wiley

ALERT

U.S. Department of Transportation Releases Proposed Rulemaking on Vehicle-to-Vehicle Communications

December 19, 2016

On December 14, 2016, the U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) unveiled its long-awaited proposal for requiring vehicle-to-vehicle (V2V) communications technology in all new vehicles, which the agency believes can reduce crashes and save lives. At a high level, the agency proposes to mandate V2V technology using dedicated short-range communications (DSR) for new light vehicles in the United States. NHTSA further proposes to require that all V2V devices must "speak the same language" through standard technology and that privacy and security measures are employed in any V2V device. If adopted, the effective date for manufacturers to begin implementing these new requirements would be two model years after the final rule is adopted, with a three-year phase-in period to accommodate manufacturers' product cycles.

The proposed rules come more than two years after NHTSA first issued an Advanced Notice of Proposed Rulemaking (ANPRM) and research report, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application." In deciding to move forward with a proposed mandate, NHTSA makes a series of notable findings. First, NHTSA suggests that V2V capability will not develop without government intervention. According to the agency, the effectiveness of any V2V communications technology depends on reaching critical mass in the marketplace and interoperability between manufacturers' equipment. Absent regulation, manufacturers may not have sufficient incentive to develop V2V technology to its full potential, because there would be no immediate safety benefits for early adopters.

Practice Areas

Connected & Autonomous Vehicles
Internet of Things
Telecom, Media & Technology

Second, NHTSA expresses its belief that V2V will be able to address crashes that cannot be prevented by current in-vehicle camera and sensor-based technologies ("vehicle resident" technologies). The agency believes that vehicle resident systems will remain complementary rather than competing even as they continue to improve. In the longer term, the agency believes that the fusion of V2V and vehicle-resident technologies will advance the further development of vehicle automation systems, including the potential for truly self-driving vehicles.

Third, although there was a question as to whether the proposed rules would be technology agnostic, NHTSA suggests that DSRC is the only tested and deployable communications technology that can accomplish the goal of improving safety on roadways. According to NHTSA, DSRC has a designated licensed bandwidth to permit secure, reliable communication, and provides very high data transmission rates in high-speed vehicle mobility conditions which are critical for detecting potential and imminent crash scenarios. Some stakeholders previously have suggested that applications envisioned for DSRC-based V2V will be available through evolving cellular technology such as LTE Advanced and 5G; however, NHTSA notes a number of drawbacks of cellular technology for road safety, including: (i) there are still areas where cellular service is not available; (ii) cellular transmission rates slow down if a user is moving or is in a high-capacity area; and (iii) this communication method could introduce security risks.

Finally, NHTSA argues that it has the legal authority to require new vehicles to be equipped with V2V technology and to use it under the Vehicle Safety Act, 49 U.S.C. § 30101 *et seq*. NHTSA has broad statutory authority to regulate motor vehicles and items of motor vehicle equipment and to establish Federal Motor Vehicle Safety Standards (FMVSS) to address vehicle safety needs. The agency estimates the total annual costs to comply with the proposed mandate in the 30th year after it takes effect would range from $2.2 billion to $5 billion, corresponding to a cost per new vehicle of roughly $135-$300.

Comments on the Notice of Proposed Rulemaking (NPRM) are due 90 days after publication in the Federal Register. The NPRM seeks comment on its comprehensive proposal for mandating DSRC-based V2V communications. The proposal includes a pathway for vehicles to comply using non-DSRC technologies that meet certain performance and interoperability standards. In addition, the NPRM seeks comment on regulatory alternatives, including (i) an "if-equipped" standard—instead of a government mandate—which would entail simply setting a conditional standard stating that "if a new vehicle is equipped with devices capable of V2V communications, then it is required to meet the following requirements;" and (ii) requiring that V2V-capable vehicles also be equipped with two safety applications in addition to V2V capability: Intersection Movement Assist and Left Turn Assist. Below, we highlight key aspects of the 392-page NPRM:

Communications Technology. NHTSA's proposal would require that new light vehicles include V2V technology able to transmit standardized Basic Safety Messages (BSMs) over DSRC. Physical and data link layers are addressed primarily by IEEE 802.11p and P1609.4; network, transport, and session layers are addressed primarily by P1609.3; security communications are addressed by P1609.2; and additional session and prioritization related protocols are addressed by P1609.12. The proposal also would require that similarly-capable aftermarket devices achieve the same DSRC performance.

Scope. The NPRM applies to light-duty vehicles: passenger cars, multipurpose passenger vehicles, trucks, and buses with a gross vehicle weight rating of 10,000 pounds or less. NHTSA believes that V2V technology also holds promise for medium- and heavy-duty trucks and buses, and the agency is working with industry to adapt the technology for these vehicles. The Federal Highway Administration also plans to issue guidance for Vehicle-to-Infrastructure (V2I) communications, which would integrate technologies to allow vehicles to communicate with roadway infrastructure.

Performance Requirements. Performance requirements cover (1) what information needs to be sent to the surrounding vehicles; (2) how the vehicle needs to send that information; (3) how a vehicle validates and assigns confidence in the information; and (4) how a vehicle makes sure the prior three functions work in various operational conditions. The NPRM draws from a variety of voluntary standards and also proposes test methods for evaluating many aspects of performance.

- *Message Format and Information*. NHTSA proposes to standardize the content, initialization time, and transmission characteristics of BSM regardless of the V2V communication technology used. Proposed content requirements largely are consistent with voluntary consensus standards SAE 2735 and SAW 2945, which contain data elements such as speed, heading, trajectory, frequency, and other information.
- *Message Authentication*. NHTSA proposes V2V devices sign and verify their BSMs using a Public Key Infrastructure (PKI) digital signature algorithm. NHTSA proposes two alternative approaches. The first is less prescriptive and would require only that a receiver of a BSM message must be able to validate the contents of a message such that it can reasonably confirm that the message originated from a single, valid V2V device, and the message was not altered during transmission. The second alternative stays silent on a specific message authentication requirement. BSMs would still be validated with an integrity check and be passed through a misbehavior detection system.
- *Misbehavior Detection and Reporting*. NHTSA proposes to mandate requirements that would establish procedures for communicating with a Security Credential Management System to report misbehavior and learn of misbehavior by other participants. This approach enhances the ability of V2V devices to identify and block messages from misbehaving and malfunctioning V2V devices. An alternative proposal imposes no requirement to report misbehavior or implement device blocking. However, implementers would need to identify methods that check devices' functionality, including hardware and software, to ensure that the device has not been altered or tampered with.

Cybersecurity. NHTSA's vehicle cybersecurity approach is built upon the following principles: (1) risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information; (ii) timely detection and rapid response to vehicle cybersecurity incidents in the field; (iii) designs-in methods and measures to facilitate rapid recovery from incidents; and (iv) accelerated adoption of lessons learned across the industry through effective information sharing.

- *Hardware Security*. NHTSA proposes that V2V equipment be "hardened" against intrusion (FIPS-140 Level 3).

- *Software and Security Certificate Updates*. NHTSA proposes that V2V devices allow for over-the-air (OTA) software and certificate updates and that device users be notified of any consent required for periodic updates.

Consumer Privacy. V2V systems would be required to be designed from the outset to minimize risks to consumer privacy. The NPRM proposes to exclude from V2V transmission information that directly identifies a specific vehicle or individual regularly associated with a vehicle, such as owner's or driver's name, address, or vehicle identification numbers, as well as data "reasonably linkable" to an individual. The NPRM contains additional privacy and security requirements with which manufacturers would be required to comply.

Safety Applications. The agency does not propose to require specific V2V safety applications at this time.

Effective Date. The agency is proposing that the effective date for manufacturers to begin implementing these new requirements would be two model years after the final rule is adopted with a three-year phase-in period: 50 percent of vehicles three years after final rule; 75 percent four years after final rule; and 100 percent five years after final rule.