The Policy

Synopsis

On January 12, 2017, the National Highway Traffic Safety Administration (NHTSA) and Department of Transportation (DOT) released a proposed mandate titled Federal Motor Vehicle Safety Standard (FMVSS), No. 150. This mandate would require all new light vehicles (i.e. most cars, trucks, and buses that weigh 10,000 pounds or less), after the year 2023, to be equipped with vehicle-to-vehicle (V2V) communications.
communication technology, as well as the standardization of the message and format of transmissions. According to the report’s executive summary [12], “the proposed rule ushers [in] a new era of vehicle safety.” V2V communication would accomplish this goal by preventing hundreds of thousands of crashes, as predicted, through various specific safeguards, such as “Intersection Movement Assist (IMA), Left Turn Assist (LTA), Forward Collision Warning, Blind Spot Warning/Lane Change Warning, Enhanced Emergency Brake Warning, and Do Not Pass Warning”.

Based on the NHTSA report, a majority of police-reported motor vehicle crashes (62%, or 3.4 million, to be precise) are classified as light-vehicle to light-vehicle. In order to significantly reduce this number, the report proposes that vehicles send Basic Safety Messages (BSMs) to each other, hence the term vehicle-to-vehicle communication. By ensuring constant communication between the user’s personal vehicle and the vehicles around it via BSMs, the vehicle would be able to predict collisions before they occur.

At a macro level, the NHTSA predicts that – at full adoption – V2V communication would, on an annual basis:

- Prevent between 439,000 and 615,000 crashes
- Save 987 to 1,366 lives
- Reduce 305,000 to 418,000 injuries
- Avert damage to 537,000 – 746,000 vehicles

This is not to say that there are not costs to the benefits. According to this report, on average and at full adoption, the total annual costs to industry will be a hefty range – from $3.804 billion to $4.717 billion; this comes out to between $196.20 and $243.27 per vehicle, an expense which should not be ignored.

Lastly, looking at the specific methods of the NHTSA’s analysis, which comprises most of the report, an overall strong case has been made for the required implementation of V2V across light vehicles. The annual benefits – crashes averted, lives saved, and damage/injuries prevented – are all calculated based on the NHTSA’s projections of V2V adoption, starting in 2021 through 2060. Additionally, in order to calculate net benefits, the NHTSA utilized a wide range of potential discount rates: the low end being 3% and high end as 7%. Lastly, the NHTSA also conducted an uncertainty analysis to provide alternative benefit calculations, in the case that adoption rates, costs, etc. do not align with the current projections.

**Context**

In 2009, the Research and Innovative Technology Administration (RITA) – a subset of the DOT, and now housed under the Office of the Assistant Secretary for Research and Technology [13] (OST-R) – released an annual Intelligent Transportation Systems (ITS) strategic plan, which was the first widely-publicized look into the DOT’s plan for connected vehicles. Subsequently, in July of the following year, RITA released a Policy Roadmap [14] on IntelliDrive, the DOT’s Connected Vehicle Research program, and held a three-day workshop [15] in Chicago centered to discuss these issues in the following weeks.

Though the DOT ended up dropping the term “IntelliDrive” in early 2011, the Connected Vehicles research being done by DOT, as a part of ITS, continued to remain the main focus. Soon thereafter, on July 6, 2012, President Obama signed into law the Moving Ahead for Progress in the 21st Century Act [16] (MAP-21).
MAP-21, a two year transportation reauthorization bill, worked to reinforce and reinvigorate ITS “by restoring the … research budget to $100 million per year and establishing a Technology and Innovation Deployment Program for $62.5 million per year” (DOT’s History of ITS, 2016, pg. 33).

In February of 2014, then-Secretary of DOT Anthony Foxx announced that DOT would expedite its V2V work. Shortly thereafter, in August of 2014, the NHTSA “released an advance notice of proposed rulemaking (ANPRM) and a supporting comprehensive research report on V2V communication technology” (DOT’s History of ITS, 2016, pg. 33). The following month, the Highway Loss Data Institute’s Predicted Availability of Safety Features on Registered Vehicles Bulletin Vol. 31, No. 15 found that “Government mandates could speed up the market penetration rate of partially automatic crash avoidance technologies by up to 15 years” (NHTSA, 2017, pg. E - 28). Finally, building upon the ANPRM and accompanying research report, the NHTSA and DOT released the aforementioned proposed mandate – FMVSS, No. 150.

The Science

Learn About the Science

- Sensors for Automated Vehicles
- Connected Cars
- Autonomous Vehicle Data Generation and Sharing

Science Synopsis

The NHTSA report concentrates on multiple types of communication – be it vehicle to vehicle (V2V), vehicle to device (V2D), or more. All these different types of communication between vehicle and “blank” are known in industry as vehicle to everything (VX) communication.

As defined by the SciPol Science Explainer on Connected Cars, “V2X communication is the transfer of information between vehicles and any entity (i.e. a road-side rainmeter) that may affect it or that it may affect (i.e. signaling to cars to decrease speed due to slippery road). This communication would be powered by a network technology that connects all devices, creating constant communication between vehicles and other technology.” V2V communication, more specifically, is defined as “the transfer of information from the vehicle to other vehicles. This communication is primarily short range and may allow vehicles to share information about speed and acceleration to speed up traffic flow, warn each other about dangers that other vehicles cannot yet perceive, or detect each other around turns or intersections before vehicle sensors themselves can detect each other.”
Dedicated Short Range Communication (DSRC) technology, proposed by the NHTSA as the conduit for V2V communication, is a wireless, radio-based communication medium for V2V (and/or V2X) communication. As defined in the SciPol Science Explainer [23], “DSRC is designed for short or medium range communication between vehicles and other vehicles or infrastructure. Radio signals are transmitted through on-board units (OBUs) on vehicles or roadside units (RSUs) on infrastructure. DSRC is expected to come before 5G since it requires less extensive infrastructure, but it is unclear whether it will be used as the primary communication network or as a supplementary network once 5G is ready.” Just for reference, “fifth generation networking (5G) is the next generation of wireless networking designed to replace 4G LTE. Since this network will have improved capacity for data collection, storage, and processing, it will be the first wireless network able to support V2X communication.” Because it is up to the various cell carriers, and other entities, as to when 5G is rolled out nationwide, DSRC looks to be the most viable medium at this point.

There are a few distinct advantages of DSRC, and V2V communication in general. First, it is simply the fact that inter-car communication does not exist. It does not matter how advanced the LiDAR or other sensors are on a user’s car, they simply are not able to receive data from other cars themselves and process it; current technology only allows a car to process what it can “see” via sensors. Second, all autonomous vehicle sensors have physical limits; for example, they simply can’t “see” through a building, predict cars coming from the right or left at an intersection, or sense the car in front of the user’s car suddenly braking. DSRC, on the other hand, “has a 300-meter transmitting range and a 360-degree unobtrusive detection angle that surpass[es] the sensing capability of sensors, cameras, and radars currently used in vehicles” (NHTSA, 2017, pg. E-3). The NHTSA report does emphasize, though, that V2V communication would be used in conjunction with vehicular sensors – complementary technologies, not in lieu of.

Looking to the security aspects of transmitting BSMs via DSRC, the NHTSA proposed a Security Credential Management System (SCMS) – a type of Public Key Infrastructure (PKI) – to ensure that third parties do not interfere with the V2X transmittance. Connecting keys/digital signature services back to the messages which will be transmitted to and from vehicles (V2X communication), by using a PKI system, the keys/digital signature services will specifically be what prevents outsiders (i.e. hackers) from sending factitious/inauthentic messages via DSRC in order to cause harm. PKI systems work by using keys and digital signature services in order to keep BSMs secure. Keys [25] are a type of cryptography in which the “public key” encrypts the material which needs to be hidden – in this case, a vehicle’s BSM, and the “private key”, held by another entity – generally the vehicle receiving the message, is used to decrypt the hidden material. In addition, it is simply impossible to decipher the the private key based on the public key, hence why, once material is secured using the public key, it is impossible to access. Digital signature services are similar to keys where there is a signing and verifying protocol respectively. In this case, the documents will have a digital signature attached; if the digital matches what the server was expecting, then the document can be accessed, else it will remain secure.

**Scientific Assumptions**

- The benefits of connected cars assume high-fidelity sensors on vehicles. It is common for people to assume
that, in order to have successful self-driving capability, cars require high-cost lidar[26]. This is an invalid assumption, because the average cost to cars for the implementation of V2V communication will be approximately $200.

- **DSRC provides robust performance.** A general assumption of the public is that DSRC, because it is similar to wifi/cellular technology, will experience drop outs at certain times or in certain rural places. "DSRC has low latency required for safety applications," says Debby Bezzina[27], managing director of the DOT Center for Connected and Automated Transportation at the University of Michigan Transportation Research Institute (UMTRI). "It’s very robust, secure and ready for production. You don’t have dropouts with DRSC like you have when using your cellphone."

- **Human augmented vehicles are the future.** Though the NPRM from the NHTSA does not make clear how much of the proposed V2V technology will be kept under the hood, as opposed to at the operator’s controls, the current assumption is that it will be mainly a background process. Human augmented vehicles are the next step[28] after V2V is implemented. Before it happens, though, "there are numerous barriers, both human-related and technology-related, that the industry must overcome to guarantee effective communication between the autonomous driving system and humans internal and external to the vehicle."

### Relevant Experts

**Michael Clamann, PhD, CHFP** [29] – Dr. Clamann is the Senior Human Factors Engineer at the University of North Carolina’s Highway Safety Research center. He researches how advancing technology can help reduce human error on our roadways; his areas of expertise include human-automation interaction and autonomous vehicle technology.

"While the spectrum dedicated to DSRC messages was allocated almost 20 years ago, automakers have been slow to adopt V2X technology. Without broad federal, state and/or local funding, or demonstrated advantages over 5G in terms of performance and cost, the future of DSRC remains uncertain."


### The Debate

**Scientific Controversies / Uncertainties**

The reception by the vehicle industry, technology corporations, and the populace at large of V2X Communication has been positive overall (an overwhelming majority). When the report was released by the NHTSA, there was a 90 day comment period, where anyone could submit their opinion via Regulations.gov. By the deadline of April 12, 2017, there had been a total of 465 comments submitted. Analyzing these comments along with various articles and blogs published online, there are a few points of controversy which popped up repeatedly:

1. **Various “health reasons” cited:** This issue was only found in the actual comments on Regulations.gov, but the majority of negative comments surrounded the microwave frequency electromagnetic fields which people would be exposed to by V2V technology, which they claimed would harm people. Many times, commenters also cited
electromagnetic hypersensitivity – a.k.a. “Wi-fi Allergy” – which is pseudomedical diagnosis and not an actual condition [31]/disease recognized by medical professionals.

2. Privacy Issues: Despite the NHTSA report having an emphasis on the security of data when it is transmitted, people cited privacy issues and potential implications of the data being leaked. Many also mentioned the general distrust in companies and/or governmental institutions having access to vehicular data.

3. Security Concerns: Similar to privacy issues, another common worry is that – if vehicular data is stored in the cloud – hackers would be able to get their hands on the vehicular data. In addition, another common problem brought up was simply the potential hacker interference with V2V communication while the cars are in motion.

Endorsements & Opposition

Endorsements:

- American Automobile Association (a.k.a. AAA or “triple-A”), Regulations.gov submitted PDF [32], April 13, 2017: “AAA endorses NHTSA’s proposal to establish a new Federal Motor Vehicle Safety Standard that will require all new vehicles to be equipped with dedicated short-range communications (DSRC) technology.”
- Cisco Systems, Inc. (Fortune 100 technology company), Regulations.gov submitted PDF [33], April 13, 2017: “Cisco Systems, Inc. hereby … support[s] … the proposed new Federal Motor Vehicle Safety Standards (FMVSS) No. 150 to add vehicle-to-vehicle (V2V) communications for new light vehicles, and to standardize the message and format of V2V transmissions.”
- National Transportation Safety Board (NTSB), Regulations.gov submitted PDF [34], March 31, 2017: “The NTSB enthusiastically supports this proposed rulemaking and believes that V2V technology will reduce crashes, injuries, and fatalities on our nation’s highways, and enhance the capabilities of currently available collision avoidance and automated technologies.”

Opposition:

- General Motors LLC, Regulations.gov submitted PDF [35], April 13, 2017: “While GM generally supports the proposed FMVSS equipment mandate, GM has some specific concerns and suggestions with the proposal …” and GM went on to five distinct points of concern/suggestion.

Other Reactions:

- United States Senators John Thune (Chairman), Cory A. Booker, and Marco Rubio of the U.S. Senate Committee on Commerce, Science, and Transportation, Regulations.gov submitted PDF [36], December 20, 2016: The letter supported the proposal overall, but offered approximately 1.5 pages of suggestions on the radio band for Dedicated Short Range Communications (DSRC).
- Waymo LLC (formerly the Google Self-Driving Car Project), Regulations.gov submitted PDF [37], April 25, 2017: They “recognize that such [V2V] communications may provide safety benefits,” but did offer criticism on the following specific matters – “GPS accuracy and gaps, Security issues, Addressing changes in V2V capability, and Mandated safety applications.”

Potential Impacts

There are many impacts which would come out of the proposed V2V mandate. Below are some of the most significant ones:
Decrease traffic jams: Whenever there’s a choke-up in traffic, V2V communication would allow for the cars to work together [38] – in essence – to spread out the cars, giving enough people alternate routes so that the congestion decreases. To quantify the socioeconomic impact of this, the average driver in a big city spends over 50 hours in traffic and loses approximately $2,000 [39] on an annual basis due to being stuck in traffic. With a significant decrease in traffic jams, the average time in traffic and money lost could be cut in half! This also isn’t even taking into account the increased lifespan of brake pads, less stress from being in bumper-to-bumper traffic, more time at work (better workplace efficiency), decreased road maintenance costs, and other beneficial factors which are hard to quantify.

Increase mileage over longer distances: Platooning [40], where multiple vehicles travel in a line at the same speed, would make driving more efficient for cars. The vehicles would be able to communicate with each other via V2V in order to accomplish this.

Increased safety features, as mentioned above: This would include, but isn’t limited to, Intersection Movement Assist, Left Turn Assist, Forward Collision Warning, Blind Spot Warning/Lane Change Warning, Enhanced Emergency Brake Warning, and Do Not Pass Warning. In addition, there is also much potential to increase the safety of road travel via V2I. This could include: [41] “warning drivers about congestion, accidents, slippery patches of road, sharp turns, etc.; merging assist; intersection safety; alerting drivers if they veer too close to the road’s edge.”

Adoption severely delayed without mandate: Without a government-supported mandate, such as the proposed FMVSS 150, the adoption of V2V communication would be entirely at the discretion of the manufacturer. This would most likely result in high-end, expensive cars adopting the technology first, while lower-end car manufacturers implement the technology down the line. Lastly, a Government mandate sets an enforced industry standard of communication and security, which only it has the power to do.

Privacy Issues with V2V/V2X Technology: The NPRM does have an emphasis on deterring and preventing the malicious use of V2V technology. For example, all V2V communication will be on an explicit channel which the FCC created in 2003 specifically for V2V. Additionally, the NHTSA has proposed that a Public Key Infrastructure [42] (PKI) be used in order to verify the authenticity of BSMs. Despite all the precautions the NHTSA has outlined to keep V2V data secure, there are a whole host malicious uses which could be possible; this would include – but isn’t limited to – snooping on the location of vehicles, sending false information (about road conditions, other drivers), using the data to blackmail users, selling the data for profit, and more.

Legal Implications: Another point of concern is that the Federal Government would potentially be able to have access your location and speed information. If this is the case, people’s primary worry is that it’d be very easy to ticket cars for speeding violations or other traffic violations.

Recommended Citation


License Info

[44] This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License [45]. Please distribute widely but give credit to Duke SciPol, linking back to this page if possible.