NHTSA Publishes Automated Driving ANPRM

Today the DOT's National Highway Traffic Safety Administration (NHTSA) published an advanced notice of proposed rulemaking in the Federal Register (85 FR 78058-78075) for the "Framework for Automated Driving System Safety". NHTSA is seeking public input on a framework that "would objectively define, assess, and manage the safety of ADS [automated driving system] performance while ensuring the needed flexibility to enable further innovation."

The Framework

In this ANPRM NHTSA is not proposing the establishment of a new Federal Motor Vehicle Safety Standard (FMVSS) for ADS as it is too early in the development process to identify the critical safety characteristics that would be necessary to develop a new FMVSS. Instead, NHTSA intends to develop "a framework approach to safety for ADS developers would use performance-oriented approaches and metrics that would accommodate the design flexibility needed to ensure that manufacturers can pursue safety innovations and novel designs in these new technologies."

In the development of this framework NHTSA plans to focus on four core functions of the ADS. Those functions are:

• How the ADS receives information about its environment through sensors ("sensing"),
• How the ADS detects and categorizes other road users (vehicles, motorcyclists, pedestrians, etc.), infrastructure (traffic signs, signals, etc.), and conditions (weather events, road construction, etc.) ("perception"),
• How the ADS analyzes the situation, plans the route it will take on the way to its intended destination, and makes decisions on how to respond appropriately to the road users, infrastructure, and conditions detected and categorized ("planning"), and
• How the ADS executes the driving functions necessary to carry out that plan ("control") through interaction with other parts of the vehicle.

NHTSA is soliciting comments on these core functions, including:

• Whether commenters agree that these are the core functions,
• Views on NHTSA's description of these functions, and
• Whether and how NHTSA should prioritize its research as it develops a safety framework.

Additionally, NHTSA acknowledges that they have identified eight other aspects of an ADS that could be of specific interest in the development of their framework. Those include:

(1) Identifying reduced system performance and/or ODD in the presence of failure,
(2) operating in a degraded mode within reduced system constraints,
(3) performing the essential task of transporting occupants or goods from starting point to the chosen destination,
(4) recognizing and reacting appropriately to communications from first responders, including fire, EMS, and law enforcement,
(5) receiving, loading, and following over-the-air software updates,
(6) performing system maintenance and calibration,

(7) addressing safety-related cybersecurity risks, and
(8) system redundancies.

NHTSA is soliciting comments on these other aspects of an ADS described above including:

• Which of these aspects the Agency should prioritize as it continues the research necessary to develop a safety framework,
• Whether it has an appropriate role to play with any or all of these elements outside of research,
• Should NHTSA's role be regulatory or sub-regulatory for each element?

Interestingly, the Agency does note that they are not specifically authorized under the Safety Act "to regulate areas such as general privacy and cybersecurity unrelated to safety".

Regulatory Mechanisms

Looking forward, NHTSA recognizes that at some point they will be responsible for regulating ADS safety. In this ANPRM, NHTSA looks at potential regulation mechanisms and sees comments on those topics as well. These proposed mechanisms include:

• Mandatory reporting and/or disclosure,
• NHTSA'S FMVSS setting authority,
• Applying the established FMVSS framework to ADS safety principles, and
• Reforming how NHTSA drafts new FMVSS to keep pace with rapidly evolving technology.

NHTSA provides the following examples of possible regulatory action:

FMVSS requiring obstacle course-based validation in variable scenarios and conditions,
FMVSS requiring vehicles to be programmed to drive defensively in a risk-minimizing manner in any scenario within their ODD [operational design domain],
FMVSS drafted in a highly performance-oriented manner,
Timing and phasing of FMVSS development and implementation,

NHTSA Soliciting Comments

As mentioned above, the Agency is soliciting public comments on this proposed rulemaking. In addition to the comments mentioned above, NHTSA includes 24 specific questions to which it is seeking public input. Comments may be submitted via the Federal eRulemaking Portal (www.Regulations.gov; Docket # NHTSA-2020-0106). Comments should be submitted by February 1st, 2021.

Commentary

NHTSA continues to run a catchup game on the regulation of automated driving systems. Part of that is the normal regulatory inertia that affects any government operation, but the other is the lack of Congressional direction and authorization to operate in a quickly changing technological environment. Having said that, today's ANPRM is a significant next step in NHTSA's effort to keep up with ADS development.

While NHTSA continues to mention cybersecurity in its ADS literature and this ANPRM, I do not think that they are taking the issue seriously enough. Not a single one of the 24 specific questions that NHTSA proposed for response addressed cybersecurity topics.

Furthermore, NHTSA missed the boat by not including a fifth 'core function' for ADS; "Protection". In keeping with the language of the ANPRM, "protection" would refer to the ability of the ADS system to continue to protect the safety of the vehicle's occupants in the event of an electronic failure due to component failure, communication (internal or external) disruption or cyberattack. In process safety terms, this means that the system has mechanisms and protocols in place to ensure that it fails in an inherently safe manner.

I think that it is important for NHTSA to encourage developers to consider system failure modalities early in the development cycle and include development of 'fail safe' mechanisms as a design criterion. As NHTSA moves into the FMVSSA development process it needs to consider identifying common failure modes and specifying minimum standards for engineering responses to those modalities.

This is more than just 'cybersecurity', though it certainly embodies a key component of operations technology cybersecurity, failure mitigation. Cyberattacks are one failure mode that must be considered in the design and development process, but other failure modes must also be addressed. Other failure modes that should be addressed include:

- Loss of signal from external devices,
- Internal communication disruption,
- Physical, mechanical, or electronic interruption of sensors,
- Interrupted or incomplete software updates, and
- Loss of power to either powertrain or electronic systems.

Developers need to demonstrate that they have taken failure mitigation into account in their design process, documenting the failure modes identified and explaining the mitigation measures adopted. Further, they need to have an identified process in place for:

- Detecting new failure modes in development testing and real-world operations,
- Developing appropriate mitigation measures, and
- Communicating those measures to vehicles in the field.

Finally, NHTSA has to have a reporting mechanism in place for reporting newly identified failure modes and the mitigation measures adopted. And NHTSA has to be prepared to (and allowed to) proactively share those failure modes with other ADS and OEM vendors using the same or significantly similar equipment.

A copy of this blog post will be filed as a comment on this ANPRM.