CAT Coalition (V2I Deployment Coalition Phase 2)

Technical Resources Working Group

Connected Vehicle Deployment Environment

Version 1.1

November 2020

Acknowledgements

The Cooperative Automated Transportation (CAT) Coalition is a collaborative effort supported by United States Department of Transportation (USDOT), American Association of State Highway and Transportation Officials (AASHTO), Institution of Transportation Engineers (ITE), and Intelligent Transportation Society of America (ITS America) that includes broad participation in both public and private sectors to promote connected and automated vehicle initiatives and research. The Technical Resources Working Group (WG) is a WG in the CAT Coalition that provides review, input, and analysis of developed connected and automated vehicle (CAV) documentation, tools, products, and resources, such as deployment guidance.

The WG relies on the expertise and feedback from its volunteer members to generate this feedback and resources, such as this document. Specifically, this resource was initiated with the support and input from Bob Rausch (Transcore), Siva Narla (ITE), and Faisal Saleem (Maricopa County Department of Transportation [DOT] and chair of the Technical Resources WG). Additional WG members provided feedback as part of a focus group for this resource, including: Peter Jager (Utah DOT), Emil Wolanin (Montgomery County, Maryland), Jianming Ma (Texas DOT), Ray Starr (Minnesota DOT), Israel Lopez (Triunity Engineering and Management), and Alan Clelland (Applied Information).

Contact Information

This resource is viewed as a living document. To provide additional feedback or lessons learned, or for additional information, please contact:

- Faisal Saleem (Maricopa County DOT and chair of the Technical Resources WG) at Faisal.Saleem@Maricopa.Gov, or
- Jeremy Schroeder (Athey Creek Consultants) at schroeder@acconsultants.org.

Table of Contents

Acknowledgements i
Contact Information i
Executive Summary and Introduction 1
The Connected Vehicle Deployment Environment 1
How to Use this Document 2
Roadside CV and ITS Systems 4
Traffic Signal Controller 4
Roadside Unit 5
Infrastructure Data 7
Network Interface Devices 9
TMC – ITS Systems 11
Traffic Control System 11
Central Back Office Networks 11
Connected Vehicle Back Office Systems and Data Hub 12
Network Firewall 13
Hardware Security Module 14
In-Vehicle Systems and Vulnerable Road Users 15
In-Vehicle On-Board Unit (OBU) or Aftermarket Safety Device (ASD) 15
Vehicle Controller Area Network (CAN) Bus 16
Other Vehicle Systems 17
Vehicle Human Machine Interface (HMI) 17
In-Vehicle or Vulnerable Road User (VRU) Mobile Applications 18
CV and ITS External Support Systems 19
CV Device Vendors 19
Security Credential Management System (SCMS) and Certification 19
Data Sharing by USDOT and Others 20
Communications 22
Localized Media 22
Wide-Area Media 24
Internet 25
Backhaul Communications 25

Executive Summary and Introduction

The Cooperative Automated Transportation (CAT) Coalition is a collaborative effort supported by United States Department of Transportation (USDOT), American Association of State Highway and Transportation Officials (AASHTO), Institution of Transportation Engineers (ITE), and Intelligent Transportation Society of America (ITS America) that includes broad participation in both public and private sectors to promote connected and automated vehicle initiatives and research. The Technical Resources Working Group (WG) is one of six WGs in the CAT Coalition and provides review, input, and analysis of developed connected and automated vehicle (CAV) documentation, tools, products, and resources, such as deployment guidance. The WG also focuses on the identification of CAV gaps regarding resource needs and institutional challenges, such as workforce development.

This document describes a holistic view of the connected vehicle (CV) deployment environment that is necessary to support a successful, interoperable CV implementation. Many of the included lessons learned relate to CV deployments for intersections with Signal Phase and Timing (SPaT) and MAP broadcasts, however this document is inclusive of other CV deployments, such as work zones and other locations that use the Roadside Safety Message (RSM). The intended audience for this document includes infrastructure owner operators (IOOs) that are implementing or want to begin a CV deployment and need to understand the overall picture of the CV environment. This resource is intended to help agency staff connect the concept for a CV deployment to procurement.

The Connected Vehicle Deployment Environment

This document describes the components of the larger CV deployment environment that is presented in Figure 1. This document organizes CV deployment components into five groups, as described below and in separate chapters of this document.

1. **Roadside Connected Vehicle (CV) and Intelligent Transportation Systems (ITS)** and components encompass a broad range of wireless and traditional communications-based information and electronic technologies. These infrastructure-based systems include vehicle detection, traffic and pedestrian signals, and supporting processing and communications equipment to control traffic movements and operations at intersections, work zones, and other locations. Key components of Roadside CV and ITS Systems are described in further detail in that chapter and include: Traffic Signal Controller, Roadside Unit, Infrastructure Data, and Network Interface Devices.

2. **Transportation Management Center (TMC) ITS Systems** include systems and security components that monitor and control traffic and the road network. Key components of these back office TMC ITS systems include: Traffic Control System, Central Back Office Networks, Connected Vehicle Back Office Systems and Data Hub, Network Firewall, and Hardware Security Module.

3. **In-Vehicle Systems and Vulnerable Road Users** include components that collect data and provide information to road users that are in vehicles, as well as vulnerable road users with mobile applications including pedestrians, bikers, workers, or law enforcement on the roadway and not in a vehicle. Standard vehicle systems that collect, process, and display data and information to drivers interface with aftermarket safety devices (ASDs), on-board units (OBUs), and mobile applications to further share and disseminate additional information to drivers and vulnerable road users. Key

components of In-Vehicle Systems and Vulnerable Road User Systems are described in more detail in that chapter and include: In-Vehicle On-Board Unit (OBU) or Aftermarket Safety Device (ASD), Vehicle Controller Area Network (CAN) Bus, Other Vehicle Systems, Vehicle Human Machine Interface (HMI), and In-Vehicle or Vulnerable Road User (VRU) Mobile Applications.

4. **CV and ITS External Support Systems** encompass external vendors for devices and the Security Credential Management System (SCMS), as well as data sharing activities with external parties like the USDOT. Key components described in more detail in that chapter include: CV Device Vendors, Security Credential Management System (SCMS) and Certification, and Data Sharing.
5. **Communications** must be secure, interoperable, networked, and both wired and wireless to exchange data from vehicles to other vehicles, roadside infrastructure, transportation management centers (TMCs) and intelligent transportation systems (ITS), and other external support systems. Communications technologies described in more detail in that chapter include: Localized Media, Wide-Area Media, Internet, and Backhaul Communications.

How to Use this Document

This initial executive summary chapter provides a high-level overview of the groups and components required as part of the CV deployment environment for a successful and interoperable deployment. This chapter is an introduction to the CV deployment environment that may be suitable for managers and decision makers. Each of the next five chapters of this document provides additional details about each component within the groups depicted in Figure 1 and is intended for staff who will be working on day-to-day details for procuring and implementing a CV deployment. Figure 1 is interactive such that readers can click on various components and be directed to the appropriate section or chapter for more information. The next five chapters are organized to provide the following information for each identified component:

- Summary of Role/Function
- Relevant standard(s)
- Anecdotal Lessons Learned from Early Deployers
- Resources / Online Supporting Materials

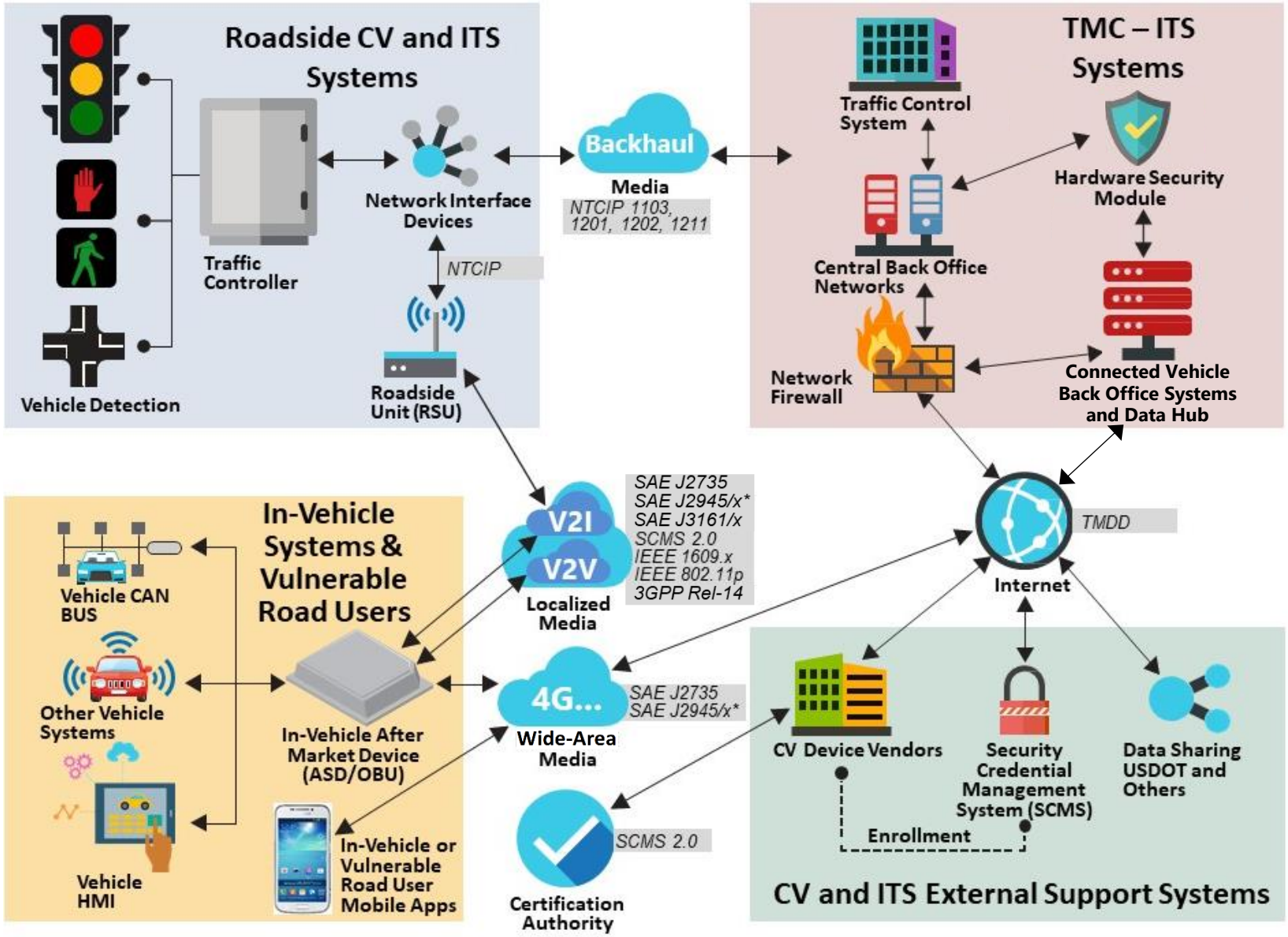
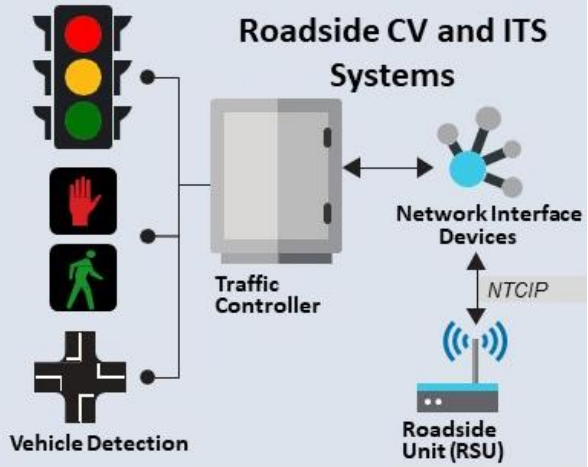


Figure 1. Interactive: click each component in the comprehensive and interoperable Connected Vehicle Deployment Environment for details

Roadside CV and ITS Systems

Roadside Connected Vehicle (CV) and Intelligent Transportation Systems (ITS) and components encompass **a broad range of wireless and traditional communications-based information and electronic technologies**. These infrastructure-based systems include vehicle and pedestrian detection, traffic and pedestrian signals, and supporting processing and communications equipment to control traffic movements and operations at intersections, work zones, and other locations.



Key components of Roadside CV and ITS Systems are described in more detail below and include:

- Traffic Signal Controller
- Roadside Unit
- Infrastructure Data
- Network Interface Devices

Traffic Signal Controller

Summary of Role/Function:

- The traffic signal controller is the roadside computer located at the intersection that will generate the current signal phase and timing parameters used to control the signal heads and pedestrian crossing signals.
- At a minimum, a **software upgrade** may be needed for advanced traffic controllers (ATCs) to output real-time data to the transportation management center (TMC) and/or roadside unit (RSU) to generate SPaT messages and configure pedestrian information. A hardware upgrade may also be needed.
- One or more separate roadside processors (RSPs) may also be needed to support specific applications.

Relevant standards:

- Traffic signal controllers that are compliant with NTCIP 1202 Version 3 Object Definitions for Actuated Traffic Signal Controller (ASC) Units are typically capable of generating an output of the SPaT parameters as NTCIP 1202 SPaT messages.
- ATC 5201 Version 06.25 Advanced Transportation Controller Standard Version 6 (AASHTO, ITE, and NEMA) defines the minimum standards for an ATC traffic signal controller.
- For the broadcasts of SPaT messages to be compliant with the SAE J2735 standards for V2I message exchange, the NTCIP 1202 SPaT messages must be converted into SAE J2735 formats prior to broadcast. This will ensure that vehicles operating V2I communication capabilities can interpret the message communications. Currently, the SAE J2735 Version 2016 is the latest version. This translation may occur in the Traffic Controller, in a separate roadside processor, or at the RSU.

Anecdotal Lessons Learned from Early Deployers:

- Older controllers may not possess the processing power to support this function, and would need a **hardware upgrade or complete replacement**.
- Caltrans and Utah DOT both have an **additional roadside processor** (RSP) to run the Multi-Modal Intelligent Traffic Signal Systems (MMITSS) application. For instance, Utah has used two versions of a separate RSP in the cabinet. One is a "beaglebone" device mounted in the cabinet, the newer version is mounted on an expansion card that mounts in the detector rack, using available bus interface unit (BIU) to interface with the traffic signal controller.
- More room in the **signal controller cabinet** may be needed for additional CV equipment like a separate RSP.
- Updated ATC **software testing** should consider:
  - Timing relationship SPaT data and the actual timing (PCAP, Sniffer, Wireshark)
  - Check for timing disruption due to communications loading
  - Timing during transition, emergency vehicle pre-emption (EVP), transit signal priority (TSP), cooperative intersection control (CIC), adaptive control, and clock changes
- Upgrades may be needed in the future as SPaT-related standards continue to evolve to interoperate with roadside equipment and vehicles that utilize newer versions of the standards.
- All BIU may be in use for advanced detection and performance metrics at complex intersections, so their use must be prioritized based on what applications or metrics are most important.

Resources / Online Supporting Materials:

- None identified at this time.

Roadside Unit

Summary of Role/Function:

- The roadside units (RSUs) facilitate communication between transportation infrastructure and vehicles and other mobile devices by exchanging data over DSRC and/or C-V2X in compliance with industry standards.
- The RSU can be integrated with a backhaul system to enable remote management and provide vehicles and other mobile devices with services and applications delivered by back office service providers.
- RSUs can also be incorporated with local traffic control systems to deliver enhance traffic management services to vehicles and other mobile devices.

Relevant standards:

- USDOT Roadside Unit Specification version 4.1 is the most recent version. An update is expected that may address some known gaps, such as some data collection needs and central signing of MAP and TIM messages that are not supported.
- For the broadcasts of SPaT messages to be compliant with the SAE J2735 standards for V2I message exchange, the NTCIP 1202 SPaT messages must be converted into J2735 formats prior to broadcast. This will ensure that vehicles operating V2I communication capabilities can interpret the message communications. Currently, the J2735 Version 2016 is the latest version. This translation may occur in the Traffic Controller, in a separate roadside processor, or at the RSU.

- NTCIP 1218 Version 1 Object Definitions for Roadside Units (RSUs) is under development to specify the protocols and data definitions between the TMC and RSU so that the TMC can monitor the operational status of the RSU, including the status of applications and processes, and configure the RSU to interface with other components in a connected vehicle environment, including connected vehicles, a traffic signal controller, the Security Credential Management System (SCMS), and other connected devices (e.g., smart phones).
- National Electrical Manufacturers Association (NEMA) TS 10 Connected Vehicle Infrastructure-Roadside Equipment Standard is currently being developed to support agencies in deploying RSUs The standard will be technology-agnostic and allow extensibility for future wireless technologies and applications, recognizing multiple configurations of an RSU device depending on agency procurement needs.

Anecdotal Lessons Learned from Early Deployers:

- **Installation and mounting considerations** include identification of mounting structures that meet line of sight requirements that are optimal for triangulation. Specific considerations for mounting an RSU on a mast arm:
  - Signal interference with signal heads
  - Wind loading
  - Dead weight
  - Other co-hosted devices (signs, antenna, video)
  - Mast arm orientation changes for parades or other events that will require indexing for proper orientation
  - Changes to the landscape that could impact signals, e.g. scaffolding for façade maintenance or changes in vegetation
  - Cross-intersection RSU wiring link
  - Placement in an urban canyon that could affect location accuracy
  - RSU Triangulation – Time of Flight
    - Specific chip set
    - Affects WSA frequency of transmission
  - Installation by contractors or agency staff with required skills is critical for integration; an experienced electrical engineer is critical to optimize radio transmission range and reception.
  - Document the precise latitude, longitude, and elevation of the RSU
  - Appropriate height to get optimum transmission range that meets any FCC requirements for minimum or maximum height.
  - **Shielded** CAT-5 Cable has proven to be best to reduce signal loss and interference from adjacent wires.
- RSUs should be capable of receiving **over the air (OTA) software updates**.
- The RSU **power source** considerations include Power over Ethernet (PoE), proper surge protection, and verification of proper power grounding.
- RSUs will **secure** SPaT messages by providing signed security credentials. The RSU will need a Hardware Security Module and a means to communicate over the Internet using IPv6 in order to be provided with security certificates.

- **Maintenance** considerations should include the availability of spare parts and creation of a maintenance plan that documents the deployment and specification used, e.g. modifications to USDOT RSU v4.1 or a custom-developed specification.
- **Network upgrades** may be required to support bandwidth rates as high as 6 Mbps and polling rates of 10 times per second per RSU [1].
- **Additional servers** may be required, i.e., to create a domain, implement DNS servers, install certificate servers, provide internet access, and support the RSU and its security infrastructure [2, 3]. It is currently not understood where the SCMS fits with a traditional enterprise environment, but certain base network services are required outside the SCMS.
- Consider the time relationship line frequency versus GPS time.
- Agencies may encounter procurement issues or delays with vendors given the evolving nature of devices. Additionally, agencies may experience interoperability issues between devices from different vendors, depending on how each vendor interprets a standard or optional parts of that standard.

Resources / Online Supporting Materials:

- [1] DSRC Roadside Unit (RSU) Procurement Specification. (2017, p 57) https://cvp.nyc/sites/default/files/2018-02/RSU_1%200_10102016_V1%209.pdf.
- [2] Security Credential Management System (SCMS) Proof of Concept (POC). (2017, p 2 - 3) https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf
- [3] How Public Key Infrastructure Works? https://www.youtube.com/watch?v=5OqgYSXWYQM

Infrastructure Data

Summary of Role/Function:

- A variety of infrastructure data is needed to generate messages that support various applications. Both static and dynamic infrastructure data are needed for applications.
- The MAP message is not created in real-time but is a static description of the geometries of the intersection and vectors describing approaches. Vehicle systems will compare GPS location readings on the vehicle against the MAP message and determine the vehicle's approach.
- As another example, dynamic infrastructure data from pedestrian detection will be needed to support a PED in crosswalk application.

Relevant standard:

- SAE J2735 v2016 is the latest messaging standard, and a supporting resource developed by the CAT Coalition entitled Clarifications for Consistent Implementation provides insights for interoperable national deployment.

Anecdotal Lessons Learned from Early Deployers:

- **Data Collection** may require Edge Computing and may include the following considerations:
  - Event data
  - Radio Frequency (RF) Data
  - System log data
  - Scalability

- A significant quantity of data is anticipated, with connected vehicles generating 4,000 GB of data per day by one estimate [4] and each RSU collecting a projected 1-5 GB of data per day [5, 6] based on vehicle saturation.

Resources / Online Supporting Materials:

- [4] Data is the New Oil in the Future of Automated Driving (2016) https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/#gs.doqxf6
- [5] Integrating Emerging Data Sources into Operational Practice. (2018, p 57) https://rosap.ntl.bts.gov/view/dot/34985/dot_34985_DS1.pdf?
- [6] Internet of Vehicles in Big Data era. (2018, II., A.) http://html.rhhz.net/ieee-jas/html/2018-1-19.htm#outline_anchor_5

Network Interface Devices

Summary of Role/Function:

- Network interface devices exist in the roadside CV and ITS systems to receive and transmit information via backhaul communications to the TMC and back office systems.

Relevant standard:

- NTCIP 1202 Version 3 Object Definitions for Actuated Traffic Signal Controller (ASC) Units is intended to support SPaT data outputs, however some modifications may be needed, e.g. creating a block object.

Anecdotal Lessons Learned from Early Deployers:

- **Port mapping** will encompass IP address assignments, subnetworks, and security management.
- Network **connectivity** considerations include:
  - IPv4 or IPv6 –Proxy or Firewall Gateway –SCMS, Amazon Web Services (AWS) with the MQTT messaging protocol
  - Configuring security for the router and switches.
  - Ensuring compatibility with other network traffic, e.g. video and electronic toll collection (ETC) readers.
- Getting IPv6 through the backhaul network to the SCMS can be challenging. Often agencies have had to tunnel IPv6 through an IPv4 network.
- **Privacy** considerations include encryption of data.
- Perform bandwidth estimates including best, medium, and worst case scenarios to identify bottle necks in the communications path.
  - Multiple major corridors with RSUs placed at every traffic signal with spacing ranging from ¼ to 1-mile.
    - Example 1 (light saturation): 1 Mbps x 100 RSUs x 13% for Ethernet Overhead (EO)= 113 Mbps average
    - Example 2 (moderate saturation): 3 Mbps x 100 RSUs x 13% EO = 339 Mbps average
    - Example 3 (heavy saturation): 6 Mbps x 100 RSUs x 13% EO = 678 Mbps average
    - Connected Vehicle saturation will increase as more vehicles are equipped with an OBU
- Upgrade key locations such as fiber hubs, node buildings, and other key strategic areas to a minimum of 10 Gbps, preferably 100 Gbps, with dual-connections between other hubs and nodes to create a ring [7].
- Upgrade critical corridor field switches to 1 Gbps, preferably 10 Gbps, switches to support existing and new ITS features [7].

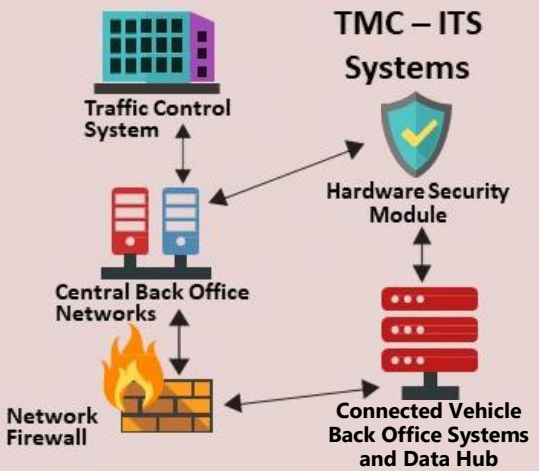
- Consider the use of Shortest Path Bridging (SPB) or other networking protocols due to spanning tree's failover issues that require extensive troubleshooting [7].

Resources / Online Supporting Materials:

- [7] Nevada DOT wanted to lay the foundations for its next-generation Intelligent Transportation System (ITS) (2019), https://www.al-enterprise.com/en/company/customers/nevada-department-of-transportation.

Click here to Return to Full CV Deployment Environment Figure

TMC – ITS Systems



Transportation Management Center (TMC) Intelligent Transportation Systems (ITS) include **systems and security components that monitor and control traffic and the road network.** These systems include traffic control systems, central networks, connected vehicle systems, network firewall, and a hardware security modules.

Key components of TMC-ITS Systems are described in more detail below and include:

- Traffic Control System
- Central Back Office Networks
- Connected Vehicle Back Office Systems and Data Hub
- Network Firewall
- Hardware Security Module

Traffic Control System

Summary of Role/Function:

- The traffic control system helps agencies to control traffic through ITS systems located along the road network, such as Advanced Traffic Management Systems.

Relevant standard(s):

- NTCIP 1103 Version 3 Transportation Management Protocols (TMP) defines a composite application layer protocol for the management of transportation equipment.
- NTCIP 1201 Version 3 Global Object Definitions identifies and defines the common object definitions that may be supported by transportation devices that are NTCIP-conformant.
- NTCIP 1202 Version 3 Object Definitions for Actuated Traffic Signal Controller (ASC) Units defines an output of the SPaT parameters from compliant traffic signal controllers as NTCIP 1202 SPaT messages.
- NTCIP 1211 Version 2 Object Definitions for Signal Control and Prioritization (SCP) provides definitions of the management information related to Signal Control and Prioritization (SCP).

Anecdotal Lessons Learned from Early Deployers:

- None identified at this time.

Resources / On-line Supporting Materials:

- Title and link to any identified resources

Central Back Office Networks

Summary of Role/Function:

- The Central Back Office Networks include a variety of existing systems that agencies use to manage operations, such as Road Condition Reporting Systems. These systems are connected with devices in

the field to collect and disseminate data and information to manage traffic, e.g. connections to road reference databases, archives of data, and data sources.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- A variety of tools should be considered to support operations management. These tools may provide the following functions:
  - System logging;
  - Operations alarms;
  - Visual displays of device status; and
  - Security monitoring.
- Back office systems can be used to automatically generate performance measurements, reports, and associated analyses. This may include metrics specific to a given project or across the entire system.

Resources / On-line Supporting Materials:

- Title and link to any identified resources

Connected Vehicle Back Office Systems and Data Hub

Summary of Role/Function:

- The Connected Vehicle Back Office Systems and Data Hub are closely related to other Central Back Office Networks, with new functions to support connected vehicles and related applications by accessing data from DOT sources, generating and signing messages for security purposes, accepting and managing data received from CVs, and related processes like over the air (OTA) download management.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- Data collection is one major function required of the Connected Vehicle Back Office Systems and Data Hub. This includes the following:
  - Monitoring roadside unit (RSU) health with a radio-frequency (RF) module;
  - Possibly monitoring the health of specified aftermarket safety device (ASD) with an RF module;
  - Event logs, which can be used for performance measurement;
  - Travel times, leveraging a travel time monitoring system or Intelligent Traffic Signal System (*ISIG*) application;
  - System logs, for troubleshooting; and
  - Basic Safety Messages, to generate a “breadcrumb” from connected vehicles.
- The Connected Vehicle Back Office Systems and Data Hub is where message generation and signing of security credentials will take place for messages that originate in the TMC. Agency staff may be required to periodically provide and update some data elements, while other data elements may be collected and processed using automated processes. The data elements may need to be assembled in the back office system to generate and sign the following messages:

  - MAP messages, with roadway and/or intersection geometry;
  - Traveler Information Message (TIM), with traffic condition and advanced traveler messages to provide information on incidents, pre-planned events, adverse weather conditions, and emergencies, as well as speed warnings, traffic signage, road conditions and other general information; and
  - Radio Technical Commission for Maritime Services (RTCM) messages, to allow the Global Navigation Satellite System (GNSS) of each vehicle on-board unit (OBU) to maintain lane-level accuracy under various conditions.
- Over The Air (OTA) download management involves the functions below. Note that this has been done for pilot projects, but may incur feasibility challenges for larger-scale deployments.
  - Configuration Management;
  - ASD firmware upgrades; and
    - ASD Application Tuning, including setting application parameters.
- The User Interface and Database Management allows for both:
  - RSU parameter management
  - ASD parameter management
- Management of connected vehicle and intelligent transportation system (ITS) devices occurring at the back office includes:
  - RSU configuration files;
  - RSU firmware updates;
  - Traffic Controller additions for NTCIP 1202v3; and
  - Security enhancements, i.e., Datagram Transport Layer Security (DTLS)

Resources / On-line Supporting Materials:

- Title and link to any identified resources

Network Firewall

Summary of Role/Function:

- The Network Firewall is a security system that monitors and controls incoming and outgoing *network* communications based on predetermined security rules. Specifically, this relates to CV communications, including publishing data online for communication to vehicles via network cellular approaches, as well as connections to the SCMS and USDOT.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- None identified at this time.

Resources / On-line Supporting Materials:

- Title and link to any identified resources

Hardware Security Module

Summary of Role/Function:

- The hardware security module is a physical device that safeguards and manages digital keys for strong authentication. In the current environment, the provision of certificates has been outsourced by agencies, e.g. Green Hill Integrity Security Services (ISS)

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- Privacy protection is supported by:
  - Obfuscating data; and
  - Aggregating data, which is then exported to the USDOT Secure Data Commons (SDC).
- The Hardware Security Module provides security management, in tandem with:
  - Security profiles for all messages;
  - X.509 or TMC to roadside unit or Advanced Transportation Controller (RSU/ATC) security; and
  - Firewall rules for external connections.

Resources / On-line Supporting Materials:

- Title and link to any identified resources

Click here to Return to Full CV Deployment Environment Figure

In-Vehicle Systems and Vulnerable Road Users

This module describes the **in-vehicle systems and vulnerable road user mobile applications** as part of the overall CV Deployment Environment. Vulnerable road users include pedestrians, bicyclists, workers in the road, or law enforcement on the roadway and not in a vehicle. This module communicates through direct V2I or V2V communications with the Roadside CV and ITS Systems module or other modules using cellular communications.

The primary interface to Infrastructure modules or other vehicles is generally referred to as an on-board unit (OBU), either as a production component or an in-vehicle aftermarket safety device (ASD). The data received from the OBU is then communicated to other components of this module to support vehicle operations by either drivers or automated vehicle systems.

Key components of In-Vehicle Systems and Vulnerable Road User Systems are described in more detail below and include:

- In-Vehicle On-Board Unit (OBU) or Aftermarket Safety Device (ASD)
- Vehicle Controller Area Network (CAN) Bus
- Other Vehicle Systems
- Vehicle Human Machine Interface (HMI)
- In-Vehicle or Vulnerable Road User (VRU) Mobile Applications

In-Vehicle On-Board Unit (OBU) or Aftermarket Safety Device (ASD)

Summary of Role/Function:

- An in-vehicle on-board unit (OBU) or aftermarket safety device (ASD) is a commercial product that is designed to be installed in a vehicle to enable a vehicle to become a connected vehicle, i.e. able to exchange data and messages with other vehicles using V2V communications and with the infrastructure using V2I communications. Further, these devices are capable of interfacing with original vehicle system equipment for purposes such as assembling the data necessary to broadcast the basic safety message or to enable messages received to be displayed on production displays or aftermarket HMIs. Newer vehicles may not require this component as it may be incorporated as part of the design.

Relevant standards:

- There is no standard specification for an OBU or ASD, however information from the Safety Pilot may be leveraged.
- The SAE J2735 standard describes data that will be assembled by the vehicle OBU or ASD for the Basic Safety Message (BSM) and exchanged using dedicated short-range communications (DSRC) or cellular V2X (C-V2X). A new or expanded, related standard will likely be developed for exchanging data using cellular communications.

- A standard is also being developed to describe data that the vehicle OBU or ASD will assemble for the Roadside Safety Message.

Anecdotal Lessons Learned from Early Deployers:

- Consider the need for **device calibration**, including inertial navigation parameters.
- **Antenna installation** includes considerations for the type of antenna and how it will be mounted on the vehicle. For example, a shark fin antenna may or may not require drilling. Different types of antennas may be needed on different vehicles, especially heavy vehicles. Antennas for buses may be through the glass.
- Before any devices are installed, **verify the vehicle is operating properly** and then disconnect the battery.
- Consider contracting a **professional installation** company to facilitate installation given the complexity of mobilization.
- Consider all **costs** that will be incurred in order to "touch" the vehicles.
- Consider **privacy and liability issues**, which may require consent agreements and differ for public agency vehicles versus private vehicles. One privacy solution may involve a periodic self-purge of log files, e.g. every 48 hours.
- Consider how the device will be **powered** from the vehicle, e.g. ignition on/off or quiescent current draw. Also consider whether and how the device will complete "work in process" when powering off, as well as issues related to battery disconnection, inrush and fusing, and grounding.
- **Requirements** may be developed that would be typical based on the type of controller.
- Consider the need for **environmental requirements** for in-vehicle systems.
- Consider how **automotive antenna radiation patterns** impact quality control and consistency. For instance, Utah DOT found that different antenna manufacturers had different radiation patterns, requiring different tuning to get optimal results, e.g. aiming the antenna to get the best results for the type and size of vehicle.
- Consider the need for **fail-safe over-the-air survival**.
- Ensure there is a **connection from the CAN bus to turn signal data**.
- Consider the need for **maintenance tracking**.
- Carefully consider the **location and placement of the antenna** on the vehicle. Reduce the distance from the transmitter to the antenna to avoid too much signal loss between the units.

Resources / On-line Supporting Materials:

- None identified at this time.

Vehicle Controller Area Network (CAN) Bus

Summary of Role/Function:

- A Controller Area Network (CAN bus) is a robust vehicle bus standard that allows controllers and devices to communicate with each others' applications without a host computer. Vehicles typically have a port interface that can be accessed by an external device given appropriate security credentials to receive vehicle telematics data for use in connected vehicle applications.

Relevant standards:

- SAE maintains a variety of CAN bus standards related to On-Board Diagnostics-II (OBD-II) that have been required for vehicles in the United States since 1996.

Anecdotal Lessons Learned from Early Deployers:

- The CAN bus **interface** may be used by other existing devices (e.g. Geotab).
- **Interference** issues may be experienced when interfacing with the CAN bus.
- The CAN bus may be accessed using a **passive or active interface**.
- The **manufacturer's cooperation** may be needed to successfully interface with the CAN bus, which may present challenges.
- It is important to **understand what data is available and what data is needed** from the CAN bus.
- **Future encryption**, e.g. "right to repair"

Resources / On-line Supporting Materials:

- None identified at this time.

Other Vehicle Systems

Summary of Role/Function:

- Vehicles include a variety of other sensors and systems that may be used to collect data, provide sensing capabilities, and offer automated driver support functions. Connected vehicle functions may supplement these systems, benefit from accessing data or status information of these systems, and/or incur additional challenges as a result of the presence of these systems. For example, the vehicle-based GPS sensor might provide data to on-board applications or the HMI and speedometer data could potentially support applications.
- Some types of vehicle automation are designed to function based on available connectivity. For example, the Traffic Optimization for Signalized Corridors (TOSCo) effort is designed for the vehicle to automatically control its speed based on data received from traffic signals. Similarly, the USDOT CARMA program is also related to cooperative systems where the vehicle automation is responding to information from other vehicles and/or the roadside.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- None identified at this time.

Resources / On-line Supporting Materials:

- None identified at this time.

Vehicle Human Machine Interface (HMI)

Summary of Role/Function:

- The human machine interface (HMI) represents a variety of visual displays, as well as possible auditory- or haptic-based systems that are used to provide advisory, alert, or warning messages to drivers based on real-time conditions. The interface may include a touch-screen or visual command capabilities on the vehicle dashboard, include audio capabilities, or be a driver's mobile device, for instance. The HMI allows the driver to interact with and customize the system for the provision of messages.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- Consider whether driver will receive **notifications via audio, visual, haptic, or some combination** thereof.
- Consider whether **additional devices or speakers** will be needed and how they will be mounted.
- **Confirm issuance of driver alerts and messages**, as designed.
- Consider **distraction issues** given how messages and alerts are provided. This may vary for different stakeholders, which may vary based on driver age, experience, and professional training.

Resources / On-line Supporting Materials:

- None identified at this time.

In-Vehicle or Vulnerable Road User (VRU) Mobile Applications

Summary of Role/Function:

- A lot of valuable information is available to road users using cellular communications and mobile devices aside from what is broadcast to vehicles and available via the in-vehicle HMI. A variety of people are on or adjacent to roadways that are not in vehicles. These individuals, collectively called vulnerable road users (VRUs), include pedestrians and bicyclists, as well as construction or utility workers and law enforcement. These VRUs, as well as drivers, may take advantage of mobile applications that provide mobility and safety information from the cloud via mobile applications. While some of this information for drivers may duplicate what is available via the in-vehicle HMI, it will likely not provide the same level of detail or timeliness.

Relevant standards:

- There is no standard specification for mobile applications, however information from the Safety Pilot may be leveraged.

Anecdotal Lessons Learned from Early Deployers:

- Consider possible **privacy and liability issues** with the use of mobile applications, which may require consent agreements and different approaches for public agency use and private use. One privacy solution may involve a periodic self-purge of log files, e.g. every 48 hours.
- Mobile applications will require agencies resources to **provide support**, especially if the app was developed by the agency, but also for ensuring up-to-date information continues to be provided.
- Mobile applications available on personal mobile devices will **use cellular service**, but **special devices will be needed if agencies wish to utilize DSRC or C-V2X** for agency staff to use in safety-critical applications that require lower latency than cellular communications can provide.
- The application may **perform differently or designed to offer different services** when being tested by a control group versus being active for the broader traveling public.
- Applications need to be **calibrated** for local environments. For example, the speed at which some apps become active could be greater than the local speed limit.

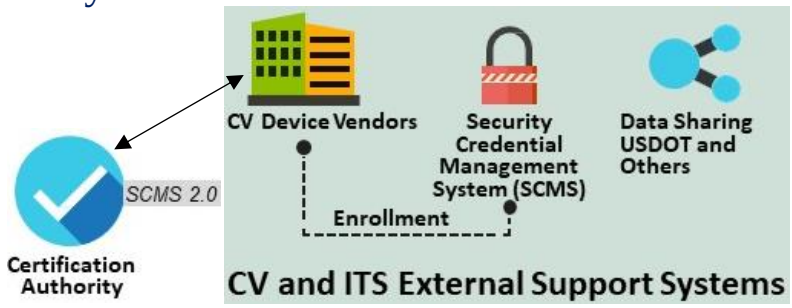
Resources / On-line Supporting Materials:

- None identified at this time.

Click here to Return to Full CV Deployment Environment Figure

CV and ITS External Support Systems

The Connected Vehicle (CV) and Intelligent Transportation System (ITS) external support systems encompass external vendors for devices and the Security Credential Management System (SCMS), as well as data sharing activities with external parties like the United States Department of Transportation (USDOT).



Key components of CV and ITS External Support Systems are described in more detail below and include:

- CV Device Vendors
- Security Credential Management System (SCMS) and Certification
- Data Sharing

CV Device Vendors

Summary of Role/Function:

- Connected vehicle device vendors develop RSUs and ASDs for procurement that conform to the latest standards and specifications, as stipulated by the procuring entity. These vendors also generate firmware and software updates for their devices to ensure ongoing compliance with standards and specifications.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- Agencies may receive controlled access from vendors in order to receive firmware updates, manage the distribution, and assign vehicles into groups for testing and upgrade management. Note that this is true for vendors of all components described in the CV deployment environment, not just CV device vendors.

Resources / On-line Supporting Materials:

- None identified at this time.

Security Credential Management System (SCMS) and Certification

Summary of Role/Function:

- The SCMS is a security measure that allows stakeholders to maintain trust in the system by verifying both vehicle and infrastructure devices, as well as the authenticity of messages sent between them in a connected vehicle environment. This allows the receiver to know a message was sent from a trusted source, enables vehicle on-board units and IOO operated RSUs to ignore any unauthorized messages, and provides safeguards to protect against the message being recycled or rebroadcast by others outside the operating agency.

- The SCMS will not eliminate all vulnerabilities in the transportation system but will reduce the risk of non-authorized systems transmitting false data, while maintaining user privacy through encrypted digital signatures and certificates.

Relevant standards:

- The IEEE 1609.2 Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages defines secure message formats and processing for use.

Anecdotal Lessons Learned from Early Deployers:

- Although first developed by the Crash Avoidance Metrics Partners (CAMP) LLC Vehicle Safety Communications 5 (VSC5) Consortium as a Proof of Concept, **numerous private-sector vendors** now offer a version of SCMS.
- There is a need for a common, managed "**root**" in the SCMS that allows multiple vendors and approaches all to tie to one common security origin to ensure interoperability.
- Current **maturity** of private-sector vendor SCMS offerings, interoperability, and compliance with original equipment manufacturer (OEM) systems is not well known, given the relatively limited number of deployments by agencies.
- Agencies need to **be fluid and accept that changes may be needed** to existing SCMS offerings by private-sector vendors in order to support a potentially more standardized or regulated SCMS for national connected vehicle operations in the future.
- The SCMS will **not comprehensively protect against every security risk** in the CV environment.
- RSUs, OBUs, and ASDs acquire certificates. Products and devices need to be **enrolled in the SCMS** and may need to be re-enrolled following maintenance activities.
- Agencies need to develop a **Security Plan** that includes a Security Management and Operations Concept (SMOC) and considers the number of certificates per week, life of certificates, and timeline for certificates to be loaded onto a device (e.g. these values were 60 per week, 7 days, and 2 weeks, respectively for the New York City CV Pilot), as well as a security profile for messages (i.e. SPaT, MAP, BSM, and TIM messages).
- Agencies must determine where messages are "signed", e.g. MAP and TIM messages at the TMC and SPaT messages at the RSU.
- Agencies will also likely need to consider: **test or production certificates**; distribution of a **Certificate Revocation List (CRL)**; ability to export detected **misbehavior**; **disabling crypto content**, i.e. "lost" devices; whether to use **IPv4 or IPv6** with a proxy server or direct firewall; and how to manage X.509 certificates.

Resources / On-line Supporting Materials:

- Security Credential Management System (SCMS) Proof–of–Concept Implementation End Entity Requirements and Specifications Supporting SCMS Software Release 1.2.2. 2016. Available at: https://wiki.campllc.org/display/SCP

Data Sharing by USDOT and Others

Summary of Role/Function:

- Agencies may choose to share collected CV data with external entities like the USDOT in order to support development of national statistics or performance measures, for example.

- Additionally, third-party CV service providers like TTS, Connected Signals, and Applied Information sometimes obtain information from IOOs or directly from vehicles and provide CV data to vehicle, all using network cellular communications.

Relevant standard:

- None identified at this time.

Anecdotal Lessons Learned from Early Deployers:

- To avoid **privacy issues**, agencies may need to scrub the data prior to sharing CV data.
- Agencies may need to conduct a **quality check** of CV data to ensure reliability and completeness before it is shared.
- Agencies may need to process data in order to map it to **metadata** or a **standard data format**.

Resources / On-line Supporting Materials:

- USDOT ITS Joint Program Office (ITS JPO), ITS DataHub: https://its.dot.gov/data and Secure Data Commons: https://its.dot.gov/data/secure.

Click here to Return to Full CV Deployment Environment Figure

Communications

The connected vehicle environment requires advanced communications technologies that are secure, interoperable, networked, and both wired and wireless to exchange data from vehicles to other vehicles, roadside infrastructure, transportation management centers (TMCs) and intelligent transportation systems (ITS), and other external support systems. Communications technologies used in the CV environment include:

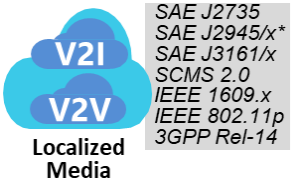
- Localized Media
- Wide-Area Media
- Internet
- Backhaul Communications

The CV environment requires communications for a variety data to be exchanged between vehicles and vulnerable road users, roadside infrastructure, TMC-ITS systems, and external support systems. This includes data and information required in near-real-time for safety and mobility purposes, as well as over the air (OTA) software updates to RSUs and aftermarket safety devices (ASDs) and OTA retrieval of log files from ASDs. Different communications mechanisms are often available to support various types of data exchanges, depending on how the CV environment is deployed within a jurisdiction, e.g. dedicated short-range communications versus cellular communications. When selecting a communications approach, agencies should consider the anticipated number of vehicles, RSUs, and frequency of encounters and alerts, as well as SCMS updates and expected size of log files that will need to be communicated.

Relevant Standards for Secure Communications:

- Datagram Transport Layer Security (DTLS) is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
- A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- Transport Layer Security (TLS) is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
- Simple Network Management Protocol (SNMP) is an application–layer protocol to manage and monitor network elements for exchanging management information between network devices.

Localized Media



Summary of Role/Function:

- Localized media exchange data and information between roadside units (RSUs) and on-board units (OBUs) or aftermarket safety devices (ASDs), i.e. roadside systems and vehicle systems.
- Localized media facilitate point-to-point, low-latency communications that take place across short distances and directly between two OBUs, or between an OBU and roadside infrastructure. Localized media support the exchange of data and information in four categories:
  - Vehicle-to-Infrastructure (V2I) communications are between vehicles and infrastructure systems.
  - Vehicle-to-Vehicle (V2V) communications are between different vehicles.

  - Vehicle-to-Everything (V2X) communications are between vehicles and passengers' and vulnerable road users' personal communications devices, including cyclists and pedestrians.
  - Infrastructure-to-Everything (I2X) communications are between the infrastructure and all local recipients, including vehicles, pedestrians, and cyclists, as well as other infrastructure, as warranted.
- Localized media can provide lower-latency communications within a short distance for smartphone applications, pedestrian applications, in-vehicle applications, and/or ASD applications. These point-to-point communications may be unicast, i.e. targeted to a specific vehicle or device, or broadcast to all users and devices within range. Although possible for smartphones to use local communications directly over WiFi or Bluetooth, these devices typically use network communications via the cloud rather than directly with devices on the roadside.
- Cellular communication technologies referred to as Cellular-V2X or C-V2X can provide direct device-to-device communications (in addition to network, cellular communications, as described in wide-area communications).

Relevant standards:

- The SAE J2735 standards cover V2I, V2V, and V2X message exchanges to ensure that vehicles operating with V2I communication capabilities can interpret the message communications. Currently, the J2735 Version 2016 is the latest version.
- The SAE J2945/x standards and SAE J3161/x standards explain how to apply the relevant standards for a specific application for DSRC and C-V2X, respectively. The standards cover the recommended practice for systems engineering and generic V2X interface requirements content, which may be adapted for wide-area communications as it describes the information exchange between a vehicle and another V2X enabled device, a device worn by or otherwise attached to a traveler, a roadside device, or a management center, to address safety, mobility, and environmental system needs.
- The IEEE 1609 standards for Wireless Access in Vehicular Environments (WAVE) defines the architecture, communications model, management structure, security mechanisms and physical access for high speed (up to 27 Mb/s) short range (up to 1000m) low latency wireless communications in the vehicular environment.
- The IEEE 802.11 standards govern telecommunications and information exchange between systems on local area networks.
- The 3GPP Release 14 Specifications describe radio access technology which are commonly referred to as C-V2X.

Anecdotal Lessons Learned from Early Deployers:

- V2X licensees must **register RSU sites**, channels, and other relevant data with the Federal Communications Commission (FCC) on the Universal Licensing System (ULS) under the call sign of the relevant license.
- DSRC and C-V2X are wireless technologies that include **enhanced security and privacy protections** than traditional Wi-Fi. Because DSRC and C-V2X each have a range of several hundred meters, many attacks would require close proximity. Since safety concerns predominately involve moving vehicles, there is a very short window for attack.
- Some agencies are trialing dual mode DSRC/C-V2X RSUs as they assess and try to understand approaches towards uncertainty in the spectrum allocations.

- The Federal Communications Commission (FCC) is in the process of re-assigning the 5.9 GHz spectrum (which includes DSRC) for other technologies and other uses such that IOOs should consider the uncertainties when determining how to implement local communications.

Resources / On-line Supporting Materials:

- The SCMS Proof of Concept document provides a general overview of security protocols, which is a role that is now often outsourced by agencies, e.g. Green Hill Integrity Security Services (ISS).

Wide-Area Media

Summary of Role/Function:

- Wide-area and cellular media provide data and information to on-board units (OBUs) or aftermarket safety devices (ASDs), i.e. vehicle systems, that originates from the TMC or other back office support systems via the cloud or internet. Wide-area or cellular communications allow devices to provide data and information via cellular towers and the cloud, not directly from device to device.
- Wide-area media support network communications, which are wide area communications that provide a connection via the cloud to infrastructure systems and devices, including personal devices used by vulnerable road users like bicyclists and pedestrians.
- Wide-area communications use existing cellular 4G LTE networks like a personal mobile phone does, and also include future 5G networks. The terms 4G and 5G refer to the "Generation" of cellular technology, and 5G is expected to provide data speeds up to 100 times faster than 4G. For transportation functions, cellular communication technologies referred to as Cellular-V2X or C-V2X, also provide direct device-to-device communications (described above in local media) as well as wide-area network communications described here.

Relevant standards:

- The SAE J2735 standards cover V2I, V2V, and V2X message exchanges to ensure that vehicles operating with V2I communication capabilities can interpret the message communications. Currently, the J2735 Version 2016 is the latest version.
- The SAE J2945/x standards and SAE J3161/x standards explain how to apply the relevant standards for a specific application for DSRC and C-V2X, respectively. The standards cover the recommended practice for systems engineering and generic V2X interface requirements content, which may be adapted for wide-area communications as it describes the information exchange between a vehicle and another V2X enabled device, a device worn by or otherwise attached to a traveler, a roadside device, or a management center, to address safety, mobility, and environmental system needs.

Anecdotal Lessons Learned from Early Deployers:

- An advantage of **wide-area cellular communications is the ability to reach vulnerable road users** like cyclists or pedestrians through their personal cellular devices.
- An unknown risk about the use of wide-area media for CV applications is the potential for **cellular networks to be overloaded during emergency events**.
- There are some third-party providers that send signal timing data into vehicles and to smartphones over network cellular.

Resources / On-line Supporting Materials:

- None identified at this time.

Internet

Summary of Role/Function:

- The Internet may be used to facilitate communications between the TMC and CVs, including publishing data online for communication to vehicles via network cellular approaches, as well as connections from the TMC to the SCMS and USDOT.
- The Internet can also be used to disseminate information from the TMC to transportation centers and other entities, for example that dispatch freight and emergency responders.

Relevant standard:

- Traffic Management Data Dictionary (TMDD) Standards support center-to-center communications as part of the regional deployment of ITS in order for centers to cooperate in managing, for example a corridor or arterial. The TMDD provides dialogs, message sets, data frames, and data elements to manage the shared use of these devices and the regional sharing of data.

Anecdotal Lessons Learned from Early Deployers:

- Many implementations have had to tunnel IPv6 through IPv4 networks due to lack of support for native IPv6.
- Firewalls, router configurations, virtual networks, and related elements are needed in order to provide network security when connecting to the Internet.

Resources / On-line Supporting Materials:

- None identified at this time.

Backhaul Communications

Summary of Role/Function:

- In order for local communications between roadside units and vehicles to function, there is a need to deliver data from a TMC to the roadside and also to send data back from the roadside to the TMC. This two-way data communications will be supported by wired or wireless backhaul communications, which is wide bandwidth data transmission that transports multiple signals and traffic types using coaxial cable, optical fiber, radio or twisted pair, and satellite communications that may be used in rural areas or as a redundant system, or other systems that the agency operates. As an example, roadside units in the field will require backhaul communications to centers.

Relevant standards:

- NTCIP 1103 Version 3 Transportation Management Protocols (TMP) defines a composite application layer protocol for the management of transportation equipment.
- NTCIP 1201 Version 3 Global Object Definitions identifies and defines the common object definitions that may be supported by transportation devices that are NTCIP-conformant.
- Traffic signal controllers that are compliant with NTCIP 1202 Version 3 Object Definitions for Actuated Traffic Signal Controller (ASC) Units are typically capable of generating an output of the SPaT parameters as NTCIP 1202 SPaT messages.
- NTCIP 1211 Version 2 Object Definitions for Signal Control and Prioritization (SCP) provides definitions of the management information related to Signal Control and Prioritization (SCP).

Anecdotal Lessons Learned from Early Deployers:

- None identified at this time.

Resources / On-line Supporting Materials:

- None identified at this time.

Click here to Return to Full CV Deployment Environment Figure