The Center for Auto Safety
1825 Connecticut Ave. NW Suite 330 Washington, DC 20009
www.autosafety.org

August 28. 2019

Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, DC 20590

Submitted electronically via www.regulations.gov

RE: Advance Notice of Proposed Rulemaking: Removing Regulatory Barriers for Vehicles With Automated Driving Systems; Docket Number NHTSA–2019-0036

The Center for Auto Safety (Center) appreciates the opportunity to comment on the National Highway Traffic Safety Administration's (NHTSA) Advance Notice of Proposed Rulemaking (ANPRM) regarding the attempted acceleration of commercial deployment of Automated Driving System – Dedicated Vehicles (ADS-DVs) that lack traditional manual controls necessary for a human driver to take control of the vehicle in an emergency. The Center, founded in 1970 and headquartered in Washington, D.C., is a membership-driven non-profit consumer advocacy organization dedicated to improving vehicle safety, quality, and fuel economy.

The Center has long been a supporter of requiring the use of proven advanced safety technology to improve the safety of all drivers, passengers, and pedestrians.[1] Accordingly, we strongly question the agency's choice to prioritize a potential roll back of important protections afforded by the current Federal Motor Vehicle Safety Standards (FMVSS), in order to accommodate the introduction of vehicle technology that is in its infancy and quite likely decades away from widespread practical utility. A more safety focused course of action would be to immediately work to write mandatory performance standards for existing advanced safety features, such as automatic emergency braking.

Further, we continue to find specious the assertion that current Federal Motor Vehicle Safety Standards (FMVSS) obstruct the future development and testing of ADS-DV technology. Current federal law grants an ability to undertake unlimited testing of such vehicles. NHTSA regulations allow for a manufacturer to request an exemption allowing up to 2,500 vehicles which fail to comply with FMVSS to be sold to the general

[1]Center for Auto Safety Testifies Before Congress on Safety Technology, May 23, 2019
https://www.autosafety.org/center-for-auto-safety-testifies-on-safety-technology/

public, presuming the application shows an equivalent level of safety in the exempted vehicle.

Accordingly, the Center respectfully requests that NHTSA reconsider its current insistence on the necessity of prioritizing the evaluation and potential truncating of current safety standards in the service of commercial entities instead of public needs. If NHTSA truly believes ADS-DV that will lack human controls are years, (as opposed to decades) away from commercial viability, now is the time to begin evaluating what new standards will be required to address critical issues posed by ADS-DV. This would be a much preferable and safety focused course instead of attempting to insert the square peg of ADS-DV into the round hole of safety standards designed for the vehicles of yesterday and today. These standards were never contemplated as being relevant to vehicles without steering wheels, brake pedals, gear selectors, or a human in control.

Vehicles that Lack Traditional Manual Controls

There is no demonstrable evidence that vehicles lacking manual controls as envisioned by the FMVSS can safely operate on (and off) America's roads, yet NHTSA is entertaining the idea of changing safety standards to accommodate such vehicles. Even Level 4 vehicles, as defined by SAE J3016, explicitly contemplate circumstances where automated driving features will not work (outside of their operating design domain) – and require human control. Until manufacturers have validated ADS-DV performance in all reasonable operating design domains and demonstrated continued safe operation of ADS-DVs lacking human control, the rationale for rewriting the rules to allow such vehicles on the road remains unexplained. The reason all vehicles currently must have traditional control features that meet or exceed the FMVSS in order to ensure comprehensive safe operation on the road is because it is understood humans will have to be in control. No case has been made showing this circumstance will be changing anytime soon, yet via this ANPRM, NHTSA suggests such a change is imminent and requires the FMVSS be rewritten immediately. Based on the available data, we remain skeptical of this position.

The "Regulatory Barriers" Fallacy Obstructs Focused Rulemaking on New AV Safety Standards

Perhaps out of convenience, NHTSA continues to propagate the theory that the current FMVSS somehow stand in the way of a safer future ushered in by ADS-DVs. Yet, this argument only makes sense because NHTSA is unwilling to conduct research and issue rulemakings (even on incredibly simple issues, such as electronic notification of recalls[2]) in a timely manner.

New rules are required to avoid any actual or perceived conflict between ADS-DV tech and the current FMVSS. However, the agency has continually espoused the notion that the current FMVSS, which were not designed in anticipation of ADS, should be modified

[2] https://www.federalregister.gov/documents/2016/09/01/2016-20926/update-means-of-providing-recall-notification

to include ADS-DV. Although NHTSA's original AV policy contemplated new safety standards applicable to highly automated vehicles,[3] succeeding AV policy statements make it plain that NHTSA is now holding fast to the unproven notion that current safety standards must be changed in order to allow for ADS-DV operation. In fact, DOT and NHTSA's stubborn insistence on chipping away at the FMVSS, and refusal to consider issuing new regulations to cover a new class of vehicles, is based on a predetermined notion these regulations present a "barrier."

This is in direct contradiction to previous NHTSA policy, where the agency has recognized that different types of vehicles require different FMVSS rules and applicability. For example, FMVSS compliance for motorcycles is different in some respects than for automobiles.[4] This precedent is also pertinent for ADS-DV, which require different compliance criteria in some respects than conventional motor vehicles. NHTSA should establish criteria for SAE Level 3, 4, and 5 vehicles and write ADS-DV specific rules with which these vehicles must comply.

The Department of Transportation's insistence on deregulation as the answer to all questions is the real barrier to a roadway to safer vehicles.

Sincerely,

Jason Levine
Executive Director

[3] https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016
[4] See Requirements for Motorcycle Manufacturers, https://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Articles/Associated%20Files/mcpkg002.pdf

APPENDIX: Responses to Questions on Possible Approaches to Revising Crash Avoidance Test Procedures

The agency requests comment on the following approaches: (1) Normal ADS-DV operation; (2) that provide absolute priority over automatic controls; (3) Test Mode with External Control (TMEC); (4) Simulation; (5) Technical Documentation for System Design and/or Performance Approach; and (6) Use of Surrogate Vehicle with Human Controls. The agency also requests comment on whether any additional alternatives are possible. In addition to answers to the questions that appear after the discussion of each approach, NHTSA requests that commenters answer these questions for each of the approaches:

A. Normal ADS-DV Operation

1. **What are the possible advantages and disadvantages of each approach?**
    a. The Center does not agree that Automatic Driving System-Dedicated Vehicle (ADS-DV) progress necessarily requires relaxation or modification of FMVSS requirements for the convenience of manufacturers. Instead, the Center believes that it is incumbent upon OEMs wishing to offer ADS-DV to demonstrate to the public that the vehicles provide safety at least equivalent to conventionally controlled vehicles with comparable technology. ADS-DV must be manually controllable when operated incidentally or in emergencies outside of its programmed ODD to assure safety of occupants, bystanders, shippers, other road users, and emergency personnel, which is explicitly contemplated by SAE J3016 Levels 3 and 4 and which include all ADS-DV. Accordingly, no ADS-DV should be permitted on public roads or placed into commercial for-hire service unless it is equipped with manual human interface controls that provide absolute priority over automatic controls when used for any situation where safety or exigencies demand that the vehicle be maneuvered outside of its ODD. Not only are such situations common and anticipated in Level 4, they include those articulated in this ANPRM (see question 14) and such common occurrences as:
        i. directions by emergency personnel to maneuver the vehicle contrary to normal traffic rules,
        ii. stopping to exchange information and provide assistance after a collision,
        iii. driving around an accident on a highway as needed to avoid fire or debris or as directed by emergency personnel,
        iv. driving the vehicle by attendants or valets onto an autotrain or car carrier truck during shipment,
        v. maneuvering into underground parking or impromptu open field parking space, unlined parking lot as directed by attendants, onto a showroom floor or vacant lot,
        vi. pulling into a gas station service bay for service or state inspection, or

vii. safety testing by NHTSA or a mechanic.

b. It is hopelessly naïve to assert that situations demanding manual vehicle control to assure safety will never arise during an ADS-DV life cycle or that comprehensive passenger safety can be assured without their consideration. Anticipating the need, ADS-DV equipped vehicles should incorporate manual controls usable by any licensed driver, and that could also be used by NHTSA test engineers to conduct applicable FMVSS tests without modification. The manufacturer of any vehicle that does not include accessible human vehicle controls senior to the automatic control system must bear the burden of proof that vehicle operations in all situations including other than programmed ODD operations, will be safe for occupants, attendants, bystanders, other road users, and property customarily associated with vehicle manufacture, transportation, sales, service, test, deployment, and operations. This includes remote operational control for passengers unable or unwilling to manually control such vehicles.

c. Advantages and disadvantages of each potential test mode are discussed in the appropriate sections below.

2. **Discuss whether each approach fits the requirements and criteria of the Safety Act and enables effective enforcement of the FMVSSs. Explain the basis for your answers.**

a. The Safety Act requires manufacturer compliance with NHTSA regulations and requirements. It does not require government regulatory compliance with or conformance to vehicle design, corporate investment objectives, or manufacturer convenience. The Center believes that only tests that use an unmodified vehicle as available to the public are valid for FMVSS compliance confirmation. Therefore, the only approach that can achieve the Safety Act requirements for FMVSS compliance that involves vehicle operation is the normal ADS-DV configuration. For that, the manufacturer must include fixed or deployable conventional controls that provide absolute priority over automatic controls when used. Any other approach does not allow effective deterministic, empirical testing of production vehicles for effective enforcement of the FMVSS.

b. Any FMVSS compliance operations-related verification testing approach that does not use unmodified production vehicles is subject to interpretation and mistakes and potentially gaming by the manufacturer or the organization responsible for the modification or simulation. Therefore, to assure compliance verification, every ADS-DV must be equipped with manual controls to enable FMVSS compliance testing. Any modification to controls or vehicle inputs will be readily detectable by the control system and potentially cause malicious software modifications intended to defeat the test objectives, as has happened

before in the context of vehicle emissions testing.[5] Even with the best constructed and best intended tests of alternative configurations of test vehicles, it will always be difficult to provide unambiguous evidence that operational tests of an analogue is equivalent to that of an unmodified vehicle.

c. Unique characteristics of each approach will be discussed in the appropriate section below

3. Can more than one of these approaches be specified by the agency as alternative ways for the agency to determine compliance with the same requirement in the same FMVSS? If so, please describe how this could be done consistent with the Vehicle Safety Act, using one or more specific FMVSS requirements as illustrative examples. If more than one approach could be specified for the same requirement in the same FMVSS, do commenters believe that the agency, in assessing compliance with the same requirement in the same FMVSS, choose one approach for one vehicle model, but another approach for a different model? If so, explain why.

a. Multiple approaches can be used to provide incremental evidence of FMVSS compliance, but no combination of tests will provide equivalent confidence that tests using established protocols for designed-in supervisory manual controls would provide. All of the alternatives to tests based on normal ADS-DV configuration will create questions about verisimilitude and statistical confidence in safety projections. Further, unless the ADS-DV includes designed-in supervisory manual controls, adaptation for FMVSS test purposes will necessarily depart from the commercially available normal ADS-DV configuration baseline which also departs from NHTSA NCAP test protocols.

b. The Center sees no acceptable alternative to a requirement that conventional manual controls be standard equipment. ADS-DV and FMVSS testing can use those controls when required, including for FMVSS tests. Additionally, no other approach is consistent with NHTSA NCAP test protocols, provides irrefutable evidence of a vehicle's compliance with requirements, is resistant to test tampering, and tests actual as-delivered motor vehicles. Inclusion of manual controls does not preclude inclusion of remote controls needed by occupants unable or unwilling to assume manual vehicle control but enables emergency or optional manual control for those who can or must use them.

c. Responsible discussion of eliminating barriers due to required safety testing must also articulate the safety goals that such tests validate and

[5] Volkswagen: The scandal explained https://www.bbc.com/news/business-34324772
Nissan Admits It Has Uncovered Falsified Emissions Tests In Japan, https://www.motor1.com/news/251706/nissan-admits-falsified-emissions-tests/
Opel, Daimler, Fiat Chrysler, Mitsubishi automated test deception, https://www.roadandtrack.com/new-cars/car-technology/a29293/vehicle-emissions-testing-scandal-cheating/

provide a reasonable alternative that validates achievement of that same safety goal by any and all tested ADS-DV. That reasonable validation alternative should be a standard applicable to all unmodified production ADS-DV so that it is, in fact, a standard consistent with the NHTSA vehicle test program requirements. The Center's focus on inclusion of conventional manual controls reflects that no such alternative standard currently exists, nor is proposed as part of this request for comments, nor is likely to be developed, approved, and codified for a very long time. As a practical matter, the only standard approach that will be available for a very long time will include conventional manual controls. Asserting that no conventional manual controls are needed is equivalent to asserting that those FMVSS tests requiring such controls are not needed, for which there is no documentary support.

4. **If only one of these approaches can be used to enforce a particular FMVSS requirement, what factors should be considered in selecting that approach? What policy or other considerations should guide the agency in choosing one alternative approach versus another for determining the compliance of a particular vehicle or item of equipment?**
    a. The Center believes that consistency with FMVSS requirements and among automobiles tested is essential to the integrity of FMVSS testing. The only way to achieve this consistency is to perform tests on vehicles purchased anonymously from retail outlets and to perform the tests on normal ADS-DV operation-equipped vehicles using human operational control interfaces common to all vehicles. Current tests have developed test equipment and protocols adapted to the human driver controls in all vehicles. The Center believes that such controls must be available in ADS-DV offered to the public for use in general transportation, and that such controls must be configured to allow standardized FMVSS tests as well as control for other uses potentially outside of the preprogrammed ODD. Therefore, only the normal ADS-DV configuration is supportable for operational FMVSS tests, and the vehicle configuration must include manual controls needed to support FMVSS testing and compliance confirmation.

5. **With respect to any single approach or combination of approaches, could it be ensured that the compliance of all makes and models across the industry is measured by the same yard stick, i.e., that all vehicles are held to the same standard of performance, in meeting the same FMVSS requirement?**
    a. Yes, performing tests on vehicles purchased anonymously from retail outlets on Normal ADS-DV configured vehicles using human operational control interfaces common to all vehicles is an approach that can provide consistency of test and interpretation of results among different vehicles. Any other approach will be inconsistent, requiring modification of the test

vehicle and/or test protocols to accommodate design variations, and potentially biasing test results toward the modified ADS-DV and away from human-driven vehicles with otherwise comparable technology. The Center sees no acceptable alternative to both a requirement for manual controls and FMVSS testing that uses those controls when required. Vehicles so configured, and only vehicles so configured, can provide the required objective, consistent test results. Once the baseline consistency with FMVSS requirements is established, it might be incumbent on the manufacturer to show that automatic controls produce comparable results in similar situations, but no such FMVSS standard currently exists.

6. **What other potential revisions or additions to terms, in addition to 'driver', are necessary for crash avoidance standards that NHTSA should consider defining or modifying to better communicate how the agency intends to conduct compliance verification of ADS vehicle?**
    a. The Center does not believe that any additional definitions are needed to allow ADS vehicle FMVSS compliance verification, while noting that the FMVSS might need to be updated or amended to reflect ADS crash avoidance functionality. To assure operational safety in many circumstances that require vehicle operation outside of its preprogrammed ODD, manual controls are required. Such controls could be used for FMVSS verification without modification. NHTSA should develop additional FMVSS unique for vehicles with ADS functionality to verify that critical capabilities demonstrated in FMVSS verification are properly executed by the automatic controls, but such additional requirements are unrelated to showing compliance with existing FMVSS. Without defining how the agency intends to conduct compliance verification if not bounded by current FMVSS, any further response to the question would be purely speculative.

7. **Should NHTSA consider an approach to establish new definitions that apply only to ADS-DVs without traditional manual controls?**
    a. As stated previously, there is no demonstrable evidence that vehicles lacking manual controls as envisioned by the FMVSS can safely operate in public. To the extent such data becomes available, yes, it would also be appropriate for NHTSA to establish new definitions that apply only to ADS-DV and their unique features. Precedents exist for FMVSS applicable to separate vehicle classes, e.g., motorcycle standards (e.g. FMVSS 122, 123) that differ from automobile standards and are uniquely associated with motorcycles. This regulatory approach would allow for preservation of existing FMVSS for conventionally controlled vehicles alongside new regulations that are appropriate for the automated driving features of ADS-DV. These new regulations could remove the implicit human capability and ethical biases of existing regulations and replace

them with criteria appropriate for programmed operation that does not have human capability or ethical bounds to accomplish the same safety objectives for occupants and other road users as the current FMVSS.

8. **For compliance testing methods involving adjusting current test procedures to allow alternative methods of controlling the test vehicle during the test (normal ADS-DV function, TMPE, TMEC), or to allow the use of a surrogate vehicle:**
    a. **How could NHTSA ensure that the test vehicle's performance using the compliance method is an accurate proxy for the ADS-DV's performance during normal operation?**
        i. Acceptable alternative methods require yet to be developed safety standards and expensive compliance validation procedures. NHTSA could assure that the test vehicle's performance using the compliance method is an accurate proxy for the ADS-DV's performance during normal operation by independent validation and verification (IV&V) of a vehicle's compliance with objective test and safety standards. For level 4 or 5 vehicles, the IV&V would typically be based on a failure modes and effects criticality analysis (FMECA) that incorporates both test and simulation results to establish acceptable confidence. The FMECA should include all safety-critical mechanical components and software functionality and have sufficiently broad scope to include all conceivable operational conditions to establish a proven level of safety with adequate confidence. This is a difficult but possible and expensive task. Pending completion of a comprehensive IV&V, the manufacturer would be in a position to seek accreditation of their control system and configuration.
    b. **If NHTSA were to incorporate the test method into its test procedures, would NHTSA need to adjust the performance requirements for each standard (in addition to the test procedures) to adequately maintain the focus on safety for an ADS-DV?**
        i. NHTSA should not perform any standards modification for an ADS-DV because it will either invalidate the test or introduce a bias with respect to other vehicles that are not ADS-DV equipped but are also subject to the same safety standards.
        ii. Safety standards need to be established and reviewed independently of the test procedure being used to establish conformance to avoid the tests becoming a tautology. It's unlikely that any ADS will have the same topology as any other, or that its control logic will be identical to any other. Adjustment of safety standards to reflect the level 4 or 5 implementation by any individual developer will necessarily be different than adjustments

made for another. If the test is modified to conform to the vehicle, it becomes tautological.

iii. To reiterate, the Center is supportive of a new set of regulations to be promulgated for ADS-DV (or simply ADS) which meet the same level of safety but leave intact existing FMVSS.

9. **For compliance testing methods that replace physical tests with non-physical requirements (simulation, documentation):**
    a. **If the test method is used to determine compliance with a real-world test, how can NHTSA validate the accuracy of a simulation or documentation?**
        i. Simulations alone cannot be used to determine compliance with a real-world test with sufficient confidence to establish adequate conformance to safety standards. NHTSA can validate the accuracy of a simulation or documentation in lieu of tests only if there are test-based results that bracket the simulated phenomenon, allowing interpolation between validated simulations rather than reliance on extrapolation. Acceptable passenger safety demands the inclusion of emergency manual control override capability in every vehicle sold to the general public. The existence of such controls obviates the need for substitution of simulations for tests.
        ii. Examples of regrettable reliance upon simulations ungrounded in actual tests abound. One notable example was the live-fire test of the fully automated DIVAD (also known as the Sergeant York) anti-aircraft gun, that memorably locked onto a reviewing stand filled with high-ranking military officers and reporters rather than the intended target during a live fire demonstration.[6] The simulation and previous tests had not accounted for the real world presence of moisture that compromised the RADAR sensors. Similarly, it is difficult or impossible to anticipate and accurately represent in simulation the many parameters present in complex driving situations such as NHTSA safety compliance tests.
    b. **If NHTSA must run real-world tests to validate a simulation or documentation, what is the advantage of non-physical requirements over these other compliance methods?**
        i. Non-physical requirements (simulation, documentation) can be useful adjuncts and supplements, but not substitutes for physical tests. For example, simulations can be useful for establishing how close physical tests are to performance boundaries (such as proximity to computer memory or processing margin limits in software stress testing) that are difficult to perform safely with

[6] http://www.todayifoundout.com/index.php/2017/02/time-military-paid-anti-aircraft-gun-locked-onto-toilets/

human testers. Validated (by test) simulations can be useful in establishing statistical confidence of conformance to safety standards in a wider range of driving conditions than practical with human drivers.[7] Documentation can be extremely useful in identifying and remediating safety-critical shortfalls in a vehicle's design, particularly documents expressly designed for that purpose such as FMECAs. Comprehensive safety confirmation analysis includes establishment of objective standards, tests, simulations, and documentation.

10. **Would non-physical requirements simply replicate the existing physical tests in a virtual world? If not, what would be the nature of the non-physical requirements (that is, what performance metrics would these requirements use, and how would NHTSA measure them)? Are there ways that NHTSA could amend the FMVSS to remove barriers to ADS-DVs that would not require using the compliance test methods described in below?**
    a. **Are there any barriers in the FMVSS or NHTSA's test procedures that could be addressed by altering or removing references to manual controls in the test procedures without substantively changing the FMVSS performance requirement?**
        i. Manual controls will undoubtedly be available in some form for those many operations in an ADS-DV life cycle that fall outside of its intended ODD. It is a conceit by the OEMs to envision an ADS-DV life cycle that will not. To validate vehicle safety, it is essential that these manual controls be designed to also support NHTSA safety tests and provide backup control capability for ADS-DV operation in safety-critical events outside of its intended ODD. There is no barrier to ADS-DV development that will be removed by altering or removing references to manual controls in the test procedures. Any such change would substantively change the FMVSS performance requirement and bias the tests toward the ADS-DV and thereby erect additional barriers to those tests for conventionally controlled vehicles.
    b. **Are there any changes that NHTSA could make to the FMVSS test procedures that could incorporate basic ADS capabilities to demonstrate performance, such as using an ADS-DV's capability to recognize and obey a stop sign to test service brake performance?**
        i. Yes, NHTSA could configure additional tests to incorporate basic ADS capabilities to demonstrate performance, such as using an ADS-DV's capability to recognize and obey a stop sign to test

[7] Measuring Automated Vehicle Safety, RAND Corp., https://www.rand.org/pubs/research_reports/RR2662.html

service brake performance.[8] The Center's recommended process for demonstrating safe performance by an ADS is laid out in detail in the Center's comments on DOT's AV 3.0.[9] Our recommended protocol would provide confidence in an ADS-DV's operation throughout its ODD, and for exceptional operations outside of its designed ODD.

11. What research or data exists to show that the compliance test method would adequately maintain the focus on ADS-DV safety? What modifications of the safety standards would be necessary to enable the use of the test method?

a. The compliance test method is necessary but not sufficient to adequately establish ADS-DV safety. Acceptable passenger safety demands the inclusion of emergency manual control override capability in every vehicle sold to the general public. Use of such manual controls allow an evaluation of compliance with NHTSA safety requirements and an unbiased comparison among various ADS-DV offerings and conventionally controlled vehicles with comparable technology levels. Biasing such tests toward unique characteristics of ADS-DV would erect comparative barriers to safety evaluation of conventional human-controlled vehicles. Given the compulsory existence of human control capability for both quotidian operational and safety needs, there is no modification of the safety standards necessary to enable the use of the test method.

13. Are there specific challenges that will be encountered with this kind of approach for vehicle compliance verification? Please be specific and explain each challenge.

a. Demonstrating compliance with NHTSA safety standards by testing normal ADS operation is necessary but not sufficient for evaluating safe ADS-DV operation. The NHTSA safety standards were written with the presumption of normal human inputs and responses to vehicle controls and performance. These inputs implicitly include human sensory capabilities, emotions, capacities, education, judgment, and ethics. It will be an enduring challenge to establish that highly automated controls exhibit the necessary range and breadth of capability to provide equal or superior safety that is the result of typical human capacities as expressed through NHTSA-compliant enabling safety features.

14. Will all ADS-DVs without traditional manual controls be capable of receiving and acting upon simple commands not consisting of a street

[8] For liability purposes, the Center maintains the manufacturer of the ADS should be held responsible for the actions of the vehicle, just as a human driver would be.

[9] https://www.autosafety.org/wp-content/uploads/2018/12/Center-for-Auto-Safety-AV-3.0-Comment.pdf

address based destination, such as "drive forward or backwards a distance of 10 feet and stop"; "shift from park to drive and accelerate to 25 mph"; "drive up onto a car hauler truck trailer"; etc.? Please explain projected challenges for ADS-DVs without traditional manual controls to complete discrete driving commands and tasks.

a. It is incumbent upon NHTSA to establish commands and other requirements necessary to enable ADS-DV safety compliance tests especially for circumstances such as 'drive up onto a car hauler truck trailer' that are likely to occur and are outside of the designed ODD. NHTSA must establish those requirements and acceptable means of inputting those commands into the ADS-DV control system that do not introduce a bias related to the vehicle being tested nor to any other vehicle whether ADS or manually controlled. A requirement for emergency manual control override capability in every vehicle sold to the general public would provide the needed capability.

15. **How would NHTSA ensure that the performance of the ADS-DV during testing is consistent with how the vehicle would perform during actual normal use?**

a. NHTSA should require that manual control inputs conforming to test standards are injected into ADS-DV control systems using the same standards and application programming interfaces (in other words in exactly the same way) as though the commands had been generated by the ADS-DV control system itself. For example, x degrees of steering wheel turn are related to y degrees of steering as would x degrees of steering command generated by the ADS-DV control system; q pounds of force on a brake pedal producing full brake system hydraulic pressure would inject a control signal into the vehicle control system that is the same as an ADS-DV controller commanding maximum brake pressure, and so on. To accomplish this NHTSA would need to mandate the existence of manual inputs suitable for the test, likely the same as the emergency manual controls, and that ADS-DV manufacturers provide a means for verifying both control inputs from either source and system response, which is well within the capability of any competent test facility.

B. Test Mode with Pre-Programmed Execution (TMPE) Questions specific to this testing method:

16. **How could engineers responsible for performing FMVSS compliance assessments of an ADS-DV without manual controls be expected to access and interface with the compliance test library menu?**

a. It isn't clear how to unambiguously replicate test results designed for human testers with TMPE. The Center does not believe it is a practical approach.

17. **Would the FMVSS need to specify the libraries available to NHTSA to test the vehicle?**
    a. Conditional access to only some portions of the unit under test software or libraries would always raise the question of whether the test is actually representative of the production vehicle. As was shown vividly in the Volkswagen diesel testing fraud, test engineers aware of a government test protocol are capable of and may be induced to game the test to show more favorable results. In that case, the Environmental Protection Agency (EPA) found that many VW cars being sold in America had a "defeat device" - or software - in diesel engines that could detect when they were being tested, changing the performance accordingly to improve results.[10] Requiring access to selected libraries or otherwise providing test access to selected software features invites the same kind of abuse in future ADS-DV safety tests conducted by NHTSA. Consequently, TMPE must only be performed alongside software audits, configuration control, and control system monitoring that would likely eliminate any cost or time benefits that TMPE might otherwise afford.

18. **Is it practical to expect that an ADS-DV without any traditional manually-operated controls can be safely and efficiently operated within the confines of a test track with only a preprogrammed test menu (i.e., without some form of external controller or other means of vehicle control input)?**
    a. No. It is both extremely unlikely and clearly impractical that any production vehicle will come preprogrammed with the geographic, operational, schedule, and test instrumentation necessary to perform TMPE. Some form of external controller or other means of vehicle control input will be required to get the vehicle from the showroom floor to the correct position at the (potentially indoor, unmarked) test facility at the right time. If such specialized locations were included in a production vehicle, then any other purchaser would also be able to direct their vehicle to that location, and that's not going to happen. Clearly, a designed-in ODD is no substitute for a human being's directions, imperatives, and judgment, and vehicles need to be equipped to allow humans to exercise those qualities when needed.

19. **Can an ADS-DV be expected to perform within tight tolerance levels using the regular onboard sensors?**
    a. 'Tight tolerance levels' is a qualitative term that will have different meaning to different readers. It is not possible to provide a meaningful comprehensive response without definition of the term.

[10] https://www.bbc.com/news/business-34324772

20. How much variation in test results across various test locations (i.e., proving grounds) is expected to result from testing an ADS-DV equipped with the same FMVSS compliance library at different locations? Could the ability to satisfy FMVSS performance requirements depend on the location the tests are performed?

a. Properly written test standards and protocols will provide consistent results in any acceptable test venue. No variation in FMVSS performance validation caused by choice of test location may be allowed.

21. Is it reasonable to assume any geofence-based operating restrictions could be suspended while the ADS-DV is operating in a "test mode" intended to assess FMVSS compliance?

a. It's difficult to see how any TMPE could be accomplished without suspending geofence-based operating restrictions. It would make no sense for test facilities to be included in geofencing of production vehicles sold to the general public as is required for NHTSA procurement of test vehicles.

22. How could vehicle-based electronically accessible libraries for conducting FMVSS testing be developed in a way that would allow NHTSA to access the system for compliance testing but not allow unauthorized access that could present a security or safety risk to an ADS-DV?

a. Secure communication interfaces can be provided by various means, but there is always some level of unauthorized access risk. Cybersecurity is never absolute if a computer is accessible to humans or communications. Unfortunately, incorporation of any means that would allow NHTSA special access but exclude others would also necessarily allow for detection of NHTSA's access and subsequent execution of software that could prejudice the test results and make them unrepresentative of normal operations. While ethical companies would no doubt make their best efforts to avoid misrepresenting test results, there is always the possibility that an individual developer or test engineer might employ surreptitious software execution (that would be very difficult for a third party to detect) affecting test results.[11]

23. Are there other considerations NHTSA should be aware of when contemplating the viability of programmed execution-based vehicle compliance verification?

[11] Ibid, Nissan Admits It Has Uncovered Falsified Emissions Tests In Japan, https://www.motor1.com/news/251706/nissan-admits-falsified-emissions-tests/
Opel, Daimler, Fiat Chrysler, Mitsubishi automated test deception, https://www.roadandtrack.com/new-cars/car-technology/a29293/vehicle-emissions-testing-scandal-cheating/

a. NHTSA safety testing may, and in some cases is expected to, excite vehicle responses that are unlikely to occur in normal operations. For this reason, software or computer processor functional margins that are marginally acceptable for normal operations may vanish under test conditions. To evaluate safety in the future, software stress testing should be included FMVSS related to all vehicles with safety-critical cyber features, especially ADS-DV which have an extensive suite of safety-critical software and processing features.

24. When changes or updates are made to the ADS, how will the TMPE content be updated to reflect the changes and how often would it be updated?

a. All motor vehicle design changes that affect safety must be reported to NHTSA. Changes or updates made to the ADS that impact TMPE content must also be reported and their consequences documented. This consideration is probably moot since it is unlikely that TMPE will be found to be acceptable for verifying vehicle safety.

C. Test Mode with External Control (TMEC) Questions specific to this testing method:

25. Is it reasonable to assume a common (universal) interface, translator, and/or communication protocol between an external controller and any ADS-DV will be developed?

a. It would require substantial investment into common standards for data, interfaces, and protocols on the part of many parties, and complementary NHTSA requirements development, to develop a common (universal) interface, translator, and/or communication protocol between an external controller and ADS-DVs. Given the current reluctance of NHTSA to require standards for (event) crash data recorders that are appropriate for the current generation of computer-assisted vehicles, much less the more demanding requirements of the nascent ADS-DV industry, it is very unlikely that such a suite of requirements, standards, protocols, and enabling instrumentation will be developed any time soon.

b. Even if such a universal interface were developed, the government is still left with the problem for potential test results falsification by malicious software executed only while under test. Since the universal interface would only be used for testing, its detection would be a signal to invoke test-defeating software that would be very hard to detect short of a highly intrusive and very expensive audit of the entire vehicle operating system. Because of this detectability and the potential for abuse, such a universal interface should not be developed or invoked.

26. What is the most viable method for securely interfacing an external controller with the ADSDV (e.g., wireless or physical access)?

a. Neither option is uniquely secure without considering all of the access points to the entire attack surface. It would be a mistake to depend on the choice of wireless vs. physical access to provide cybersecurity without a comprehensive software safety and cybersecurity assessment.

27. Could a means of manual control be developed that would allow NHTSA to access the system for compliance testing but not allow unauthorized access that could present a security or safety risk to an ADS-DV?

a. It would be a mistake to glibly assert any particular TMCE technology provides selective secure access without a comprehensive cybersecurity and software safety assessment. Technologies that have been implemented for aircraft operations are promising starting points,[12] but cost and context are important considerations not addressed in the question. The question needs to be answered not only in the context of test commands, but also with respect to all vehicle vulnerabilities potentially affecting either test commands or the underlying executable vehicle operational firmware and software. The narrow answer is technically yes, but programmatically it would require intensive efforts to accomplish and would also require heretofore unavailable compliance by industry to (currently nonexistent) governmental software design and content requirements, so as a practical matter this is likely not an option.

28. Is it reasonable to assume any geofence-based operating restrictions could be suspended while an external controller intended to assess FMVSS compliance is connected to the ADS-DV?

a. As discussed in answer to Question 1, this is an example of operation outside of the vehicle's ODD. Operation outside of the ODD even for the purpose of FMVSS tests is not necessarily indicative of operations restricted to the ODD. If the vehicle were configured for an external controller connected to the ADS-DV, unless that external controller is part of the vehicle's commercially available standard configuration it would be a customization for FMVSS testing that is inconsistent with the requirement for testing commercially offered vehicles.

29. Are there other considerations NHTSA should be aware of when contemplating the viability of using an external controller-based vehicle certification?

a. As in any test, the requirements validation is only applicable to the unique test configuration. Any subsequent changes to either hardware, software, or firmware configuration may invalidate test results. Configuration

[12] Cybersecurity on Aircraft, ALPA, http://www.alpa.org/advocacy/cybersecurity-on-aircraft
Cyber-Security, a new challenge for the aviation and automotive industries, http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf

control for such tests must include any external controllers attached to the test vehicle. Safety implications of changes to hardware, software, test standards, protocols, to any of the external control, test vehicle, or communications implementation need to be included in the safety assessment for the test itself and for subsequent operations of the tested vehicle and any derivatives.

D. Simulation Questions specific to this (Simulation) testing method:

30. How can simulations be used to assess FMVSS compliance?

a. By definition, simulations are not physical tests. Simulations can be used to assess FMVSS compliance only when the simulations have been validated by test, and then only when the simulation is within a parameter range that is unequivocally demonstrated to provide equally valid results.

31. Are there objective, practicable ways for the agency to validate simulation models to ensure their accuracy and repeatability?

a. Yes, IV&V can provide the needed confidence. There is an extensive literature on IV&V execution,[13] and many reputable organizations qualified to conduct IV&V.

32. Is it feasible to perform hardware-in-the-loop simulations to conduct FMVSS compliance verification testing for current FMVSS?

a. While certain FMVSS tests might be performed via hardware in the loop (HWIL) simulations, HWIL test conduct will always be detectable by the vehicle software and thus susceptible to gaming and malicious biasing of test results while under test potentially making them unrepresentative of the actual operational vehicle. It is also difficult to see how unaltered production vehicles can be ready for HWIL test without intrusive modifications, rendering them other than production vehicles. Further, modifications for HWIL tests might well bias the FMVSS compliance tests away from human-driven comparable technology vehicles, erecting barriers to their development in the process.

33. Is it feasible to perform software-in-the-loop simulations to conduct FMVSS compliance verification testing?

a. Current FMVSS compliance testing does not require software in the loop (SWIL) testing. Potential future requirements for software stress testing, for example, might well be performed by SWIL tests. There does not appear to be a current need.

[13] MIL-STD-3022, DEPARTMENT OF DEFENSE STANDARD PRACTICE: DOCUMENTATION OF VERIFICATION, VALIDATION, AND ACCREDITATION (VV&A) FOR MODELS AND SIMULATIONS http://everyspec.com/MIL-STD/MIL-STD-3000-9999/MIL-STD-3022_4197/

E. Technical Documentation for System Design and/or Performance Approach Questions specific to this testing method:

34. How can the documentation-focused approach ensure compliance with FMVSS, considering it neither verifies that the vehicles on the road match the documentation nor confirms that the vehicles on the road comply with the FMVSS?

a. The documentation-focused approach alone cannot assure compliance with FMVSS. It can be an important adjunct to the process. Future FMVSS for ADS-DV certification would benefit from a requirement for a vehicle FMECA as part of its overall safety evaluation. Other documentation such as software stress test results would also complement the vehicle safety assessment and should be part of vehicle certification and licensing.

35. If technical documentation were acceptable for compliance verification, how would the manufacturer assure the agency that the documentation accurately represents the ADS-DV and that the system is safe?

a. Technical documentation alone in lieu of test is not acceptable for operations-related FMVSS compliance verification.

36. Exactly what kind of documentation could be submitted for each kind of FMVSS requirement? Provide specific examples with detailed explanation of the documentation required.

a. Technical documentation alone in lieu of test is not acceptable for operations-related FMVSS compliance verification.

F. Use of Surrogate Vehicle with Human Controls Questions specific to this testing method:

37. To what extent could equivalence of the vehicle components used for conventional and ADS-DVs be demonstrated to assure that surrogate vehicle performance would be indicative of that of a surrogate ADS-DV?

a. Component FMVSS compliance tests may be perfectly acceptable for certain standards that are unrelated to the ADS-DV vehicle control or operations. These might include passive components and components that can be evaluated independent of the vehicle itself by alternate means.

38. How can the agency confirm that the maneuver severity performed by a surrogate manually drivable vehicle, during FMVSS compliance tests, is equal to that of the subject ADS-DV? For example, how can the characterization maneuvers and subsequent scaling factors in the FMVSS No. 126 ESC test on the surrogate vehicle be confirmed as equivalent on the ADS-DV?

a. Component FMVSS compliance tests that may be perfectly acceptable for certain standards are only those unrelated to the ADS-DV vehicle

operations or control or subject to vehicle control system inputs. These might include passive components and components that can be evaluated independent of the vehicle itself by alternate means. Characterization maneuvers and subsequent scaling factors in the FMVSS No. 126 ESC test, for example, on the surrogate vehicle could only be confirmed as equivalent on the ADS-DV with great difficulty and comparison of all applicable control inputs, outputs, and vehicle mechanical and logical characteristics and properties. As a practical matter, it is unlikely to be acceptable without very expensive and lengthy analysis and evaluation, but it is probably possible in certain circumstances for certain tests. NHTSA would need to evaluate every test and vehicle based on its unique design and state.

39. If results from FMVSS compliance tests of a conventional vehicle performed by its manufacturer differ from the results of NHTSA tests of an equivalent ADS-DV (particularly if the conventional vehicle complies with the agency's standards, but the ADS-DV does not), can the conflicting results be reconciled? If so, how?

a. Conflicting results could be reconciled, but typically with difficulty and considerable expense. On the other hand, reconciliation of conflicting results can be an extremely valuable entry point into understanding the details of both conventional vehicle and ADS-DV characteristics that could illuminate critical operational features or shortcomings of either or both. Reconciliation does not mean acceptance, however, and conflicting results need to be resolved in favor of compliance with the FMVSS, not merely observing that differences exist.