Response to NHTSA ANPRM Docket ID 2020-0106

Framework for Automated Driving System Safety

Steven E. Shladover, Sc.D.

(Personal perspective of a retired annuitant from the University of California PATH Program)

January 2021

Thank you for the opportunity to comment on this proposed approach to development of a Federal safety framework for ADS. It is encouraging to see that NHTSA has given careful consideration to the important issues and that it has recognized the complexity and immaturity of the technology and the importance of software in governing the behavior of the ADS. These factors point to the need for an assertive regulatory approach to protect public safety rather than relying on voluntary actions by ADS developers.

I have provided answers below to the questions to which I have devoted considerable thought in recent years, after more than 45 years of professional work on automated driving.

Question 1: Describe your conception of a Federal safety framework for ADS that encompasses the process and engineering measures described in this document and explain your rationale for its design.

The Federal safety framework needs to be based on several important principles, which provide the underlying rationale behind the proposed framework:

(a) ADS technology is still in its infancy, so knowledge about the technology and its associated safety potential and risks is still evolving rapidly, which means that the framework needs to be dynamic rather than static.
(b) ADS technology integrates the function of the driver into the vehicle software and hardware, so it violates the "traditional" boundary between Federal and state regulatory roles and therefore requires a somewhat different regulatory approach from NHTSA's historical approach.
(c) The ADS development community includes many organizations outside the motor vehicle industry that have a very different culture, lacking experience with safety-critical systems and government regulations. They are also susceptible to typical Silicon Valley pressures to "move fast, break things and seek forgiveness rather than permission".
(d) The ADS developers have invested heavily in development of their technology and are anxious to protect their competitive positions by disclosing as little information as possible about how their technology works in order to protect their intellectual property and public image.
(e) Large segments of the general public are skeptical about the safety of ADS technology, so their trust in the technology will have to be earned through meaningful regulatory "seals of

approval" that are based on significant disclosures about the ADS technologies that are proposed for public use.

(f) Just a few new serious injuries or fatalities caused by misbehaviors of immature ADS prototypes or products are likely to generate a serious public opinion backlash against all ADS, damaging the entire industry's longer-term prospects for public acceptance.

(g) The hazardous situations that ADS will encounter on the road are so diverse that it is not feasible, at the current state of knowledge, to define a collection of testing scenarios that can convincingly demonstrate that an ADS that passes that test could be considered safe enough for use on public roads.

(h) A substantial amount of new research will be needed to develop a level of fundamental knowledge sufficient to support the use of quantitative engineering measures of ADS performance to produce credible estimates of the real-world safety of any specific ADS.

Based on this foundation, the Federal regulatory framework for ADS should:

1) Be defined to be flexible and dynamic, so that it can be adjusted as ADS technology advances and the understanding of the ADS safety challenges grows.
2) Rely as much as possible on existing technical standards developed by open consensus-based standards development organizations (that do not require participants to "pay to play") such as SAE and ISO.
3) Establish mandatory requirements rather than relying upon voluntary actions by ADS developers (which would be too easy for the "bad actors" in the industry to ignore).
4) Begin with a robust stakeholder outreach program to develop a societal consensus regarding "how safe is safe enough", including not only industry representatives, but also public agencies, emergency responders, traffic safety advocates and the general public.
5) Set minimum national requirements for ADS safety, while permitting state and local governments to require higher levels of safety to meet their local needs and concerns. This is important because the ADS takes over the dynamic driving task from the driver, which would normally be subject to state and local regulatory authority.
6) Focus initially on the safety of the development process, rather than trying to quantitatively assess the safety of the ADS in action, because this is what is currently technically feasible, relying on process standards such as UL4600, ISO 26262 and ISO PAS 21448. ADS developers should be required to self-certify that they have followed these standards (or key sections of these standards), and in cases where they have not followed them completely, they should be required to provide supportable explanations for why this does compromise the safety of their ADS.
7) Require assessment of safety of ADS responses to specific scenarios at a later time, after enough research has been done to determine how to do that effectively (how to define the relevant scenarios and the performance thresholds that need to be met to be rated "safe enough").

8) Require that the ADS recognize when its ODD limitations have been violated, and then bring the vehicle to a minimal risk condition in the absence of driver action (or transfer control to a driver if a driver is available).
9) Require open reporting of all significant adverse events that occur when an ADS is driving, analogous to the reporting requirements that NHTSA imposed on Nuro in response to its exemption request.
10) Require collection of comprehensive diagnostic data about crashes and near-crashes using a new event data recorder, and require that these data be made available to government regulators and traffic safety researchers so that civil society as a whole can learn how to improve ADS safety over time, building on these experiences (analogous to the Auto-ISAC and current aviation safety reporting to the FAA).
11) Require that all consumer-facing documentation of ADS capabilities and limitations be consistent with the reality of ADS performance, including all in-vehicle displays, owner's manual, training material and marketing and advertising materials.
12) Avoid any pressures to create liability shields for ADS developers, because liability exposure provides a potent financial incentive in favor of ADS safety.

Question 2: On which aspects of a manufacturer's comprehensive demonstration of the safety of its ADS should [NHTSA] place a priority and focus its monitoring and safety oversight efforts and why?

Focus initially on the engineering and development processes that they follow to identify and mitigate as many relevant hazards as possible, because this is what is most tractable at the current state of knowledge and within the scope of the existing consensus standards. After substantial new research has been done, it may become feasible to identify a relevant set of safety-critical scenarios and performance criteria associated with each of those scenarios to assess the safety of the ADS.

Question 3: How would your conception of such a framework ensure that manufacturers assess and assure each core element of safety effectively? and

Question 4: How would your framework assist NHTSA in engaging with ADS development in a manner that helps address safety, but without unnecessarily hampering innovation?

UL4600 provides a very comprehensive checklist that manufacturers should use as their starting point. If they follow its guidance completely, it will be reasonably likely that they have assured each core element of safety effectively. If NHTSA were to require ADS developers to follow the UL4600 guidance and provide cogent explanations for any deviations that they take from UL4600, that could provide a reasonable level of assurance about the completeness of their safety approach (nothing could "ensure" it with certainty).

UL4600 places no limitations on the technological innovations or specific technologies that the ADS developers may choose to employ, leaving them free to innovate. It only requires that they

apply a comprehensive safety process to the development and implementation of the ADS, regardless of its specific technologies.

Question 5: How could the Agency best assess whether each manufacturer had adequately demonstrated the extent of its ADS' ability to meet each prioritized element of safety?

This type of assessment is not really feasible at the current state of the art for a couple of reasons:

(a) the hazard environment is not yet defined in a comprehensive fashion, and when it is, it will be very extensive in scope and complexity;

(b) demonstrating a safe response to the full range of hazards would be an extremely costly and time-consuming endeavor.

These issues of complexity argue against the concept of "demonstrating" the safety of the ADS, and weigh in the direction of certifying that the development process has given proper attention to safety.

Question 7: Can you suggest any other core element(s) that NHTSA should consider in developing a safety framework for ADS? Please provide the basis of your suggestion.

The core elements that NHTSA identified are focused on the internal functions that the ADS performs in conducting the dynamic driving task, but they do not account explicitly for the external driving hazard environment in which the ADS needs to operate. ADS developers expend significant resources trying to identify and describe these hazards, and after those investments have been made the results represent significant intellectual property that they are disinclined to share with others. It would be more efficient for the entire industry if the hazard environment definitions could be pooled across the industry through a combination of NHTSA coordination and NHTSA investment. This would not only aid the ADS developers (especially the smaller ones) in overcoming a major development hurdle, but it would also provide safety regulators with a common set of baseline conditions to use to assess the safety of each ADS that is proposed.

Question 8: At this early point in the development of ADS, how should NHTSA determine whether regulation is actually needed versus theoretically desirable? Can it be done effectively at this early stage… [without] delaying or distorting paths of technological development…? and

Question 9: If NHTSA were to develop standards before an ADS-equipped vehicle or an ADS that the Agency could test is widely available, how could NHTSA validate the appropriateness of its standards?...and

Question 10: Which safety standards would be considered the most effective… and should therefore be given priority over other possible standards?

Answering these three questions requires careful thought about the nature of the regulations themselves. If the regulations were to be viewed only in the context of traditional FMVSS, with precisely-specified performance measures and testing procedures, it would not be possible to implement regulations at the current time without adversely impacting ADS development. However, regulations that compel ADS developers to follow solid safety management principles and processes as defined in existing standards such as UL4600, ISO 26262 and ISO PAS 21448 can be implemented immediately, without distorting technology decisions and without having adverse impacts on ADS development schedules or costs. These system development processes and their associated safety cases are inherently costly and time consuming, but they should be viewed as essential prerequisites to the development of any safety-critical system and not as "extra" burdens imposed by regulators. The safety-conscious ADS developers will do this regardless of whether regulations require it, but the regulations are the essential mechanism for ensuring that all ADS developers follow industry best practices for development of safety-critical systems.

Question 12: What types and quanta of evidence would be necessary for reliable demonstrations of the level of performance achieved for the core elements of ADS safety performance?

Unfortunately, the hazard environment is so complex, and the potential ADS responses to those hazards are so diverse that it is not going to be practical to produce "reliable demonstrations of…ADS safety performance" for the foreseeable future. The concept behind this question (demonstrating safety performance based on experimental data) needs to be set aside until a great deal more knowledge and experience is acquired about the hazard environment and about efficient methods for assessing ADS responses to those hazards (i.e., determining how to develop and validate simulations that could achieve sufficient fidelity to be usable for this purpose). There is no good way of designing a suitable obstacle course or test for either NCAP or regulatory compliance at the current state of knowledge about the hazard environment. Any such test would be too vulnerable to "gaming" by the ADS developers, designing a system to pass the test, without any assurance that it would behave safely in the real world.

Question 14: What additional research would best support the creation of a safety framework?

Several important topic areas need serious research attention (and investment of resources):

(a) Identifying the most effective approach for building the U.S. societal consensus regarding how safe ADS need to be in order to be acceptable for public use. This includes building the stakeholder community, defining how best to interact with the stakeholder community, and developing agreement on the relevant safety baseline(s) to which ADS should be compared and the relevant safety measures of effectiveness.
(b) Building alliances with the major international activities that are addressing the same challenges of how to assess ADS safety and how to define the most effective regulatory approaches for ensuring and certifying ADS safety. Although the overall regulatory

frameworks for motor vehicle safety are very different around the world, there are still important lessons to be learned from the experiences of other countries (which have made considerably more progress in this regard than the U.S.). Harmonizing the technical aspects of safety assurance internationally will also facilitate more rapid and efficient market introduction of safe ADS, since the development work is multi-national in scope.

(c) Defining a common language and criteria for specifying the use cases that will be relevant for ADS safety assessment in the longer term. A similar effort was initiated in the Pegasus Project in Germany and related activities are ongoing throughout the world, but this remains an immense challenge that will require significant additional effort. It is important to converge on a unified approach to this in order for ADS development and evaluation to proceed efficiently at the global level and so that the safety assessments and certifications can have high credibility with the stakeholder community.

(d) Defining technically valid methods for using prospective measurements of the performance of ADS prototypes to estimate their real-world safety in comparison with the retrospective data that exist on current traffic safety (rates of fatalities, injuries of varying degrees of severity, property damage, and other economic losses).

(e) Defining technically valid methods and test cases for verifying and validating simulations of ADS performance so that their outputs can be trusted for purposes of efficiently assessing the real-world safety of each ADS.

(f) Developing a well-integrated approach to ADS safety assurance that efficiently combines the best elements of the existing approaches that rely on process audits, scenario-based assessments and normative driving protocols. None of these existing approaches represents a complete solution in itself, but they have complementary strengths that should be capitalized upon.

Question 21: Should NHTSA consider an alternative regulatory path…. that could allow for flexible demonstrations of competence with respect to the core functions of ADS safety performance?

No. This is not a realistic approach for producing a technically credible indication of safety, but looks like it would be an open invitation for ADS developers to cheat on the process and take technical shortcuts. The safety challenges are inherently complicated because of the complexity of the traffic environment and the complexity of the ADS technology. Cherry-picking a few cases to demonstrate competence provides no assurance of the ability of an ADS to respond safely to the multitude of combinations of adverse situations that WILL arise in real-world operations (both external hazards and failures in the ADS and its host vehicle).