



HAL
open science

Safety demonstration of autonomous vehicles: a review and future research questions

Tchoya Florence Koné, Eric Bonjour, Eric Levrat, Frédérique Mayer, Stéphane
Géronimi

► To cite this version:

Tchoya Florence Koné, Eric Bonjour, Eric Levrat, Frédérique Mayer, Stéphane Géronimi. Safety demonstration of autonomous vehicles: a review and future research questions. 10th Complex Systems Design & Management, CSD&M 2019, Dec 2019, Paris, France. 10.1007/978-3-030-34843-4_15 . hal-02427540

HAL Id: hal-02427540

<https://hal.science/hal-02427540>

Submitted on 3 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Safety demonstration of Autonomous vehicles: a review and future research questions

Tchoya Florence Koné, Eric Bonjour, Eric Levrat, Frédérique Mayer, Stéphane Géronimi.

Abstract The safety demonstration and validation of Autonomous vehicles (AVs) remains a challenging activity. In this paper, we firstly review what those challenges are and how they affect the safety validation of the AV. Then, we particularly focus on the simulation-based validation process, which seems to be inevitable among the recommended safety validation approaches. We show what is actually done and required in terms of scenarios generation, their assessment taking into account uncertainty and the simulation architecture to test and validate them. Finally, we end our review by summarizing key research questions that need to be addressed to help with this safety validation issue.

1 Introduction.

An automated vehicle (AV) is a vehicle, which is able, according to the conditions of its operating environment and the level of automation, to move with or without human intervention. The Society of Automotive Engineers¹ (SAE) identifies six levels of automation: No Automation (Level 0), Driver Assistance (Level 1), Partial Automation (Level 2), Conditional Automation (Level 3), High Automation (Level 4), and Full Automation (Level 5).

For its operation, an automated vehicle collects information about its environment, processes them, plans its trajectory and decides on actions to be performed. To implement this, manufacturers use specific technologies such as sensors and localization systems, communication systems and intelligent control systems. These embedded technologies are sometimes new, difficult to specify and have functional performance limitations regarding environmental conditions. This affects standard safety validation procedures, which face new challenges and are

Tchoya Florence Koné
Université de Lorraine / Groupe PSA
tchoyaflorence.kone@mpsa.com

Eric Bonjour & Frédérique Mayer
Université de Lorraine, laboratoire ERPI, 8 rue Bastien Lepage 54000 Nancy (Fr)
eric.bonjour@univ-lorraine.fr frederique.mayer@univ-lorraine.fr

Eric Levrat
Université de Lorraine, Laboratoire CRAN, UMR CNRS 7039
Faculté des Sciences et Technologies BP 239, Vandoeuvre les Nancy 54506 (Fr)
eric.levrat@univ-lorraine.fr

Stéphane Géronimi
Groupe PSA, Vélizy A - Route de Gizy / 78140 Vélizy-Villacoublay Cedex (Fr)
stephane.geronimi@mpsa.com

now limited. In fact, the ISO 26262 standard, which has been considered since 2011 as the reference in the automotive field with regard to the guarantee of functional safety, is no longer sufficient. Also, conventional validation techniques such as validation by "miles needed to be driven", are irrelevant. Kalra & al.² showed that it would require hundreds of millions of kilometers or sometimes hundreds of billions of kilometers, to carry out validation tests by this method. In addition, formal proof based approaches are not suitable for complex systems because of the combinatorial explosion regarding proof algorithms³. Another approach is about simulation-based method. It has also been proved to be difficult because of the amount of test cases that have to be generated³. However, it remains the most promising method. This seems to be obvious given the difficulty of carrying out experiments, especially in urban areas.

In the light of all the above elements, some questions are overwhelming. How are the challenges for AVs safety validation looking like? How to ensure the safety demonstration of AVs by simulation-based method?

In this paper, we present a general review of existing works about these questions and we summarize other research questions that need to be addressed to deal with this issue.

The remainder of the paper is organized as follows:

Before exploring the safety validation with simulation, section 2 comes back in more detail to challenges in AVs safety validation. Section 3 deals with the first objective to be addressed in safety validation by simulation process: the generation of the scenarios needed for simulation. Then, section 4 is about the statistical assessment of scenarios with the consideration of uncertainty. Section 5 gives an overview about the simulation framework with regard to the safety demonstration and testing system. Section 6 summarizes the conclusion and future research questions that could be addressed to contribute in AV safety demonstration.

2 Challenges in AV safety validation.

The first difficulties related to the AVs were publicized in 2004, with the DARPA Grand Challenge, organized by the DARPA, the Defense Advanced Research Projects Agency. This is the first competition in the world involving self-driving and unmanned ground vehicles. Lessons learned⁴ at the end of the DARPA project included the development of much more powerful sensors, the impossibility of validating vehicles in a real and dynamic environment, and the maintaining of the driver in the loop to deal with unexpected scenarios.

However, the awareness of the complexity related to the validation of AVs began with the arrival of the first systems that initiated the projects of autonomous driving, namely ADAS (Advanced Driver Assistance Systems). Because of their usefulness especially for the protection of the road users, these systems quickly attracted increased interest. The importance of such utility therefore required that

Safety demonstration of AVs: a review and future research questions.

these systems be robust and reliable. However, they were based on detection systems and faced a large number, or even infinite number, of parameters that can be identified during a mission profile. Conventional methods have quickly proved to be insufficient or obsolete for their validation.

In this section, we mainly focus on the difficulties in safety validation of AVs with regard to technological issues, the presence of uncertainties and the limitation of ISO 26262 standard.

2.1 Specificities and technological issues.

AVs use specific technologies such as sensors and localization systems, communication systems and intelligent control systems (especially with self-learning AI algorithms) to achieve their mission. These are the subject of many works in order to make them successful but problems still remain.

First, manufacturers encounter geolocation and perception issues. In fact, what makes perception right and accurate is the quality of sensors. This quality depends on parameters such as sensitivity, linearity, noise, selectivity, saturation, bandwidth or geometric resolution. Sensors performance and limitations may vary according to their parameters configuration. Some sensors are more suitable to the detection of nearby objects like ultrasonic sensor and 3D camera but they have some disadvantages in rainy conditions. Long-range radar and LIDAR are appropriate to detect remote objects but with a restricted measurement angle for the radar and poor performance for the Lidar in fog and snow conditions. In addition to weather conditions, sensors are also sensitive to many other factors like sand, salt or dust. Li & al.,⁵ stated that the environment is complex and factors such as the alternation of structured and unstructured roads, heavy shadow, pavement distress, dirt, puddles, the frequent change in the appearance of a road, the curvature of roads, accentuate the challenge in road detection. All those limitations and performance variations have to be taken into account while testing AVs. The validation process has to check that AVs can detect nearby or distant objects, ensure that they will perform successfully in poor weather conditions or degraded environment configurations.

Then, trajectory planning and decision-making is another issue. The planning module has to deal with both “innate dynamic constraints and restricted planning space”⁶. Indeed, the dynamics of the environment constrains the system to make a decision within a bounded time; otherwise, the AV could be dangerous or in danger due to its passivity⁷. The ability of the system to react in a dynamic environment, face the question of ethics by making moral decisions and act quickly must be tested for the AV validation. Finally, the use of V2X communications is envisaged for the AV but this can also be the subject of various dysfunctions or threats like data interception, connection hijacking, jamming of transmissions, and denials of service and therefore needs to be considered in the validation.

2.2 Difficulty in compensating for the presence of uncertainties.

The main characteristic of the behavior of autonomous systems is related to the treatment of the uncertainty with which they are confronted.⁸ Uncertainty can be classified in different categories: (1) epistemic uncertainty related to the lack of knowledge about the environment, (2) uncertainty of sensor measurements, (3) interpretation uncertainties generated by sensor fusion algorithms and associating levels of confidence with different objects, (4) decision-making uncertainties concerning the various arbitrations possibly contradictory among which the system must decide; for "sensitive" scenarios, and (5) uncertainties related to the dynamics of evolution of the system and the environment.

Uncertainty prevents designers from defining test cases with precision and completeness. It therefore appears that, to demonstrate the safety of AVs, a more effective strategy has to be defined taking into account these different categories of uncertainty.

2.3 Limitation of the ISO 26262 standard.

ISO 26262 deals with the safety of a vehicle in terms of the absence of unreasonable risk due to a malfunction of electrical and electronic systems. However, in the case of AVs, it does not take into account safety breaches, in the absence of default, caused by the performance limitations, of decision-making components³.

This standard provides a V-cycle safe development and test process, which is difficult to apply to the development of safe autonomous vehicles⁹. According to Koopman & al., this process is now facing five major challenges. The first one is the absence of the driver in the decision-making loop. Indeed, in a traditional engineering approach (of a vehicle with driver), the manufacturer does not care much about the deviations in the behavior of road users (other vehicles, pedestrians, etc.) that the vehicle can meet on the road or the environment in general. The manufacturer transfers this responsibility to the driver. This is no more possible with AVs. The other challenges are about the complexity of the requirements, the presence of non-deterministic algorithms, inductive learning algorithms and fail-operational systems, which are not in the scope of this standard. In addition, the validation of the self-adaptive behavior of AVs makes it impossible to predict all situations in the design process¹⁰.

Therefore, manufacturers can no longer limit their safety analysis to this standard and have to think about new certification approaches. Work is underway to fill this need. One of them is the development of the Safety Of The Intended Functionality (SOTIF) standard. It is a reference that aims at providing a complement to the ISO 26262 by focusing on the safety of the functional performance of systems. It targets specific characteristics such as sensing and processing of complex algorithms, whose dysfunctions may be due to performance limitations of desired

Safety demonstration of AVs: a review and future research questions.

functions. The actual edition of the future reference is mainly dedicated to emergency intervention systems (e.g. emergency braking systems) and Advanced Driver Assistance Systems (ADAS), but can be considered for higher levels of automation with additional measures. The purpose of SOTIF's activities is to reduce the known dangerous scenarios and show that the residual risk due to unknown potentially dangerous scenarios is acceptable. However, the combinatorial explosion of potentially chaotic situations makes the completeness of physical tests difficult to conceive in an experimental way². It becomes necessary to explore the universe of critical situations with other strategies, and in particular by simulation.

3 Scenarios generation for simulation-based validation.

Simulation appears to be a promising way to address the impossibility of carrying out only road and track tests for the validation of AVs. In this section, we review the activities performed in the context of the validation of AVs by simulation: the scenarios identification in industrial domain, the concepts definition and their modeling, and the scenarios generation.

3.1 Scenarios identification in the industrial domain

Work is going on to determine the relevant scenarios needed for the validation of autonomous vehicles.

The first identification strategy concerns the use of experience. The main goal of this approach is to use previous experiences based on prior driving functions like ADAS systems or manual driving systems to identify a first list of scenarios that manufacturers qualify to be relevant. Returns from drivers can be used to complete this list; they are suitable to inform the manufacturers about events or misuses they observed during driving. In the same way, accident databases are helpful for identifying critical situations that may be a challenge for AV.

As not all scenarios can be derived from previous experiences due to the complexity of the AV, others strategies have to be used. One strategy is to use specific driving to collect information and target specific scenarios. Another one, refers to the knowledge of the experts about the technologies implemented on the AV. It should also be noted that governments are busy revising regulations, defining the procedures to be followed by manufacturers to validate and deploy their AVs, and identifying some scenarios that need to be tested by manufacturers. Added to previous approaches, due to the difficulties in validating AVs, all the actors around the AV (customers and suppliers) join together in working group to share knowledge and define common generic scenarios.

3.2 Concepts definition and their modeling.

In order to handle the identification and generation of the scenarios for AVs validation, manufacturers have to clearly define what a scenario is and what it is made up of.

From combinatorial approaches¹¹ to ontology-based approaches^{12, 13, 14}, through the concept of maneuvers^{15, 16} methods are multiplying to bring answers.

Concepts that mostly appear in the context of these works are scene, situation, event and scenarios. Authors generally adopt definitions that are consistent with their generation approach or they propose new ones according to their own vision. To make sure that definitions are common to all, work is going on to set up a consensus on all these concepts used for scenario generation. Authors¹⁷ reviewed existing definitions^{18, 14} of the terms “scene, situation and scenario” and suggested new ones for each of them in the context of Autonomous vehicle. The definitions proposed by Ulbrich & al., have been considered as reference in the primarily version of the Safety of The Intended Functionality (SOTIF). However, they are still subject to discussion.

3.3 Scenario generation

AVs will face a multiplicity of real situations due to the variations of environmental conditions related to traffic conditions, weather, infrastructure, or other road users' behaviors. Since it is difficult to predict all these situations, manufacturers have to identify new ways to approach and master the scenario generation process. To do that, different solutions have been proposed in the literature. The first one consists in addressing the AV deployment by level of automation. In this way, the vehicle is limited to a number of tactical maneuvers and can perform its mission in an identified area called ODD (Operational Design Domain). The ODD describes the specific operating domain in which the system is designed to function properly. Therefore, scenarios to be generated are limited to this ODD and the generation space can be mastered. In the same logic, another approach is the identification of AVs use cases. Since there may be many use cases for AVs, authors generally choose those they consider relevant or consistent with their purpose^{19, 20}. Thus, these use cases are studied carefully to generate the scenarios necessary for their evaluation. In addition, some authors propose to focus on special situations : highway situations, intersections situations²¹, vulnerable users²². Other approaches are based on the possible maneuvering of the vehicles to create dynamics between scenarios and imagine future scenarios¹⁶. The last identified method is about the prioritization of the scenarios. Menzel & al.²³, proposed a classification for scenarios in three levels of abstraction that can be converted into each other: functional, logical and concrete scenario. The

functional scenario describes all the entities and their relations in a linguistic scenario notation understandable by human. The second one, logical scenario; uses the functional scenario to describe it on a state space level with the help of parameter ranges. Finally, concrete scenario permit to add concrete values to precedent parameters defined in logical scenarios.

The proposed approaches have proved their necessity. However, they do not give means to ensure the completeness of situations that the vehicle will encounter. Therefore, manufacturers need a complete generation strategy, which includes this estimation or which offers the possibility of extrapolating the generation to scenarios that one would not have thought of.

4 Quantification of uncertainty - probabilistic evaluation of scenarios and their coverage.

There are exiting methods to address uncertainties ²⁴: probability theory; fuzzy set or possibility theory and evidence theory.

Some have been applied into the design by improving the AV capabilities according to categories of uncertainties they may face. In fact, D. Althoff & al., ²⁵ presented a method for the safety assessment of trajectories. In the proposed method, the future trajectories are represented as directed graphs and the uncertain states of the obstacles are represented by probability distributions. The safety assessment of the trajectories result in determining their collision probability in dynamic and uncertain environment. Another application is a system design for preventive traffic safety in intersection situations²¹: “it exploits the developed overall probabilistic framework for modeling and analysis of intersection situations under uncertainties in the scene, in measured data or in communicated information.” The intersection situations involve all traffic participants. In their work, Laugier & al., ²⁶, aim at assessing risk of collision for the ego-vehicle. They used a probabilistic approach for the analysis of dynamic scenes and collision risk assessment. The approach takes into account the uncertainties in modelling the environment, detecting and tracking dynamic objects. The last example²⁷ deals with a situational assessment method to improve the decision-making of Intelligent alternative-energy vehicles (IAVs). The method takes into account the risks of uncertainty in a dynamic traffic environment and the risks assessment is done within and beyond the prediction horizon. It is based on a stochastic model of the environment, an estimation of the collision probability based on trajectory prediction, and the collision probability for the planned maneuvers and trajectories. Risk is finally assessed by taking into account the collision time, the mass of vehicles, as well as the relative velocity.

One of the identified methods,²⁸ addresses the consideration of the uncertainty during the overall safety verification of the system. M. Althoff proposes to use the reachability analysis technique for the safety verification of dynamical systems. It consists, for a set of initial states and parameters, in calculating the exact or

Safety demonstration of AVs: a review and future research questions.

approximate set of states that can be reached by a system. If the achievable set does not interfere with any set of dangerous states, the safety of the system is guaranteed. To apply it to the safety of AV, he extends the concept to stochastic analysis "stochastic reachability analysis" which will measure the probability of reaching a set of dangerous states. To do this, he use some methods including Markov chains, which approximately computes the stochastic reachable set of arbitrary dynamics.

All these methods, by taking into account uncertainty, help with the safety improvement of the capabilities or performance of the systems under development. However, we can barely find some methods which tackle the way of quantifying uncertainties related to scenarios execution during AV safety validation. AV and its operating environment are subjects to uncertainties, and these uncertainties must be evaluated and quantified because they influence the confidence people will have in the validation strategy.

5 Simulation framework.

The simulation framework is based on two dimensions: the specification of the validation system and its architecture.

5.1 Specification of an AV safety demonstration and testing system.

The required system to test and validate the safety of AVs must be able to deal with specific aspects. In the simulation-based toolchain proposed by Hallerbah & al.,²⁹ the safety issue is addressed by the identification of critical scenarios based on a set of metrics that depends on traffic or safety related requirements. Another procedure may be integrated in the test system to manage safety critical scenarios like the scenario-based risk analysis proposed by Galizia & al.³⁰ Then, about modules to be integrated, Sun & al.³¹ presented a system to test and evaluate the behavior of Unmanned ground vehicles that first includes the test content design, which is modular and designed stage by stage with a level of complexity that is progressive. The system also contains a hierarchical test environment design developed according to the levels of the test content design, the test methods and the evaluation method. In addition, to carry out the testing framework and the test procedure, manufacturers may need to define some guiding principles like the isolation of testing variables, the characterization of the test environment for test repeatability.³² Other aspects may be incorporated like taking into account uncertainty and the overall evaluation of the level of confidence to attribute to the AV in correlation to its future acceptance.

5.2 Simulation architecture for safety validation

In the automotive engineering literature, architectures have been proposed to tackle the verification and validation of Autonomous systems.

First, Sarmiento & al.,³³ propose an automated method for generating scenarios. The method starts by the use of RNL (Restricted-form of Natural Language) for the description of the scenarios, and then deduces some Petri-Net models that are used as input to generate the scenarios. It includes a scenarios verification module, a method of model transformation (defined as mapping rules) and criteria for browsing the reachability tree of Petri-Nets to generate scenarios.

Then, Mullins & al.,³⁴ developed a testing method of autonomous vehicles, which deals with the issues of the dimensionality of the configuration space and the computational expense of high-fidelity simulations. The method is focused on finding performance boundaries of the system to generate challenging scenarios. It combines the adaptive sampling algorithm with a software-in-the-loop simulation to generate test scenarios. The resulting tool is called RATP (Range Adversarial Planning Tool). Scenarios are clustering according to their similar behaviors using performance type and then boundary sets of these clusters are identified. This helps test engineers with the evaluation of the « trending behaviors of the system »

Another test framework for automated driving systems is also proposed by the Department of Transportation,³². The proposed test framework targets both Black-box and White-box testing and each of the core scenario components can be used for both of them. The structure of the test procedures includes aspects such as test subject and purpose, test personnel, facilities, and equipment, test scenario (Input, Initial conditions, Execution, Data measurement and metrics). Guiding principles are defined to carry out the testing framework and the test procedure. Tactical maneuver behaviors, Operational Design Domain (ODD) elements, object and event detection and response (OEDR) capabilities and Failure mode behaviors are identified as the main components of a scenario. In complement to simulation architecture, track testing and open-road testing architectures have been proposed.

Finally, Hallerbach & al.²⁹ propose a simulation-based toolchain for the identification of critical scenarios which consist of a model in the loop testing procedure. The simulation environment includes a vehicle dynamics simulation, a traffic simulation and a cooperation simulation. Newly developed traffic metrics are used in combination with standard safety metrics to determine the criticality of scenarios. The authors defined “critical scenarios as scenarios that need to be tested, regardless, whether the requirements are functional or non-functional.” Questions addressed by the simulation-based toolchain are: the typology of scenarios that have to be tested according to the vehicle development process, the functional and non-functional requirements needed for the evaluation, the consistency of the test with the test environment, the advantages and constraints of a specific test environment. Concrete scenarios are created thanks to a parameter variation module applied to the parameters of logical scenarios. Then tailored metrics are used to classify those concrete scenarios into critical or not critical.

Safety demonstration of AVs: a review and future research questions.

Overall, these architectures provide ways to describe, formalize and generate scenarios, and deal with the identification of challenging or critical scenarios and their classification. They also discuss the test structure and the test process. However, none of them gives an estimate of the uncertainty associated with the generated scenarios. They also do not give the final level of confidence of the AVs based on the simulated scenarios.

6 Conclusion and future research questions.

This paper reviewed the question of AV safety validation. First, we identified the difficulties related to the validation process. Then, we focused on the activities related to the simulation-based validation method.

Whereas this review can help manufactures to identify the challenges faced by the AVs validation and the necessary activities to process this validation by simulation means, it also produces several research questions that need to be investigated in future work:

- Are the concepts retained by the consortium and their definitions suitable to be applied directly to simulation scenarios generation?
- Does the validation process take into account the limitations and variations of the performance of the system properly?
- How to quantify uncertainty related to scenarios execution and correlate this quantification to the confidence manufacturers can attribute to AVs at the end of the validation process?
- Does the identified and selected scenarios be sufficient to test and validate the AVs? Which road tests have to be planned to complete the validation?
- How to set up a simulation architecture able, on the one hand, to handle the generation of scenarios taking into account the uncertainty and, on the other hand, to manage the AV safety validation by evaluating, based on the simulated scenarios, the AV safety level?

These questions showed that a lot of work is yet to be done in the AV safety validation activity. However, this review does not intend to be exhaustive. Other issues are, for instance, the resistance of AVs against communication attacks, the safety demonstration of AI algorithms, ethical aspects of AV decision-making, the acceptance of AVs by the populations and the reengagement of the driver when there is a failure to hedge the system-level safety for AVs¹⁰.

Authors' position

Although, many ADAS/AD are already in the street, it must be mentioned that, we still have the driver in the loop to ensure the controllability of the vehicle in critical situations. High or fully AV, which are currently deployed, have someone in the vehicle to take back control in case of performance limitation and are

Safety demonstration of AVs: a review and future research questions.

mainly dedicated to the procedure of tests (Open road testing, Track testing); therefore they cannot be placed on the market as long as the safety and regulation issues are not solved.

The current challenges for AVs validation are due to the mixed environment, in which they will evolve. The AV will have to deal with the deviations in the behavior of road users (other vehicles, pedestrians, etc.) that it can meet on the road or the environment in general.

The classification of the SAE about the six levels of automation is a response to deal with the complexity of the environment, as it means that, the deployment of the AV has to be done by defined Operational Design Domain (ODD). This shows that we are aware that the AV will face some situations, in which it could not be able to react, and for which there still be a risk of loss of controllability of the vehicle. This classification also means that, the more we advance in levels of automation, the less the human driver gets involved in the driving task. In other words, the importance of the driving responsibility is now affected to the AV, which is now the guarantor of the vehicle control. Therefore, before reaching one hundred percent of penetration rate for fully AV, the driver will still be the best resort to ensure controllability of the vehicle.

So, we believe that the less we will have non-automated vehicles, the less the risk due to their behavioral deviations will be. This may be possible if the penetration rate of fully and safe AV is accelerated. But, due to the difficulties we identified in this review, this is currently not possible.

Acknowledgment

This work has been carried out under the financial support of the French National Association of Research and Technology (ANRT in French – convention CIFRE N° 2017/1246) as well as Groupe PSA.

References

1. NHTSA. NHTSA. <https://www.nhtsa.gov/technology-innovation/automated-vehicles#issue-road-self-driving>.
2. Kalra N, Paddock SM. Driving to Safety. *RAND Corp - www.rand.org*. 2014. doi:10.7249/RR1478
3. Raffaëlli L, Vallée F, Fayolle G, et al. Facing ADAS validation complexity with usage oriented testing. In: *ERTS*. ; 2016. <http://arxiv.org/abs/1607.07849>.
4. Alexander L, Allen S, Bindoff NL. *Handbook of Intelligent Vehicles*. Vol 1.; 2013. doi:10.1017/CBO9781107415324.004
5. Li Q, Chen L, Li M, Shaw SL, Nüchter A. A sensor-fusion drivable-region and lane-detection system for autonomous vehicle navigation in challenging road scenarios. *IEEE Trans Veh Technol*. 2014;63(2):540-555.

Safety demonstration of AVs: a review and future research questions.

- doi:10.1109/TVT.2013.2281199
6. Liu W, Weng Z, Chong Z, et al. Autonomous vehicle planning system design under perception limitation in pedestrian environment. In: *CIS-RAM.* ; 2015:159-166. doi:10.1109/ICIS.2015.7274566
 7. Petti S, Bank EI, Fraichard T. Safe Motion Planning in Dynamic Environments. 2014;(September 2005). doi:10.1109/IROS.2005.1545549
 8. Zhao L, Arbaretier E, Tlig M, et al. Validations par Virtualisation et Simulation : de nouveaux champs méthodologiques et techniques pour une ingénierie de conception sûre des systèmes autonomes. 2019.
 9. Koopman P, Wagner M. Challenges in Autonomous Vehicle Testing and Validation. *SAE Int J Transp Saf.* 2016;4(1):2016-01-0128. doi:10.4271/2016-01-0128
 10. Koopman P, Wagner M. Autonomous Vehicle Safety: An Interdisciplinary Challenge. *IEEE Intell Transp Syst Mag.* 2017;9(1):90-96. doi:10.1109/MITS.2016.2583491
 11. Duan J, Gao F, He Y. Test scenario design for intelligent driving system. 2018;(August). doi:10.1007/s12239
 12. Geng X, Liang H, Yu B, Zhao P, He L, Huang R. A Scenario-Adaptive Driving Behavior Prediction Approach to Urban Autonomous Driving. *Appl Sci.* 2017;7(4):426. doi:10.3390/app7040426
 13. Bagschik G, Menzel T, Maurer M. Ontology based Scene Creation for the Development of Automated Vehicles. 2017. <http://arxiv.org/abs/1704.01006>.
 14. Geyer S, Kienle M, Franz B, et al. Concept and development of a unified ontology for generating test and use-case catalogues for assisted and automated vehicle guidance. *IET Intell Transp Syst.* 2013;8(3):183-189. doi:10.1049/iet-its.2012.0188
 15. Bach J, Otten S, Sax E. Model based scenario specification for development and test of automated driving functions. *IEEE Intell Veh Symp Proc.* 2016;2016-Augus(Iv):1149-1155. doi:10.1109/IVS.2016.7535534
 16. Zhou J, Re L. Reduced Complexity Safety Testing for ADAS & ADF. In: *IFAC-PapersOnLine.* Vol 50. Elsevier B.V.; 2017:5985-5990. doi:10.1016/j.ifacol.2017.08.1261
 17. Ulbrich S, Menzel T, Reschka A, Schuldt F, Maurer M. Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving. In: *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC.* ; 2015. doi:10.1109/ITSC.2015.164
 18. Dickmanns ED. *Dynamic Vision for Perception and Control of Motion.*; 2007. doi:10.1007/978-1-84628-638-4
 19. Wachenfeld W, Winner H, Gerdes JC, et al. Use Cases for Autonomous Driving. *Auton Driv Tech Leg Soc Asp.* 2016:519-521. doi:10.1007/978-3-662-48847-8
 20. Wilbrink M (DLR), Schieben A (DLR), Markowski R (DLR), et al. Designing cooperative interaction of automated vehicles with other road users in mixed traffic environments. Definition of interACT use cases and scenarios. 2017;(1):0-73.
 21. Weidl G, Breuel G. Overall Probabilistic Framework for Modeling and Analysis of Intersection Situations. *Networked Veh.* 2012. https://link-springer-com.bases-doc.univ-lorraine.fr/content/pdf/10.1007%2F978-3-642-29673-4_24.pdf. Accessed October 18, 2017.
 22. Merdrignac P. Système coopératif de perception et de communication pour la protection des usagers vulnérables. 2015.
 23. Menzel T, Bagschik G, Maurer M. Scenarios for Development, Test and Validation of Automated Vehicles. 2018. <http://arxiv.org/abs/1801.08598>.

Safety demonstration of AVs: a review and future research questions.

24. Lopez I, Sarigul-Klijn N. A review of uncertainty in flight vehicle structural damage monitoring, diagnosis and control: Challenges and opportunities. *Prog Aerosp Sci.* 2010;46(7):247-273. doi:10.1016/j.paerosci.2010.03.003
25. Althoff D, Weber B, Wollherr D, Buss M. Closed-loop safety assessment of uncertain roadmaps. *Auton Robots.* 2016;40(2):267-289. doi:10.1007/s10514-015-9452-1
26. Laugier C, Paromtchik I, Perrollaz M, et al. Probabilistic analysis of dynamic scenes and collision risks assessment to improve driving safety. *IEEE Intell Transp Syst Mag.* 2011;3. doi:10.1109/MITS.2011.942779
27. Xie G, Zhang X, Gao H, Qian L, Wang J, Ozguner U. Situational Assessments Based on Uncertainty-Risk Awareness in Complex Traffic Scenarios. *Sustainability.* 2017;9(9):1582. doi:10.3390/su9091582
28. Althoff M. Reachability Analysis and its Application to the Safety Assessment of Autonomous Cars. 2010. doi:10.1017/CBO9781107415324.004
29. Hallerbach S, Xia Y, Eberle U, Koester F. Simulation-based Identification of Critical Scenarios for Cooperative and Automated Vehicles. 2018:1-12. doi:10.4271/2018-01-1066
30. Galizia A De, Bracquemond A, Arbaretier E. A scenario-based risk analysis oriented to manage safety critical situations in autonomous driving. 2018:1357-1362.
31. Sun Y, Yang H, Meng F. Research on an Intelligent Behavior Evaluation System for Unmanned Ground Vehicles. 2018:1-23. doi:10.3390/en11071764
32. DOT- Department of Transportation. A Framework for Automated Driving System Testable Cases and Scenarios. 2018;(September).
33. Sarmiento E, Leite JCSP, Almentero E, Sotomayor Alzamora G. Test Scenario Generation from Natural Language Requirements Descriptions based on Petri-Nets. *Electron Notes Theor Comput Sci.* 2016;329:123-148. doi:10.1016/j.entcs.2016.12.008
34. Mullins GE, Stankiewicz PG, Hawthorne RC, Gupta SK. Adaptive generation of challenging scenarios for testing and evaluation of autonomous vehicles. *J Syst Softw.* 2018;137:197-215. doi:10.1016/j.jss.2017.10.031

Safety demonstration of AVs: a review and future research questions.

Appendix: Typology of contents

Table 1: Classification of papers wrt the AV engineering aspect they addressed

Perception module	Planning/Decision module	The automated vehicle safety assessment/validation	Challenges in AV safety demonstration	Uncertainty and risk assessments	Other systems
5	6, 7, 25, 27	2, 4, 8, 16, 28, 30, 32	9, 10	21, 24, 25, 26, 27, 28, 29, 30	7, 11, 24, 25, 27, 31

Table 2: Classification of papers wrt to the addressed AV solution (The level of automation)

ADAS L1 (Driver Assistance), ADAS L2 (Partial Automation)	L3 ADS (Conditional Automation), L4 ADS (High Automation)	L5 ADS: Fully automation
3, 11, 16, 26	16, 30	2, 4, 5, 6, 8, 9, 16, 28

Table 3: Classification of papers wrt the addressed safety demonstration method

Open road testing	Track testing	Simulation-based method
2	4	3, 8, 29, 33, 34

Table 4: Classification of papers wrt the addressed scenarios modelling approaches

Concepts definitions	Ontology-based method	Concepts of maneuvers	Use cases definitions	Combinatorial test
14, 17, 23	12, 13, 14	15, 16	19, 20	11