

Validation and Verification of Automated Road Vehicles

Venkatesh Agaram, Frank Barickman, Felix Fahrenkrog, Edward Griffor, Ibro Muharemovic, Huei Peng, Jeremy Salinger, Steven Shladover, and William Shogren

PTC Inc. vagaram@ptc.com, NHTSA frank.barickman@dot.gov, Institut für Kraftfahrzeuge (ika) fahrenkrog@ika.rwth-aachen.de, NIST edward.griffor@nist.gov, Continental ibro.muharemovic@continental-corporation.com, MTC hpeng@umich.edu, General Motors Jeremy.salinger@gm.com, CA PATH sess@berkeley.edu, Harman William.shogren@harman.com

Abstract

Ubiquitous, commercial deployment of automated road vehicles is desirable in order to realize their potential benefits such as crash avoidance, congestion mitigation, reduced environment impact, reduced driver stress, and increased driver productivity. A rigorous application of systems engineering, which includes validation and verification as crucial elements of assurance, is needed for the design and development of automated road vehicles. We discuss, without implying any form of joint recommendation, several areas of relevance to a common understanding of validation and verification of automated vehicles, namely customer expectations for vehicle response, industry standards for terms and definitions, industry standards for how measurement should be done, deeper knowledge of driving behavior today to serve as a reference, and standardized processes that encompass minimum performance requirements.

1 Introduction

The growth of sensors, actuators, and computational power in automobiles is facilitating the development of automated road vehicles but several crucial elements such as the customers' expectations, the road and traffic scenarios to be negotiated by the vehicles, the validation of customers' expectations, the verification of the functional and non-functional requirements, as well as the certification of the vehicles as roadworthy over their life, are still evolving. The validation and verification of automated road vehicles is not currently governed by standards or regulation although the National Highway Traffic Safety Administration

(NHTSA) is actively working on the development of test protocols for lower levels of automation.

Systems engineering of road vehicles that fully or partially depend on the system performance for monitoring and assessing the hazards in the driving environment, for motion control such as steering, acceleration and deceleration, and for fallback dynamic driving tasks, is complex, from the technology integration perspective as well as from the perspective of dependable operation in complex road and traffic conditions. The uncertain road and traffic conditions make it very difficult to accurately identify the complex design envelopes of the automated vehicles. This in turn, necessitates incorporation and integration of a large number of disparate technologies whose robustness in complex road scenarios is difficult to ensure over the life of the vehicles. Neither regulation nor comprehensive standards are available for such complex systems but a rigorous system engineering discipline must nevertheless be exercised to design for and deliver high performance and dependability.

Adherence to systems engineering discipline relies heavily on requirements validation, as well as on verification of functional specifications derived from those requirements. The identification of requirements however needs a good understanding of the full range of road and traffic scenarios in which the automated vehicles would operate. Some considerations would be highway driving in presence of conventional vehicles and vehicles with varying degrees of automation, versus driving in ambiguous conditions that exist on local roads with pedestrians, bicyclists, and often unclear signs and signals. The scenarios could be so diverse and complicated that lengthy learning programs would have to be established in order to conceive, tune, and refine practicable control algorithms for a commercially viable vehicle.

There is much unknown about customers' expectations, the set of road and traffic scenarios which are of relevance to automated vehicles, the tests that can represent the relevant scenarios, and the range of performance acceptable to different customer segments. It is not clear at which level of testing and tuning a prototype vehicle will be considered dependable or trustworthy enough for commercialization. In addition, it is unclear whether the automated vehicles will be accepted by the public as safe to use in daily life. Currently, individual carmakers, suppliers, and other companies are developing automated vehicles based on their understanding of what might be needed by tomorrow's customers. In the absence of performance standards, companies pursue their own methods of collecting data pertaining to the scenarios that they believe the automated vehicles would experience.

The authors of this chapter, who represent an automotive OEM, two automotive suppliers, a standards organization, three research organizations, and a regulatory body, have presented their views about validation and verification of

automated road vehicles in an effort to achieve a common understanding and terminology that could facilitate communication about the challenges across the automotive and information technology industries, in order to make it easier to design, develop, and deploy automated vehicles.

2 The Validation and Verification Challenge

Historically, validation and verification has been done for vehicles that are much less complex than the automated road vehicles being developed today. Automated road vehicles need to be evaluated against human driving abilities, which is a much more difficult proposition. The main reason for this difficulty is that we don't fully understand how humans, in negotiating complex road and traffic scenarios, interact with conventional non-automated vehicles, and we cannot anticipate how humans will adapt, in the future, to different levels of automated vehicles. The question is "How can we achieve confidence that automated road vehicles will provide the desired value in both safety and travel convenience/utility"? Additionally, there are many "flavors" of automated driving systems, which include many unique aspects, each requiring extensive testing based on simulation, test track, and/or on-road evaluations. Moreover the simulations will have to include the entire vehicle system, representative operating scenarios and representative human response. Essentially, two types of guidelines have been created to help build confidence in active safety products, namely, those which focus on the processes used for development and testing, and those which focus on objective tests at all levels for each feature

Due to the fact that automated vehicles will have capabilities which are a significant departure from today's production vehicles, it is necessary to create social norms for the response of such vehicles, i.e., common expectations for how automated vehicles maneuver and interact with others in their vicinity, as well as, consistent terminology for roadway and environmental conditions, test conditions, and performance metrics. These norms might be established through cross-industry precompetitive cooperation in relevant technical work groups. They could then be used to guide performance testing for behavior, sensor interference, and security.

Different levels of automated vehicles find themselves at different experimental stages of development. Considering the evolutionary development of automated driving, the fundamental knowledge of sensing reliability, performance and safety is improving. However, as different active safety technologies are combined and automated driving features are developed, the learning curve increases exponentially. Consequently, redundancies and fallbacks are often architecturally developed based on that learning. Currently, a significant amount of time is in-

vested in developing not only novel methods but also self-learning algorithms for testing the automated driving functions that are necessary to deliver safe, reliable, secure and robust self-driving vehicles. Consequently, as the level of automation increases, considerations of system failures need to include those functions that can be transferred to the driver (“fail silently”) and those that cannot be transferred to the driver (“fail operationally”).

Validation and verification of automated road vehicles is bounded by four main areas: (i) the human-machine interface which governs how the vehicle and the driver interact, (ii) the customer-satisfaction which covers how comfortable the driver feels, (iii) the cybersecurity of the invariably connected automated vehicles, and finally, (iv) the operating environment which is made up of an extremely large number of driving scenarios. Also, considering the paucity of experiential data, the robustness of automated vehicle designs of higher levels of automation can be improved by collecting the performance data from semi-automated vehicles after deployment, in order to identify “rare events” and hidden risks. This knowledge can potentially be shared across the industry on a precompetitive basis, to facilitate more capable and safe vehicles sooner.

Vehicle regulators like the NHTSA aim to implement testing protocols that ensure minimum performance in automated road vehicles. The NHTSA is surrogate for a vehicle owner/occupant and other road users. Its objective is to regulate testing to validate the minimum level of safety that the automated road vehicles must provide. In this regard, the safety principles proposed by the Crash Avoidance Metrics Partnership (CAMP) [1-3] could be a viable starting point for the development of validation and verification of automated road vehicles, beginning with objectively determining the level of automation of the vehicle.

The NHTSA has been developing protocols for testing lower level automation functions like park-assist and has been working towards developing a systematic way of applying that methodology to higher levels of automation. Safety test protocols need to cover the reliable functioning of sensors, the ease of understanding of the human interfaces, and demonstrate that the safety risk is acceptable. The main complexity today resides in different automated vehicle systems designed with different interfaces, control systems, and functioning paradigms which can be very confusing.

Validation and verification of automated road vehicles faces significant challenges today due to the variation in how different systems respond to similar situations, sometimes conflicting with the expectations of either their drivers or the drivers of other vehicles. Also, the communication with the drivers via chimes, cluster indications, etc., needs to be “implicit” and be able to address the dependencies between overlapping information [4]. Further, the automated functions cannot be tested for all operating scenarios, but must be expected to perform within safety guidelines in all scenarios.

Most of the automation approaches use localization (understanding of the vehicle state relative to its surroundings) achieved through onboard systems because the integrity of the off-board data may be lacking. Though localization is critical to situational response, it cannot be tested for all possible situations.

Finally, automation below level 3 will require a model of the driver as part of the “situation” and that also needs incorporation into testing considerations.

In terms of regulation of automated road vehicles, one of the challenges is striking a balance between public safety and encouragement of innovation when technical standards do not exist. At the level of the states in the USA, manual driving is regulated through registration and driver licensing. Should this model be extended to automated road vehicles, then that could form the basis for validation and verification, keeping in perspective that it needs to be achieved at an affordable price and in an unambiguous way. One could apply functional safety principles manifested in ISO26262 as guidelines for developing dependable automated vehicles. However, that standard would have to be augmented with a pass / fail criterion to be useful in a regulatory framework, which in turn would need considerable research and data. Also, some have suggested that results of the validation tests should be reportable to interested members of general public to enhance public confidence in the safety of the systems, but this needs to be traded off against protection of developers’ intellectual property. Finally, third party safety process review or safety design review can also be used to enhance public confidence but it adds undue expense and has significant IP issues.

The definition of validation [5] is – “The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves evaluating acceptance and suitability with external customers.” The definition of verification [5] is – “The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process.” Verification is part of the technical assessment (checking requirements) – methodology for impact analysis of automated driving applications in the European research project AdaptIVe. Validation is part of safety and environmental impact assessment as well as the user-related, in-traffic and technical assessment.

The automated driving functions can be classified based on the time of operation into – (i) Event based – function that operates for a short period of time (typically vehicle stands still at the end, i.e., the automated driving ends), and (ii) Continuously operating – function that operates for a longer period of time (typically vehicle is still moving at the end of a maneuver, i.e., automated driving continues). Different evaluation approaches for event-based and continuously operating function can be foreseen. Independent of the chosen approach the main evaluation criteria for AdaptIVe are that the automated driving systems need to

operate within the range of normal driving behavior (i.e., not disturb normal driving in mixed traffic) and should at least be as safe as non-automated driving.

The impact assessment of automated driving applications is constrained due to – (i) today’s accident data not including collision of automated vehicles, (ii) accident reconstruction rendered more difficult to automated vehicle function, and (iii) the not-yet-understood complex interaction between automated and non-automated vehicles.

Safety impact assessment can be a three step approach based on (i) identification of relevant scenarios, focused on crashes and other (relevant) driving situations, (ii) investigation of relevant scenarios in detail similar to scenario reconstruction approach, and (iii) identification of new scenarios such as transition of control or minimum risk maneuver.

There are at least five different approaches of evaluation that can be applied to capturing the operating environment of automated road vehicles, namely, the test matrix approach, the naturalistic field operations approach, the Monte Carlo simulations approach, the worst-case evaluation approach, and the accelerated evaluation approach. The most likely predictor of system behavior is a full system simulation against the characterization of the operating environment provided by all of these. Though multiple vehicle subsystems have well developed simulations there are serious obstacles to integrating them into a single whole system simulation. Efforts to provide such a ‘federated’ simulation environment are in process at NIST and a number of academic institutions, including UC Berkeley and Vanderbilt University.

The test matrix approach is repeatable, easy to execute, and fast, which the FMVSS and NCAP will likely continue to use although it does not ensure learning, the selection of the matrix is somewhat arbitrary, and “scoring” does not relate to real-world safety benefit. The naturalistic field operational testing, which is being used by Google, is directly related to the real world but is a slow and expensive method with low exposure to safety critical scenarios. The Monte Carlo simulation approach, which is based on the data from the naturalistic field operation testing, is suitable for simulations and driving simulators but is not amenable to accelerating the scenarios. The worst case evaluation approach explores and focuses on weakness, which is an advantage but it needs vehicle models and control models, and is numerically challenging. Moreover, its relationship with the real-world scenarios is not clear. The accelerated evaluation approach takes the naturalistic driving data along with the disturbance model of the behavior of other vehicles, and skews the disturbance statistics to accentuate the portions of interest and skews back to understand the real-world safety benefits. This can accelerate the testing or simulations by 100 – 10,000 times and still compute real-world safety benefits although it needs a large quantity of driving data to begin, which can be an area of pre-competitive collaboration.

3 Paving the Way for Validation and Verification

Validation and verification of automated road vehicles will be governed by safety and security, as well as by performance, comfort and convenience. Given the fact that many of the functions at different levels of automation are in different experimental stages, and will need a long time before they can be commercialized, a collaborative effort between OEMs, suppliers, research organizations, standards organizations, and regulatory bodies could help remove some easily removable obstacles. Some relevant research questions related to the validation and verification topic are:

1. Is crash safety the dominant function for validation & verification? How does verification & validation of other functions e.g., passenger comfort, compare in terms of understanding and complexity?
2. What are the roles of standards and perhaps regulation in the area of validation & verification? Would they be beneficial or would they be an impediment to innovation?
3. Can we follow the example of other technology driven functionalities in order to develop a template for validating and verifying automated vehicles and eventually standards?
4. Is there an opportunity to identify automated vehicle subsystems for a standards exercise or precompetitive exchange without seriously impacting competitive advantage?
5. Would it be possible to share road study data in a precompetitive manner to improve verification & validation?
6. How can we improve communication about systems and components between OEMs and suppliers to improve the efficiency of verification & validation of automated vehicles? Example - common definitions, terminology, etc.
7. Would it be possible to consider standards for the operating environment for verification & validation? Example - weather, road conditions, traffic scenarios, etc.
8. What are appropriate test tools (field, test track, simulation, HIL) for validation & verification? Do we need new test tools or are the existing test tools sufficient?
10. Are different approaches needed for different types of automated driving functions (automated parking function vs. highway automated driving function or V2V functions vs. non cooperative functions)?

The opinions of the authors in the context of these questions are presented in the following.

Validation and verification can involve customer satisfaction, human-machine interface, cybersecurity, and challenging operating environments. Some have suggested that automated vehicles must achieve the overall status that is no worse than when humans drive cars. The change in traffic patterns due to introduction of automated road vehicles cannot be fully predicted.

Safety is the highest priority. Technology introduction should not make road traffic unsafe. Moreover, there is a fine balance between safety features and ease of use – the potential safety benefit is diminished if customers shut off a function due to annoyance or due to lack of understanding.

Systems engineering needs to cover safety engineering and security engineering, adding complexity. The level of system complexity governs the complexity of breaking down verification & validation into different tests. Systems working differently but performing the same overall function create additional validation and verification complexity. The potential for sensor algorithm errors creates a new level of complexity for validation and verification. Finally, validation and verification of automated vehicles is much more complex because its reference is the ability of what a human does or can do, and that in itself is not well understood. More knowledge about normative human behavior and expectations would improve validation.

Acceptance tests are expensive due to the large number of options. It is challenging to do validation and verification cost effectively. Mixed traffic conditions must be taken into account for validation and verification but for cost reasons vehicle manufacturers and their suppliers may need to restrict themselves to microscopic traffic simulation. Manufacturers may need to consider “worst case scenario” and “accelerated evaluation” in order to reduce the cost of validation and verification yet cover unusual scenarios that will occur in real world.

Common industry standards around terms and definitions help the development process. Examples include common terminology for driving situations, environments, road classes, and traffic situations, etc. Precompetitive collaboration between industry, government, and research organizations on social norms and expectations of road users, consistent terminology, and shared data quality assurance is desirable.

Common industry standards around how measurement should be done would help improve communication and understanding. The driver of an automated vehicle needs to know when and how he or she needs to take back control. Some have suggested this should be consistent from vehicle to vehicle.

If road and traffic scenario data is to be shared among OEMs, suppliers, and other organizations, then a common understanding of what that data should be and how to interpret it needs to be established. Such joint data could potentially help promote better understanding and acceptance, and inform decisions about policy and not just technical issues.

Data collection from vehicles after launch is an opportunity to identify rare events in order to expose hidden risks that don't occur in pre-release testing, and this could be an area of precompetitive data sharing without risking intellectual property.

Simulation and modelling is becoming more and more reliable but we still need physical testing to be confident, particularly when dealing with safety certification. Consequently, it will be used in the development domain but unlikely to enter the certification arena in the near future, given the complexity involved.

4 Conclusion

The authors have discussed validation and verification of automated vehicles from the perspectives of manufacturers, suppliers, researcher organizations, standards organization, and regulation, and find that the main areas for future exploration, in order to make it easier to design, develop, and deploy automated vehicles, should be driven by the following needs:

1. Development of common industry terms and definitions.
2. Creation of common customer expectation for automated vehicle response.
3. Development of common industry standards around how performance should be measured.
4. Better knowledge of driving behavior as it is today from the data already available.
5. Collection of post-launch data to help identify rare events.
6. Increased use of modeling and simulation to reduce verification costs.
7. Incorporation of driver models into verification and validation.

4 Acknowledgement

The authors would like to acknowledge Mary Doyle of the Society of Automotive Engineers for capturing the details of the breakout session on Verification and Validation of On-Road Automated Vehicles held at the Automated Vehicle Symposium 2015.

The first author would like to acknowledge Paul Perrone of Perrone Robotics for preparing the initial ground for the breakout session on Verification and

Validation of On-Road Automated Vehicles held at the Automated Vehicle Symposium 2015.

5 References

- [1] Barickman, F, “USDOT-Crash Avoidance Metrics Partnership Automation Research Project Overview”, SAE Government and Industry Meeting, Washington, D.C., 2014
- [2] Christensen, A, Cunningham, A, Engelman, J, Green, C, Kawashima, C, Kiger, S, Prokhorov, Danil, Tellis, L, Wendling, B, Barickman, F, “Key Considerations in the Development of Driving Automation Systems”, 24th Enhanced Safety Vehicles Conference, Gothenburg, Sweden, June, 2015
- [3] Tellis, L, “Key Considerations in the Development of Driving Automation Systems”, Automated Vehicles Symposium, Ann Arbor, Michigan, 2015
- [4] Griffor, E. R. and Nass, C., “Implicit Communication: Design for Human-Machine Interaction”, Handbook of System Safety and Security, Editor Griffor, E. R., Elsevier-North Holland Publishing, 2016 (to appear)
- [5] 1490 WG - IEEE Guide: Adoptions of the Project Management Institute (PMI) Standard: A Guide to the Project Management Body of Knowledge (PMBOK Guide), 2008, 4th edition

6 Full Authors’ Information

Venkatesh Agaram
PTC Inc.
3310 West Big Beaver Road
Suite 100
Troy, Michigan
USA
E-mail: yagaram@ptc.com

Frank Barickman
National Highway Traffic Safety Administration, Vehicle Research and Test Center
10820 SR 347
East Liberty, Ohio
USA

E-mail: frank.barickman@dot.gov

Felix Fahrenkrog
Institut für Kraftfahrzeuge, RWTH Aachen University
Steinbachstraße 7
Aachen
Germany
E-mail: fahrenkrog@ika.rwth-aachen.de

Edward Griffor
National Institute of Standards and Technology, U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899-1070
USA
E-mail: Edward.griffor@nist.gov

Ibro Muharemovic
Continental Corporation
One Continental Drive
Auburn Hills, Michigan
USA
E-mail: ibro.muharemovic@continental-corporation.com

Huei Peng
Michigan Mobility Transformation Center, Lay Auto Lab
1231 BEAL AVE
G036
Ann Arbor, Michigan
USA
E-mail: hpeng@umich.edu

Jeremy Salinger
General Motors
30500 Mound Road
Mail Code 480-106-RE2
Warren, Michigan
USA
E-mail: Jeremy.salinger@gm.com

Steven Shladover
California PATH Program, University of California
1357 South 46th Street
Building 452
Richmond, California
USA

12

E-mail: sess@berkeley.edu

William Shogren
Harman International
39001 West 12 Mile Road
Farmington Hills, Michigan
USA
E-mail: William.shogren@harman.com

5 Keywords

Validation and verification – automated road vehicles – commercial deployment - systems engineering – customer expectations – industry standards – terms and definitions – driving behavior – measurement standards