DOT's HAV Safety Assessment – A Truncated Version

Below we provide a truncated version of the voluntary 15 point "Safety Assessment" outlined in Section 1, Vehicle Performance Guidance for Automated Vehicles, of the U.S. Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA)'s Federal Automated Vehicles Policy (Policy). Please note that the explanations below are excerpts directly from the Guidance, not Beveridge & Diamond's reformulation of the wording.

1. **Data Recording and Sharing**

Manufacturers and other entities should have a documented process for testing, validation, and collection of event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues. Data should be collected for both testing and operational (including for event reconstruction) purposes. This provision of the guidance will not take effect until after NHTSA completes the Paperwork Reduction Act process for its data collection and reporting requirements. Once that process is complete, any resulting adjustments have been made, and NHTSA has published a notification in the Federal Register, this provision of the Guidance will be effective.

2. **Privacy**

HAV manufacturers and other entities, either individually or as an industry, should take steps to protect consumer privacy. Manufacturers' privacy policies and practices should ensure:

a. ***Transparency**: provide consumers with accessible, clear, meaningful data privacy and security notices/agreements which should incorporate the baseline protections outlined in the White House Consumer Privacy Bill of Rights and explain how Entities collect, use, share, secure, audit, and destroy data generated by, or retrieved from, their vehicles;*

b. ***Choice**: offer vehicle owners choices regarding the collection, use, sharing, retention, and deconstruction of data, including geolocation, biometric, and driver behavior data that could be reasonably linkable to them personally (i.e., personal data);*

c. ***Respect for Context**: use data collected from production HAVs only in ways that are consistent with the purposes for which the data originally was collected (as explained in applicable data privacy notice/agreements);*

d. ***Minimization, De-Identification and Retention**: collect and retain only for as long as necessary the minimum amount of personal data required to achieve legitimate business purposes, and take steps to de-identify sensitive data where practical, in accordance with applicable data privacy notices/agreements and principles;*

e. ***Data Security**: implement measures to protect data that are commensurate with the harm that would result from loss or unauthorized disclosure of the data;*

f. ***Integrity and Access**: implement measures to maintain the accuracy of personal data and permit vehicle operators and owners to review and correct such information when it is collected in a way that directly or reasonably links the data to a specific vehicle or person; and*

g. ***Accountability**: take reasonable steps, through such activities as evaluation and auditing of privacy and data protections in its approach and practices, to ensure that the entities that collect or receive consumers' data comply with applicable data privacy and security agreements.*

3. **System Safety**

Manufacturers and other entities should follow a robust design and validation process based on a systems-engineering approach with the goal of designing HAV systems free of unreasonable safety risks. This process should encompass designing the intended functions such that the vehicle will be placed in a safe state even when there are electrical, electronic, or mechanical malfunctions or software errors.

4. **Vehicle Cybersecurity**

Manufacturers and other entities should follow a robust product development process based on a systems-engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities. This process should include systematic and ongoing safety risk assessment for the HAV system, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation ecosystem. The identification, protection, detection, response, and recovery functions should be used to enable risk management decisions, address risks and threats, and enable quick response to and learning from cybersecurity events. As with safety data, industry sharing on cybersecurity is important. Each industry member should not have to experience the same cyber vulnerabilities in order to learn from them. That is the purpose of the Auto-ISAC, to promote group learning. To that end entities should report any and all discovered vulnerabilities from field incidents, internal testing, or external security research to the Auto-ISAC as soon as possible, regardless of membership. Entities involved with HAVs should consider adopting a vulnerability disclosure policy.

5. **Human Machine Interface**

Understanding the interaction between the vehicle and the driver (commonly referred to as "human machine interface (HMI)") has always played an important role in the automotive design process. Manufacturers and other entities should have a documented process for the assessment, testing, and validation of the vehicle HMI. Considerations should be made for the human driver, operator, occupant(s), and external actors with whom the HAV may have interactions (other vehicles, pedestrians, etc.). HMI design should also consider the need to communicate information to pedestrians, conventional vehicles, and automated vehicles regarding the HAV's state of operation relevant to the circumstance (e.g., whether the HAV system identified a pedestrian at an intersection and is yielding).

6. **Crashworthiness**

   a. ***Occupant Protection:*** *An HAV is expected to meet NHTSA crashworthiness standards, because, regardless of the effectiveness of crash voidance capabilities of an HAV, manufacturers and other entities still need to consider the possibility of another vehicle crashing into them. Furthermore, entities should develop and incorporate new occupant protection systems that use information from the advanced sensing technologies needed for HAV operation to provide enhanced protection to occupants of all ages and sizes.*

   b. ***Compatibility:*** *The expectation of due care also extends to the crash safety performance of non-occupied automated vehicles. These vehicles should provide geometric and energy absorption crash compatibility with existing vehicles on the road. HAVs intended for product or service delivery or other non-occupied use scenarios should conform to vehicle crash compatibility expectations appropriate for that vehicle type.*

7. **Consumer Education and Training**

Manufacturers and other entities should develop, document, and maintain employee, dealer, distributor, and consumer education and training programs to address the anticipated differences in the use and operation of HAVs from those of the conventional vehicles that the public owns and operates today.

8. **Registration and Certification**

NHTSA understands that vehicles may change levels of automation over the vehicle's lifecycle as a result of software updates. As more HAVs are tested and sold commercially to be used on public roadways, older vehicles may be modified to provide similar functionality to new vehicles…Further, manufacturers should also provide on-vehicle means to readily communicate concise information regarding the key capabilities of their HAV system to human drivers and owners of such vehicles.

9. **Post-Crash Behavior**

Manufacturers and other entities should have a documented process for the assessment, testing, and validation of how their HAV is reinstated into service after being involved in a crash.

10. **Federal, State and Local Laws**

Manufacturers and other entities should have documented plans detailing how they intend to comply with all applicable Federal, State, and local laws… Traffic laws vary from State to State (and even city to city); the HAV should be able to follow all laws that apply to its Operational Design Domain. This should include speed limits, traffic control devices, one-way streets, access restrictions (e.g., crosswalks, bike lanes), U-turns, right-on-red situations, metering ramps, and other traffic circumstances and situations. Given that laws and regulations will inevitably change over time, manufacturers and other entities should develop processes to update and adapt HAV systems to address new or changed legal requirements.

11. **Ethical Considerations**

Even in instances in which no explicit ethical rule or preference is intended, the programming of an HAV may establish an implicit or inherent decision rule with significant ethical consequences… it is important to consider whether HAVs are required to apply particular decision rules in instances of conflicts between safety, mobility, and legality objectives.

12. **Operational Design Domain**

The manufacturer or other entity should define and document the Operational Design Domain (ODD) for each HAV system available on their vehicle as tested or deployed for use on public roadways. The ODD should describe the specific operating domain(s) in which the HAV system is designed to properly operate. The defined ODD should include the following information to define HAV systems' capabilities: Roadway types on which the HAV system is intended to operate safely; Geographic area; Speed range; Environmental conditions in which the HAV will operate (weather, daytime/nighttime, etc.); and Other domain constraints.

13. **Object and Event Detection and Response**

Object and Event Detection and Response (OEDR) refers to the detection by the driver or HAV system of any circumstance that is relevant to the immediate driving task, as well as the implementation of the appropriate driver or HAV system response to such circumstance. For purposes of this Guidance, the HAV system is responsible for performing the OEDR while in its ODD and automation is engaged. Entities should have a documented process for assessment, testing, and validation of their OEDR capabilities.

14. **Fall Back (Minimal Risk Condition)**

Manufacturers and other entities should have a documented process for transitioning to a minimal risk condition when a problem is encountered. HAVs operating on the road should be capable of detecting that their HAV systems have malfunctioned, are operating in a degraded state, or are operating outside of their ODD, and of informing the human driver in a way that enables the driver to regain proper control of the vehicle or allows the HAV system to return to a minimal risk

condition independently. Fall back strategies should take into account that—despite laws and regulations to the contrary—human drivers may be inattentive, under the influence of alcohol or other substances, drowsy, or physically impaired in some other manner. Fall back actions should be administered in a manner that will facilitate safe operations of the vehicle and minimize erratic driving behavior. Such fall back actions should also minimize the effects of errors in human driver recognition and decision-making during and after transitions to manual control. In cases of higher automation where a human driver may not be present, the HAV must be able to fall back into a minimal risk condition that may not include a driver. A minimal risk condition will vary according to the type and extent of a given failure, including automatically bringing the vehicle safely to a stop, preferably outside of an active lane of traffic (assuming availability). Manufacturers and other entities should have a documented process for assessment, testing, and validation of their fall back approaches.

15. Validation Methods

Given that the scope, technology, and capabilities vary widely for different automation functions, manufacturers and other entities should develop tests and validation methods to ensure a high level of safety in the operation of their HAVs.

Beveridge & Diamond's Transportation and Infrastructure Projects team, led by Fred Wagner, former Chief Counsel of the Federal Highway Administration, David McCray, counsel for GoMentum Station and former Assistant Chief Counsel at the California Department of Transportation, and James Auslander, is well-versed in the Policy and the federal government's efforts to create a regulatory framework that encourages this game-changing technology. Please contact Fred, David, or Jamie with questions regarding the Safety Assessment or automated vehicles more broadly.