SQUIRE PATTON BOGGS

A Brave and Safer New World: NHTSA Proposes Rules Mandating Vehicle-to-Vehicle Communications to Promote Safety

On December 13, 2016, the US Department of Transportation's National Highway Traffic Safety Administration (NHTSA) released a proposal to mandate the deployment of vehicle-to-vehicle (V2V) communications technology in all new US light-duty vehicles, such as passenger cars. NHTSA's eagerly anticipated proposal – set forth in a nearly 400-page Notice of Proposed Rulemaking (NPRM) – is the first of its kind worldwide. It sets the stage for the rapid deployment of technologies with the "potential to revolutionize motor vehicle safety." Communications among vehicles on the road could significantly reduce the number of motor vehicle crashes.

Car Talk – Understanding Vehicle-to-Vehicle Communications

V2V is a "crash avoidance technology that relies on communication of information between nearby vehicles to warn drivers about potentially dangerous situations that could lead to crashes." V2V works by using dedicated short range communications (DSRC) technology to send so-called "basic safety messages" containing certain vehicle information – such as path prediction and the location, speed and breaking status of other cars – to determine whether to warn a driver, thereby mitigating the risk of a possible crash. NHTSA predicts that the technology could save between 955 to 1,321 lives annually. The agency also estimates V2V annual costs at US$2.2 billion to US$5 billion (approximately US$135 to US$301 per vehicle). In comparison, the cost savings of V2V use are estimated at US$53 billion to US$71 billion.

The Proposal in Brief – What Is On the Table

NHTSA's proposal builds upon an earlier advance notice of proposed rulemaking and research report issued by the agency in 2014, and incorporates input gathered over more than a decade from major stakeholders, including the "automotive industry, state and local transportation departments, and academic institutions to prove out and develop consensus standards that support a coordinated, national deployment of V2V technology."

Under NHTSA's proposal, interoperability is critical to the success of V2V: in order for V2V to work properly, cars need to "speak the same language." Specifically, "vehicles need to communicate a standard set of information to each other, using interoperable communications that all vehicles can understand." Failure to ensure interoperable communications might also stifle innovation if manufacturers' cars can only communicate within brand.

NHTSA's proposal also rests on the foundation that a critical mass of cars communicating with one another on the road is vital. According to the NPRM, "V2V can only begin to provide significant safety benefits when a significant fraction of vehicles comprising the fleet can transmit and receive the same information in an interoperable fashion." Put another way, the more people who purchase vehicles with V2V communications, the more significant the network of cars with the ability to communicate with one another and prevent accidents. NHTSA explains that if consumers believe others are not investing in V2V technologies, they will also be less likely to invest. Finally, without a government mandate to deploy and continue to improve upon V2V communications, NHTSA asserts that manufacturers will "inevitably face changing economic conditions and perhaps imperfect signals from vehicle buyers and owners" based on incomplete information about V2V's safety benefits, which could disincentivize automakers from further V2V investment.

While NHTSA seeks comment on a number of alternative approaches, the proposed rule as currently structured would require V2V systems meeting certain core performance-based standards:

- DSRC technology, which sends and receives Basic Safety Messages (BSMs) between vehicles equipped with V2V technology
- Standardized content for message format and information based on previously released standards
- V2V device signature and verification of BSMs using Public Key Infrastructure
- Communication with a Security Credential Management System to report misbehavior, which would allow V2V devices to block messages from defective or malicious devices
- A heightened level of hardware security to prevent others from appropriating a device's security credentials
- "Security by Design" measures that would prevent V2V devices from transmitting information linked – or linkable – to a specific car or consumer

V2V functionality, once deployed, would mitigate the risk of crashes and save lives. V2V applications include:

- Intersection movement assist, which "warns the driver when it is not safe to enter an intersection because of high potential for colliding with one or more vehicles"
- Left turn assist, which "warns the driver there is high probability they will collide with an oncoming vehicle when making a left turn"
- Emergency electronic brake light, which "warns the driver to be prepared to take action when a V2V-equipped vehicle travelling in the same direction but not in the driver's line-of-sight decelerates quickly"

- Forward collision warning, which "warns the driver of the risk of an impending rear-end collision with another vehicle ahead in traffic in the same lane and direction of travel"
- Blind spot warning, which "provides the driver of a vehicle that a vehicle in an adjacent lane is positioned in a vehicle's 'blind spot' zone"
- Lane change warning, which "warns the driver of a vehicle during a lane change attempt if a vehicle is present or a vehicle is approaching and will be entering the 'blind spot' zone"
- "Do not pass" warning, which "warns the driver that it is not safe to pass a slower-moving vehicle because the vehicles are approaching from the opposite direction"

However, NHTSA is not proposing that specific safety applications using V2V technology be required.

The Details – Proposed New Federal Motor Vehicle Safety Standard No. 150

NHTSA proposes to create Federal Motor Vehicle Safety Standard (FMVSS) No. 150, which would require the deployment of, and create communication performance requirements for, V2V technology operating on DSRC spectrum.

V2V Communications. V2V communications would include a number of elements: "radio technology for the transmission and reception of messages, the structure and contents of 'basic safety messages' (BSMs), the authentication of incoming messages by receivers, and, depending on a vehicle's behavior, the triggering of one or more safety warnings to drivers."

Reliance on DSRC Technology. The FCC has allocated the 5.850-5.925 GHz band (5.9 GHz Band) for DSRC use. NHTSA's proposed rule relies heavily on the use of DSRC to ensure fast and reliable BSMs.

V2V technologies operating on DSRC employ omnidirectional radio signals that provide 360 degree coverage and a range of approximately 300 meters, which "exceeds the capabilities of ultrasonic sensors, cameras, and radar" and other vehicle-resident technologies by nearly double. The practical implication is that with DSRC, drivers have more warning time and additional visibility "around corners and 'through' other cars."

While current automated systems rely on so-called "vehicle-resident" technologies like sensors and cameras, NHTSA explains that "data acquired from GPS and telecommunications like V2V could significantly augment such systems." Indeed, combined with other technologies, V2V communications operating on DSRC can improve the accuracy of these more traditional predictive safety systems in a way that is impossible with existing radar or camera technology alone. Also, BSMs sent by DSRC technologies can be "updated and broadcast up to 10 times per second by surrounding vehicles" also equipped with V2V capabilities.

Under NHTSA's proposal, BSM content would be governed by pre-existing standards developed by the Society of Automotive Engineers (SAE) – specifically, SAE 2735 and SAE 2945 – and would contain data such as speed, heading and trajectory, using standardized, common language.

Of immediate concern to manufacturers is the Federal Communications Commission's (FCC) current proceeding to consider sharing the DSRC spectrum with unlicensed technologies, such as Wi-Fi. Commenters have expressed serious concerns over the potential for interference to DSRC's life-saving technologies from unlicensed users of the spectrum. The FCC has begun testing to determine whether DSRC can operate and perform its core, life-saving functions free from interference if the DSRC spectrum is, in fact, shared by unlicensed users.

The NPRM also contemplates that alternative technologies that perform similar to – and that have the ability to communicate with – DSRC also be permitted. As a result, NHTSA proposes to require that any V2V device be capable of operating with a "standardized messaging set co-developed with the automotive industry, and academic institutions and recently finalized via a Society of Automotive Engineers (SAE) standard."

Anonymous Autonomous – Security and Privacy Measures

In an age of increased cybersecurity awareness, NHTSA proposes that V2V devices incorporate substantial privacy and security measures. That proposal is consistent with the approach outlined in NHTSA's 2014 research report, which was based on the implementation of Public Key Infrastructure (PKI). According to the NPRM, PKI in this context comprises three major elements: (1) a Security Certificate Management System (SCMS) that "issues, distributes, and revokes security credentials for devices" and that also reports misbehavior; (2) V2V devices that "send/receive messages to/from the [SCMS] for digital security credentials that provide the means of message authentication"; and (3) a communications network that "facilitates two-way encrypted communications between an SCMS and a device." NHTSA would also require that manufacturers deliver "over-the-air" security and software updates.

Finally, information gathered from V2V technologies will have some level of anonymity; V2V devices will be prohibited from operating such that they "collect, broadcast, or share information linked or linkable . . . to individuals or their vehicles." Interestingly, NHTSA and auto manufacturers will be able to identify malfunctioning V2V devices absent any personally identifiable information.

While the agency chose not to require a specific safety application in the NPRM, it does note that any safety application chosen must be able to distinguish legitimate messages from those delivered by defective devices or bad actors. Notwithstanding the approach adopted in the NPRM, NHTSA also seeks comment on alternative approaches to message authentication.

V2V to HAV – What Is the Relationship Between These Automation and Communication Technologies?

Although V2V and highly automated vehicle (HAV) technologies are separate and distinct, NHTSA asserts that they are "highly complementary to each other." There is general consensus among industry stakeholders that automated driving functions – like adaptive cruise control and automated emergency braking – are enhanced and could provide additional assistance in mitigating the risk of crashes when working with V2V functionality. Because NHTSA's proposed rule will require that V2V be deployed in all light-duty vehicles, including highly automated vehicles, we are likely to see the benefits of the two technologies working together sooner rather than later.

What Is Next?

NHTSA proposes that manufacturers begin implementing the requirements "two model years after the final rule is adopted" with phase-in occurring over three years. Thus, for a rule issued in 2019, phase-in would begin in 2021, and compliance with the rules would be required by 2023.

Interested parties have until March 13, 2017 (90 days from the release of the NPRM) to respond by submitting comments directly at www.regulations.gov. We encourage you to reach out to us to share your thoughts on what these proposed rules mean to you and in what direction you think the rules should go.

Regardless of how the final rules appear, it is safe to say that with this proposal, we are indeed entering a brave new world with safer technologies.

Contacts

Rodney E. Slater
Partner, Washington DC
T +1 202 457 5265
E rodney.slater@squirepb.com

Robert Kelly
Partner, Washington DC
T +1 202 626 6216
E robert.kelly@squirepb.com

David Rice
Partner, San Francisco
T +1 415 743 2419
E david.rice@squirepb.com

Timothy H. Goodman
Principal, Washington DC
T +1 202 457 6140
E tim.goodman@squirepb.com

Koy Miller
Associate, Washington DC
T +1 202 457 5321
E koyulyn.miller@squirepb.com

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.