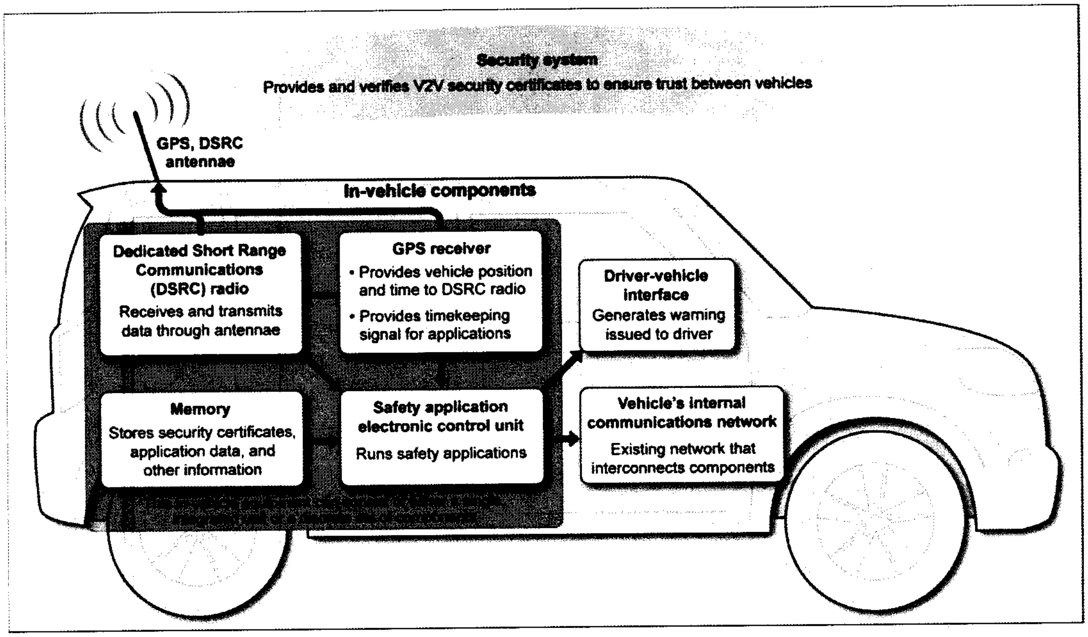
Figure V-1 In-Vehicle Components of a V2V System



Sources: Crash Avoidance Metrics Partnership and GAO.

a) Production feasibility of vehicle-based components

The Safety Pilot Model Deployment hardware consists of pre-competitive, prototype components—some that would be required for a production implementation and others that would not. For example, the extensive data acquisition systems, which are used to log driver behavior and vehicle information, collect information that is used only for the needed post-test analysis. Most likely, they would not be needed by the agency if the V2V system was deployed in mass production.

However, many components being used in the Model Deployment could be leveraged to develop products further for full scale production. In some cases, prototype components used in the Safety Pilot have the appearance and packaging of what could be a regular production device. NHTSA's current understanding, based on discussions with industry OEMs and suppliers, is that securing and preparing manufacturing facilities is the major factor to transitioning from building prototype components to ramping up to produce mass market components, and that the device in its current form is nearly production-feasible today.

A minor condition for production feasibility is the need for automotive-grade DSRC microchips for devices that would be permanently mounted in a vehicle (e.g., integrated OEM or aftermarket retrofit devices). Automotive grade components are usually certified to more stringent environmental conditions and quality (defects per parts per million) requirements than consumer electronics. Each vehicle manufacturer has its own set of specifications for the components it purchases for the vehicles it produces. Automotive grade components must be able to operate in more extreme conditions such as temperature, vibration, and electro-magnetic interference that go beyond the conditions for typical consumer grade components. The Safety Pilot employs prototype DSRC microchips that are based on consumer grade components that are custom-modified to be DSRC-capable. Actual DSRC chips will need to be developed for production and qualified as automotive grade components. As the prototype microchips are based on existing consumer grade wireless microchips with minimal modification, the agency believes feasibility for these components moving to production should not be an issue to move forward.

b) Projected availability of vehicle-based components

Discussions with equipment suppliers have indicated that there is the potential to have an adequate supply of readily available, mass-produced, internal components for a V2V device approximately 2.5 to 3 years after NHTSA moves forward with some type of regulatory action.[121]

4. Non-vehicle-based hardware

In addition to the vehicle-based V2V components, a V2V system also requires equipment to be located along roadsides and, if expanded V2I capabilities are sought, to be embedded in other infrastructure support equipment such as traffic signals or stop signs.

Roadside equipment is the term used to refer to the physical wireless communications infrastructure that supports communication between the vehicle and the SCMS, and between the vehicle and V2I applications. There are two types of RSEs with which a vehicle can communicate: RSEs that serve as a wireless communications link between the vehicle and the SCMS so that the vehicle can receive new security certificates, report misbehavior, and receive CRL updates, and RSEs that broadcast messages needed to support V2I applications. The equipment necessary to support both functions can be located within one RSE device. RSEs could employ DSRC, or could potentially use some other communications medium such as existing 3G/4G cellular networks or Wi-Fi.

a) External equipment used in Safety Pilot

There are 26 DSRC-equipped roadside units being used to support the Safety Pilot Model Deployment program. The DSRC RSEs used in the Model Deployment are all technically capable of both storing and forming messages to support V2I applications and to support communications between OBE and the SCMS.[122] Specifically, the Model Deployment program

---

[121] Preliminary estimates are based on confidential information provided by two suppliers.

[122] All RSEs used in the Safety Pilot Model Deployment conformed to "5.9GHz DSRC Roadside Equipment" Device Specification Version 3.0. See www.its.dot.gov/safety_pilot/pdf/T-10001-T2-05_RSE_Device_Design_Specification_v30.pdf (last accessed Feb. 7, 2014).

is evaluating DSRC RSE devices that allow vehicles to receive updated security certificates[123] and messages to support V2I applications (SPaT, curve warnings, and curve speed warnings). The Model Deployment is also evaluating the use of existing 3G/4G cellular networks to provide vehicles with updated security certificates, because DOT wanted to examine the feasibility of supporting communications between vehicles and the SCMS though an existing communications infrastructure. While it is important to note that a nationwide network of RSE DSRC devices does not exist at this time and Congress has yet to allocate funds to build such a network, existing 3G/4G cellular networks could potentially be used to support communications between vehicles and the SCMS in the event that a nationwide network of RSE devices is not available.

b) External equipment needed for widespread deployment

In a widespread deployment scenario, NHTSA expects much more communication between vehicles and the SCMS than has occurred in the context of the Safety Pilot. For communications to support the security system, the data will be exchanged between the OBE and the SCMS using the well-known Internet Protocol (IP). The basic transaction will be that the OBE will send a request message bearing the SCMS IP address to the RSE, and the RSE will forward this to the backhaul,[124] where it will eventually be routed to the SCMS following the conventional Internet routing process. It is estimated that around 19,000 roadside DSRC units would be needed to support communications between vehicles and the SCMS under the current security framework.[125]

C. Overview of software enabling system operation

V2V communications is based on the wireless exchange of messages between vehicles. The messages provide information that a device can then use to provide a warning about potential danger through a safety application. Fundamentally, the basic hardware of a DSRC device is analogous to a common radio that not only receives information but transmits data as well. As a result the "core" of a DSRC device will be the software that gives devices the "intelligence" needed to determine and transmit current vehicle conditions and perform the necessary evaluations to potentially issue a warning. At the most basic level, a device will require low-level components to both transmit and receive the basic safety message; a relatively simple operating system; connection to a driver-vehicle interface; and algorithms to control the issuance of warnings (along with continual device diagnosis).

---

[123] The security system used in Safety Pilot Program did not involve distribution of a CRL but used a "test" CRL to prove transmittal, receipt, and action.

[124] "Backhaul" is a term used to refer to all telecommunications infrastructure, such as fiber optic cables and routing switches, needed to support IP protocol transactions.

[125] Communications Data Delivery System Analysis for Connected Vehicles: Revision and Update to Modeling of Promising Network Options, at 31 (Booz Allen Hamilton, Inc., May 2013). [Hereafter, "BAH CDDS Final Report"]. See Docket No. NHTSA-2014-0022.

Overall, both vehicle manufacturers and consumer electronic device manufacturers have years of significant experience developing similar software for the myriad devices and products they produce. They are skilled at managing suppliers to develop these components or, in some cases, developing device software in-house as part of their core intellectual property.

V2V devices present a new challenge to the agency regarding software and potential regulatory action. NHTSA's FMVSSs are generally performance-based, but the agency has not yet attempted to regulate software using performance tests, and software is increasingly pervasive in today's vehicles. The agency will need to consider carefully how to develop appropriate tests to regulate the software-based aspects of V2V communications and safety applications. NHTSA's research program concerning vehicle automation includes research into how the agency might regulate safety-critical software.

D. Interoperability

1. Interoperability and its importance

In order for the information in a V2V communication to be useful, it must be received timely, it must be reliable, and it must be transmitted in a standard format. Vehicles participating in the V2V communications network communicate with other connected vehicles using standardized DSRC message types broadcast on a standardized network, IEEE 1609.4, over a standardized wireless layer, IEEE 802.11p.[126] DSRC provides local-area, low-latency[127] network connectivity, and is generally intended to support broadcast messaging between vehicles and between vehicles and roadside access points. It is a variant of Wi-Fi that allows nearly instantaneous network connections, as well as broadcast messaging that requires no network connection. It uses 75 MHz of spectrum located in the 5.85 to 5.925 GHz frequency band.[128] Vehicles currently use channel 172 to transmit messages that support safety of life applications. Interoperability, in short, is the ability for different devices using V2V systems sourced, manufactured, and installed by various OEMs and aftermarket retailers to communicate with each other in a reliable and timely manner. If devices from different sources fail to "speak the

---

[126] See Section V.D.1.c) below for more information on these standards.

[127] Latency is a measure of the time delay experienced in a system, usually between the sending, and subsequent reception, of information. In communications, the lower limit of latency is determined by the physics of transmitting a message, where the medium (radio, fiber optics, copper wiring, etc.) being used for communications can affect transmission speed. In addition, delays can also be incurred by the addition of data handling protocols, message routing and switching, and a few other smaller factors. For more information, see www.o3bnetworks.com/media/40980/white%20paper_latency%20matters.pdf (last accessed Feb. 25, 2014). DSRC can be considered to be low latency because it consists of point to point communication over very short distances (less than 300 m) with relatively few messaging protocol requirements using radio (in air, radio transmits information at approximately light speed).

[128] This is usually referred to as the 5.9 GHz band.

same language," then the system as a whole will not be "interoperable," and will consequently degrade and break down.

a) Communication between vehicles

V2V communications consists of two types of messages: safety messages and certificate exchange messages. The safety messages are used to support the safety applications, and the certificate exchange messages ensure that the safety message is from a trusted source. The safety messages are transmitted in a standardized format so that they can be read by all other vehicles participating in the network. To satisfy this requirement, each DSRC-equipped vehicle would need to broadcast and receive safety messages in a standardized format and specified performance level in terms of characteristics like accuracy and range.[129] Additional details on standards related to V2V can be found in Section V.D.1.c). The safety messages include information about the vehicle's behavior such as the vehicle's GPS position, its predicted path, its lateral and vertical acceleration, and its yaw rate. The messages are time-stamped so the receiving vehicle knows when the message was sent. This information can be used by other vehicles for a variety of crash avoidance applications.

NHTSA's current research is based on the assumption that the V2V system will use a Public Key Infrastructure (PKI) to authenticate messages, so that other vehicles will trust the m.[130] PKI uses certificates to inform a receiving device that the message is from a trusted source, and it uses cryptography to send encrypted message content. For V2V communications, BSM messages are trusted but not encrypted, while messages that contain security information (e.g., certificates) are trusted and the contents encrypted.[131]

The security system currently being researched for V2V would use a type of cryptography known as "asymmetric cryptography."[132] In asymmetric cryptography, there are two keys that are mathematically linked in such a way that what is encrypted with one key can only be decrypted with the other. Although the keys are mathematically linked, it is extremely difficult to derive one key based on knowledge of the other. This property allows one key, the "public key," to be widely distributed while the other key, the "private key," is held only by the owner. Asymmetric cryptography (both encryption and decryption) is computationally harder

[129] Such as, for example, the parameters as defined in SAE J2735.
[130] BAH CDDS Final Report, at 9.
[131] Certificates decrease latency as compared to encrypting the BSM itself; encrypting the BSM, sending it, and the n the other vehicle receiving, decrypting, and translating it could take longer than what would support effective functioning of the safety applications.
[132] Also known as public key encryption.

than symmetric cryptography and is one of the reasons many security experts believe asymmetric cryptography to be more secure.[133]

Many Internet security protocols use asymmetric cryptography as the basis for their infrastructure. Secure socket layers/transport layer security (SSL/TLS),[134] the protocol used in most secure online transactions, uses asymmetric encryption to authenticate the server to the client, and optionally the client to the server. Asymmetric cryptography is also used to establish a session key. The session key is used in symmetric algorithms to encrypt the bulk of the data. This combines the benefit of asymmetric encryption for authentication with the faster, less processor-intensive symmetric key encryption for the bulk data.[135] The secure form of Hypertext Transfer Protocol is HTTPS, which operates as a PKI system and uses SSL. SSL\TLS also operates on its own as a PKI system, independently of HTTPS. For a further discussion of symmetric and asymmetric cryptography, please see Section IX.

b) Vehicle-to-Vehicle Message Sets

For vehicle communication to succeed among OEM-installed in-vehicle devices and aftermarket devices, communication messages must be standardized so that the devices speak the same language. SAE J2735 is intended to help address this purpose so that all V2V safety applications are built around a common framework. SAE J2735 defines the design specifications for the safety messages, including specifications for the message sets,[136] data frames,[137] and data elements.[138]

---

[133] Symmetric encryption is a very common encryption scheme that many use routinely, possibly without knowing the exact name for it. In fact, before 1973, all known encryption algorithms were symmetric. If the reader has ever "password protected" a .zip file, where the same passphrase (key) is used to both lock and unlock the .zip file, then symmetric encryption was used. Similarly, a "Secret Decoder Ring," where a ring containing 2 sets of alphanumeric strings (located on different halves of the ring) can be rotated relative to each other to develop an encryption scheme, is another example of symmetric cryptology, as the orientation of the two sides of the ring used to encrypt a message is also needed to decode the secret message. One challenge with symmetric cryptography is controlling key distribution so that the key does not fall into unintended hands.

[134] Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a protocol primarily used to encrypt confidential data sent over an insecure network, such as the Internet.

[135] For an overview of SSL/TLS encryption, see http://technet.microsoft.com/en-us/library/cc781476(v=ws.10).aspx (last accessed Jan. 28, 2014).

[136] As defined in SAE J2735, a message is a well-structured set of data elements and data frames that can be sent as a unit between devices to convey some semantic meaning in the context of the applications. A message set is a collection of messages based on the ITS functional-area to which they pertain.

[137] As defined in SAE J2735, from a computer science perspective, data frames are viewed as logical groupings of other data frames and of data elements to describe "structures" or parts of messages used in SAE J2735 and other standards. A data frame is a collection of two or more other data concepts in a known ordering. These data concepts may be simple (data elements) or complex (data frames).

[138] As defined in SAE J2735, a data element is a syntactically formal representation of some single unit of information of interest (e.g., a fact, proposition, observation) with a singular instance value at any point in time,

(1) The Basic Safety Message

The currently-published version of SAE J2735, published in November 2009, is the second version of the standard. It specifies 15 message sets, with Basic Safety Message the most important one.[139]

As explained above, the BSM is used to exchange safety data regarding vehicle state. The message is broadcast routinely to surrounding vehicles with a variety of data content. The BSM is split into two parts to guarantee that the core information for vehicle safety (Part I) has priority and is transmitted more often. It also minimizes the amount of data communicated (most of the time) between devices, helping to reduce channel congestion.

BSM Part I contains the core data elements, such as vehicle position, speed, heading, brake system status, and vehicle size. Details of the BSM Part I content are found in Table V-1.

---

about some entity of interest (e.g., a person, place, process, property, object, concept, association, state, event). A data element is considered indivisible.

[139]For more information on the other message sets defined in SAE J2735, see www.sae.org/standardsdev/dsrc/ (last accessed Jan. 28, 2014).

Table V-1 Contents of BSM Part I[140]

Part I	
Data Frame (DF)	**Data Element (DE)**
Position (DF)	
	Latitude*
	Elevation*
	Longitude*
	Positional accuracy*
Motion (DF)	
	Transmission state*
	Speed
	Steering wheel angle
	Heading*
	Longitudinal acceleration*
	Vertical acceleration
	Lateral acceleration
	Yaw rate*
	Brake applied status
	Traction control state
	Stability control status
	Auxiliary brake status
	Brake status not available
	Antilock brake status
	Brake boost applied
Vehicle size (DF)	
	Vehicle width
	Vehicle length
	*Required in Safety Pilot Model Deployment

BSM Part II contains a set of data elements that can vary by vehicle model. Part II data are only broadcast when an event happens that changes the Part II data content. Part II is then appended to Part I data and broadcast; otherwise, only Part I data is transmitted in the BSM. The content of Part II data depends on the triggering events – not all Part II data will be transmitted simply because *some* Part II data is transmitted. For example, when a vehicle activates ABS, a

---

[140] Based on SAE 2735-2009. For more information, see "Vehicle Information Exchange Needs for Mobility Applications: Version 2.0, Revised Report (Aug. 1, 2012, FHWA-JPO-12-021) at http://ntl.bts.gov/lib/46000/46000/46089/Final_PKG_FHWA-JPO-12-021_508_PDF.pdf (last accessed Jan. 28, 2014).

data element named "ABS activated" is set and the vehicle's BSM transmissions include a Part II message indicating that its ABS is active.[141] This event type data is being used in the Safety Pilot Model Deployment to support the EEBL safety application. Consequently, Part II data are transmitted less frequently. Details of the BSM Part II content are found in Table V-2.

Table V-2 Contents of BSM Part II[142]

Part 2 (all elements optional, sent according to criteria to be established)	
Data Frame (DF)	**Data Element (DE)**
Vehicle safety extension (DF)	
	Event flags (DE) – A data element consisting of single bit event flags:
	Hazard lights
	Intersection stop line violation
	ABS activated
	Traction control loss
	Stability control activated
	Hazardous materials
	Emergency response
	Hard braking
	Lights changed
	Wipers changed
	Flat tire
	Disabled vehicle
	Air bag deployment
Path history (DF)	
	Full position vector (DF)
	Date and time stamp (DE)
	Longitude (DE)
	Latitude (DE)
	Elevation (DE)
	Heading (DE)
	Transmission and speed (DF) – same as in Part 1
	Positional accuracy (DE)
	Time confidence (DE)
	Position confidence set (DF)
	Position confidence (DE)
	Elevation confidence (DE)
	Speed and heading and throttle confidence (DF)

[141] For the same event, the traction control loss, stability control activated, and the hard braking flags may be set as well depending on the event type and causation.
[142] *See supra* note 140.

	Speed confidence (DE)
	Heading confidence (DE)
	Throttle confidence (DE)
	GPS status (DE)
	Count (DE) – number of "crumbs" in the history
Crumb data – set of one of 10 possible path history point set types, consisting of various combinations of:	
	Latitudinal offset from current position (DE)
	Longitudinal offset from current position (DE)
	Elevation offset from current position (DE)
	Time offset from the current time (DE)
Accuracy (DF) – See J2735 standard for more information	
	Heading (DE) – NOT an offset, but absolute heading
Transmission and speed (DF) – same as in Part 1, NOT an offset	
Path Prediction (DF)	Radius of curve (DE)
	Confidence (DE)
RTCM Package (DF) – RTCM (Radio Technical Commission for Maritime Services) is a standardized format for GPS messages, including differential correction messages.	
Full position vector (DF) – see full contents above under Path history	
RTCM header (DF)	
	GPS status (DE)
	Antenna offset (DE)
	GPS data – see SAE J2735 and RTCM standards for more information
Vehicle status (DF)	
	Exterior lights (DE)
	Light bar in use (DE)
Wipers (DF)	
	Wiper status front (DE)
	Wiper rate (front) (DE)
	Wiper status rear (DE)
	Wiper rate (rear) (DE)
Brake system status (DF) – same as in Part 1	
	Braking pressure (DE)
	Roadway friction (DE)
	Sun sensor (DE)
	Rain sensor (DE)
	Ambient air temperature (DE)
	Ambient pressure (DE)
	Steering, sequence of:
	Steering wheel angle (DE)
	Steering wheel angle confidence (DE)
	Steering wheel angle rate of change (DE)
	Driving wheel angle (DE)

Acceleration set (DF) – same as in Part 1	
	Vertical acceleration threshold (DE)
	Yaw rate confidence (DE)
	Acceleration confidence (DE)
Confidence set (DF)	
	Acceleration confidence (DE)
Speed confidence (speed, heading, and throttle confidences (DF)	
	Time confidence (DE)
Position confidence set (DF)	
	Steering wheel angle confidence (DE)
	Throttle confidence (DE)
Object data, sequence of:	
	Obstacle distance (DE)
	Obstacle direction (DE)
	Time obstacle detected (DE)
Full position vector (DF) – see contents under path history	
	Throttle position (DE)
Speed and heading and throttle confidence (DF) – same as above under "Full position vector"	
	Speed confidence (DE) – same as above under "Speed and heading and throttle confidence"
Vehicle data (referred to as a "complex type" in J2735, rather than an element or frame)	
	Vehicle height (DE)
	Bumper heights (DF)
	Bumper height front (DE)
	Bumper height rear (DE)
	Vehicle mass (DE)
	Trailer weight (DE)
	Vehicle type (DE)
Vehicle identity (DF)	
	Descriptive name (DE) – typically only used for debugging
	VIN string (DE)[143]
	Owner code (DE)[144]
	Temporary ID (DE)
	Vehicle type (DE)

---

143 SAE J2735 is a data dictionary that defines potential data elements for a number of messages (e.g., V2V, V2I, I2V, probe messages). Data elements are currently defined within the standard for a broad range of future safety and non-safety application messages. The vehicle identification data elements are defined for communication between emergency and fleet vehicles for applications such as traffic signal preemption, in which the road side equipment (traffic signal controller) requires confirmation of the identity of the vehicle.

144 Id.

Vehicle class (drawn from ITIS code standard)	
J1939 data (DF)	
Tire conditions (DF) – see J2735 standard for list of data elements	
Vehicle weight by axle (DF) – see J2735 standard for list of data elements	
	Trailer weight (DE)
	Cargo weight (DE)
	Steering axle temperature (DE)
	Drive axle location (DE)
	Drive axle lift air pressure (DE)
	Drive axle temperature (DE)
	Dive axle lube pressure (DE)
	Steering axle lube pressure (DE)
Weather report, defined as a sequence of the following:	
	Is raining (DE) – defined in NTCIP standard
	Rain rate (DE) – defined in NTCIP standard
	Precipitation situation (DE) – defined in NTCIP standard
	Solar radiation (DE) – defined in NTCIP standard
	Mobile friction (DE) – defined in NTCIP standard
	GPS status (DE)

The SAE J2735-2009 standard contains only technical design specifications for the BSM, so in order to specify the usage of the BSM as defined in J2735, such as the transmission rate, power level, data integrity, etc., another set of standards for the minimum communication performance requirements for the BSM must be developed. The SAE DSRC Technical Committee is currently in the process of developing minimum performance requirements for BSM communication, named SAE J2945-1, based on the knowledge gained through the CAMP VSC-A project, the V2V-Interoperability project and the Safety Pilot Model Deployment.

Standards Need V-1 SAE Standards Maturity

Standards Need:	SAE J2945 & SAE J2735
Description:	Currently these standards are in development. Timeframe for completion and impact on future regulatory is to be determined by outside organizations

(2) Other options besides the BSM

The BSM is developed specifically for vehicle-to-vehicle communication, to allow devices from different OEMs and suppliers to interact in the system. This dedicated message was cooperatively developed as a standard involving both U.S. and EU representatives. Currently there is no planned alternative to using the collaboratively-developed BSM to transmit and receive vehicle information for use in safety applications. The BSM has been developed and refined over the course of the last decade specifically to support common V2V communication.

(3) Current maturity level of V2V message sets

The BSM is developed for vehicle-to-vehicle communication to allow devices from different OEMs, suppliers, and aftermarket device manufacturers to communicate with each other for V2V and V2I applications. The preliminary design specifications for the BSM are contained in the current version of SAE J2735 and preliminary minimum performance requirements will be contained in SAE J2945 when finalized.

Over the course of the Safety Pilot, it was identified that the current published J2735-2009 will not support interoperability as a stand-alone document, due to ambiguities in the standard that were causing OEMs and suppliers to interpret the standard and define the BSM inconsistently. During the V2V-I project, future revision items were identified for various DSRC standards for further improvement for interoperability.

Nevertheless, the vehicles in the Safety Pilot Model Deployment program are transmitting BSMs to each other and using those BSMs to activate safety applications. Results from the Safety Pilot and the CAMP Interoperability project will be used to further develop performance requirements for the BSM.

c) Technical Standards related to V2V

(1) Development and use of technical standards related to V2V

To support wireless communication between two or more vehicles and/or between vehicles and fixed or nomadic devices, a set of ITS V2X Cooperative System Standards are needed. These standards ensure that vehicles are interoperable and can interpret messages received from these other sources. The current set of cooperative system standards is found in Table V-3.

Table V-3 Cooperative System Standards for V2V Communications

Cooperative System Standards
IEEE 802.11p-2010
IEEE P1609.0/D5.8
IEEE 1609.2-2013
IEEE 1609.3-2010
IEEE 1609.4-2010
IEEE 1609.12-2012
SAE J2735, Version 2
SAE J2945.1, Version 1

These cooperative system standards were developed specifically to support V2V and V2I wireless interfaces. They establish a wireless link for V2V and V2I communications (IEEE 802.11p), establish protocols for information exchange across the wireless link (IEEE 1609.x), and define message content for communicating specific information to and from equipment and devices via DSRC (SAE J2735 and SAE 2945.x) or other communications media.

OST-R's Intelligent Transportation Systems Joint Program Office's Standards Program funds and manages ITS cooperative system standards efforts in support of V2V and V2I technologies. The content of these standards is developed collaboratively with contributions from diverse stakeholders. The VSC-A and CAMP projects have made significant contributions to many of the standards described above.[145]

The cooperative system standards are, to be clear, consensus standards voluntarily followed by industry, as compared with regulations issued by a government agency like NHTSA. NHTSA has no authority to enforce standards that it does not promulgate. However, if NHTSA eventually decided, for example, to mandate DSRC (in order to enable certain safety applications), part of that mandate would likely include requirements that DSRC devices be interoperable in order to ensure that they function properly. Part of ensuring interoperability is making sure that DSRC works, exchanges information the same way every time, and uses standardized messages. Each of the cooperative system standards discussed in this section facilitates some part of DSRC operation, so NHTSA may look to these standards and incorporate elements of them if the agency decides to pursue a DSRC mandate.

(2) SAE J2735 - DSRC Message Set Dictionary

The SAE J2735 standard specifies message sets, data frames, and data elements that make up messages/dialogs specifically for use by applications intended to use the 5.9 GHz DSRC for WAVE communications systems. The messages for V2V safety applications are defined in SAE J2735 as the BSM parts 1 and 2 (detailed information for BSM part 1 and 2 can be found in Section V.D.1.b) other parts of SAE J2735 define the message sets for other ITS applications, such as weather and mobility.

SAE's DSRC Technical Committee issued the current published version of J2735 in November 2009, as version 2 of the standard (referred to as J2735-2009 or version 2 of J2735). At present, the SAE J2735-2009 standard has been implemented for testing and experimental

---

[145] Specifically, VSC-A and CAMP have contributed to the development of SAE J2735 (DSRC Message Set Dictionary); SAE J2945.1 (DSRC BSM Minimum Performance Requirements); IEEE 1609.0 (Architecture); IEEE 1609.2 (Security Services); IEEE 1609.3 (Networking Services); IEEE 1609.4 (Multi-Channel Operation); IEEE 1609.12 (Identifier Allocations); and IEEE 802.11p (Wireless Access in Vehicular Environments (WAVE)).

purposes only, with no wide-scale deployment. As indicated in the discussion on maturity of the BSM message sets, revisions will be necessary to the J2735-2009 standard to support widespread deployment of a V2V system. Current expectations are that a revised standard will be published in late 2014.

(3) SAE J2945 - DSRC Minimum Performance Requirements

The SAE J2945.1 standard specifies the minimum communication performance requirements of the DSRC Message sets and the necessary BSM data elements to support V2V safety applications. The J2945.1 standard is part of a future family of J2945.x standards.[146] The current draft standard consists of multiple sections with each section describing the specific requirements for using the BSM for V2V safety applications. The content of the current draft J2945.1 is listed in Table V-4. To date, an early rough draft version of J2945.1 exists and it only includes the minimum communication performance requirements for the BSM message. It is anticipated the published version of J2945 will be available in late 2014.

Table V-4 Contents of Draft J2495.1 Standard[147]

Section	Section Title
1	Scope
2	References
3	Common Section
3.1	PSID Assignment
3.2	SSP (Service Specific Priority)
3.3	Message Priority Mapping
4	DSRC BSM Minimum Performance Requirements
4.1	Power option
4.2	DSRC Communication Channel Operation for BSM (or V-V Safety)
4.3	BSM Transmission Interval Requirements
4.4	Transmission Power Requirements
4.5	Security and Privacy Requirements
4.6	GPS configuration Requirements
4.7	Data Frame/Elements Requirements
5	Future Consideration
6	Application-level Requirements?
7	Other stuff*

*Note: [sic], per the current draft form of the standard

[146] Each J2945.x standard will provide the critical interface information needed to support one or more applications. Associated design specifications for data frames and data elements for the respective J2945.x standards are defined in the SAE J2735-2009 (DSRC Message Set Dictionary standard) and will also be included in future published versions of J2735.

[147] This outline is from the current draft J2945.1, and will likely change as the standard is further developed.

(4) IEEE 1609 - Standard for Wireless Access in Vehicular Environments (WAVE)

The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure V2V and V2I wireless communications. Together these standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management, and others.

(5) IEEE 1609.0 - Guide for Wireless Access in Vehicular Environments (WAVE) Architecture

IEEE 1609.0 is not a standard, but an architecture guide. It provides the descriptions of each of the full-use IEEE 1609 standards and their relationships to other relevant standards (such as IEEE 802.11), and includes guidance on how they should work together. The protocol architecture, interfaces, spectrum allocations, and device roles are all described. The guide is intended for organizations that will implement DSRC, such as State departments of transportation, automobile and original equipment manufacturers, aftermarket equipment makers, application developers, and standards developers. The guide describes the history of the development of the IEEE 1609 standards that includes the ITS architecture, the FCC allocation of the spectrum, and the original standards activity in the development of ASTM 2213-03. Also described are the IEEE 1609 trial use standards and IEEE 802.11. There is also a summary of the deployment history of DSRC devices in an annex to the guide. Overall WAVE system operations are described and an example system configuration is provided based on the published full use standards. The protocol architecture is described, including a description of the data plane,[148] the management plane,[149] and how WAVE messages and IPv6 messages are treated. Internal and external interfaces are described. The channel configurations, channel types and allowed operations are detailed according to the current FCC rules as well as a description of how the control channel and the service channels can be configured. The guide also explains channel coordination, channel switching, and time synchronization.

(6) IEEE 1609.2 - Security Services for Applications and Management Messages

The safety-related content of WAVE applications, and particularly vehicle safety applications, makes it necessary to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay. Recipients of safety messages have to be assured that the messages they receive are authentic and are sent by a source authorized to transmit those

[148] The data plane, also known as the user plane, forwarding plane, carrier plane, and/or bearer plane, is the part of a network architecture that handles user traffic.
[149] Part of a network architecture which provides an administrative interface to the system.

messages. Additionally, the fact that the WAVE technology may be implemented in communication devices in personal vehicles as well as in other portable devices whose owners may have some expectation of privacy means that the security services may need to be designed to avoid, for example, revealing personal, identifying, or linkable information to unauthorized parties in systems where PII may be involved. This standard describes security services for WAVE management messages and application messages designed to meet these goals. This standard was intended to be used primarily for DSRC.

(7) IEEE 1609.3 - Networking Services

IEEE 1609.3 specifies how various message types (e.g., WAVE Short Messages, WAVE Service Advertisements, and WAVE Routing Advertisements) are assembled, packaged, and handled between an application and IEEE 1609.4 for transmission or upon reception. It describes how to build, route, process, and interpret WAVE low latency messages, as well as messages based on other well-known protocols such as the User Datagram Protocol and Internet Protocol Version 6 (IPv6). The standard includes information on what messages go on the control channel, what messages go out on the service channels, advertising specific services, authenticating the messages, accessing applications hosted on an external network (e.g., the Internet) and methods for how this can be accomplished.

(8) IEEE 1609.4 - Multi-Channel Operations

This standard describes multi-channel radio operations for WAVE. It is used in conjunction with other IEEE 1609 standards and IEEE 802.11-2012 to implement DSRC communications in the 5.9 GHz frequency band. WAVE operates using IEEE 802.11 outside the context of a basic service set. In order to implement functions such as user priority access to the media, routing data packets on the correct channel with the desired transmission parameters, and the ability to coordinate switching between the control channel and service channels, additional functions are required between the IEEE 802.11 medium access control and the Logical Link Control. This standard specifies how these functions are implemented.

(9) IEEE 1609.12 - Identifier Allocations

WAVE is specified in the IEEE 1609 family of standards, within which a number of identifiers are used. IEEE 1609.12 describes the format and use of the provider service identifier, and indicates identifier values that have been allocated for use by WAVE systems.

(10) IEEE 802.11p-2012 - Medium Access Control and Physical Layer Specifications for WAVE

IEEE 802.11 is a set of standards that specify the physical layer for implementing wireless local area network using Wi-Fi bands. The base version of the standard was released in 1997 and has had subsequent amendments. IEEE 802.11 is approximately 2,800 pages long, but only certain parts of the standard are required for implementing DSRC operating at 5.9 GHz for

V2V communications. IEEE 802.11p is an approved amendment to 802.11 standards to add WAVE that is required to support ITS applications. In March 2012, IEEE published the latest version of this standard, 802.11p-2012, which includes all the amendments to this standard published prior to 2012.

The purpose of this standard is to describe the operation of what are commonly known as Wi-Fi devices, including devices such as the wireless routers and the transceivers in computers. To accommodate the rapid exchange of trajectory information between vehicles traveling at high speed, IEEE 802.11p was amended to enable operation without setting up a basic service set. It allows security services, such as authentication, to be provided by other standards. It describes adjacent channel and alternate adjacent channel interference criteria and transmission masks corresponding to requirements of the FCC rules for DSRC. The entire standard applies to V2V and V2I communications, because it defines the structure for how devices should communicate using the 5.9 GHz frequency band but there are no performance criteria or test procedures described in this amendment.

(11) Maturity of the standards

Table V-5 describes the standards representing the core cooperative system standards, in particular those that support V2V and V2I. While versions of these standards have already been developed and published, some are currently undergoing revision to support evolving needs such as the current Safety Pilot Model Deployment activity.

Table V-5 ITS V2X Cooperative System Standards Latest Publication and Current Status

Standard	V2V Relevance	Latest Publication Date	Current Status
IEEE 802.11p-2010	DSRC-specific Wi-Fi device operations	July 2010	Finalized and published.
IEEE P1609.0/D5.8	Guide to other 1609 standards	Not yet published.	In sponsor ballot[150]
IEEE 1609.2-2013	Security	April, 2013	Finalized and published.
IEEE 1609.3-2010	Data exchange/message structure	December, 2010	Finalized and published.
IEEE 1609.4-2010	Channel switching modes	February, 2011	Finalized and published.
IEEE 1609.12-2012	Message identification	September, 2012	Finalized and published.
SAE J2735, Version 2	Basic safety message elements	November 19, 2009	Revision underway and expected to be published in late 2014.
SAE J2945.1, Version 1	Basic safety message requirements		No published version yet. Expected to be published in late 2014.

d) Relative Positioning

Relative positioning is a critical system function/element used to enable V2V safety applications. The essential function of the safety applications, their ability to warn the driver of an impending collision, depends on the ability of the automobiles within DSRC range to report their GPS positions to each other with confidence in their accuracy. GPS positioning matters because two interacting devices need to understand where they are in relation to each other.

Relative positioning is calculated by the difference in the reported GPS position between two vehicles in close proximity. The quality of a relative positioning solution between two cars depends on how accurate the two separate GPS positioning were.[151]

---

[150] For a description of the IEEE ballot process, see http://standards.ieee.org/develop/balloting.html (last accessed Jan. 9, 2014).

[151] Several different modes of absolute positioning have been investigated in the positioning research performed by CAMP, including standalone GPS, Wide Area Augmentation System (WAAS), and Real Time Kinematic (RTK). WAAS is an augmented GPS that uses ground reference stations to measure deviations from ground truth in the GPS signal and provide corrections to the geostationary WAAS satellites over the continental United States. Although WAAS specifications call for a position accuracy of 7.6 m or better 95 percent of the time, actual accuracy performance has typically been better than 1.0 m lateral accuracy and 1.5 m vertical accuracy. RTK functions on the principle of examining the difference in the phase of the carrier wave of the GPS signal between two reference stations (fixed or mobile). This difference is used to improve the raw GPS calculated distance between the stations. While RTK has the potential of high accuracy with errors measured down to a few centimeters, it comes in as more

Absolute positioning by itself might seem more useful to V2V communications, insofar as one might think that V2V-based safety applications would have the best chance of warning a driver correctly given the most precise information possible about the driver's location and the location of other vehicles. However, relative positioning has an inherent benefit as applied to V2V communications, as it relieves the burden of correcting for absolute positioning that would require additional communication with a RSE for each GPS location transmission, which would in turn require a comprehensive infrastructure network.

Error/biases in GPS raw measurements exist and are caused by natural effects and are almost identical over a geographic area. These natural biases are cancelled out in a relative positioning scheme performed over DSRC ranges. Using the relative positioning approach allows vehicles to calculate their position in relation to each other with a high degree of confidence, assuming that they have the same bias. The ability of a vehicle to determine its position in relation to other vehicles, rather than to determine its absolute position on the Earth, together with the other information transmitted in the BSM, is what is necessary to support the safety applications.

2. Current maturity level of V2V wireless communication channels

a) Securing a dedicated spectrum

It is widely accepted that V2V communications have a specific home in the wireless spectrum, but whether that home is sufficiently protected against intrusion that might impair the effectiveness of safety applications enabled by V2V is less clear at present. In 1999 the FCC allocated 75 MHz in support of the Intelligent Transportation Systems[152] on a primary basis. While this is referred to as a dedicated spectrum, it should be noted there are other allocations in this band, including the Fixed Service Satellite (co-primary) and Amateur Radio (secondary). Additionally, the lower 25 MHz overlaps the Industrial, Scientific, and Medical (ISM) band. Government Radiolocation is authorized on a primary basis as well. In February of 2004, the FCC released another Report and Order setting forth licensing and service rules for DSRC services. In 2006, the FCC released an Amendment of the Commission's Rules[153] that, among

---

costly in terms of computational and bandwidth requirement. *See:* VSC 2 Consortium, "Vehicle Safety Communications – Applications (VSC-A) Final Report: Appendix Volume 2 Communications and Positioning," Report No. DOT HS 811 492C, September 2011, at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014). [Hereafter, "VSC-A Final Report: Appendix Volume 2"].

[152] Amendment of Parts 2 and 90 of the Commission's Rules to Allocate the 5.850-5.925 GHz Band to the Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Services (ET Docket No. 98-95) at http://transition.fcc.gov/oet/dockets/et98-95/ (last accessed Jan. 9, 2014).

[153] Federal Communications Commission, Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz band (71 Fed. Reg. 52747, Sept. 7, 2006) at www.gpo.gov/fdsys/pkg/FR-2006-09-07/pdf/FR-2006-09-07.pdf (last accessed Feb. 18, 2014).

other things, designated channel 172 exclusively for vehicle-to-vehicle safety communications for accident avoidance and mitigation, and safety of life and property applications. The amendment also designated Channel 184 exclusively for high-power, longer-distance communications for public safety applications involving safety of life and property, including road intersection collision mitigation. These FCC decisions established DSRC as the incumbent in the band on a co-primary basis with the Fixed Service Satellite, and the FCC's continued recognition of this highlights the allocation of this spectrum for ITS.

In 2003, DOT announced the VII Proof of Concept initiative. At this point efforts shifted slightly from R&D into Test and Evaluation (T&E). This has continued for a number of years, culminating in the Safety Pilot. Data from the V2V Safety Application Research and the Safety Pilot will support a decision concerning the DSRC technology and if the technology can be used to address motor vehicles crashes.

The importance of DSRC has not been lost over the many years it has taken to develop and test it. In the latest 5 GHz NPRM, the FCC again notes the need to protect DSRC when they asked "what types of sharing technology or techniques could be used to protect non-radar systems, such as the DSRCS which includes both road side units (RSU-fixed) and on board units (OBU-mobile) operating under a primary allocation."[154]

b) Existing signal interference issues

Signal interference can pose challenges to V2V communication if other devices are operating at the same frequency as DSRC devices and preclude the transmission or reception of messages that could impact the effectiveness of safety applications. Existing signal interference deals with what devices are already using the signal and how the addition of devices using the same frequency (signal) would disrupt the signals of any existing devices operating at the same frequency. Early in the development of DSRC, the Institute for Telecommunication Sciences, the research arm of the National Telecommunication and Information Administration, was contracted to perform analysis work on signal interference by the Federal Highway Administration. Two reports are notable. The first report tested European and Japanese DSRC devices against DOD radar systems in a laboratory setting (the United States had nothing to test at that point in time).[155] The second examined the occupancy of the DSRC band as well as adjacent bands, meaning what other users and/or existing services occupy the band or nearby

[154] Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz Band (ET Docket 13-49) at http://apps.fcc.gov/ecfs/comment/view?id=6017164516 (last accessed Jan. 9, 2014).
[155] Electromagnetic Compatibility Testing of a Dedicated Short-Range Communication (DSRC) System that Conforms to the Japanese Standard (Nov. 1998, NTIA Technical Report TR-99-359) at www.its.bldrdoc.gov/publications/details.aspx?pub=2390 (last accessed Jan. 28, 2014).

adjacent bands that could leak into the 5.9 GHz band.[156] The testing with European and Japanese devices showed that "when combined with the additional isolation achieved by antenna alignment (estimated to be 40 dB), the engineers found that all of the existing 5-GHz radars (other users/services in the 5 GHz band)[157] should be compatible with the DSRC system that was tested [in a worst case scenario] for extremely small separation distances (several meters or less)." Based on these findings, the agency believes interference should be minimal and not present a major impact on the effectiveness of the system.

The second report noted that interference from the Fixed Service Satellite (FSS)[158] to DSRC is possible. Typically, the FSS uplinks are in remote and rural locations. These earth-based facilities use a high-powered uplink to transmit data to geostationary satellites, predominantly over the eastern Atlantic or mid to eastern Pacific Oceans. Their primary function is trans-ocean communications and there are relatively few around the country. An in-band sharing agreement was developed and submitted to the FCC several years ago. In essence, it calls for new sites to be coordinated such that incumbents have priority. This is a standard approach for co-primary allocations. The FCC has not yet acted on the agreement.

c) *Current status of the spectrum*

On June 28, 2010, President Obama directed the Secretary of Commerce to work with the FCC to identify and make available 500 megahertz of spectrum over the next 10 years for wireless broadband use. On February 22, 2012, the President signed the Middle Class Tax Relief and Job Creation Act of 2012 into law. The Act requires the Assistant Secretary of Commerce (through NTIA), in consultation with the Department of Defense (DoD) and other impacted agencies, to evaluate spectrum-sharing technologies and the risk to Federal users if Unlicensed-National Information Infrastructure (U-NII) devices were allowed to operate in these bands.

The most common types of U-NII devices include those that use Wi-Fi communication. These devices, in general, operate without a license, but are not supposed to interfere with licensed devices, and have no interference protection.[159] The NTIA was required to issue a report eight months after enactment (October 22, 2012) on the portion of the study on the 5.350-5.470

---

[156] Measured occupancy of 5850-5925 MHz and adjacent 5-GHz spectrum in the United States (Dec. 1999, NTIA Technical Report TR-00-373) at www.its.bldrdoc.gov/publications/2404.aspx (last accessed Jan. 28, 2014).
[157] *Id.*
[158] Fixed Service Satellite (FSS) is the official classification for geostationary communications satellites that provide broadcast feeds to television stations, radio stations, and broadcast networks. FSSs also transmit information for telephony, telecommunications, and data communications. For more information, see www.hq.nasa.gov/webaccess/CommSpaceTrans/SpaceCommTransSec3/CommSpacTransSec3.html#3_1_3 (last accessed Feb. 25, 2014).
[159] The risk with these devices, however, is that they may be easily modified in ways that could result in them interfering with DSRC operation. Because they are unlicensed, moreover, it would be difficult to enforce against modified devices causing such interference. This continues to be an area of concern to NHTSA.

GHz band. The Act requires the report on the portion of the study on the 5.850-5.925 GHz band no later than 18 months after enactment (August 22, 2013). NTIA published in January 2013 the results of their initial study evaluating known and proposed spectrum-sharing technologies and the risk to Federal users if the FCC allows U-NII devices to operate in the 5.850-5.925 GHz band.[160] The NTIA report identified a number of risks to FCC-authorized stations operating DSRC systems for ITS in the 5.850-5.925 GHz band and suggested mitigation strategies to explore.

On April 10, 2013, the FCC published in the *Federal Register* its NPRM to revise Part 15 of its Rules to permit U-NII devices in additional portions of the 5 GHz spectrum, including the 5.850-5.9250 GHz, so as to "increase wireless broadband access and investment."[161] While the FCC NPRM proposes permitting U-NII devices in the 5.850-5.9250 GHz band, DSRC, as the incumbent, would retain its primary allocation of the band – U-NII devices would have to operate on a non-interfering basis under the FCC Part 15 Rules.[162] In June 2013, at the request of DOT, NTIA forwarded to the FCC the comments and concerns that DOT expressed relating to the deployment and protection of DSRC in the 5.850-5.925 GHz band.

The Institute for Electrical and Electronics Engineers 802 standards committee has established a working group, known as the IEEE 802.11 DSRC Coexistence Tiger Team, that provides an international multi-stakeholder technical forum that includes industry experts previously involved in developing standards for both wireless local area networks and vehicular wireless communications.[163] While NTIA's January 2013 5 GHz Report indicated that NTIA would follow up with quantitative studies in connection with domestic and international regulatory proceedings involving the 5350-5470 MHz, 5850-5925 MHz, and other bands, NTIA believes that industry participants should first be afforded adequate time to identify acceptable

---

[160] The NTIA 5 GHz Report is available at www.ntia.doc.gov/report/2013/evaluation-5350-5470-mhz-and-5850-5925-mhz-bands.

[161] 78 Fed. Reg. 21320, at 21321 (Apr. 10, 2013).

[162] One of the primary operating conditions under Part 15 is that the operator must accept whatever interference is received and must correct whatever interference is caused. Should harmful interference occur the operator is required to immediately correct the interference problem, even if correction of the problem requires ceasing operation of the Part 15 system causing the interference. See 47 C.F.R. Section 15.5.

[163] In August of 2013, the Regulatory Standing Committee of IEEE 802.11 created a "Tiger Team" to bring together interested participants to exchange technical ideas and explore possible solutions to the band sharing issue as proposed in this NPRM. This group, referred to as the DSRC Coexistence Tiger Team, operates under the auspices of the IEEE 802.11 working group. Conference calls are conducted weekly, and submissions and emails are openly available to the public on IEEE document servers.

technology approaches for coexistence in the 5850-5925 MHz band. [164] The Tiger Team's meetings have been productive, providing a venue for presenting and discussing concepts regarding potential coexistence approaches. On January 24, 2014, the Tiger Team sent a letter to the FCC to summarize activities coordinated by IEEE 802.11.[165] As discussed in the letter the current work items for the group include:

- Review of ITS/DSRC field trials conducted to date
- Review of work to date on coexistence
- Presentations on use cases
- Presentation of possible coexistence approaches
- Modeling/simulation of possible coexistence approaches
- Prototype testing of candidate approaches

Thus far, the group has engaged in extensive discussions about the status and performance of DSRC systems, explored requirements for band sharing, and had presentations on some preliminary candidate approaches for sharing techniques. If viable candidates for sharing are identified as part of this effort, NTIA anticipates extensive field testing will be conducted by WLAN and DSRC stakeholders outside of IEEE 802.11.

While DOT is encouraged by the work of the Tiger Team, the candidate approaches presented thus far do not yet contain adequate content to evaluate whether spectrum can safely be shared without creating harmful interference. As the work of the Tiger Team progresses and mature technical proposals are submitted for review, DOT will continue to work with the NTIA to review and analyze these sharing approaches.[166] Once this analysis is complete, DOT, along with the NTIA and the FCC, will be better positioned to assess how the proposed changes to existing rules and regulations for harmonization across such a large swath of spectrum will impact DSRC. NTIA and DOT will continue to work with the FCC to explore different avenues to facilitate and encourage inter-industry and inter-agency collaborative efforts to assess the possibility of sharing in the 5.850-5.925 GHz band.

---

[164] Letter from Lawrence E. Strickling, Assistant Secretary for Communications and Information to the Honorable Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology Committee on Energy and Commerce (Jan. 27, 2014).

[165] The letter is available at https://mentor.ieee.org/802.18/dcn/14/18-14-0007-02-0000-dsrc-coexistence-tt-status-letter-to-oet.docx.

[166] DOT submitted comments to the NPRM through NTIA in June 2013. See http://apps.fcc.gov/ecfs/document/view?id=7022424618 (last accessed Jan. 28, 2014).

Research Need V-1 Spectrum Sharing Interference[167]

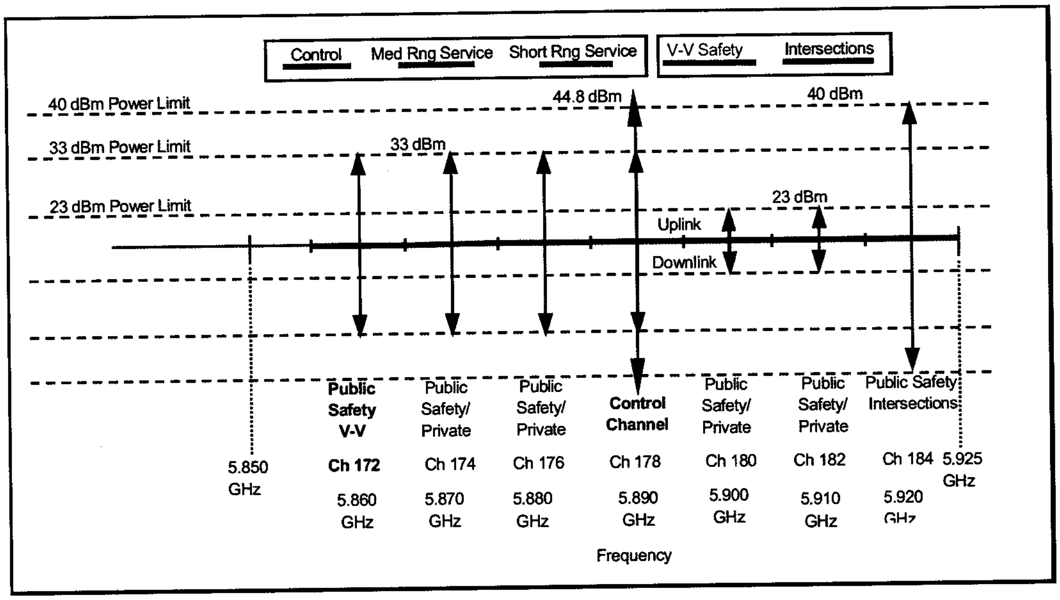
Research Activity:	Effect of spectrum sharing on V2V Crash Avoidance Performance
Description:	Evaluate the impact of unlicensed U-NII devices on the transmission and reception of safety critical warnings in a shared spectrum environment.
Target Completion:	US DOT is working with NTIA and other stakeholders to evaluate sharing proposals made by the communications industry in order to help ensure that there will be no interference to DSRC-enabled V2V safety applications caused by any sharing of the spectrum with unlicensed devices.
Current or planned NHTSA research addressing this need: US DOT will continue to coordinate with NTIA and other stakeholders on the issue of shared spectrum testing.	

d) V2V wireless communication channels

Currently, 75 MHz of wireless spectrum is allocated for DSRC by FCC. This spectrum is divided into seven non-overlapping 10 MHz channels, plus a 5 MHz guard band at the beginning of the frequency range. The FCC band plan for this spectrum specifies particular usage, power limits, etc. for these channels as shown in Figure V-2 below.

[167] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

Figure V-2 Band Plan for DSRC Channel Spectrum



As a radio, the DSRC unit operates on one frequency (or "channel") at a time – consider, for example, the AM/FM radio in vehicles today, which can receive one station or another depending on how it is tuned (tuning being the act of shifting signal reception from one radio frequency to another), but does not receive clearly when it is between stations, and cannot be tuned to more than one frequency at once.

The current V2V operation uses two radios, one tuned to channel 172 and dedicated for safety communications and another tuned to channel 174 for security-related communications. In addition, a third channel, 178, is used as a control channel to manage channel switching[168] to support messages on other channels related to other services/applications, such as mobility or environment.

Early on in the VSC-A project, researchers initially attempted to use channel 178 as both a "control" channel[169] and for transmission of the BSM, but using a single channel for both unduly restricted BSM transmission, potentially hindering safety. It was thought that a channel switching mode could be used on a single radio to support the BSM as well as use the other channels for other messages, because the channel switching mode would cause the BSM transmissions to switch from channel 178 to some other channel. However, because a radio can

[168] Channel switching is the use of a dedicated channel to route incoming messages to multiple "service" channels that use the incoming information. This method allow for a single radio to be used to support multiple functions.
[169] The control channel "tells" the radio which channel to "listen" to for specific information as well as transmitting that same information when the device is ready to transmit information.

only transmit or receive on a single channel at a time, channel switching only solves part of the problem – the radio still has to take turns between the BSM and the other necessary messages.

The sections that follow explain the modes of operation and how the research indicated the need to implement a dedicated channel for the BSM.

(1) Channel Switching Mode

In order to transmit and receive messages on different channels, DSRC will have to switch from one channel to another, which it may need to do in order to perform different functions necessary for V2V communications.

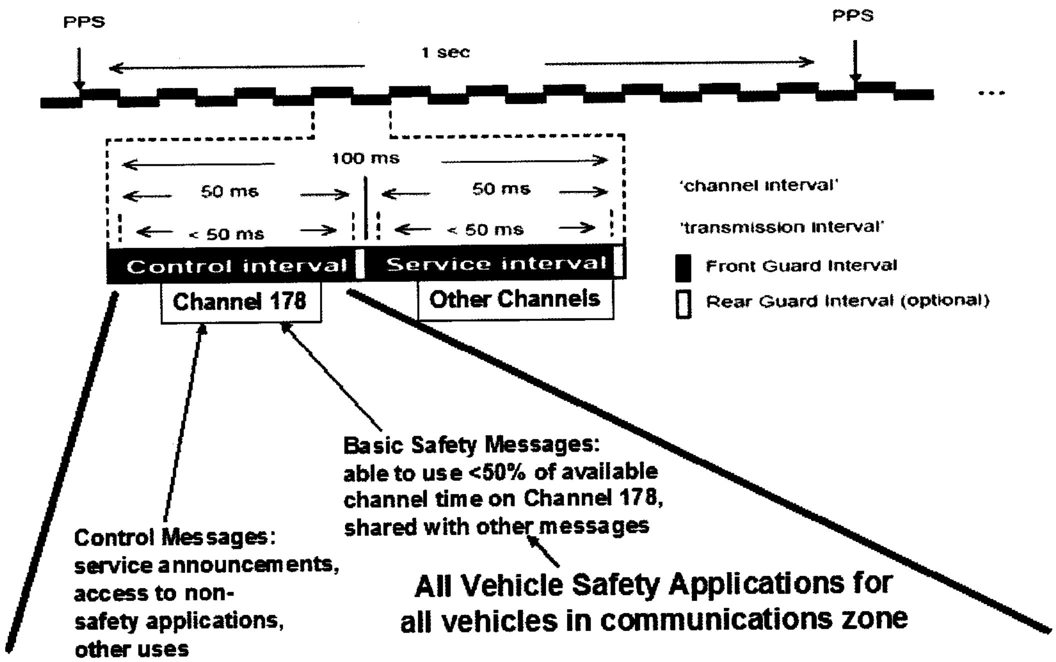
Time is an important facet of V2V communications, because BSM transmissions need to be received in a timely manner in order to warn drivers of potential dangers in time for them to react, among other things. If DSRC is switching from one channel to another, it may experience a time lag as the next channel is being picked up, which may potentially affect receipt of important transmissions. The IEEE 1609.4 standard[170] divides time for purposes of DSRC transmission into 100 millisecond sync intervals (the equivalent of 10Hz). The sync intervals are then sub-divided into a Control Channel (CCH) interval and a Service Channel (SCH) interval, and a time division mechanism is defined for a device to switch between the CCH and a SCH every 50 ms to transmit and/or receive DSRC messages.

As shown in Figure V-3 below, Channel 178 is designated as the "Control Channel." It was originally envisioned that all vehicle and roadside units accessing this spectrum would use the control channel to determine what information is available on other channels, and then switch to the other channels to access the information.[171]

---

[170] For more information, see VSC-A Final Report: Appendix Volume 2.
[171] Id.

Figure V-3 Time Division Channel Usage



During the VSC-A research initiative, vehicles participating in V2V safety communications using this channel switching operation sent and received BSMs on the CCH during the CCH interval. This would allow vehicles to participate in non-V2V safety communications on a SCH during the SCH interval for other DSRC services. While this safety communication model is not required by IEEE 1609.4, or any other standard, it was considered as the baseline approach for the initial research.

One of the main advantages of the above approach is that it allows a single-radio vehicle to participate in V2V safety by exchanging BSMs with its neighbors and also to avail itself of DSRC services that are offered during SCH intervals (e.g., by RSE). This capability is especially attractive as part of an initial DSRC deployment strategy to boost market penetration. One of the main disadvantages of this approach, however, is that safety messages are effectively limited to the CCH interval, and thus channel congestion is a significant concern. At high channel loads, the probability that two or more packets "collide" due to overlapping transmissions can become significant. As explained below, the research has indicated ways of mitigating the disadvantages, and NHTSA plans to do additional testing on congestion mitigation.

Due to a required 4 ms front guard interval V2V communications can only use a maximum of 46 ms out of the 100 ms sync interval. In other words, effectively only 46 percent "potentially" available bandwidth is available to be used because the remainder must be used for non-BSM transmissions, such as security, mobility, environment, and possibly commercial (auto diagnostics, requested assistance information) transmissions on other channels providing this information. Determining channel capacity via analysis is quite complex due to the MAC protocol used in DSRC. However, a simple calculation shows why 1609.4 time division causes a concern for V2V safety. As explained below, research indicates methods of addressing this concern are available. If a DSRC channel supports 6 Mbps, this is equivalent to 2,000 messages/second for 3,000-bit messages (the approximate size of an average BSM). At 10 messages/second/vehicle, this is equivalent to 200 vehicles in a given transmission region. With BSMs confined to the CCH interval, the capacity is cut to about 45 percent due to the guard interval and the need to complete packet transmissions before the start of the SCH interval. In this simple example, that is equivalent to 90 vehicles in a region. It is not difficult to construct realistic traffic scenarios in which a capacity of 90 vehicles in a transmission region represents a significant constraint.

(2) Multi-Channel Operation versus a Dedicated Safety Channel

Having two radios, one of which is always tuned to the dedicated safety channel, may help to avoid the need for channel switching and enable the vehicle to broadcast and receive BSMs the entire time it is in operation.

Having also determined that communication channel congestion could limit V2V safety system performance,[172] the CAMP VSC-A project team analyzed 11 scenarios of one- and two-channel operational approaches, within the constraints of IEEE 1609.4. This is discussed further in the Congestion Mitigation section of this paper – Section V.E.2.b).

3. Interoperability performance requirements

This section of the paper discusses the performance requirements for DSRC, GPS, and other system components that are understood to achieve interoperability.[173] This section covers four major topics: (1) overview of system performance requirements; (2) overview of requirements for exchanging messages (3) research history and technical maturity; (4) recommendations.

---

[172] CAMP, VSC-A Final Report (Sept. 2011, Report No. DOT HS 811 492A). See www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2011/811492A.pdf (last accessed Jan 28, 2014). [Hereafter, "VSC-A Final Report"].

[173] This section provides a general discussion of performance requirements for DSRC and GPS. Requirements needed to support specific safety applications are discussed in Section VI.

a) Overview of V2V program system performance requirements

This section describes how the specifications were developed. It provides a top-level view of the major factors that influenced the development of performance requirements for the V2V system.

The following factors were taken into account in developing the V2V system performance requirements.

1. Connected Vehicle Model Deployment safety application characteristics
2. Transmitting power a DSRC radio could provide
3. Receiving ability at a given area with a given transmitting power
4. Language vehicles speak when they communicate with one another
5. Language used for communication between vehicles and RSEs
6. Information necessary to be included in the BSM
7. Information necessary to be included in the communication between vehicles and the infrastructure.
8. Media devices could use to carry messages when they communicate with one another
9. Media devices could use to carry messages when they communicate with RSEs
10. Basic Safety Message data accuracy needs to be specified
11. Error tolerance and error correction capability (considering potential distortion) of over the-air signals being received by OBE
12. Capability of the system to accommodate all communication within a given area of coverage and for a given number of vehicles (DSRC channel congestion mitigation)
13. Method of synchronizing communication system network
14. The method of verifying and validating messages from other vehicles
15. The method of verifying and validating messages from other ECUs in a vehicle itself
16. Security scheme to protect data communication
17. Security scheme to initiate and ensure trusted key establishment
18. Security scheme to support key management
19. Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust at the Infrastructure side
20. Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust on the on-board DSRC devices
21. Security scheme to protect Personally Identifiable Information (PII)

b) Research history and technical maturity/readiness

Following is a summary of related research findings on performance requirements for DSRC and interoperability, a list of references, and a table for cross referencing to research activities, reports, standards, and the current status.

Initial system performance requirements were defined during the VSC project that started in 2002 and ran until 2005. During the VSC project, the VSC Consortium developed an initial set of safety applications that could be improved by communications with sources outside the vehicle. The VSCC then estimated benefits in lives saved and injuries avoided of these applications. VSCC and DOT then selected a subset of those applications for further development based on their potential safety benefits. VSCC developed communications performance requirements for the following eight applications.

- Traffic Signal Violation Warning
- Curve Speed Warning
- Rollover Warning
- Emergency Electronic Brake Lights
- Cooperative Forward Collision Warning
- Left Turn Assistant
- Lane Change Warning
- Stop Sign Movement Assistance

These requirements included the following.

- Message packet size of 200 to 500 bytes (all 8 scenarios)
- Maximum required range of communications of 50 to 300 meters (all 8 scenarios)
- One-way, point-to-multipoint broadcast messages (7 of 8 scenarios)
- Two-way, point-to-point messages (1 of 8 scenarios)
- Periodic transmission mode (6 or 7 of 8 scenarios)
- Event-driven transmission mode (1 or 2 of 8 scenarios)
- Allowable latency of 100 milliseconds (6 of 8 scenarios)
- Allowable latency of 20 milliseconds (1 of 8 scenarios)
- Allowable latency of 1 second (1 of 8 scenarios)[174]

The outcome of this project was, however, that the communications requirements would need further refinement as prototype vehicle safety applications are developed from a safety-systems design perspective.[175]

The extension of the VSC project, the VSC-A project, further refined and added to the minimum performance requirements. The VSC-A project developed performance requirements

---

[174] For more information, see Vehicle Safety Communications Project - Final Report (Report No. DOT HS 810 591) at www-nrd.nhtsa.dot.gov/pdf/surplus/nrd-12/060419-0843/PDFs/MainReport.pdf (last accessed Jan. 28, 2014).
[175] Id.

for GPS performance,[176] warning repeatability, maximum warning latency, true and false positive warning rates, EEBL, FCW, BSW+LCW, DNPW, IMA, and CLW.[177]

The requirements were refined yet again in the V2V Interoperability project, known as V2V-I.[178] These requirements were broken up into both functional (high-level) requirements and performance (detailed) requirements.[179] The V2V-Interoperability Report contains design requirements for the on-board equipment (DSRC radio, GPS receivers, and processors). Some of the requirements that were developed during these projects have been worked into a number of IEEE and SAE standards. For further reference on the development of the standards, please see Section V.E.

The performance requirements that were used and implemented in the specification documents for the VADs and ASDs during the Safety Pilot Model Deployment were developed directly from the V2V-I Project. During the Model Deployment over 3,000 vehicles have been equipped with V2V and V2I technologies and are driving around the public roadways of Ann Arbor, Michigan. Sixty-four of these vehicles are equipped with integrated OEM solutions (CAMP-developed device) that have been fully integrated into the vehicles, 300 vehicles have aftermarket technology installed, and 2,850 vehicles are outfitted with vehicle awareness devices that can transmit the BSM to other vehicles but cannot receive information with which to alert the driver. Many of these systems have internal components designed and built by a number of different manufacturers and suppliers. These vehicles have been operating together, as a system, providing alerts and advisories to drivers as a representation of how a fully functional V2V system might work. While this is a research project, and is built using prototype hardware, the performance requirements are adequate to ensure system functionality – i.e., the vehicles are capable of communicating with each other. The identified requirements are based on working systems that were collaboratively developed between NHTSA and CAMP, but since they are

---

[176] The VSC-A project performance requirement for GPS were further refined during the GPS available study. For a discussion of the performance requirements for GPS, *see:* Section V.D.1.d) "Relative Positioning."

[177] For more information, see VSC 2 Consortium, "Vehicle Safety Communications – Applications (VSC-A) Final Report: Appendix Volume 1 System Design and Objective Test," (Sept. 2011, Report No. DOT HS 811 492B) at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014) [Hereafter, "VSC-A Project Appendix Volume 1"]; see also VSC-A Project Appendix Volume 2 for full system requirements and further information.

[178] The critical system requirements were published prior to the Safety Pilot Model Deployment as the VAD and ASD system specifications. See System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014) and System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Dec. 26, 2011) at www.its.dot.gov/meetings/pdf/T2-05_ASD_Device_Design_Specification_20120109.pdf (last accessed Feb. 20, 2014).

[179] The critical requirements can be found in sections 4 and 5 of System Requirements Description, 5.9 GHz DSRC Vehicle Awareness Device Specification, Version 3.6 (Jan. 25, 2012) at www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014)

based on non-production systems, the agency does not consider them finalized, recognizing that at more work is necessary as discussed earlier in this section before production-level deployment can be realized. The following table shows a summary of the high-level requirements, including the maturity of the performance requirements that have been employed in the V2V program research. The table also shows the range of different research projects from which the Safety Pilot performance requirements were leveraged.

Table V-6 Performance requirements used in V2V research

Requirement	Research Activities	Requirements Exist for Safety Pilot	Finalized	Under Development	Comments
Safety application requirements	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	Application compliance test procedures, BSM Min Performance Req./SAE J2945
DSRC transmission range	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	e.g., 300 meters, 360 degrees, BSM Min Performance Req./SAE J2945
DSRC receiving range	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	e.g., 300 meters, 360 degrees, BSM Min Performance Req./SAE J2945
Language vehicles speak when they communicate with one another	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		communication protocol SAE J2735, IEEE 1609.2 and IEEE 1609.3 and IEEE 1609.4
Language used for communication between vehicles and RSEs	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	communication protocol IEEE 1609.2 and IEEE 1609.3 and IEEE 1609.4
Information necessary to be included in the V2V communication	VSC, VSC-A, V2V-I, Safety Pilot	✓		✓	BSM protocols; SAE J2735, BSM Min Performance Req./ SAE J2945
Information necessary to be included in the communication between vehicles and RSEs	VSC-A, V2V-I, Safety Pilot	✓		✓	WSM Protocols; IEEE 1609.3 & 1609.4
DSRC radio channel operational mode and usage for communication with other vehicles	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		IEEE 1609.4, BSM Min Performance Req./ SAE J2945
DSRC radio channel operational mode and usage for communication with RSEs	VSC, VSC-A, V2V-I, Safety Pilot	✓	✓		IEEE 1609.4, BSM Min Performance Req./ SAE J2945
Basic Safety Message data accuracy needs to be specified	V2V-I, Safety Pilot	✓		✓	BSM Minimum Performance Requirements/SAE J2945
Error tolerance and error correction capability (considering potential distortion) of over the air signals being received by OBE	VSC-A, V2V-I, Safety Pilot	✓		✓	IEEE 802.11p
Ability of the system to accommodate all communication within a given area of coverage and for a given number of vehicles (DSRC channel congestion mitigation)	VSC-A, V2V-I			✓	DSRC channel congestion mitigation research will continue beyond 2013 decision
Method of synchronizing communication system network	VSC-A, V2V-I, Safety Pilot	✓	✓		GPS (UTC) time; BSM Min Performance Req./ SAE J2945

Ability to verifying and validating messages from other vehicles	VSC-A, V2V-I, Safety Pilot	✓	✓		
Method of verifying and validating messages from other on-board ECUs (within a given vehicle. E.g., vehicle data bus)					Need for plausibility checks, data bus security is under consideration
Security scheme to protect V2V communication	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	Prototype SCMS design
Security scheme to initiate and ensure trusted key establishment	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	
Security scheme to support key management	VSC, VSC-A, V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	
Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust at the Infrastructure side	V2V-CS, V2V-VSCS				
Physical security to protect security components and elements that will be essential pieces of establishing and sustaining the network trust on the on-board DSRC devices	VSC, VSC-A, V2V-CS, V2V-VSCS			in planning	
Security scheme to protect Personally Identifiable Information (PII)	V2V-I, V2V-CS, V2V-VSCS, Safety Pilot	✓		✓	

c) *Software performance requirements*

Research is needed to determine if the software components that NHTSA may require as part of an FMVSS can be regulated using objective tests, without requiring the use of specified algorithms. NHTSA has not previously regulated system aspects as detailed as software components. This may be necessary because a performance test may allow multiple pathways to compliance but may not result in full interoperability among devices. Because software can allow for multiple methods of producing the same result, there is a gap in our understanding of how potential multiple software solutions by different device manufacturers (or vehicle manufacturers) would affect the V2V system's ability to be interoperable.

As an example, congestion mitigation has currently been tested during the V2V-I project using two different mitigation algorithms. These algorithms were specified under the system requirements and units were fielded with these predetermined algorithms. They worked well and predictably under all test scenarios because all software components were the same. Had they instead been performance metrics such as "the channel busy ratio must stay below 70 percent at all times," we do not know if different suppliers would have developed individual mitigation solutions and whether they would be interoperable. There is a risk that if different suppliers were to use different mitigation strategies, vehicles may not receive BSMs with the frequency needed for the safety applications to function.

Research Need V-2 Impact of Software Implementation on DSRC Device Performance

Research Activity:	DSRC Device Performance Requirements
Description:	Finalize requirements for V2V device software standards, performance, and requirements needed to ensure interoperability with other vehicles and roadside equipment, support safety applications, and adhere to security and privacy communications requirements.
Target Completion:	Mid-2015 (draft report to NHTSA)

Current or planned NHTSA research addressing this need:
Working with both industry (CAMP) as well as independent (third-party) automotive and communications research companies, NHTSA is developing a complete description of functional, performance, and operational requirements for the on-board vehicle systems needed to support V2V communications.

d) Additional performance requirements research

Current performance requirements exist in a pre-competitive, prototype research state. We have been able to achieve a large scale (2,800 vehicles) test in which vehicles could reliably talk to each other, yet these requirements are not FMVSS-ready given that test procedures to gauge compliance with the requirements do not exist for all components of the system. Additionally, test procedures that do exist have not been evaluated to ensure that they produce objective, repeatable results, and minimum requirements necessary for some components of system such as the minimum broadcast frequency of the BSM necessary to support safety applications have yet to be determined.

NHTSA is currently engaged in research with Booz Allen Hamilton[180] to examine the minimum performance measures for DSRC communication and system security. This research will include functional and performance requirements for the DSRC device and present NHTSA with a list of recommended changes to these requirements as currently laid out for the Safety Pilot Model Deployment. An example of these recommendations would be how to deal with end-of-life issues on the DSRC components and security system.

In order to participate in the V2V system, the current design assumes that V2V devices will carry up to three years of security certificates. It is possible that V2V devices may retain these certificates upon their retirement. If the certificates were somehow obtained by a malicious

[180] NHTSA Task Order DTFH61-11-D-00019-T-13016 DSRC Communications Performance Measures.

party, they could be used to participate in the system without permission. To maintain the security of the system, some requirements for device end-of-life (e.g., forced memory purging of certificates, destruction of a malfunctioning or non-functional device, or some other end-of-life measure) will likely be necessary in exchange for participation in the SCMS, although it remains to be determined whether such requirements would be from NHTSA or from the entity managing the SCMS.

Research Need V-3 DSRC Data Communication System Performance Measures

Research Activity:	DSRC Device Performance Requirements
Description:	The purpose of this research is to finalize the operational modes and scenarios, key functions, and qualitative performance measures that indicate minimum operational performance to support DSRC safety and security communication functions.
Target Completion:	Mid-2015 (draft report to NHTSA)

Current or Planned NHTSA research addressing this need:
The research to be completed under Need IV-2 will also address this research need.

Once performance requirements have been identified, objective performance metrics to measure those requirements will need to be developed to support FMVSS-level testing. NHTSA should be able to leverage the certification testing work used to support the Safety Pilot, although performance testing conducted for the Safety Pilot will need to reflect any changes the performance requirement research may suggest.

Research Need V-4 Development of Safety Application Test Metrics and Procedures

Research Activity:	Safety Application Objective Test Procedures & Performance Requirements
Description:	This research will take the performance measures and objective test procedures used during the research of V2V applications and develop FMVSS level performance measures and safety application objective tests.
Target Completion:	2016 (draft test procedures)

Current or Planned NHTSA research addressing this need:
CAMP, NHTSA, and the Volpe Center are completing projects to address the development of objective test procedures for IMA and LTA safety applications. This research activity will include investigation of the rationale for and validation of various performance measures; test the practicability and need for non-ideal conditions testing; and evaluate the applicability of the tests to V2V based or V2V/Vehicle-based sensor combined systems.

E. System Limitations

1. What are the known system limitations for V2V communication?

V2V safety systems use messages broadcast by vehicles to enable cooperative crash warning applications. Traditional crash warning applications, on the other hand, use vehicle-based radar, lidar,[181] mono camera, stereo camera or combinations of these sensors to perform similar threat detection in order to enable crash warning applications. Each sensor has unique characteristics that translate into system advantages and disadvantages. This section discusses system limitations of V2V safety systems by comparing their characteristics to those of traditional crash warning systems. The discussion is based on the information summarized in the following table.

Table V-7 Collision Avoidance Sensor Summary

○ Bad ◔ Poor ◑ Fair ◕ Good ● Excellent

Sensor Type	Radar 24 GHz	Radar 77GHz	Lidar	Mono Camera	Stereo Camera	Radar + Camera	V2V
Field of view	56^0	18^0	27^0	36^0	48^0	$18^0/36^0$	360^0
Typical range	60 m	200 m	10 m	(50 m)	(150 m)	200 m / 50 m	300 m
Accuracy	0.2 m	0.2 m	0.2 m	?	?	0.2 m / ?	< 1.5 m
Relative reliability in snow, fog, heavy rain	◕	◕	◕	◑	◑	◕	●
Reliability in direct sun and shadows	●	●	●	◑	◕	●	●
Reliability in "urban canyons"	●	●	●	●	●	●	◑
Reliability in tunnels and under heavy foliage	●	●	●	◕	◕	●	◕
Vulnerability to damage or misalignment	Yes	Yes	Yes	No	No	yes	No
Generally considered sufficient to react to	no	No	No	no	yes	yes	Yes

[181] Lidar detects distant objects and determines their position, velocity, or other characteristics by analysis of pulsed laser light reflected from their surfaces. (Lidar operates on the same principles as radar and sonar.)

fixed objects (by OEMs)							
Number of objects (vehicles) that can be tracked/processed at any given time	17	17	17	?	?	17/?	TBD >200
Capable of close range, low speed range-rate estimates (city safe capability	No	No	Yes	No	No	No	for warning applications only
Requires multiple vehicles to be equipped	No	No	No	No	No	No	Yes
Supports pedestrian detection	need multi-sensor system	need multi-sensor system	need multi-sensor system	need multi-sensor system	yes	yes	TBD
Sufficient to support activation of active safety systems	No	No	No	No	yes	yes	TBD

a) Field of view and range limitations

The figures below illustrate a generic traffic scenario for both a conventional crash avoidance system and a V2V-based safety system. Assuming all vehicles are equipped with V2V, the orange vehicle in Figure V-4 receives messages from the other vehicles in a 360° area bound by a 300 meter radius, enabling safety applications that monitor the entire surroundings for crash imminent threats. The conventional system shown in Figure V-4 includes forward-looking long range radar and mono camera, as well as short range radar on each rear corner for blind zone detection. The forward sensor fields of view are illustrated by the blue shading, which depicts the long-range radar, and the white shading, which depicts the mono camera. The white shading at each rear corner depicts the short-range blind spot radars. As illustrated, the forward-looking radar can be obstructed by the first vehicle directly ahead in its lane, and thus is often unable to track other vehicles in the same lane. Similarly, the camera can be obstructed by objects such as the commercial truck in the illustration. With the four sensors shown, the conventional system is limited to reliably detecting and monitoring only two of the vehicles shown, the vehicle directly in front and the vehicle in the blind zone at the rear left of the equipped (orange) vehicle. By contrast, the V2V system can warn of threats from any direction using a single GPS sensor and DSRC communications.

Figure V-4 V2V System

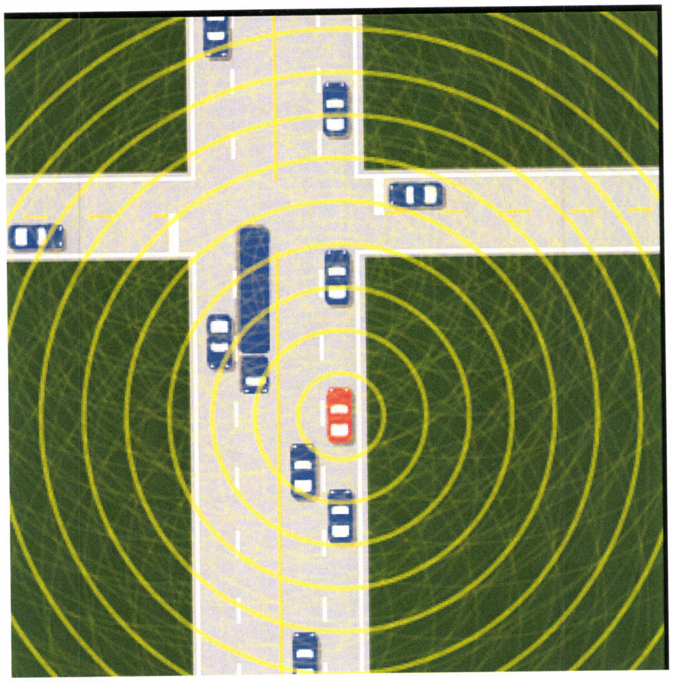
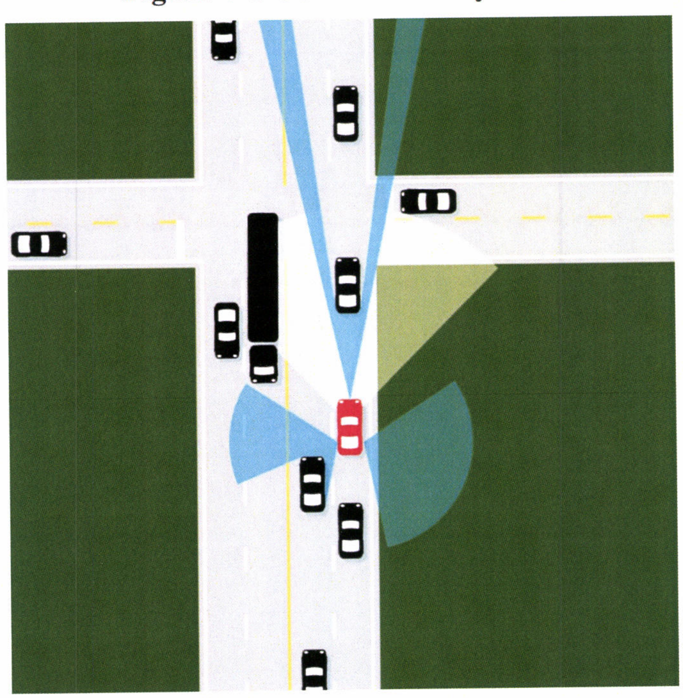


Figure V-5 Conventional System



b) *System availability limitations*

V2V system availability degrades gracefully[182] when subjected to reduced GPS availability (e.g., urban canyons or under extremely heavy foliage) or prolonged GPS outages (tunnels). In its current state, the V2V safety system is relatively immune to intermittent GPS outage (less than 1 second), which accounted for the majority (93%) observed during the 20,000 miles of data collected in the DOT-CAMP system performance testing.[183] Prolonged outages of 2 to 5 seconds result in graceful degradation of the system (safety applications), potentially limiting the applications to only those that require road-level positioning accuracy (e.g., intersection movement assist) and not allowing those that require lane-level accuracy (e.g., forward collision warning).

c) *Basic safety message congestion limitations*

Large scale deployment of V2V safety communications will require a communication system that will function and be able to support interoperability even when penetration of V2V into the vehicle fleet becomes widespread. There will be situations during normal driving conditions where a large volume of vehicles are driving in close proximity to each other, such as heavy freeway traffic. It will be important to ensure that the volume of messages in such "congested" situations does not somehow compromise the effectiveness of the system (and thus the effectiveness of the safety applications that might be enabled by the system) by saturating devices with messages, making it difficult to quickly sort out which are safety-critical and which are not, or even to transmit in general.

Testing of the scalability of the communications network has been conducted under two main projects, the Vehicle Safety Communications – Applications project[184] and the V2V-

---

[182] Fault tolerance, or graceful degradation, is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its' operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naïvely designed system in which even a small failure can cause total breakdown.

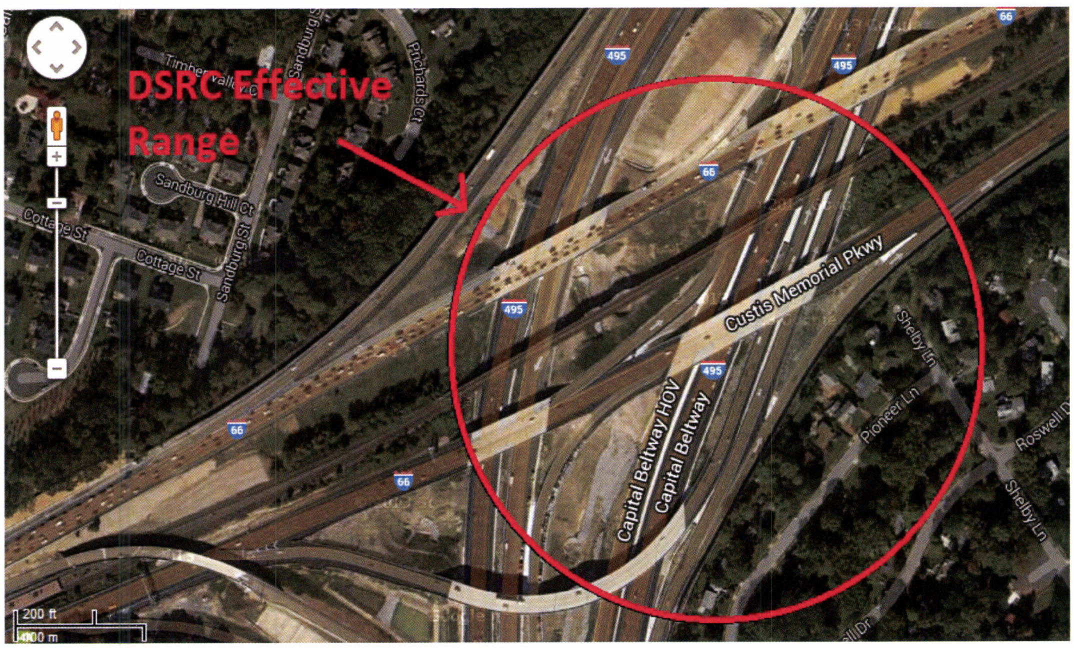
[183] Vehicle-to-Vehicle Safety System and Vehicle Build for Safety Pilot (V2V-SP) Final Report, Vol. 2: Performance Testing (Crash Avoidance Metrics Partnership on behalf of the Vehicle Safety Communications 3 Consortium, April 10, 2014). *See*: Docket No. NHTSA-2014-0022

[184] VSC-A was a 3-year collaborative effort between DOT and CAMP to develop and test communications-based vehicle safety systems to determine if DSRC at 5.9 GHz, in combination with vehicle positioning, can improve upon autonomous vehicle-based safety systems and/or enable new communications-based safety applications. The VSC-A project also developed performance requirements for GPS performance, warning repeatability, maximum warning latency, true and false positive warning rates, Emergency Electronic Brake Lights, Forward Collision Warning (FCW), Blind Spot Warning and Lane Change Warning (BSW+LCW), Do Not Pass Warning (DNPW), Intersection Movement Assist (IMA), and Control Loss Warning (CLW). See VSC-A Project Appendix Volumes 1 and 2 for full system requirements and further information. *See also:* Vehicle Safety Communications – Applications (VSC-A), Second Annual Report, January 1, 2008 through December 31, 2008 (Report No. DOT HS 811 466) at www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications (last accessed Jan. 28, 2014).

Interoperability project.[185] During VSC-A, 60 vehicles were tested for scalability of the network to see the effects of different data rates, multiple radios, and broadcast frequencies. The V2V-I project tested a grouping of 50, 100, 150, and 200 vehicles under a number of different V2V safety applications in multiple testing locations across the country.

As a point of reference, Figure V-6 shows the interchange between I-495 and Rt. 66 outside of Washington, DC. This interchange contains 2 express lanes and 4 regular lanes for I-495 running north and south and passing underneath Rt-66, which has 3 lanes running east and west. When off ramps are added, this leads to a total of 22 lanes of traffic in a 300 m radius. In grid-lock conditions, assuming an average car takes 24 ft. of lane space, this interchange can have over 800 vehicles in range of a single radio. The agency is conducting additional congestion research to better understand congestion limits and mitigation needs.

Figure V-6 I-495 & Rt 66 Interchange



Also tested during the V2V-I project were two algorithms for congestion mitigation.[186] These algorithms are designed to limit the frequency of BSMs broadcast during periods of high

---

[185] More information can be found in Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project - V2V-Interoperability, Draft Final Report, Section 4.2 (April 17, 2014). (Hereafter, "V2V-I Final Report"). See Docket No. NHTSA-2014-0022.

[186] Algorithm X is a transmission control protocol for scalable V2V safety communications that supports adaptive control of the message transmission rate and transmission power. Algorithm Y controls message transmission rate based on reported CBP from the neighboring vehicles and that measured by the host vehicle. The algorithm adapts

channel usage and at the same time ensure that vehicles were able to receive sufficient data to support the safety applications.[187]

Also developed under the V2V-I project was a proof of concept simulator designed to numerically simulate large vehicle networks. The V2V-I project found that even during the 200 vehicle test, at the maximum normal transmit rate of 10 Hz, the channel was not saturated, and all safety applications tested functioned normally. Although channel saturation was not reached, both congestion mitigation algorithms were able to demonstrate decreasing channel congestion while showing good safety application performance.[188]

Current research has shown that the V2V safety applications perform reliably in test scenarios with up to 200 vehicles in communication range. However, research conducted by CAMP and NHTSA has yet to estimate the number of other DSRC-equipped vehicles that a single DSRC radio would need to be exposed to in an environment (such as heavy freeway traffic) where channel congestion would be significant. Because the number of vehicles using the network within a particular broadcast area is not known, it is therefore not possible to compare the results of this testing to levels of channel congestion that might be experienced after full penetration of the technology.

Channel congestion may impact DSRC's effectiveness, which may in turn impact the effectiveness of DSRC-supported safety applications. Congestion mitigation may, therefore, be an issue that the agency needs to consider in developing potential future regulatory requirements for DSRC. NHTSA has planned additional research on this subject to address that need.

d) Relative positioning limitations

Based on testing during the initial phase of the Safety Pilot Model Deployment of several different GPS receivers of varying performance, quality and price, NHTSA believes that off the shelf, automotive GPS receivers on the market today are able to perform very well in V2V applications, although that statement should be qualified. GPS availability and solution accuracy deteriorate, for example, in deep urban environments and other areas of limited sky coverage. This will cause lane-level accuracy to degrade towards road-level accuracy in driving environments with limited sky visibility. While most of the safety applications require lane-level accuracy, and would thus be unavailable in those situations, road-level accuracy still allows the use of EEBL and IMA applications in these GPS-challenging locations. Any final determinations regarding the necessary performance for GPS units will be informed by the final results of the

---

the message rate up and down in order to maintain a desired level of channel utilization. For more information, see: V2V-I Final Report Section 4.2 and Appendix A, V2V Safety Communications Scalability Algorithms Details.

[187] V2V-I Final Report, at 79.

[188] V2V-I Final Report, at 79.

Safety Pilot, Driver Clinic system performance, and other ongoing research. Additionally, the deployment of new satellites, navigation industry improvements, and collaboration between the navigation industry and the automotive industry will improve GPS receiver accuracy and identify ways to address current challenging GPS environments.[189]

It should be noted that GPS receiver performance in the market is quoted in terms of the absolute positioning accuracy. The BSM minimum performance requirements for the vehicle positioning are currently phrased in terms of accuracy to an absolute position for purposes of the Safety Pilot, requiring the vehicle's reported latitude and longitude to within 1.5 meters of the actual position.[190] A relation must be made between the relative positioning performance required by the V2V safety applications and the receivers' advertised absolute positioning performance.

e) Comparison to sensor-based system

The V2V safety system communications is not impacted by weather (rain, fog, snow, sunlight or shadows). Radar and lidar perform reliably under all lighting conditions, while camera systems have some issues with shadows and lighting transitions, which are typical conditions for tunnels and under foliage during daylight. Additionally, V2V safety system communications are impaired by limited sky visibility, as in highly dense urban areas. In contrast, various conventional crash avoidance sensors perform reliably in urban canyons. In summary, both V2V safety systems and conventional crash warning systems have system availability limitations.

(1) Other Limitations for Conventional Sensor-based Systems

- Vulnerability to misalignment from impact (lidar and radar)
- Insufficient to react to stopped objects with a single sensor (lidar and radar)
- Limited number of vehicles can be processed (tracked) for threat determination
- Incapable of close range, low speed range-rate estimates (radar, camera)

(2) Other Limitations for V2V Safety Systems

- Requires a significant number of vehicles to be equipped for system effectiveness
- Accuracy is currently only sufficient for collision warning applications (see relative positioning section for future positioning improvements in Section V.E.1.d)

---

[189] Intelligent Transportation Systems: Vehicle-to-Vehicle Technologies Expected to Offer Safety Benefits, but a Variety of Deployment Challenges Exist (Nov. 2013, GAO-14-13). See www.gao.gov/assets/660/658709.pdf (last accessed Feb. 12, 2014).

[190] System Requirements Description: 5.9 GHz DSRC Vehicle Awareness Device Specification (Version 3.6, Jan, 25, 2012). See www.its.dot.gov/newsletter/VAD%20Specs.pdf (last accessed Jan. 28, 2014), requirement number SRD-USDOTOBE-003-ReqPOS003v001: Vehicle Position.

- Additional testing and field experience needed to establish level of trust of V2V messages sufficient to activate vehicle control applications

2. Potential mitigation strategies for known system limitations

a) System availability

For short duration GPS outages lasting a few seconds, devices can make use of inertial navigation units to predict the location of the vehicle. These units contain a number of accelerometers, gyros, and angular rate sensors that can be combined with mathematical models of vehicle dynamics to take the vehicle's position at loss of GPS and estimate the position further for a few seconds. Because of noise and error build-up in the sensors, the accuracy of the estimated position degrades the longer the estimation runs. Currently there are no long-term solutions for extended-duration GPS outages.

b) Basic Safety message congestion

Future research is currently planned under an extension of the V2V-I project, currently known as V2V-IE (phase 2). During this phase, physical testing will be conducted using up to 400 DSRC devices, both in vehicles and in specially-designed static test carts. This second phase will also work to refine the simulation, calibrating it against the data recorded during the first phase of the V2V-I project and data recorded during the field testing in phase 2. The goal of the simulation work is to simulate vehicle interactions far more numerous than what the agency believes can be practically field-tested. Following both the field testing and simulation work, the algorithms initially tested in phase 1 of the V2V-I project will be refined using the data collected during each. Finally, as the project closes, findings will be incorporated into SAE J2945 and other applicable SAE standards, which will facilitate development of devices that contain standardized congestion mitigation capability.

Research Need V-5 BSM Congestion Sensitivity

Research Activity:	Basic Safety Message Congestion Mitigation
Description:	Complete congestion mitigation and scalability research to identify bandwidth congestion conditions that could impair performance of safety or other applications, and develop appropriate mitigation approaches.
Target Completion:	Early 2015 (draft report to NHTSA)
Current or Planned NHTSA research addressing this need:	
Analysis, research and testing of potential congestion challenges and mitigation strategies will be completed by CAMP under the existing Interoperability task.	

Additionally, NHTSA believes that a DSRC channel congestion mitigation algorithm is important to ensure that the system identifies the most critical threats in densely populated traffic scenarios (assuming all equipped with V2V), to avoid missed threats and consequent risk to drivers.

c) Relative positioning improvements

Improvements to GPS signals and industry plans to produce automotive-grade receivers capable of using these signals will allow for increased positional accuracy in the future. The relationship between the specified absolute positioning performance of a receiver and its required relative positioning when measured against a different receiver needs to be better understood, and the study relating these two will lead to a more informed positioning performance requirement for V2V systems.

Given the observed differences in relative positioning performance in mixed pairs of receivers, such a relationship will need to be generalized for different receivers. CAMP has proposed, as part of Task 5 of the Vehicle-to-Vehicle Safety System Light Vehicle Builds and Model Deployment Support, a course of research to derive this relation. The path outlined in the proposal included a literature search for any previously-found relationships between relative and absolute positioning; an analysis of CAMP's previously-collected test data that includes both relative and absolute positioning, such as the Safety Pilot Performance Testing, and additional data collection activities. This additional data collection will expand the diversity of receivers from what is found in the literature search and from previous CAMP testing. The goal of this data collection and analysis will be to produce a generalized relationship between relative and absolute positioning for the receiver pairs tested.

Research Need V-6 Relative Positioning Performance Test

Research Activity:	Definition of Certification Requirements and DSRC Device Test Procedures
Description:	Research will be required to determine how to test relative positioning performance across GPS receivers produced by different suppliers and yield a generalized relationship between relative and absolute positioning.
Target Completion:	Onboard requirements (mid 2015), and draft test procedures (late 2015).
Current or Planned NHTSA research addressing this need:	
NHTSA is investing in developing the equipment and procedures to test adherence to communication standards and performance requirements (including relative positioning) as outlined in J2945 and other standards.	

The additional data collection CAMP is proposing as part of the relative positioning requirement definition offers an opportunity to evaluate the peculiarities of positioning performance observed during the Safety Pilot performance testing. These short periods (several minutes) of erroneous position were observed at particular geographic locations and were attributed by CAMP to particular combinations of vehicle and GPS receiver having differing positional biases. The testing of a wider range of different receivers will allow for the opportunity to observe these types of peculiarities, and a more informed assessment of their effect on positioning performance.

CAMP has additionally proposed collaborative work between them and the GPS suppliers to improve receiver performance for V2V safety. Using the GPS industry's expertise with CAMP's experience with V2V safety, this collaboration plans to identify improvements that could be made to the supplier's existing GPS hardware and software, further studying the effect of mixed receivers on relative positioning performance, and gaining a better understanding of tuning receivers explicitly for V2V applications leading towards the goal of a upgrading automotive grade GPS receiver.[191]

Research Need V-7 Vehicle and Receiver Positioning Biases

Research Activity:	Interoperability Research
Description:	Research to understand potential erroneous position reporting due to positional biases across multiple GPS receiver combinations.
Target Completion:	2014 (Published final reports)

Current or Planned NHTSA research addressing this need:
Recent work has been completed as part of Phase I of the NHTSA-CAMP V2V Interoperability project and FHWA-CAMP Light Vehicle Driver Acceptance Clinics Project System Performance Test task. The final reports are under publication review and should be published in CY14. Additional research is being performed in Task 5 of the FHWA-CAMP Light Vehicle Build and Model Deployment Support Project. The final report is expected to be published in early CY2015. The research findings will be reflected in CAMP's draft submission to the SAE J2945 subcommittee. No additional research is planned.

3. Device installation constraints and requirements

a) OEM Devices

OEM devices are likely to be installed during the construction of the vehicle. This results in fewer constraints on installation than other V2V devices require. Basic constraints should include GPS antenna location and offset (the antenna should be located in an area of the vehicle that is free of electro-magnetic interference and allows for an unobstructed view of the sky), and location of the transceivers (they should be located in an area of the car free of EMI that does not interfere with the transmission or reception of the BSM or security information). Since the

---

[191] Vehicle-to-Vehicle Safety System Light Vehicle Builds and Model Deployment Support (V2V-MD), Technical Proposal, Vol. 1 Statement of Work (Crash Avoidance Metrics Partnership on behalf of the Vehicle Safety Communications 3 Consortium, Feb, 15, 2012). See Docket No. NHTSA-2014-0022.

devices will be integrated into the vehicle, care needs to be taken not to overly restrict the manufacturer's ability to select internal locations for supporting hardware.

b) Aftermarket Devices

The agency believes a certified installer would likely be needed to complete the installation for aftermarket safety devices. It is imperative that all V2V components be properly installed to ensure that an aftermarket device functions as intended. Whereas some vehicle owners may choose to replace their own brakes or install other components on their vehicles themselves, installation requirements for ASDs will likely not be conducive to a do-it-yourself approach. Improper installation of a GPS antenna has the potential to affect V2V communications for that vehicle via false warnings, improperly timed warnings, etc. An improperly installed aftermarket device may put all other V2V-equipped vehicles it encounters at risk until the given vehicle stops communicating, or until its messages are rejected for misbehavior. After completing the installation into the vehicle, correct configuration settings for x, y, z offsets are critical for system operation.

4. Managing device updates and improvements

a) OEM Devices

OEM devices allow for a variety of different methods for upgrades and improvements due to their integrated nature. These devices will be integrated into the vehicle data bus, which will allow them to make use of the same methods that OEMs currently use to manage vehicle firmware updates. OEMs also have a large distribution network, allowing for a pre-existing pathway for vehicle owners to have a reputable entity upgrade vehicle-specific DSRC software updates. A similar method can be leveraged to renew security credentials and service misbehaving units.

OEM devices can also leverage the current methods of upgrade that existing consumer electronics use today. A smartphone connected to the car via Bluetooth, or acting as a mobile hotspot, can be used to wirelessly update security certificates. Also, built-in DVD and Blu-ray players in existing infotainment systems might serve as a physical method of installing upgrades and new security credentials. Lastly, any method used to upgrade software components in aftermarket devices can be leveraged to upgrade OEM devices as well.

b) Aftermarket Devices

There are a range of methods from the consumer electronics industry that can be used to provide updated applications, certificates, etc., for aftermarket safety devices. These include:

- Wi-Fi Access, Satellite
- Cellular Access
- Flash or SD Memory Card

An ASD could receive updates in virtually the same way that cell phones, tablets, and laptops acquire updates – by connecting the device to a Wi-Fi network and downloading any updates or improvements over the Internet or satellite. Alternatively, an ASD could use a cellular connection to a back office server. The main challenge with this approach is determining how to cover the cost of the data transferred over the cellular provider network. One solution would be to link the device to the owner's personal cell connection. A third way for an ASD to receive updates is to use a flash or SD memory card. This approach was used in the Safety Pilot Model Deployment when software updates were required for VADs and self-contained devices. This approach is somewhat analogous to using a DVD to update the GPS maps in OEM or aftermarket navigation systems. Security certificates could also be downloaded from a computer to the memory card and then loaded to the device.

F. Global activities and differences in V2V systems

1. Research and/or implementation of V2V communications in other regions

Significant V2V research and development activities are underway in both Europe and Asia. For Asia, Japan and Korea appear as the regional leaders for development leading to eventual production implementation. Europe has made clear statements toward implementing V2I mobility-focused applications by the 2015 timeframe.

2. Differences between the current U.S. regional vision and other regions

a) Comparison of U.S. to EU

The U.S. approach focuses on a core set of crash-critical V2V safety applications. In previous research conducted by the U.S. DOT under the Vehicle Infrastructure Integration (VII) Program, the major focus was V2I applications and establishing an infrastructure. The shift in primary focus to vehicle-based V2V applications facilitates implementation of ITS safety technologies without the costly infrastructure implemented through State and local government investment while achieving safety benefits at overall lower costs. While the EU has defined crash-critical safety applications as well, the priority in the EU is driver safety advisories (not safety-critical warnings), driver support messages (such as eco-driving), and commercial applications such as insurance.[192] The breadth and content of EU applications, including mobility applications, reflects their market-driven approach, whereas the V2V safety focus in the U.S. reflects the potential for reducing crashes.[193] In the EU standards development activities encompass a broader set of applications while DOT is primarily focused on developing standards

---

[192] Global V2X Deployment: Contrasts with U.S. Approach, at 35 (Bishop, Jan. 21, 2013) at Docket No. NHTSA-2014-0022

[193] Id.

to support V2V crash avoidance applications.[194] Release 2 of the ETSI standards, planned for 2017, will focus on crash avoidance.

European carmakers have committed to begin introducing DSRC systems in 2015 and it is likely that initial European introductions would be on high-end vehicles and/or newly re-designed vehicle models; a different approach than requiring DSRC on all vehicles. While initial introduction in Europe could come much sooner than the U.S., the number of equipped vehicles could grow faster after the initial start in the U.S., if the U.S. pursues a DSRC mandate for all new vehicles. However, vehicles deployed initially in Europe would address mobility, sustainability, and "soft" safety on "day one" for equipped vehicles, while the U.S. approach to address crash-critical safety in the initial deployment and to provide a framework for other areas, such as mobility and others would be more challenged to give benefits on "day one." Therefore the benefits obtained in the first years of deployment will be quite different between the U.S. and other regions of the world. Additionally, because the focus in the EU for DSRC systems is mobility and environment rather than safety, which primarily entails communications between vehicles and infrastructure rather than between vehicles, security is much less of a concern, and it is likely that DSRC mobility and environment applications can be rolled out without the need for a SCMS. This would eliminate the SCMS cost from DSRC implementation in the EU, although that would change if the EU was to move towards requiring DSRC-based safety applications. However, the current European model would entail infrastructure costs that are not envisioned in the initial stages of V2V implementation in the U.S.

In terms of spectrum allocation, the U.S. allocation calls for seven channels of 10 MHz each (a total of 75 MHz of spectrum located in the 5.85 to 5.925 GHz frequency band), with one channel designated as a control channel and one channel exclusively for safety. The EU allocation calls for the 5.875-5.905 MHz band to be designated for safety-related ITS functions with three 10 MHz channels, including the possibility of two additional channels being granted in the future. No control channel exists in the EU approach.

Activities on the infrastructure side in Europe are promising for a deployment corresponding to OEM introductions, but this is not a certainty. Advances in ITS have typically been fragmented and slow due to the EU Member States being sovereign nations. EasyWay, a major ITS deployment initiative sponsored by the European Commission, which supplements deployment funding at the national level, has published a Cooperative-ITS Roadmap aiming at 2017 deployment of V2X. In addition, the Amsterdam Group aims at 2015 deployment. Given these concerns, European Commission officials at the 2012 ITS World Congress noted they are

---

[194] Id.