2015 FHWA
Vehicle to Infrastructure Deployment Guidance and Products

V2I Guidance Draft v9a
September 29, 2014

Table of Contents

Guidance

Introduction

This guidance is intended to assist Federal Highway Administration (FHWA) staff and transportation system owner/operators deploy Vehicle to Infrastructure (V2I) technology not only in terms of the Federal-aid Highway program requirements but also practices to help ensure interoperability and efficient & effective planning/procurement/operations. It is not intended to be an introduction to the Connected Vehicle (CV) technology; however, there are several quick reference web links to videos, slide presentations, and information modules related to the fundamental principles of connected vehicle technology in the appendix.

Deployment of V2I technologies is not mandated and is not coupled with the National Highway Traffic Safety Administration's (NHTSA) advance notice of proposed rulemaking for Vehicle-to-Vehicle (V2V) communications.[1] The NHTSA rulemaking will not require State and local DOTs to deploy any connected vehicle infrastructure. However, it is important for the State and local agencies to understand a) what the decision could mean to them, b) what they need to know to prepare for an emerging connected vehicle environment, and c) what investments could be made in light of federal highway aid limitations to leverage a nationwide fleet of equipped vehicles in support of State and local policy and operational objectives. The guidance, associated guides, toolkits, and products are to be a useful resource to help those considering V2I deployment and to leverage developments in V2V communications.

New and emerging connected vehicle technologies offer an opportunity to significantly enhance safety through communications between vehicles. There is also a potential to leverage this technology to improve mobility and further enhance safety though interaction with the road infrastructure. Although in many respects this technology resembles traditional ITS deployments, it is different in many ways:

- The technologies go beyond "connected" to be cooperative, allowing data and information from many sources to be fused in real-time;
- It thus requires a level of national interoperability and functionality not found in today's ITS deployments;
- Because of its cooperative nature, it requires attention to security and privacy beyond today's ITS deployments;
- The basic technologies that form connected vehicle systems are evolving at a dynamic pace.

As such, these technologies require a focused set of guidance.

[1] U.S. Department of Transportation Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communications Technology (NHTSA 34-14 issued August 18, 2014); http://www.nhtsa.gov/About+NHTSA/Press+Releases/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications

This guidance was developed through cross modal cooperation at the Federal, State, and local levels. This guidance is intended to assist transportation agencies in making appropriate investment and implementation decisions when deploying connected vehicle systems. It does not negate or replace existing processes, but rather is intended to provide a clear statement of FHWA policy regarding such processes as planning, funding, siting, procuring, using, and providing access, among other critical actions.

In the event that there are inconsistencies between this guidance and existing laws and regulations, the existing laws and regulations take precedence.

As deployments come online and the technology matures this guidance will be assessed for relevancy, compatibility with real world deployment issues, and newly enacted transportation and communication statues and regulations. When needed this guidance will be updated and modified.

Background: The Connected Vehicle Environment

Connected Vehicle Environments (CVE) are systems comprised of hardware, software, and firmware that allow for the dynamic transfer of data between vehicles and between vehicles and the infrastructure including, at a minimum, Wireless Access in Vehicular Environment (WAVE) messages defined in Society of Automotive Engineers (SAE) J2735 that are broadcast on Dedicated Short Range Communications (DSRC). Moreover, the SAE J2735 DSRC standard is implemented for safety critical applications which cannot tolerate interruption or may be a threat to life.

However, non-safety-critical applications can use the DSRC protocol stack or other wireless media. For example, there are non-critical circumstances were communications with infrastructure and handheld devices that are implemented more effectively using multiple technologies—DSRC, cellular or Long-Term Evolution (LTE), publicly available Wi-Fi, satellite, wide or local area networks, or internet. Some points of connection may exchange data applications and may be primarily (or solely) enabled through DSRC; some applications may be primarily enabled through cellular, Wi-Fi, or other communications modes; and some applications may dynamically switch between communications modes in real-time. In many cases, the applications and/or radio will be capable of selecting the best communication mode to use at any time.

Most recently, the U.S. DOT has referred to Connected Vehicle as vehicle-to-vehicle communication technology and has been associated with vehicle telematics that connect vehicles to various information applications.[2] Moreover, the Basic Safety is the primary message set proposed to send data between vehicle and between vehicles and the infrastructure under the CVE. The CV can transmit and receive basic safety messages (BSMs) following the WAVE protocol, established in Standard IEEE 802.11p which uses the ITS band of 5.9 GHz (5.85 –

[2] DOT has long used the term "connected vehicle" to refer to the vehicle-to-vehicle communication technology that supports crash avoidance applications. However, the term has expanded to associate vehicle telematics that connect vehicles to various information applications through other forms of communications. Refer to Harding, J., Powell, eta, Vehicle-to-vehicle communication: Readiness of V2V technology for application; Report No. DOT HS 812 014, issued August 2014.

5.925 GHz). The content and format of a BSM are defined in Standard SAE J2735. The CVE uses the metric system and all applications should be developed and operate under it.

V2I components of CV Environments include: Roadside Units (RSUs), Signal Phase and Timing (SPaT) enabled traffic signal controllers, data links between V2I components and a traffic management center (TMC) or other back office, and any sensors or relays that link to or serve these components. An individual V2I deployment site could support more than one application, strategy, or impact area (i.e., safety, mobility, air quality, etc.). Generally, distribution of certificates through the CV security operations is not considered a safety application. CV technology also should consider pedestrians, bicyclists, and other possible nonmotorized users that may be within highways rights-of-way.

Although autonomous vehicles are not addressed in this guidance, this technology is not precluded by the FHWA V2I deployment guidance and may, in fact, be addressed by this guidance in the future. Appendix A contains a list of definitions, symbols, and abbreviations.

We seek public feedback on the proposed V21 components. Should any modifications be made?

V2I Deployment Policy Statement

Vehicle-to-infrastructure (V2I) services will take advantage of and build upon emerging vehicle-based technologies being deployed to support vehicle-to-vehicle (V2V) services. FHWA has not conducted a full benefit cost anlaysis of deployment of V2I services, but DOT believes the deployment may result in significant safety benefits and may also result in mobility and environmental benefits; and will be of significant interest to State, regional, and local transportation agencies.[3] Deployment of these services will be strongly encouraged by FHWA, but will be voluntary. FHWA will develop materials needed to support deployment (e.g., guides, tools, and best practices); ensure that deployed services are geographically interoperable; and ensure that deployed services are developed in accordance with the requirements in Part 940 of Title 23 within the Code of Federal Regulations (23 CFR 940) and other applicable regulations.

The following sections define key areas of deployment guidance.

Planning

CV technologies, including V2I applications, have the potential for a fundamental advancement in surface transportation safety and operations. While interactions between vehicles and infrastructure have been mostly passive and detached across the network to date, CV technology will allow them to work together, both actively and cooperatively. While we do not yet know the magnitude, this could provide opportunities for congestion reduction, safety improvements beyond V2V safety applications, as well as improved traveler services and information. To fully realize its potential, V2I site deployments, operations, data access, and exchanges (among other

[3] Refer to Harding, J., Powell, eta, Vehicle-to-vehicle communication: Readiness of V2V technology for application; Report No. DOT HS 812 014, issued August 2014.

functions) will require even closer collaboration between transportation modes, public jurisdictions, and the private sector.

To this end, Metropolitan Planning Organizations (MPOs), Local Public Agencies (LPAs), transit operators, and States should begin considering V2I strategies in their long range planning. Topics of discussion could include: a general understanding of the system, which application options work well under what conditions, pros and cons of each option, capital costs and availability of funding, integration with the existing systems including traffic management and communication networks, long term impacts, cooperation and coordination across MPO boundaries and across State boundaries, staff needs, and the integration of these options into the existing Statewide or Regional ITS Architectures.

The National ITS Architecture provides a common framework to guide planning, defining, and integrating intelligent transportation systems at the Statewide and regional levels.[4] It is a mature product that reflects the contributions of a broad cross-section of the ITS community (transportation practitioners, systems engineers, system developers, technology specialists, consultants, etc.). The architecture defines:

- The functions (e.g., gather traffic information or request a route) that are required for ITS;
- The physical entities or subsystems where these functions reside (e.g., the field or the vehicle);
- The information flows and data flows that connect these functions and physical subsystems together into an integrated system.

The Connected Vehicle Reference Implementation Architecture (CVRIA) is an initiative that is defining the architecture views for connected vehicle technologies and identifying their key interfaces to analyze where standards may be optimal for interoperability or beneficial for operations. A standards development plan is in process to identify and prioritize candidate standards needed in support of connected vehicle implementation. The plan will consider adoption of existing industry standards from other areas, adaptation of existing standards, or development of new standards if existing standards are not viable. Ultimately, once the connected vehicle architecture views are mature, they will be incorporated into the National ITS Architecture.

To support planning for connected vehicle environments, the following work is ongoing:

- The FHWA is developing a planning guide to support analysis of investment options. A companion deployment guide is also under development to provide technical considerations for costing, siting, and installing connected vehicle technologies;
- Application requirements are emerging and can be found on the Connected Vehicle Reference Implementation Architecture website: www.its.dot.gov/arch/index.htm.

[4] Regional ITS Architecture Guidance Document Version 2.0, July 2006: On January 8, 2001, the US Department of Transportation published the FHWA Final Rule and FTA Policy, which implement section 5206(e) of the Transportation Equity Act for the 21st Century (TEA-21). TEA-21 required ITS projects funded through the highway trust fund to conform to the National ITS Architecture and applicable standards. http://ops.fhwa.dot.gov/publications/regitsarchguide/

Federal-aid Eligibility of V2I Equipment and Operations

A number of V2I activities are eligible for Federal-aid funding. However, specific program requirements should be met, and eligibility may need to be determined on a case-by-case basis.[5]

General Eligibility – Equipment, installation, preventive maintenance, and operational costs that support V2I applications and which are compatible with the basic CV standards for interoperability and security standards, are eligible for Federal-aid funding where eligibility for ITS investments has been previously established (also see "Transportation Systems Management & Operations: Operating Cost Eligibility Under the Federal-Aid Highway Program" – http://ops.fhwa.dot.gov/travelinfo/resources/ops_guide.htm).

Expenses associated with maintaining CV systems are considered to be operating costs and are eligible for Federal-Aid funding. Examples of these costs include: system maintenance activities to ensure peak performance (such as preventive computer maintenance); replacement of defective or damaged computer components; or other traffic management system hardware (including street-side hardware). However, routine upkeep items that are not critical to maintaining continuous operation of the system (e.g. painting, grounds keeping, etc.) are not eligible for Federal-aid funding.

Marginal additional costs to purchase and install ITS equipment or communication technology capable of being upgraded or modified to operate in a deployed CV V2I environment at a future date are eligible for Federal Aid funding. In fact, it is recommended that as soon as CV technologies are available, such equipment should be the standard for deployment.

Procurement of spare "system-critical" parts (i.e., essential for the successful operation of the system) that are susceptible to failure, regardless of reason, are eligible if identified in a deployment maintenance and replacement plan (see reliability guidance).

Safety - V2I safety applications are eligible for HSIP funds if they address a State's Strategic Highway Safety Plan (SHSP) priority, are identified through a data driven process, and contribute to a reduction in fatalities and serious injuries. Additional information is available in the HSIP MAP-21 Interim Eligibility Guidance.[6]

Mobility – Costs that support V2I mobility and safety applications and which are compatible with the basic CV standards for interoperability and security may be eligible for NHPP and STP funds. NHPP-funded projects should be used for a facility located on the National Highway System (per 23 U.S.C. 119(c)) and should lead to advancement of the mobility, freight, condition and safety goals established at 23 U.S.C. 150(b) (per 23 U.S.C. 119(e)(2)). Just being one of the eligible projects listed at 23 U.S.C. 119(d) alone does not make the project NHPP eligible. Eligibility for funding under the Surface Transportation Program is determined by the provisions at 23 U.S.C. 133.

[5] Refer to FHWA Operations Regulation and Policy http://www.ops.fhwa.dot.gov/opsregulationpolicy.htm and Transportation Systems Management & Operations: Operating Cost Eligibility Under the Federal-Aid Highway Program. Reference http://www.ops.fhwa.dot.gov/travelinfo/resources/ops_guide.htm#fed

[6] http://www.fhwa.dot.gov/map21/guidance/guidehsip.cfm

Congestion Mitigation and Air Quality (CMAQ) Improvement Program –Each CMAQ project should meet three basic criteria[7]: *it should be a transportation project, it should generate an emissions reduction, and it should be located in or benefit a nonattainment or maintenance area.*[8] All phases of eligible projects – not only construction- are eligible for CMAQ funding. This includes studies that are part of the project development pipeline (e.g., preliminary engineering) under NEPA. However, general studies that fall outside project development do not qualify for CMAQ funding. Additional information is available in the CMAQ under MAP-21 Interim Program Guidance.

FHWA determines the eligibility of all projects, except those related to transit. FTA determines the eligibility of transit projects. While the eligibility determination is not made jointly, the FHWA, FTA, and EPA field offices should establish and maintain a consultation and coordination process for timely review of CMAQ funding proposals, including those related to V2I.

ITS projects that support V2I applications, including equipment and installation costs, may be eligible for CMAQ funding provided they meet the basic eligibility requirements. CMAQ funds may also be used for operational assistance subject to the limitations as described in section VII.A.2 of the CMAQ Interim Program Guidance. Examples of V2I projects/applications, such as SPaT, eco-drive, Congested Intersection Adjustment, and traveler information systems, are eligible for CMAQ funds as they can be effective in relieving traffic congestion, enhancing transit bus performance, and improving air quality.

Transit projects that support V2I applications may be eligible for CMAQ funds. The FTA administers most transit projects. For such projects, after the FTA determines a project eligible, CMAQ funds will be transferred, or "flexed," from the FHWA to the FTA, and the project will be administered according to the appropriate FTA program requirements. Section VII.F.6 of the CMAQ Interim Program Guidance included a detail discussion of CMAQ eligible transit projects.

Although use for purely research deployments with test vehicles (e.g. ITS JPO's Safety Pilot Model Deployment) would not meet the eligibility test, deployments where 1) fully functioning equipped cars (either factory or aftermarket installations) will be interacting with the technology and impacting mobility and 2) may ultimately be incorporated in the wider deployment of the technology, would be eligible.

V2I Deployments and NEPA

V2I deployments are covered under 23 CFR 771.117(c)(21) as a Categorical Exclusion (CE) for certain intelligent transportation systems (ITS).[9] Since the deployments by definition have the primary function to improve the efficiency or safety of a surface transportation system, support the CV security system and enhance passenger convenience, they are covered by this section. Additionally these deployments will be typically within the existing operational right of way,

[7] http://www.fhwa.dot.gov/environment/air_quality/cmaq/
[8] http://www.fhwa.dot.gov/environment/air_quality/cmaq/reference/intelligent_transportation_systems/
[9] http://www.gpo.gov/fdsys/pkg/CFR-2011-title23-vol1/pdf/CFR-2011-title23-vol1-sec771-117.pdf

conform to the criteria in section 23 CFR 771.117 (a), and are not likely to trigger the unusual circumstances provisions discussed in 23 CFR 771.117 (b).

Interoperability

To operate properly, V2I deployments should to be compatible with any CV security policies that may be developed, support the distribution and/or receipt and use of security certificates to the maximum extent possible, and protect privacy at the highest level appropriate to the performance of a Connected Vehicle (CV) Environment.

An operable CVE relies on the exchange of information, predominantly a Basic Safety Message (BSM) emanating from vehicles, but other messages as well.[10] Specifically, FHWA recommends that a BSM conform to SAE J2735 and should also be "signed" with a valid certificate in order to establish a trust relationship with those receiving and acting upon the message. We request comments on this proposed SAE J2735 conformation. Since vehicles and devices may interact with equipment from all over the Nation, the requirements for transmission and receipt of BSMs, including certificates, should be standard across the Nation and across vehicle makes and models; device makes and models; and applications when related to safety-critical messages. Similarly, V2I deployments should conform to these same requirements in order for successful exchange of information between vehicles, devices, and applications within the CV environment. Standard SAE J2735 establishes the current accepted message set for a connected vehicle environment, although this is subject to change as part of NHTSA's ongoing V2V rulemaking process.[11]

Although deployment of V2I components is voluntary, to the greatest extent possible, the functionality and utility of deployed applications will be consistent between transportation modes/regions and for deployed V2I equipment and/or applications to be eligible for Federal – aid funding and should comply with existing ITS and CV guidance/processes provided by U.S. DOT[12]. Upcoming reference manuals and reports will highlight where local choice is an option or where uniformity is required or offers a greater benefit.

Table 1 illustrates the types of messages, and the message handler, required to enable a variety of V2I applications. Note that the list of applications in Table 1 is illustrative and not exhaustive.[13] It is anticipated that industry will create additional applications that serve driver needs and agency requirements.

[10] http://www.standards.its.dot.gov/Factsheets/Factsheet/71

[11] NHTSA 34-14 press release issued August 18, 2014; http://www.nhtsa.gov/About+NHTSA/Press+Releases/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications

[12] http://ops.fhwa.dot.gov/publications/regitsarchguide/

[13] The Connected Vehicle Reference Implementation Architecture (CVRIA), a subset of the National ITS Architecture, defines functionality and information exchanges needed to provide connected vehicle applications, and supports connected vehicle project planning and development activities at State and local levels when an agency is ready to consider V2I deployment.

Table 1. V2I Messages by Application and Message Handler

	Position Correction Message Handler	Map Message Handler		BSM/ Approaching Vehicle Agregator				Traffic & Rail SignalMessage Handler			Local Weather and Road Surface Message Handler (Map Overlay)		Roadside Signage DMS Arbitrator	Local/Back Office User Interface
	Position Correction Message	Local Map Message	Traffic Signage Data	Approaching Vehicle Mess	BSM (V2I)	Vehicle Weather Data	Oversize Vehicle Detection	SPaT Messages (SRM, SSM)	Rail Crossing SPaT	Ped Crossing SPaT	Local Weather Message	Road Surface Condition Mess	Dynamic Roadside Sign Mess	Installation, Configuration, Maintenance
INFLO-Queue Warning (Q-WARN) (TME Based)	✓	✓		✓	✓	✓							✓	✓
INFLO-Speed Harmonization (SPD-HARM) (TME Based)		✓		✓	✓	✓							✓	✓
Intelligent Traffic Signal System (ISIG)	✓	✓			✓			✓						✓
Emergency Vehicle Priority	✓	✓			✓			✓						✓
Transit Signal Priority	✓	✓			✓			✓						✓
Freight Signal Priority	✓	✓			✓			✓						✓
Pedestrian Mobility		✓			✓			✓		✓				✓
Eco-Traffic Signal Timing;	✓	✓			✓			✓						✓
Eco-Approach and Departure at Signalized Intersections;	✓	✓			✓			✓						✓
Eco-Traffic Signal Priority; and	✓	✓			✓			✓						✓
Eco-Driving - Connected Eco-Driving.	✓	✓			✓			✓						✓
Dynamic Low Emissions Zones	✓	✓			✓			✓						✓
Dynamic Eco-Lanes	✓	✓			✓			✓						✓
Enhanced Maintenance Decision Support System (MDSS).	✓	✓			✓	✓					✓	✓		✓
Information for Maintenance and Fleet Management Systems.	✓	✓			✓	✓					✓	✓		✓
Weather-Responsive Traffic Management.		✓	✓	✓	✓						✓	✓	✓	✓
Motorist Advisories and Warnings.		✓	✓	✓	✓						✓	✓	✓	✓
Information for Freight Carriers.	✓	✓			✓	✓					✓	✓		✓
Information and Routing Support for Emergency Responders.	✓	✓			✓	✓					✓	✓		✓
Red-Light Violation Warning (RLVW)		✓	✓					✓			✓	✓		✓
Stop Sign Gap Assist (SSGA)		✓	✓	✓	✓								✓	✓
Curve Speed Warning (CSW)		✓	✓	✓	✓						✓	✓	✓	✓
Stop Sign Violation Warning (SSVW)		✓	✓								✓	✓		✓
Railroad Crossing Violation Warning (RCVW)		✓	✓					✓	✓		✓	✓		✓
Spot Weather Information Warning (SWIW)		✓	✓	✓	✓						✓	✓	✓	✓
Oversize Vehicle Warning (OVW)	✓	✓	✓	✓	✓		✓						✓	✓
Reduced Speed Zone Warning (RSZW)	✓	✓	✓	✓	✓						✓	✓	✓	✓

Evaluation

Due to the newness of CV - V2I technology it is important to determine the effectiveness in meeting an identified need, benefits/cost, and user satisfaction assessment of these early deployments and the value of the investment. Evaluations are critical to understanding not only the technology as a whole but the specific applications, how/when to deploy, and assist in the planning process. There are general ITS project resources that will be useful for this purpose; for example the ITS Evaluation Guidelines – ITS Evaluation Resource Guide found at www.its.dot.gov/evaluation/eguide_resource.htm.

ITS Equipment Capability and Compatibility[14]

Early deployments of connected vehicle field infrastructure are likely to be installed alongside (or as part of) existing ITS equipment (e.g. Dynamic Message Signs, CCTV cameras, vehicle detections stations, etc.) and existing traffic signal controllers. One reason for this is that ITS deployments are already located in areas where V2I communications are likely to be most needed and beneficial. Also, these locations provide an opportunity to leverage existing power sources, cabinet space, and backhaul communications, which will minimize deployment costs. Installation of connected vehicle field infrastructure is conceptually no different than installation of other ITS equipment. The same considerations of siting, foundations, mounting points, power, physical accessibility and security, backhaul networks, and so forth that have become standardized and accepted in ITS practice, will be considerations in connected vehicle infrastructure deployments. In addition, new requirements may need to be considered for connected vehicle infrastructure deployments; such as, ensuring adequate line of sight for antennas and conducting mapping surveys of the surrounding roadway geometry.

In many cases, connected vehicle infrastructure will need to be integrated with existing field equipment in order to enable direct data communications between the infrastructure and vehicles. One example of this is where traffic signal controllers have new CV applications integrated into their functionality in order to broadcast signal phase and timing information directly to vehicles for safety and mobility applications. This type of integration of connected vehicle equipment with existing field equipment will require the use of standard interfaces and message sets that are currently being developed by FHWA and will be provided in V2I Reference Implementation documents (expected in late 2015).

In many ways, one can think of connected vehicle infrastructure as the next generation of ITS equipment being installed in the field with the potential to have a transformational impact on transportation operations and safety. As such, it is important to start considering V2I communications requirements and standards when new ITS equipment and traffic signal controllers are purchased and installed (procurement and installation guidance are described later in this document).

FHWA highly recommends that for any ITS equipment and traffic signal controllers, purchased in the future, and the deploying agency follow the systems engineering process and deploy the equipment in an environment that is CV ready. This guidance defines CV as a roadside installation that has the following characteristics:

- Reliable power supply;
- Two secure backhaul communications links, if required by implementing agency (one for ITS or traffic signal data and one for connected vehicle data);

[14] Any entity seeking to install equipment or provide service related to V2I must comply with all applicable Federal Communications Commission (FCC) rules governing DSRC. See FCC Report and Order on DSRC, available at: (https://apps.fcc.gov/edocs_public/attachmatch/FCC-03-324A1.pdf). Among other things, if an entity intends to deploy systems to provide V2I services under an FCC license, it must comply with all applicable FCC licensing rules and FCC rules implementing the National Environmental Policy Act and the National Historic Preservation Act.

- ITS equipment or controllers that are NTCIP standards compliant;
- Electronic map or geometric description of the surrounding area available in SAE J2735 compliant format;
- Roadside cabinet space sufficient to house an external processor (size depends on intended application) that may be installed in the future; and
- Considerations / plans regarding future mounting location(s) for a DSRC Roadside Unit (RSU) that will enable future V2I communications.

Connected vehicle infrastructure deployment standards and practices are still in development and will continue to be so until applications have been deployed and operating for several years. Practical field experience with connected vehicle system and applications deployment will continue to accumulate as new prototypes and model deployments are brought into the field. The Safety Pilot Model Deployment has significantly scaled up the field deployment of both infrastructure equipment and back office systems relative to prior test beds and demonstrations. In addition, U.S. DOT plans to initiate more connected vehicle pilot deployments in the coming years with an emphasis on V2I applications. Lessons learned and best practices from these pilot deployments will be invaluable guides to future deployments and will be the basis for updates to FHWA's V2I Reference Implementation and this V2I Deployment Guidance.

Hardware/Software Device Certification

It is the U.S. DOT's intent to enter a Cooperative Agreement with one or more facilities that will conduct qualification and certification testing for various connected devices (e.g., Vehicle Awareness Devices and Roadside Equipment), and applications used in large-scale connected vehicle deployment.[15] The Cooperative Agreement would identify an approach for a Connected Vehicle Certification Testing program. U.S. DOT has proposed a four (4) layer approach to connected vehicle devices and applications certification that includes Security Credential Management Systems (SCMS).

The four (4) layer approach consists of certifying a basic device to meet environmental and communications protocol requirements. Moreover, a basic device consists of hardware, software and radio components. The four (4) layers of certification are:

1. Environmental Abilities (e.g., temperature, vibration, weather);
2. Communication Protocol Abilities (e.g., the radio service interoperability for DSRC);
3. Interface Abilities (i.e., both the message syntax and contents are formatted properly);
4. Overall Application Abilities (i.e., verifies the system level function)

A basic device should be certified at layers one (1) Environmental Abilities and two (2) – Communication Protocol Abilities. However, an application should be certified in all four layers if it resides on a basic device. Therefore, this structure allows for multiple applications to be hosted on one device and use lower layer certifications (layers 1, 2, and 3). U.S. DOT will make available the certification facilities and SCMS certificates once they are finalized or receive the proper approvals.

[15] Connected Vehicle - Next Stage Certification Environment grant; http://www.federalgrants.com/Connected-Vehicle-Next-Stage-Certification-Environment-46654.html

Reliability

Typically, deployment of V2I Safety applications will augment existing devices, signs, or signals. However, given that the deployment is meant to improve safety or mitigate a design exception, operational reliability is paramount and should be incorporated in the design, procurement, and deployment.

V2I mobility applications will not necessarily backup existing schemes and have standalone functionality.

Reliability of deployed equipment should be incorporated into the system engineering process.[16] To ensure availability of the application, an equipment maintenance and replacement plan should be established holistically for all CV deployments. The idea of this concept and a resulting set of maintenance requirements build on the proven Systems Engineering approach. The systems engineering approach is recommended as the preferred method for developing ITS projects with FHWA's Rule 940.[17] (see http://ops.fhwa.dot.gov/docs/tmsmaintcptandplans/chapter3.htm).

Equipment and applications deployed on the NHS or using Federal-aid highway funds will be purchased from a qualified provider and will be certified through an industry approved process when available.

Use of Right of Way

Use of Right of Way (ROW) for V2I road-side unit (RSU) follows current regulations and funding eligibility. The State DOT should consider the engineering requirements, roadway safety, and sight distances when choosing the location of the V2I RSU in the right-of-way.

Installation of connected vehicle infrastructure within the ROW will be allowed as long as its use has a public benefit and does not impair the safety of the roadway. Private sector secondary use is permissible as long as it 1) does not interfere with or degrade the current and future primary mobility/safety applications; 2) the private application will be opt-in and the highway user will be able to disable at any time, at no cost to the user; and 3) a fair market value of the private application's use will be established.[18]

Private use arrangements are subject to 23 U.S.C. 156 and require the State to charge the fair market value for non-highway use or to obtain an exception from FHWA based on "a social, environmental, or economic purpose." (§ 156(b) and 23 CFR 710.403(d)). For Interstate right-of-way use an airspace agreement is necessary (23 CFR 710.405(d)). The Federal share of net income from the revenues obtained by a State from the use of the right-of-way should be used by the State for title 23 projects; preferably for deployment and operation of the V2I network.

For Federal purposes, secondary use messages are not considered advertising (e.g., displayed in a vehicle or on a personal device) under the Highway Beautification Act; however State law or policies could supersede this distinction.

[16] http://ops.fhwa.dot.gov/publications/seitsguide/
[17] FHWA Rule 940/FTA Policy, http://www.ops.fhwa.dot.gov/its_arch_imp/policy.htm
[18] http://transition.fcc.gov/eb/mdrd/rules/pole.html

Allowance of Private Sector Use[19]

FHWA supports the ability to maximize the possibility of private investment to leverage costs for deployment and operations. Public Owners/Operators of infrastructure communication systems (fiber optics, radio relay, etc.) can allow off-public right-of-way private sector use of the system for V2I communication as long as there is a public sector benefit. This should include for following:

- There is a public sector benefit of the V2I RSU;
- The private sector use does not interfere with or degrade the primary safety / mobility applications;
- The private sector application will be opt-in by highway users and highway users will be able to disable the application at any time;
- The roadway facility owner and/or Public Owners/Operators of the infrastructure system are not charged for any private sector use.

Public Owners/Operators of the infrastructure communication system may use, for example, a privately owned RSU to:

- Control traffic management signals and/or devices;
- Monitor roadway traffic performance;
- Distribute security certificates to vehicles, devices, or applications;
- Provide traveler information to vehicles through V2I communications.

The cost associated with installation and operation of private sector use or components would not be eligible for Federal-aid beyond the operation of the communication backhaul.

Design considerations for facilities

V2I applications may be utilized to mitigate safety and operational impacts that arise due to substandard geometric features of highways. This can be done at the network level or as part of a design exception. Therefore, the minimum design standards can be modified to take into account the safety and mobility benefits.

To operate in coordination with the national level, deployed equipment needs to be interoperable and coordinated with other modes of transportation (i.e. light and heavy duty vehicles, transit systems, railroad crossings, etc.). To the maximum extent possible, all devices and applications deployed by jurisdictions and modes should leverage this technology between the transportation entities and should not be standalone deployments.

Projects to construct or reconstruct highways should be designed in a manner that accommodates the concurrent or possible future installation of V2I roadside equipment.

[19] http://transition.fcc.gov/eb/mdrd/rules/pole.html

Use of existing structures and infrastructure

Installation of connected vehicle equipment on existing structures/infrastructure will be allowed as long as its use has a public benefit and does not create potential safety issues. Private sector secondary use is permissible as long as it complies with the Uses of the Right of Way section contained elsewhere in this guidance. Designers should consider how CV technologies will affect pedestrians, bicyclists, and other nonmotorized users within the highway right-of-way and how CV technologies may affect access to transit services, and how CV technology can enhance livability.

Use on public sector fleets (including incident responder vehicles)

Depending on specific program requirements, Federal-aid highway funds can be used to procure components that enable V2I applications that are installed on public sector vehicles. This includes all the components associated with both the collection of data and dissemination of that data from the vehicle to the infrastructure, as well as information dissemination from the infrastructure to the vehicle. Federal-aid funds can also be used to procure infrastructure-based components that enable V2I applications. This includes, and is not limited to, roadside equipment and components installed in maintenance garages and traffic/emergency operations centers. Instrumenting private contractor equipment performing maintenance/response or providing workzone safety capabilities can be federally funded as long as it provides a public benefit and the public sector retains ownership/control of the CV equipment.

To achieve interoperability, all of the above components will need to comply and be consistent with Connected Vehicle architecture and standards. Funds cannot be used for maintenance of any of the components described above unless identified in the equipment maintenance and replacement plan (see reliability guidance). [20]

The applications utilized on public fleets should comply with any guidance and recommendations that may be developed pertaining to demands on the driver's attention with respect to the collection of data (e.g., recording current road conditions) and presentation of information within the vehicle.
Through the system design process and the implementation of the applications, V2I messages should comply with Connected Vehicle Reference Implementation Architecture (CVRIA) and Basic Safety Message (BSM) standards.[21] [22] Also, the messages should be prioritized in a manner that considers the immediacy/urgency of the message and its consequence (e.g., safety messages would take priority over mobility and environment messages). The applications

[20] Ad hoc or non-critical maintenance activities would not be eligible for Federal-aid; however, this memorandum is collective and concise example of systematic "maintenance" programs, which are eligibility for Federal-aid under a preventive maintenance project. (http://www.fhwa.dot.gov/preservation/memos/011126.cfm)
[21] Connected Vehicle Reference Implementation Architecture (CVRIA) is **a** standards development plan that will allow identification and prioritization of the standards needed in support of connected vehicle implementation. http://www.standards.its.dot.gov/DevelopmentActivities/CVReference
[22] The purpose of Basic Safety Message standard, SAE J2735 DSRC Message Set Dictionary standard, is to support interoperability among safety, mobility, and sustainability applications through the use of standardized message sets, data frames and data elements. http://www.standards.its.dot.gov/Factsheets/Factsheet/71

deployed on public sector fleets should also be consistent and integrated with other CV deployments on the broader vehicle fleets (e.g., private sector vehicles).

Although the ability of first responders to preempt traffic signals is an important safety application, its unwarranted use could have serious mobility implications. If this application is deployed, it should be done in concert with guidance to those operators of vehicles with capability of preemption highlighting the negative impacts of misuse, when it should/should not be used, and disciplinary consequences of misuse.

Procurement Process

Quality procurements for the assets that support Connected Vehicle environments will enable consistent, secure, and interoperable implementations. A generation of ITS deployment has provided many agencies with more mature practices for procurement. These practices can guide Connected Vehicle Environment procurements.

Evidence from hundreds of evaluation documents point to proactive stakeholder engagement as a determinant for deployment success. The key theme of stakeholder engagement is one that runs through the course of the entire procurement process, as the procurement will need to satisfy the needs of varied entities affected through the Connected Vehicle deployment.

There are several actions that are key to quality deployments:

- Identify what existing assets are candidates for modification to reduce the costs for delivery of power and communications to the deployment location. Whether in a rural or in an urban location, it is likely that there are various assets that are 'owned' by different entities. Gaining information on what assets are deployed, their operating capabilities, their supporting infrastructure (including mounting structures, power, and communications), and their provisions for maintaining the "legacy" assets will quickly focus the selection of candidate locations.

- Consult the ITS Costs Database for comparisons and ranges of unit and system costs. This database is fed from ITS program evaluation reports from various sectors on implementations of ITS. Much of the information generated in the ITS Costs Database originates with U.S. DOT model deployments and field operational tests. As CV test beds and pilot sites proliferate, unit cost information will be added to this database.

- Consult with the agencies that manage the statewide acquisition of information technology products to streamline the acquisition of connected vehicle assets (similar to procuring other ITS assets). Since most people outside the transportation community are not aware of Connected Vehicles, deployers will be expected to provide basic education and training on the technology and how it would benefit the public agencies. The FHWA is a resource for providing the basic information, and may be available to provide direct support for engaging with the IT investment authorities.

- Apply the specifications that are produced by U.S. DOT as the basis for amending their own existing Qualified Products Lists. Vendors and solution developers are most

effective when there is less variation to the specifications toward which they are building. Establishing a State or local Qualified Products Lists introduces a level of rigor that better secures the interoperability among agencies working in the same geographic area, and locations far from the implementation considered by the agency.

- Modify existing guides for project development to include connected vehicle assets as part of the project cost estimation. Amend the project development guide sections for ITS assets to feature the Connected Vehicle assets. Allow for contingencies consistent with other ITS roadside assets like dynamic message signs. Project cost estimation should consider the costs for all of the systems engineering components articulated in various guides available through FHWA. One such resource is *Systems Engineering for Intelligent Transportation Systems* available at http://ops.fhwa.dot.gov/publications/seitsguide/index.htm. The FHWA will be developing new reference materials for project cost estimations.

- Apply the *Connected Vehicle Footprint Analysis* produced by AASHTO to consider the typical profile and plan view drawings that could be applied for developing implementation plans. The plans will need to reflect the assessments made previously on the existing assets and supporting infrastructure. The design guides that exist among the State DOT's should be modified to incorporate elements of the AASHTO examples to standardize drawing plans.

- Establish test procedures and systems acceptance methodologies that minimize the risk to the agency. Ensure that during systems acceptance that data produced from the locations are not the sole possession of the Design-Build contractor, if one is used, but that the data can be validated by the agency working through an independent party.

- Coordinate with the agency's asset management unit to maintain accurate records of when items were deployed. This establishes a baseline for determining the lifecycle of the units. This will support the efforts by the agency to develop appropriate funding plans to sustain the operation of the system over time.

- Establish an operations and maintenance plan for the deployed system. Similar to the initiation of the Connected Vehicle Environment implementation, the choices are to contract with design/build entities or to work with a turn-key provider. There may be advantages to consider with the type of operations and maintenance plan in delivering: staff with appropriate technical expertise; responsiveness in repair once the environment is in an operational state; and, flexibility in obtaining support services through a number of providers.

Legacy systems/devices

Legacy systems and devices may be owned and operated by public agencies, private companies, or the general public. This guidance addresses those systems and devices that are under the jurisdiction of public agencies. The principles apply to other legacy systems and devices and may be applied through other agreements, coalitions, and similar cooperative efforts.

Legacy systems or devices critical to the function of active safety applications should be retrofitted or replaced in order for the safety application to continue to do its job. Other legacy systems and devices may be augmented by V2I safety applications that may be intended to improve safety or mitigate a design exception. Similarly, legacy systems and devices may support or be supplemented by other V2I applications. In these instances, retrofitting or replacement of legacy systems or devices may not be required in order for the V2I applications to provide their services. However, support for V2I and other connected vehicle applications and functions should be considered as these legacy systems and devices are upgraded and replaced.

The system engineering process should be used in establishing equipment maintenance and replacement plans for legacy systems. For replacement systems using Federal-aid funding, the system engineering process should be used per requirements in Part 940 of Title 23 of the Code of Federal Regulations (23 CFR 940). Among the issues to be considered in the system engineering analysis are the functionality necessary to support V2I application requirements, the number of devices affected, the useful life of equipment and life-cycle costs, and processes for replacing equipment.

Communication Technology

The selection of the V2I communications technology will be based on a systems engineering analysis and will be consistent with application interoperability across the Nation. Use should comply with established requirements for non-interference.[23]

Although DSRC is the anticipated communication technology for V2V safety applications, there could be other communication methods available or better suited for V2I mobility applications. The important factors when considering alternatives to DSRC are: capability of V2V On-board Units (OBUs), national interoperability, certified application support, and the technology's attributes meeting the needs of the application/installation.

Deployers will be expected to reference the analyses/white papers/reference guides that FHWA is developing (see Products/Tools).

Dedicated Short Range Communications (DSRC) Service Licensing

On December 17, 2003, the Federal Communications Commission adopted a Report and Order establishing licensing and service rules for the Dedicated Short Range Communications (DSRC) Service, in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850-5.925 GHz band (5.9 GHz band).[24] [25] [26] The DSRC service involves vehicle-to-vehicle and vehicle-to-infrastructure communication to protect and enhance the safety of the traveling public. Also, the band is also eligible for use by non-public safety entities and for private commercial operations.

[23] 47 C.F.R. §15.5 is an existing FCC regulation to ensure that unlicensed devices do not cause interference with licensed users and require operators of unlicensed devices to immediately correct the problem or cease operation if interference occurs.
[24] http://wireless.fcc.gov/services/index.htm?job=service_home&id=dedicated_src
[25] http://wireless.fcc.gov/services/index.htm?job=licensing&id=dedicated_src
[26] 47 C.F.R. §95.1501 - This subpart sets out the regulations governing Dedicated Short-Range Communications Service On-Board Units (DSRCS-OBUs) in the 5850-5925 MHz band. DSRCS Roadside Units (RSUs) are authorized under part 90 of this chapter and DSRCS, RSU, and OBU are defined in § 90.7 of this chapter.

However, the safety applications always have primary status over non-safety applications. Roadside infrastructure is licensed to both public safety and non-public safety entities pursuant to 47 CFR Part 90, while on-board units are licensed by rule (i.e., no individual license is required) under 47 CFR Part 95.

Therefore, the National Telecommunication and Information administration authorizes the use of this frequency spectrum for governmental entities while the Federal Communications Commission issues licenses for the private sector which is based on each applicant's area-of-operation (i.e., by County, State, multi-State, or Nationwide). Those applicants who are approved will each be granted a non-exclusive license for the geographic-area requested. Given the likeliness of cross border and/or overlapping geographic-area issues, applications, and potential efficiencies, it is stressed that a high level of jurisdictional cooperation and coordination across these boundaries will be necessary.

Besides States/local governmental entities and non-public safety entities, there is a wider-group that can hold an authorization to operate Roadside units (RSUs) in the DSRC 5.9 GHz band; specifically entities meeting requirements of 47 CFR 90.33 and 90.35 of the FCC Rules. Entities engaged in the operation of a commercial activity can receive authorizations to provide commercial mobile radio service or to operate stations necessary for transmission of communications (i.e., toll collection, and parking guidance). Further it should be noted that the licensing requirement only applies to equipment used for transmission; equipment designed and operated only to receive do not require siting licenses.

Although safety communication has precedence, identification and removal of interfering non-safety signals could be problematic, particularly if the interfering deployment was licensed and sited first. FHWA recommends that once an application deployment is identified in the planning process, site licensing should be undertaken. To this end, a guide to DSRC licensing is being developed for use by public agencies.

Data Connection and Latency

The data connection and latency are key factors in the CV implementation to improve mobility and further enhance safety through interaction with the road infrastructure. DSRC can communicate directly between vehicles and infrastructure with low latency but it is a line-of-sight technology and has limited range. Therefore, the key infrastructural features and aspects of deployment may be fundamentally different for the same application using different communications technology (e.g., solely DSRC, DSRC and cellular, Wi-Fi, satellite, Internet). In many cases, the applications and/or radio will be capable of selecting the best communication mode to use at any time.

However, a reliable data connection and low latency should be maintained to ensure a safe and a reliable CV environment. The reliable data connection should be highly available based on three key principles: elimination of single point of failure, reliable crossover, and detection of failures in real-time. While, the low latency will be based on the communication media; however, it should be measured from end-to-end or between the originating and the responding application.

Connected Vehicle Privacy Principles

An operable Connected Vehicle Environment relies on the exchange of information between vehicles (V2V) and between vehicles and infrastructure (V2I). V2V applications are enabled through broadcast and receipt of a Basic Safety Message (BSM) by vehicles. The transmission of data to and from a particular vehicle gives rise to individual privacy concerns.

The U.S. DOT takes privacy very seriously. We are committed to supporting deployment of a CV environment that both protects personal privacy and promotes this important safety, mobility and environmental technology. For this reason, the U.S. DOT has worked closely with its partners to develop a technical approach to CV communications that helps protect individual privacy. CV equipment in motor vehicles transmits the generic information used by V2V and V2I applications in a very limited geographical range. These generic BSMs do not identify specific drivers or vehicles. Additionally, the U.S. DOT and its partners incorporated into the design of the CV environment multiple mechanisms specifically to minimize risks to individual privacy, including a Certificate Management Security System (SCMS) (discussed below).

Also, the U.S. DOT has emphasized that deployment of technologies and applications in the connected vehicles environment should be guided by the Fair Information Privacy Principles (FIPPs), which are based on tenets of the Federal Privacy Act of 1974 and mirrored in the laws of many U.S. States. These include:

- Transparency- Ensure that consumers have information about the data being collected and transmitted by the V2I system and how that data will be used;
- Individual Participation and Redress- Ensure that consumers have a reasonable opportunity to make informed decisions about the collection, use, and disclosure of their PII or other data that may be used to identify them directly or indirectly, and reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate;
- Purpose Specification: Make clear the purpose(s) for which the V2I system collects, uses, maintains, or disseminates specific data elements, such as basic safety functions as well as potential mobility, environmental, or commercial applications;
- Data Minimization: Explain why the data collection isn't excessive and how long data will be retained;
- Use Limitation: Assure consumers that the collected data will not be used for purposes incompatible with the specified purposes;
- Data Quality and Integrity: Explain how the V2I system will assure data quality and integrity throughout the data lifecycle and in all associated uses;
- Security: Explain what physical, technical, and procedural measures system administrators will take to protect collected data;
- Accountability and Auditing: Explain how the V2I system will ensure that the privacy controls are executed.

FHWA will work to identify and disseminate data privacy best practices as applications and the V2I system develops.

Connected Vehicle Security

The Security Certificate Management System (SCMS) is a critical component of the CV environment designed to protect the security and privacy of the BSM data exchanged by vehicles and between vehicles and infrastructure. As currently envisioned, the CV SCMS will be a complex Public Key Infrastructure (PKI) that creates, manages, stores, distributes, and revokes digital certificates that accompany and validate each BSM. It is this PKI that will allows users of the CV environment's unsecure public network to securely and privately exchange BSM data through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority.

A PKI typically consists of the following elements:

- A certificate authority that issues and verifies digital certificates. A certificate includes the public key or information about the public key;
- A registration authority that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor;
- One or more directories where the certificates (with their public keys) are held;
- A certificate distribution and management system which includes the communications system and its organizational and operational elements.

The U.S. DOT has determined that the PKI for the connected vehicles environment should be organized such that no single organization within the PKI holds enough information about a participant to link a BSM transmitted by a vehicle to a specific driver or identified vehicle.

Data Access

In general, Federal law does not assign ownership, access, and use limitations to broadcast data. As a result, the U.S. DOT and FHWA do not currently have a specific policy assigning data ownership or limiting access to BSM data.

There is a need to balance access to data for use in developing mobility, environmental, and other applications (including potential private sector applications) with the consumer's concerns regarding privacy. In order to address consumer concerns about privacy and enhance consumer acceptance, V2I applications should contain sufficient controls to mitigate potential privacy and security risks appropriately. Two critical controls directly relevant to data access are transparency and consent. Consistent with DOT's Connected Vehicle Privacy Principles, public and private sector application developers should ensure that consumers understand and, for opt-in applications, consent to the collection of their data.

The FHWA is evaluating these issues and will develop a white paper to explore such topics as the scope of data generated in the V2I system, the expected uses of such data, the public sector's need to access this data for safety, mobility, and environmental applications, and the private sector's role regarding the use and collection of V2I data.

Manual on Uniform Traffic Control Devices

V2I applications providing traffic control information to drivers should be consistent with the Manual on Uniform Traffic Devices (MUTCD).[27] It is not expected that every roadside sign, signal, or pavement marking will be mirrored within the vehicle. If they are, generally these displays will be implemented by the OEMs. The information the on-board unit (OBU) receives should be sufficient for it to generate the appropriate sign/symbols or convey that information in a manner consistent with the MUTCD. In addition, all information conveyed to the driver should comply with and cannot contradict information conveyed by the signs, signals and markings on and along the road (as defined by the MUTCD). In-vehicle systems should also convey priority captured by signs, signals and markings (e.g., regulatory signs take priority over warning signs).

Using Public-Private Partnerships (P3s)

To the extent possible P3s and other commercial relationships should be considered for deployment. However, such arrangements should assure that the "commercial" applications protect the public interest, do not compromise the safety and mobility objectives, provide for safe maintenance practices, and hold the jurisdiction harmless due to lack of both public and private services. These arrangements should be established through P3 agreements that guarantee the precedence of the V2I safety and mobility applications, including the ability to terminate the relationship in the event that the private sector use should degrade the V2V or V2I environment. The public owner/operator of the V2I infrastructure should also ensure that the arrangement produces a net life-cycle benefit to the public and value for the transportation agency. Additionally, such deployments should be compatible with the CV security system, support the distribution and receipt and use of certificates to the maximum extent possible, and uphold the privacy principles of Connected Vehicle (CV) environment.

Current FHWA policy allows State Departments of Transportation (DOTs) to use Federal-aid funds in innovative long-term contracts with private developers under certain conditions. In such agreements, the State grants exclusive rights (a "concession") to a developer (concessionaire) who assumes responsibility for the highway's construction, operations, and upkeep. In the case described here, the developer would take responsibility for the deployment and operation of the V2I system.

P3 concession contracts often allow the concessionaire to collect and retain revenue from tolls, but in this instance tolls would not be applicable. The "business model" of CV V2I P3 is different in the sense that, instead of the private entity receiving payment from the highway user for access to a toll lane or facility, revenue to the private entity would most likely come from use of the communications channel to generate fee-for-service opportunities or advertising revenue.

Additional information on transportation P3s can be found at http://www.fhwa.dot.gov/ipd/p3/index.htm.

[27] Refer to FHWA Operations Regulation and Policy http://www.ops.fhwa.dot.gov/opsregulationpolicy.htm

Conclusion

It is recognized that since this initial guidance was developed concurrently with a period of rapid maturity of the Connected Vehicle technology, it will need to be continually assessed for relevancy, compatibility with real world deployment issues, the evolution of the CV technology and security, and new transportation and communication statues and regulations. As early deployments come online or jurisdictions take on planning activities, it will be important for lessons learned, identified gaps, or innovative approaches be acknowledged, shared, and incorporated into updates to this guidance and its associated guides and toolkits.

Products/Tools

To support the V2I Deployment Guidance a number of guides, best practices compilations, and toolkits are being developed. Below is a list of major efforts underway. Although all of these may not be completed and/or in their final form at time of guidance issuance, they are scheduled to be delivered in 2015. Much like the guidance it is anticipated that it will need to be continually assessed, updated, and supplemented to stay current with the CV state of art.

System Engineering Process for Vehicle to Infrastructure

Augment the Systems Engineering (SE) for Intelligent Transportation Systems manual and provide guidance for professionals involved in developing systems engineering documents covering the evaluation, selection and implementation of Connected Vehicle (CV) V2I technology.

V2I Benefit Cost Analysis Tool

Tool to assist adoption of an investment strategy that dedicates funding to the capital and ongoing operational costs for connected transportation.

V2I Planning Guide

Provide planning staff with an increased awareness of the benefits and opportunities for deploying these technologies by State DOTs and MPOs that guidance on inclusion of the technology in long range plans and project selection process.

Guide to V2I Cyber-Security

Provides deployers with: (1) an analysis of extensibility of security and trust system to additional points of connection, including V2I, devices, backhaul, and others; (2) an analysis of additional risks from extensibility and cyber security; and (3) an analysis of the potential impacts to the existing transportation system/network. It will also provide definitions of the organizational functions and processes for operating the security function, along with cost models for operations and maintenance.

Guide to Licensing DSRC Roadside Units

A guide to requirements that a transportation owner/operator will use to navigate the process of licensing, be they in a position to develop or manage an outsourcing contract or understand / deal with private sector commercial deployments.

Guide to V2I Communication Technology Selection

A description of the technology options available and why certain options may be more appropriate for some applications than others.

V2I Message Lexicon

A list of allowable standard messages and formats for transmitted information for In-Vehicle use. Although the OEMs will control the message/warning type provided to the user, what type of information and its form the RSU sends needs to be standardized.

Guide to Initial Deployments

A guide to transportation system owner/operators which are on a path from no V2I deployment to a build out of the various scenarios. This would include prioritization methodology, staged deployment applications, co-location with existing ITS infrastructure, legacy equipment, utility based on V2V market penetration, etc.

Warrants for Deployment

A set of criteria which can be used to define the relative need for and appropriateness of a particular V2I application.

Appendix A

This section has quick reference web links to videos, slide presentations, and information modules related to the fundamental principles of connected vehicle technology. These videos are described as Talking Technology & Transportation (T3) webinars and sponsored by the Intelligent Transportation Systems (ITS) Professional Capacity Building Program (PCB) under the Department of Transportation (DOT) ITS Joint Program Office (JPO). This section is divided into two (2) parts: Connected Vehicle Fundamental Concept Videos and Connected Vehicle Information Modules.

Connected Vehicle Fundamental Concept Videos

Connected Vehicle Basics
Summary of Video: The webinar features two speakers (Valerie Briggs & Brian Cronin) from the U.S. DOT who introduce the Connected Vehicle Research Program, explain the concept, describe the technology, and explain the benefits and challenges of connected vehicles. Also, the webinar discusses how connected vehicles affect safety, mobility, and the environment.
Video: http://www.pcb.its.dot.gov/t3/s140424_cv_basics.asp
Presentation 1: http://www.pcb.its.dot.gov/t3/s140424/s140424_cv_basics_presentation_lister.pdf
Presentation 2: http://www.pcb.its.dot.gov/t3/s140424/s140424_cv_basics_presentation_briggs_cronin.pdf
Question/Answer Transcript: http://www.pcb.its.dot.gov/t3/s140424/s140424_cv_basics_qa.asp

Vehicle-to-Vehicle Communication: A New Generation of Driver Assistance and Safety
Summary of Video: ITS-JPO has developed an information video that demonstrates the following technologies: Dedicated Short Range Communications (DSRC), Vehicle to Vehicle (V2V) communication system, Blind Sport Warning (BSW), Forward Collision Warning (FCW), Emergency Electronic Brake Light (EEBL), Intersection Movement Assist (IMA), and Do Not Pass Warning (DNPW).
Video: http://www.its.dot.gov/library/media/v2v_video.htm
NOTE: Immediately after this video, there are several more videos (10+) available which explain various V2V applications (or scenarios), CV testbed, CV Safety Pilot, Dedicated Short Radio Communication (DSRC), and so more.

Connected Vehicle Information Modules

Connected Vehicles – Module 13
Summary of Video: This module describes the background, current activities, and future direction of the connected vehicle initiative. The module examines the anticipated roles and responsibilities of the principal participants; the major technologies and systems development efforts; the range of expected applications of the connected vehicle system; the potential institutional, policy, legal, and funding challenges facing the initiative; and the expected development and deployment timeline for a connected vehicle environment.
Link: http://www.pcb.its.dot.gov/eprimer/module13.aspx

Appendix B

Definitions

Term	Description
Aftermarket Safety Device (ASD)	A connected device in a vehicle that operates while the vehicle is mobile, but which is not connected to the data bus of the vehicle.
Backhaul	The closed network communication links between a Traffic Management Center (or other back offices), links between TMCs, and field installations (such as traffic signal controllers, traffic cameras, and other sensors). This could also include the link between the Security Credential Management System and roadside distribution device.
Basic Safety Message (BSM)	The core data set transmitted by the connected vehicle (vehicle size, position, speed, heading acceleration, brake system status) and transmitted approximately 10x per second. A secondary set is available depending upon events (e.g., ABS activated) and contains a variable set of data elements drawn from many optional data elements (availability by vehicle model varies). This would be transmitted less frequently. The BSM is tailored for low latency, localized broadcast required by V2V safety applications but can be used with many other types of applications.
Connected Device	Any device used to transmit to or receive messages from another device. A connected device can be sub-categorized as an OBE, ASD, VAD, or RSE. In many cases the connected device will be a DSRC device, but other types of communications can and are expected to be supported.
Connected Vehicle (CV)	A vehicle containing an OBU or ASD. Note that vehicles may alternatively include a Vehicle Awareness Device (VAD), which transmits the BSM but does not received broadcasts from other devices and cannot directly support vehicle-based applications.
Connected Vehicle Reference Implementation Architecture (CVRIA)	A set of system architecture views that describe the functions, physical and logical interfaces, enterprise/institutional relationships, and communications protocol dependencies within the connected vehicle environment. The CVRIA defines functionality and information exchanges needed to provide connected vehicle applications.
Dedicated Short Range Communications (DSRC)	DSRC is a technology for the transmission of information between multiple vehicles (V2V) and between vehicles and the transportation infrastructure (V2I) using wireless technologies.
Intelligent Transportation Systems (ITS)	Systems that apply data processing and data communications to surface transportation, to increase safety and efficiency. ITS systems will often integrate components and users from many domains, both public and private.

Term	Description
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged. The dependence of the CV Environment on successful exchange of data between independent components results in a requirement that all V2I deployments.
Latency	A measure of time delay experienced in a system, the precise definition of which depends on the system and the time being measured. For a data element in this context, latency is the time difference between the time that data value is acquired by the source and the time the message is transmitted.
NTCIP	The National Transportation Communications for Intelligent Transportation System Protocol (NTCIP) is a family of standards designed to achieve interoperability and interchangeability between computers and electronic traffic control equipment from different manufacturers.
On-Board Equipment (OBE)	This term refers to the compliment of equipment located in the vehicle for the purpose of supporting the vehicle side of the applications. It is likely to include the DSRC radios, other radio equipment, message processing, driver interface, and other applications to support the use cases described herein. It is also referred to as the Vehicle ITS Station. When referring to the DSRC radio alone, the correct term is OBU (see below).
On-Board Unit (OBU)	A vehicle mounted device used to transmit and receive a variety of message traffic to and from other connected devices (other OBUs and RSUs). Among the message types and applications supported by this device are vehicle safety messages, a primary subject of this standard, used to exchange information on each vehicle's dynamic movements for coordination and safety.
Original Equipment Manufacturer (OEM)	An original equipment manufacturer refers to the entity that originally manufactures and item that may be branded and sold by others. In the Connected Vehicle Environment, it is commonly used to refer to automobile manufacturers.
Public-Private Partnerships (P3)	Public-private partnerships (P3s) are contractual agreements formed between a public agency and a private sector entity that allow for greater private sector participation in the delivery and financing of transportation projects.

Term	Description
Roadside Equipment (RSE)	Term used to describe the compliment of equipment to be located at the roadside; the RSE will prepare and transmit messages to the vehicles and receive messages from the vehicles for the purpose of supporting the V2I applications. This is intended to include the DSRC radio, traffic signal controller where appropriate, interface to the backhaul communications network necessary to support the applications, and support such functions as data security, encryption, buffering, and message processing. It may also be referred to as the roadside ITS station. When speaking of the DSRC radio alone, the correct term is RSU (see below).
Roadside unit (RSU)	A connected device that is only allowed to operate from a fixed position (which may in fact be a permanent installation or from temporary equipment brought on-site for a period of time associated with an incident, road construction, or other event). Some RSEs may have connectivity to other nodes or the Internet.
Signal Phase and Timing (SPaT)	In the context of this standard, SPaT is a message type that describes the current state of a signal system and its phases and relates this to the specific lanes (and therefore to maneuvers and approaches) in the intersection.
Security Certificate Management System (SCMS)	A public key infrastructure approach to security involving the management of digital certificates that are used to sign and authenticate messages among legitimate but unknown vehicles and/or equipment and/or other points of connection.
Systems Engineering	An interdisciplinary practice which focuses on how to design and manage complex projects/deployments over their life cycles. It ensures that all likely aspects of a system are considered and integrated into a whole.
Vehicle	A self-propelled transport device, along with any attachments (e.g., trailers), that is a legal user of the transportation network.
V2I Reference Implementation	An interface system that supports the collection, integration, and dissemination of data between infrastructure and vehicles to enable integrated, interoperable V2I safety, mobility, and environmental applications.
V2V	Short for vehicle-to-vehicle communications: a system designed to transmit basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes.
V2I	Short for vehicle-to-infrastructure communications: a system designed to transmit information between vehicles and the road infrastructure to enable a variety of safety, mobility, and environmental applications.

Symbols and Abbreviations

Term	Meaning
BSM	Basic Safety Message
CV	Connected Vehicle
DSRC	Dedicated Short Range Communications
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transportation Systems
MUTCD	Manual on Uniform Traffic Control Devices
OBE	On-Board Equipment (synonym for On-Board Unit)
OBU	On-Board Unit
PTV	Public Transport Vehicle
RF	Radio Frequency
RSE	Roadside Equipment (synonym for Roadside Unit)
RSU	Roadside Unit
SAE	Society of Automotive Engineers International
SPaT	Signal Phase and Timing
TMC	Traffic Management Center
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle