly accepted) set of scenarios?
- What is the impact for horizontal issues i.e. ethics, security, data management, deployment, etc... associated to the validation process?

.