Connected Vehicle Deployment Technical Assistance

Roadside Unit (RSU) Lessons Learned and Best Practices

www.its.dot.gov/index.htm

Final Report – May 2020
FHWA-JPO-20-804

U.S. Department of Transportation

Section 1: Introduction

This document captures lessons learned and best practices for Roadside Units (RSUs) as experienced by the United States Department of Transportation's (USDOT's) Connected Vehicle (CV) Pilot sites. The USDOT awarded cooperative agreements collectively worth more than $45 million to three pilot sites in New York City; Wyoming; and Tampa, FL to implement a suite of connected vehicle applications and technologies tailored to meet their region's unique transportation needs. These pilot sites are helping connected vehicles make the final leap into real-world deployment so that they can deliver on their promises to increase safety, improve personal mobility, enhance economic productivity, reduce environmental impacts and transform public agency operations. Moreover, these sites are laying the groundwork for even more dramatic transformations as other areas follow in their footsteps.

The purpose of this document is to synthesize, at a high-level, key lessons learned, and best practices related to RSUs to assist other early deployers as they deploy connected vehicle technologies in their jurisdictions. Connected vehicle technologies are still an emerging technology. Before starting a connected vehicle project, it is important for deployers to understand the complexity and maturity of the technology. The intent of sharing these lessons learned is to assist future deployers in understanding some of the technical challenges related to deploying the technology so that they can more easily deploy consistent and interoperable systems.

RSU lessons learned and best practices were collected from documents and technical presentations produced by the CV Pilot sites, discussions from CV Pilot Technical Roundtables, and other sources. Content is captured for the acquisition/procurement, design, installation, and testing of RSUs.

An RSU (depicted in Figure 1) is a wireless communications transceiver that is mounted along a road or pedestrian passageway. RSUs broadcast data to onboard units (OBUs) or exchanges data with OBUs in its communications zone. OBUs are devices located in vehicles to collect data from the vehicle and/or provide an interface through which intelligent transportation systems (ITS) services, e.g. travel information and warnings, can be provider to the driver. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required. RSUs prepare and transmit messages to the vehicles and receive messages from the vehicles for the purpose of supporting the vehicle-to-infrastructure (V2I) applications.

Figure 1. A Roadside Unit (RSUs) installed in New York City (Source: New York City DOT)

Figure 2 depicts the functional perspective of the RSU – depicting the activities that the RSU performs, inputs, outputs, controls, and enablers. The intent of this functional focus is to help ensure interoperability and avoid precluding the potential integration of RSU functionality within other ITS field equipment, where increased efficiency, effectiveness or market sustainability are possible.

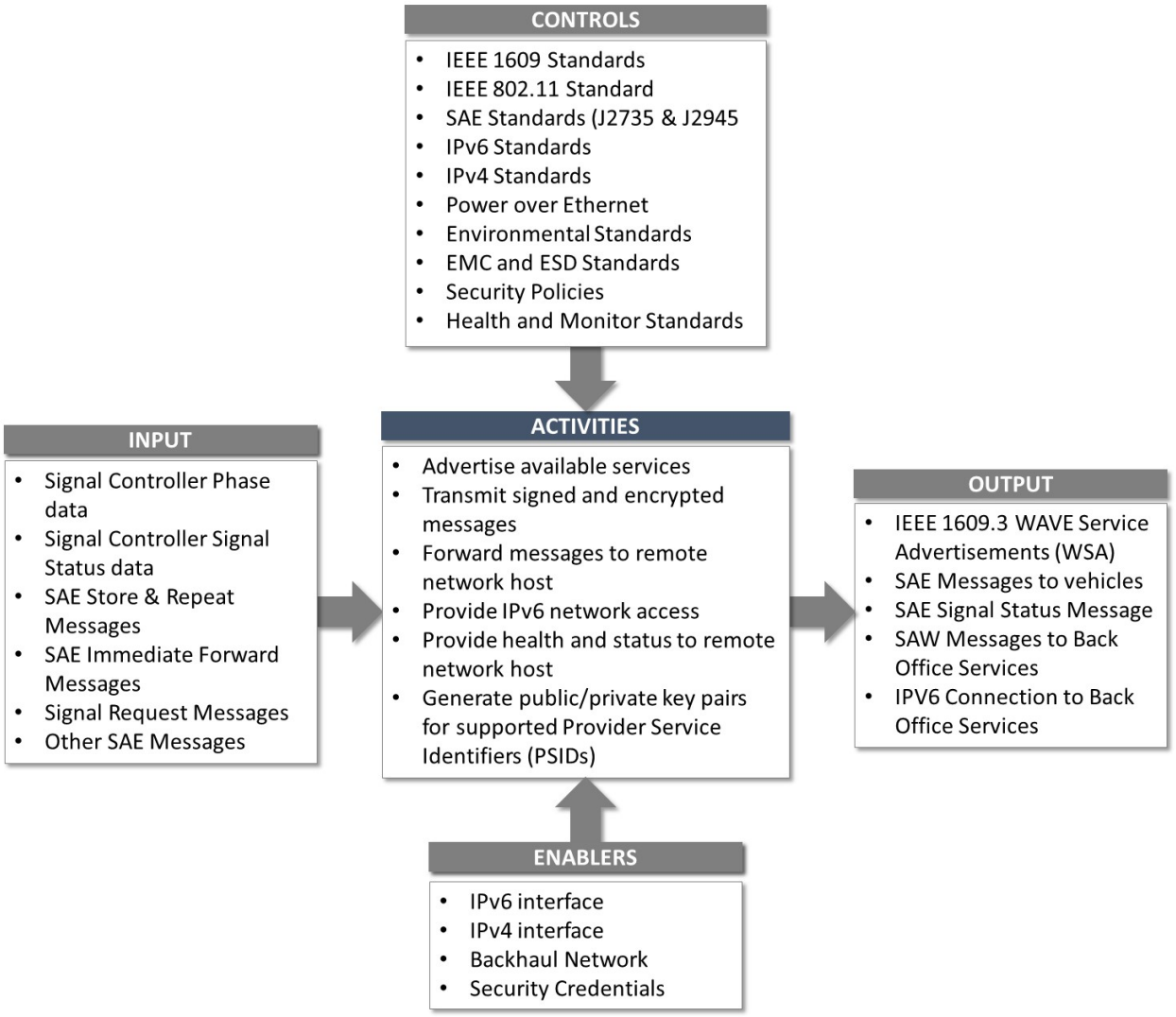

Figure 2. Roadside Unit (RSU) Context Diagram. (Source: USDOT)

Deploying a production-level end-to-end connected vehicle system takes more than transmitting signal phase and timing (SPaT), MAP, and basic safety messages (BSMs). While "demos" are easy – especially without detailed performance measurements – deploying a complete connected vehicle ecosystem requires a significant amount of planning, engineering, and testing. The lessons learned and best practices, documented in this report, are intended to assist agencies as they deploy connected vehicle technologies. Just as a fully deployed traffic management system is a complex system of systems which extends from the intersection traffic controller to the central management and optimization of signal timing patterns and operation and maintenance management and data collection and analysis, the deployment of a connected vehicle eco system requires attention to large scale management of devices, tracking of performance data, detection of anomalies and dispatching of maintenance crews, monitoring of communications reliability, and overall monitoring of device health and operation.

The functional block diagram shown in Figure 2 depicts the basic or minimal RSU functionality. RSUs are "smart" devices and can provide many additional services depending on your system design and concept of operations. For example, RSUs installed in the New York City CV Pilot provide additional functionality. Examples of additional functionaility from CV Pilot RSUs include:

a. Providing security credential management system (SCMS) access so that OBUs can topoff or update their certificates. Because the backhaul network is IPv4, the RSU acts as a gateway to the proxy server at the Transportation Management Center (TMC) to provide the OBU with direct access to the SCMS to update their certificates on a weekly basis. This service is advertised through the RSU using wave service announcements (WSAs) and the OBUs initiate a connection if they need a certificate top-off.

b. Providing store and forward processing for OBU log data. New York City CV Pilot OBUs use DSRC communications while traveling through the connected vehicle infrastructure to upload data they collect which includes:

    1) Event data captured whenever an alert is generated;

    2) Radio Frequency (RF) Operational Data to indicate other OBUs they see and which RSUs they came into contact with;

    3) A System Status Log to report on the health of the OBUs systems; and

    4) Breadcrumb Data collected at 10 second intervals (note this data is being collected to evaluate the accuracy of the event data during system integration only).

c. Collecting and uplinking to the TMC BSM data which is used to compute travel times and to help in determining the range of operation. In this case, the RSU is configured with "detection zones" and captures one BSM for each vehicle entering a zone and relays this to the TMC where it is used to computer travel times. These zones can also be used for queue detection and congestion detection (vehicle speeds) and offloads the preprocessing so that the traffic controller can use this data for signal optimization.

d. Broadcasting firmware updates and configuration changes using a network coding scheme.

This collection of additional capabilities are unique to the NYV CV Pilot, but were essential to the long term goals for supporting operations and maintenance and for the data collection required for performance monitoring and analysis. These requirements were added to the initial specification to meet the specific needs of the New York City CV Pilot, but others developing connected vehicle infrastructures should consider such issues as data collection, operations and maintenance (O&M) data needed to monitor and manage the system.

Document Organization

This document is organized into five sections. Section 1 provides an introduction. Sections 2-5 include lessons learned organized by the following categories – Acquisition and Procurement, Design, Installation, and Testing. In total there are sixty-seven (67) lessons learned and best practices. The following outline includes a summary of the lessons learned and includes hyperlinks to subsections within each section.

Section 1: Introduction

Section 2: RSU Acquisition and Procurement Lessons Learned and Best Practices

Section 3: RSU Design Lessons Learned and Best Practices

  - Design 03: Insist that your vendor's RSU be certified conformant by an independent laboratory.
  - Design 04: Clarify the RSU's transmission of WSAs in terms of automatic or manual transmission.
- Network, Backhaul, and Security Considerations
  - Design 05: Be cognizant that the most recent version of the internet protocol (IPv6) is not offered on every network.
  - Design 06: Monitor IPv4 and IPv6 network status to gain insights.
  - Design 07: Consider implementing data collection procedures and techniques that reduce the burden on the communications network and account for the limitations of backhaul bandwidth.
  - Design 08: Consider the entire RSU network and security measures.
- SCMS-related Considerations
  - Design 09: Understand what applications will be deployed early in the process to support enrollment with the SCMS for specific PSIDs as well as specific SSPs (if necessary
  - Design 10: Understand that application certificates will need to be refreshed periodically.
  - Design 11: Consider when RSU applications certificates will expire.
  - Design 12: Consider where connected vehicle messages will be signed – at the RSU, TMC, or by a Third Party.
  - Design 13: Ensure that device vendors can support enrollment/bootstrapping.
- Over-the-Air (OTA) Considerations
  - Design 14: Leverage Over-the-Air (OTA) support networks for software/firmware updates.
  - Design 15: Recognize that while OTA updates provide opportunities, it is not without challenges.
- Other Design Considerations
  - Design 16: Ensure that RSUs have sufficient computing power.
  - Design 17: Augment connected vehicle solutions with more traditional ITS technologies where necessary.
  - Design 18: Design RSUs to continue broadcasting through jamming activities.
  - Design 19: Secure a significant amount of time to review design documentation.
  - Design 20: Include extensibility requirements for "future proofing".
  - Design 21: Coprocessors or another secondary processing unit is not needed and creates security holes.

Section 4: RSU Installation Lessons Learned and Best Practices

- General Installation Considerations
  - Installation 01: Develop installation checklists and procedures.
  - Installation 02: Consider the location of existing ITS devices and line of sight when selecting sites for the installation of RSUs.
  - Installation 03: Optimize RSU installations to prevent damage to RSU's antennas and improve RF propagation.
  - Installation 04: Verify optimal RSU height and resolve discrepancies in RSU elevation.
  - Installation 05: Ensure that RSUs are properly grounded.

  - Installation 06: Short-haul Wireless connections may be needed to bridge the gap between the RSU and the cabinet.
  - Installation 07: Signage on structures may disrupt RSU antennas.
- Installation Timing/Scheduling Considerations
  - Installation 08: Start the permitting process early.
  - Installation 09: Conduct site visits and account for a slower rate of installation of RSUs than OBUs, as they require dispatch crews.
- Other Installation Considerations
  - Installation 10: Ensure that RSU information from the asset management system is readily available on the RSU for device management and tracking.

Section 5: RSU Testing Lessons Learned and Best Practices

- Overarching Testing Considerations
  - Testing 01: Ensure detailed testing is conducted for RSU software and hardware.
  - Testing 02: Ensure rigorous requirements verification and acceptance testing.
  - Testing 03: Conduct testing early with actual infrastructure.
  - Testing 04: Complete testing of individual components of the system prior to system-level testing.
  - Testing 05: Give a considerable amount of attention to testing prior to devices becoming operational.
  - Testing 06: Test for security challenges relating to communication.
  - Testing 07: Understand that testing for *Pilot* does not equal testing for *Scale*.
  - Testing 08: Perform multiple/regression testing to verify that a previously tested system still performs the same way after changes were made in the field to another component.
  - Testing 09: Test the RSUs resiliency and ability to recover from failure.
  - Testing 10: Continually test systems and check their requirements.
  - Testing 11: Examine all possible root causes before power-cycle/reset/reboot of the device.
- Testing Location Considerations
  - Testing 12: Arrange a testing location that can accommodate the necessary test runs.
- Tools Considerations for Testing
  - Testing 13: Leverage Radio Frequency (RF) tools to support testing.
  - Testing 14: If using licensed spectrum, consider purchasing interference tracking equipment to detect potential interference from other users in the 5.9 GHz band that can compromise data exchange.
- Other Testing Considerations
  - Testing 15: Test the OTA download and upload mechanisms before extensive installation of the OBUs and RSUs.
  - Testing 16: Test for RSU Traveler Information Message (TIM) transmission range.
  - Testing 17: Ensure that RSUs will run 24/7/365 without problems.
  - Testing 18: Ensure RSUs can collect and forward all participant data.

  Testing 19: Ensure that Security is Considered from the Beginning and Testing is Conducted on a Secure System.

Section 2: RSU Acquisition and Procurement Lessons Learned and Best Practices

This section documents lessons learned and best practices for the procurement of RSUs.

Personnel and Stakeholder Engagement Considerations

- **Procurement 01: Obtain stakeholder feedback early for determining the details of the devices.** Meetings with stakeholders should be held early in the project to gain insight on the participants' needs (and expectations) in developing systems engineering deliverables – Concept of Operation (ConOps), System Requirements Specification (SyRS), System Architecture Document (SAD), and System Design Document (SDD).

- **Procurement 02: Engage with procurement and contracting personnel early in the process.** Ensure that contracting and procurement personnel are involved from the beginning of the project. Due to the challenges of using traditional procurement mechanisms, deployers found that involving contracting and procurement personnel from the beginning of the project can help prevent possible delays caused by miscommunication. Agencies need to work with their contracts office to ensure that the technical requirements are met when selecting a vendor/consultant. Traditional mechanisms for procurement that agencies follow may not fit well with software/technology-heavy projects. In addition, some agencies may be required to use lowest bid contractors/equipment for their projects and may need to work with their contracts office to ensure that the technical requirements were met when selecting a vendor/consultant. For the THEA CV Pilot, THEA had the ability to sole source research projects. In addition, the THEA team was able to leverage existing contract vehicles to bring contractors onboard before award to support planning and systems engineering activities for Phase 1 (Concept Development) activities. Working with procurement and contracting personnel early in the process, may result in opportunities to streamline and simplify procurement and contracting efforts.

- **Procurement 03: Bring in Subject Matter Experts (SMEs) to support procurement efforts.** Consider bringing in system engineers and connected vehicle experts to vet the project requirements prior to releasing the RFPs. Taking this approach enables deployers to contract with qualified consultants and ultimately receive a better final product. Consider a team of on-site and off-site connected vehicle experts – including individuals with experience in systems engineering, standards, cybersecurity, and wireless communications. Having that expertise enables agencies to verify deliverable accuracy and ensure that they are meeting program goals and system requirements. For early deployers, SMEs may be difficult to identify as there have been a limited number of full deployments of the technology. Consideration should be given to engaging SMEs that have been engaged in connected vehicle standards activities and successful deployments from across the country, if possible. SMEs with proven systems project management and systems engineering capabilities should also be considered.

- **Procurement 04: Review preliminary contract specifications with the vendor community prior to releasing the procurement.** Consider reviewing the preliminary contract specifications with the vendor community through Requests for Expressions of Information (RFEIs) and face-to-face technical reviews – prior to formal release – to ensure that the final specifications are practical, sustainable, saleable, and feasible within a reasonable budget for time and costs. The New York City

CV Pilot site issued a RFEI to elicit comments and information for the purposes of informing the City with respect to the matters raised. Collecting this input from the community is especially important for emerging technologies such as connected vehicle technologies – which have not been deployed at a large scale. It is also important to review the offerings available from several vendors early in the procurement process. It should be noted that RSU capabilities vary and as an edge device can perform many additional capabilities that may be required to meet stakeholder needs. For example, deployers may require the RSU perform additional functions to support f data collection, security management, and localized data analysis at the RSU. These functions may not exist in all RSUs offered by vendors. Deployers should carefully review what is available and what can be done within the RSU as well as what changes might be required to the traffic controller (i.e., changes to accommodate SPaT), network connectivity, and configuration management. Additionally, understanding the ongoing role for the vendor during operation is important. Will the agency be "managing" the devices, or does it plan to support remote management by the vendor? RSUs are complex devices and require careful management of the configuration and operation parameters to function properly. Vendors should also be able to assist with suggestions for your testing program, test equipment needed, and spares and staff training. Often, the vendor has some software tools that could be a great help during integration and troubleshooting.

- **Procurement 05: Organize a Change Control Board (CCB) of project stakeholders early in the project planning phase**. For the THEA CV Pilot Team, the CCB was valuable to capture the needs of each stakeholder as well as to resolve conflicting system requirements during the Design / Build phase. In each case, the ongoing Requirements Management by the CCB resulted in system requirements that were added, deleted, or changed, while still fulfilling the original needs of each stakeholder.

Systems Engineering, Standards, and Technology Maturity Considerations

- **Procurement 06: Use a System Engineering Process to structure the project.** To isolate and correct issues as early as possible in the project, a systems engineering process breaks the project down into levels of Units/Devices, Subsystem Integration, System Verification and System Validation, separated by Quality Gates (QG). At each QG, the CCB could choose to proceed, to change requirements or to abandon a technology found to be ineffective or unsafe. Simply developing a procurement document and then deploying the procured technology in the field would have been problematic for the CV Pilot sites. For example, use of mobile devices was found to be ineffective for safety applications due to location accuracy needed for crash avoidance.
- **Procurement 07: Procurement of "developmental" devices and evaluation of "prototypes" can present challenges to the procuring agency.** In the case of the RSU procurements, there will likely be many new features related to data collection, software updates, and security implementation that may be difficult to define in the procurement specification. For traditional ITS procurements, agencies are used to publishing detailed device specifications and then choosing the low bidder. For RSU procurements, it may be necessary to modify the specifications in some cases to insure a practical and reliable implementation. It should be noted that even applications that have been deployed for other connected vehicle projects may be immature. As such specifications and requirements may be moving targets. Agencies will need to partner with the vendor as part of the

design process to ensure requirements are met and work with the vendor to resolve various practical design issues.

- **Procurement 08: Conduct Technology Readiness Level (TRL) assessment for connected vehicle hardware elements and applications.** Use Technology Readiness Levels (TRL) to assess the development level for connected vehicle hardware and applications. TRLs are a method for estimating the maturity of technologies during the acquisition phase of a program, developed at NASA. The use of TRLs enables consistent, uniform discussions of technical maturity across different types of technology. TRLs are based on a scale from 1 to 9 with 9 being the most mature technology. The CV Pilot Sites noted that it would have been useful to accurately assess the connected vehicle hardware—primarily the OBUs and RSUs—as to where they were on the TRL scale. This assessment would have indicated the larger scope and cost of testing that they encountered. In hindsight, the initial TRL of the connected vehicle hardware was in the 5 to 7 range, while the required TRL for the hardware is 8 to 9. The general rule of thumb for development is that the development/test costs grow exponentially as you move up the scale and peak at TRL 8.

- **Procurement 09: Consider the maturity of connected vehicle devices and applications prior to procurement.** Some deployers noted that the units they procured required substantial technical support from the vendor during their initial deployment. Connected vehicle technology and application maturity may be lower than initially anticipated and industry application performance requirements may not be available. Agencies should utilize the System Engineering process (needs, requirements, specifications, traceability) and leverage existing device vendor experience. To address the emerging nature of connected vehicle technology, some deployers have explicitly stated in their procurements that they were only interested in purchasing turn-key applications. In such cases, the vendor is responsible for any necessary application development. Turn-key V2I applications are difficult to implement as there is a vehicle (OBU) and infrastructure (RSU) component to the application. An interface control document (ICD) should be developed to better understand and document the interfaces. The Wyoming CV Pilot developed an Interface Control Document for the physical object connections and data flows identified in the System Architecture Document. The document describes the interfaces and message flows for each data flow in the WYDOT CV Pilot.

- **Procurement 10: Leverage standards and understand that standards and technology will evolve.** Leverage existing standards, specifications, and processes in procuring connected vehicle technologies, including but not limited to IEEE 1609.x, SAE J2735, SAE J2945/x, the USDOT's RSU 4.1 specification, etc. Agencies should understand that evolving standards and technology can cause the specifications to be a moving target. It usually requires at least some troubleshooting.
Further, functionality such as probe data collection (e.g., collecting OBU logs), while included in the standards (J2735) is not supported by the OEMs and over-the-air (OTA) collection of such data is not part of the standards. Use of the service channels can support such data collection, but there are many aspects of an end-to-end deployment which are not included in the standards such as OTA firmware/software updates and OTA data collection from the devices. In addition, many of the standards are now undergoing some changes – and there are additional guides and changes in the security sections (1609.2). It is important to determine which version of the common standards to use when working with vendors.

- **Procurement 11: Be cognizant that additional requirements may need to be considered when procuring devices.** When developing requirements for security, event recording, over-the-air (OTA) updates, radio frequency (RF) monitoring and other management applications , be cognizant that these are new areas not covered by the standards and they will need to be addressed in the system design and procurement specifications. For example: Security requirements may be different for some of these devices and it will be necessary to develop a security plan for all of the applications as an integral part of the stakeholder's security objectives.

Vendor Capabilities and Support Services Considerations

- **Procurement 12: Reduce risk by selecting multiple suppliers.** To reduce risk, it is wise to select more than one supplier in the event that a supplier is unable to commit to previous agreements. With multiple selected vendors, an agency can disqualify any non-performing vendor(s) (if needed) and continue with the performing vendor(s) for the full complement of units. When awarding to multiple vendors, planning, and testing for interoperability become even more important, and more costly. Keep in mind that until there is universal maturity, different devices can and often do behave differently. Such issues must be determined and addressed during the testing phase of the project and multiple vendors can and are likely to increase the cost of integration. While selecting more than one vendor may be a good approach, agencies should not over commit to a particular vendor. If a particular vendor underperforms, it may be difficult to obtain additional units from other vendors because of manufacturing lead times. It is important to note that vendors have made choices where the standards are silent. There may be limitations on the number of WSAs and not all of the radios support continuous and alternating modes in any configuration.

- **Procurement 13: Procure vendor support for the entire project lifecycle.** Due to the emerging nature of connected vehicle technology, many deployers emphasized the importance of considering the level of technical support needed from vendors during the procurement process. The level of technical support varies depending on the deployer and project phase. In addition, deployers have experienced varying levels of support were provided by different vendors. With any emerging technology, having the right vendor expertise on-site and on-call can expedite problem resolution and troubleshooting. Many vendors may be small companies with development staff overseas. Future deployers should inquire where the development staff resides to avoid 24-hour delays to respond to issues. Including clear requirements for vendor support can reduce additional needs for additional costs later in the project. While it might be expected that vendors will account for this level of support in the proposals, agencies should keep in mind that few vendors have deployed a large number of RSUs and may not account for the level of support needed to deploy a real-world deployment.

- **Procurement 14: Documentation may be lacking from device vendors and needs to be kept up to date over the course of the project.** The CV Pilot sites found a lack of user and admin documentation with some of their RSUs. This presented challenges and required the sites to require the vendor to conduct onsite training. Agencies should ensure that they procure services for training and technical support from vendors. It is also important to remember that some of this documentation may be evolving based on the changes (challenges) discovered during integration. Documentation should be kept up to date as project personnel can change over time. It is also

important to document the configuration parameters and the rationale during incremental deployment – to serve as a future reference as the system expands.

- **Procurement 15: Conduct multiple technical scans to better understand vendor capacity, depth, and resources.** Consider conducting multiple technical scans to understand the vendors' technical depth and resources. This can be done by using a request for proposal (RFP) and on the road testing to identify promising suppliers who can meet the system, cost, and project timing requirements. Prior to selection, obtain a better understanding of vendors' depth and resources to deliver. Vendors of RSUs and OBUs may not have the capacity and staff to supply the required devices for a project, which may result in delays. Technical scans are critical to scrutinize and select the best suppliers. Since this technology cannot be purchased off the shelf yet, the New York City CV Pilot Site did a RFEI demonstration/evaluation. While demonstrations are useful, agencies should be cautioned that demonstrations are not real-world tests.

Budgeting and Cost Considerations

- **Procurement 16: Consider sharing cost of RSUs and applications among stakeholders.** Agencies should consider sharing the costs of RSUs and applications among stakeholders, where applicable. For example, detection, transit, emergency, communications, signal controllers are roadside devices that are procured by multiple agencies. At lower cost, the RSU can be cost-shared while each agency specifies the software applications needed to replace their legacy equipment. Transit signal priority (TSP) phase selectors, Bluetooth travel time readers, cellular modems, edge computers, GPS receivers, and other equipment will cost more per location than an RSU. Cost-sharing among agencies provides opportunities for cost savings.

- **Procurement 17: Consider total cost of ownership over the RSU service life.** RSUs are capable of supporting software applications that replace single-purpose equipment within existing budgets. Travel time readers, cellular modems, vehicle counters, transit signal priority and emergency preemption phase selectors, plus outdoor Wi-Fi hot spots are examples of equipment currently being purchased and maintained that may be replaced with an RSU running multiple software applications. While an RSU may be used to replace numerous devices, it should be noted that deploying a RSU as part of a connected vehicle deployment will likely require more resources to deploy and test the equipment when compared to more conventional devices. The CV Pilots expended a good amount resources to make the connected vehicle devices operational. While a number of applications may be simple to deploy, integrating the components into a full system can be complex and will require time and effort to deploy as a complete system. These challenges may escalate for early deployers as vendor may be providing weekly updates to devices as they mature.

Phasing, Scheduling and Timing Considerations

- **Procurement 18: Consider the time needed for large scale purchases.** One of the biggest challenges of the procurement process is the unexpected delays caused by lengthy negotiations and slow progress for issuing contracts with vendors. Deployers who have faced this challenge recommended forecasting possible delays in the process early in the project and to also allocate enough time for the procurement cycle. The time for an agency to issue a purchase order (PO) or contract for each vendor may be much more extensive than expected. It is also important to consider the practical schedule for the construction of electronic equipment. From New York City CV Pilot experiences,

procuring custom devices in small quantity (10-50) occurred rather quickly (8-12 weeks) but procuring production quantities took up to 16-20 weeks since the devices required additional functionality and were not "off the shelf" devices. This is common with prototype of low technology maturity systems. As the technology matures, procurement timelines are likely to reduce. In the near-term, many vendors may sell agencies that they can deliver a certain number of devices in a given timeframe (e.g., XX number of devices in YY weeks). Vendors may or may not be able to meet those commitments due to several reasons including overseas manufacturing a well as the ability for the vendor to gear up and produce large numbers of devices. A lessons learned from the New York City CV Pilot was to include a line item in their contract for on-site engineering support with one-week terms so that they had a "contract vehicle" by which to request (and pay for) vendor assistance. Such a line item is fair to both the agency and the vendor as it provides an opportunity for both to work out the integration issues and troubleshoot issues that may not have been anticipated. Often "remote" troubleshooting can delay resolution and end up costing both parties more in the long run. Most agencies can deal with support on the basis of a Man Week on site including expenses.

- **Procurement 19: Consider splitting procurement into multiple phases to minimize risks.** The New York CV Pilot separated the procurement process into two phases with a prototype phase and production phase. Splitting the procurement process in this manner allowed them to smooth out any kinks on a limited number of devices before scaling up to procure the complete set of devices for the deployment.

- **Procurement 20: Filing for Federal Communications Commission (FCC) Licensing may take more time than originally expected.** Spectrum permits must be obtained prior to operating an RSU. Filing for DSRC licensing for RSUs can be a time-consuming process as applications have to be done through the FCC on an individual basis. The CV Pilot sites initially spent more time on filing for DSRC licensing than originally expected. FCC licensing consists of the three-step process presented below. Agencies should plan to allow several months to obtain an FCC permit.

    - *Apply for an FCC Registration Number (FRN)* through the FCC's Commission Registration System (CORES). The FRN establishes personal registration login information, and the online process requires organization and contact information such as the applicant's name, address, and Employer Identification Number (EIN). To identify individuals within a transportation agency or authority who already have an FRN, search the CORES website by entity for an associated FRN and related contact information: https://apps.fcc.gov/coresWeb/publicHome.do.

    - *Apply for Non-Exclusive Geographic-Area Licensing* based on the public or private entity's legal jurisdictional area of operations for authorization to operate in all channels in the 5.9 GHz band. Licenses will be granted for a term of 10 years and may be renewed. This step requires completion of FCC Form 601 (FCC Application for Radio Service Authorization: Wireless Telecommunications Bureau Public Safety and Homeland Security Bureau) using the FRN and Schedule D16. The form is available at: https://transition.fcc.gov/Forms/Form601/601MainForm_ScheduleA.pdf

    - *Registration of Individual RSU Sites* requires information regarding the make and model of the RSU; mounting latitude, longitude, and height, as well as site elevation; channels; and

support structure type to be entered into the FCC online database under the geographic-area license. Registration for each RSU location requires a separate application. However, registrations for multiple sites may be submitted simultaneously, which may reduce the total time to receive the approvals needed for deployment.

Additional information for registering an RSU and filing an application is listed on the FCC DSRC Service website at: http://wireless.fcc.gov/services/index.htm?job=licensing&id=dedicated_src.

Referenced FCC forms can be found at: https://transition.fcc.gov/Forms/Form601/601MainForm_ScheduleA.pdf.

Procurement-Related Resources

The following are documents that provide additional information related to procurement lessons learned and best practices:

- New York CV Pilot: FHWA-JPO-17-455, https://rosap.ntl.bts.gov/view/dot/36389
- New York CV Pilot: Device Acquisition and Installation Experiences Webinar (July 30, 2018) https://www.its.dot.gov/pilots/pdf/New York City_CVP_SiteAcquisitionInstallation.pdf, https://itsa.adobeconnect.com/_a932559885/pkdk4gxzgjcu/?proto=true and https://www.its.dot.gov/pilots/New York City_acquisition_qa.htm
- THEA CV Pilot: FHWA-JPO-17-463, https://rosap.ntl.bts.gov/view/dot/36240
- THEA CV Pilot: Device Acquisition and Installation Experiences Webinar (August 7, 2018) https://www.its.dot.gov/pilots/pdf/CVP_Acquisition_InstallationWebinarTHEA.pdf, https://itsa.adobeconnect.com/_a932559885/pdymo99buz1e/?proto=true and https://www.its.dot.gov/pilots/thea_device_qa.htm
- Wyoming CV Pilot: FHWA-JPO-17-471, https://rosap.ntl.bts.gov/view/dot/35425
- Wyoming CV Pilot: Device Acquisition and Installation Experiences Webinar (July 23, 2018) https://www.its.dot.gov/pilots/pdf/WYDOT_CVP_Acquisition.pdf, https://itsa.adobeconnect.com/_a932559885/ppm3ozwdeknj/?proto=true and https://www.its.dot.gov/pilots/wydot_installation_qa.htm

Section 3: RSU Design Lessons Learned and Best Practices

This section documents lessons learned and best practices for the design of RSUs.

Standards Considerations

- **Design 01: Design systems using published U.S. Standards.** Agencies considering CV deployments are highly recommended to use the most recently published ITS standards; any use of unpublished standards or standards in progress is strongly discouraged. If a U.S. standard does not exist, it is suggested to design using available international standards. In the event that no relevant standard exists, agencies are advised to use other relevant documents including USDOT's V2X Hub Deployment Guide and RSU Specification document v4.1 as initial points of reference. Deployers should avoid the use of unpublished standards. During the CV Pilot, all THEA system requirements were met while conforming to a baseline of standards published on January 1, 2017 at the start of Phase 2 Design/Build. The THEA team filled out gaps in USA standards using published international standards that resulted in USA standards development efforts, such as NTCIP 1218.

- **Design 02: Apply and update standards conformance where appropriate.** All messages being used should conform to the latest versions of SAE J2735, SAE 2945/x, IEEE 802.11, IEEE 1609.x, and related standards. Vendors are expected to work with the deployer agency to determine the appropriate version for each standard/device specification that has been accepted for general use. To ensure standards were being followed in a consistent manner, the CV Pilot Sites developed the following materials:

    - *The Information Flows Triples* spreadsheet documents the source and destination physical objects and the information flows exchanged between the objects from each CV Pilot site.
    - The CV Pilot sites also made their *Data Object Alignment* spreadsheets available to stakeholders interested in deploying connected vehicle projects that are interoperable with the CV Pilot sites. Connected vehicle messages include mandatory and some optional data objects. Data Object Alignment spreadsheet are available for the following message types: Basic Safety Message (BSM); Traveler Information Message (TIM); Intersection Geometry (MAP) Message; Signal Phase and Timing (SPAT) Message; and Wireless Access in Vehicular Environments (WAVE) Service Advertisement (WSA) Message.

    The spreadsheets are available upon request by emailing cvpilots@dot.gov.

- **Design 03: Insist that your vendor's RSU be certified conformant by an independent laboratory.** Agencies should require their vendors to be certified conformant by an independent laboratory. Since virtually no agency has the laboratory facilities, test equipment, and expertise to perform conformance testing, requiring certification is a reasonable starting point – but does not guarantee interoperability. It should be noted that not all of the "edge" or "corner" conditions for all of the standards may be extensively tested during the certification process. It is important to determine the functions you will be using and verify that they are part of the certification process. For example, the CV Pilot sites found that alternating channel operation was not extensively tested for certificaton.

- **Design 04: Clarify the RSU's transmission of WSAs in terms of automatic or manual transmission.** During the CV Pilot deployment, the RSU's transmission of wave service advertisements (WSAs), in terms of manual or automatic transmission, was not defined in RSU Specification v4.1. As a result, different vendors applied different practices. Deployers need to coordinate with RSU vendors and the standards community to develop a common understanding of the requirements and standard solutions. Consideration should be given to refining requirements in the RSU specification v4.1 (requirements 570-572). Deployers should coordinate with the vendors for common understanding of the requirements. However, many issues may not become evident until a significant number of devices (both RSUs and OBUs) are being tested. By way of example, interference between RSUs and the interaction of WSAs and overlapping coverage require a carefully planned approach to the deployment of which services are supported by which RSUs.

Network, Backhaul, and Security Considerations

- **Design 05: Be cognizant that the most recent version of the internet protocol (IPv6) is not offered on every network.** RSUs utilize IPv6 messaging. Though IPv6 can coexist with IPv4, IPv6 is the best answer to sufficiently address speed, security, efficiency, and operational ease desired for the operation of connected vehicle systems. During transition from IPv4 to IPv6, many of the CV Pilots' network devices did not support IPv6. Some devices were able to apply simple firmware updates, but others may require the purchase of new hardware. In summary, early deployers should be cognizant that the most recent version of the internet protocol is not offered on every network natively and that there may be lengths in the network that do not support IPv6 that you may have to plan around.

- **Design 06: Monitor IPv4 and IPv6 network status to gain insights.** When monitoring network traffic on the backhaul system from the RSU to the TMC, it is recommended that the network monitoring setup include two monitoring instances, one for IPv4 and one for IPv6 as each can have independent traffic monitoring characteristics. To help monitor the status of the project, the Wyoming CV Pilot developed an open source dashboard tool that monitors IPv4, IPv6 and DSRC network status and provides information visually on a map as well as charts and graphs. It also provides information for active Traveler Information Messages (TIMs) and vehicle counts past an RSU. The Wyoming CV Pilot uses this dashboard to internally monitor the network status of RSUs. Open source code is available at: https://github.com/Trihydro/smdm

- **Design 07: Consider implementing data collection procedures and techniques that reduce the burden on the communications network and account for the limitations of backhaul bandwidth.** While not required, some deployers may want consider data collection procedures and techniques that reduce the burden on the communications network. This was the case for the New York City CV Pilot where all municipal systems within New York City utilize the New York City Wireless Network, limiting the bandwidth that the New York City CV Pilot had access to. While the Tampa and Wyoming pilots are collecting vehicle data continuously, the New York City CV Pilot is only doing event-based data collection to address these limitations. Whenever a configurable event occurs (e.g. hard breaks, steering turns or hard accelerations), all BSMs before and after an event for a configurable amount of time and from other equipped vehicles within a configurable region of interest are combined, compressed, and encrypted into what becomes an "event" record. Connected vehicle infrastructure naturally provides the opportunity for edge processing and the

aggregation of connected vehicle information to foster better mobility. New York City looked to incorporating edge computing concepts into their data management plans to further address their needs for a more scalable data collection. As opposed to having all data processing occur at the TMC, New York City designed their system architecture to have some data processing occur at "edge" devices (RSUs, OBUs). By performing local processing at the edge instead of streaming all the data to a central cloud for processing, New York City was able to significantly reduce the amount of bandwidth used.

- **Design 08: Consider the entire network and security posture.** RSUs require a secure network when using public address LTE SIM cards and public fiber networks. An agency buying just an RSU radio for lowest price would need to address those issues by themselves. For example, THEA submitted RSUs to a "white hat" evaluator for cyber penetration testing, recommendations, and attack response plan. THEA also worked with the City's IT staff and network security contractor to develop the network plan that was tested for security readiness by a "white hat" evaluator.

SCMS-related Considerations

- **Design 09: Understand what applications will be deployed early in the process to support enrollment with the SCMS for specific PSIDs as well as specific SSPs (if necessary).** Prior to procuring a SCMS vendor, entities should know what applications their devices will be supporting. When deploying secure connected vehicle devices that are signing messages with certificates from a SCMS, knowing the applications the devices will support, and the messages utilized by those applications is extremely important. As part of the initialization/set-up process for these connected vehicle devices, they will need to enroll with the SCMS for specific PSIDs as well as specific SSPs (if necessary). If these devices are deployed without enrolling with the proper PSIDs and SSPs, you may be required to re-initialize those devices, which could entail pulling RSUs off mast arms.

- **Design 10: Understand that application certificates will need to be refreshed periodically.** Application certificates, which is what RSUs use to advertise and provide their services, are only valid for a limited time (usually one week). These types of certificates are not pre-generated for future validity periods like pseudonym certificates and must be requested on a week-to-week basis. Deployment agencies need to have mechanisms in place to allow RSUs to connect to the SCMS on at least a weekly basis in order to request and download new certificates. It should be noted that the overlap period for certificate renewal must be taken into consideration.

- **Design 11: Consider when RSU applications certificates will expire.** The validity period for RSU application certificates is generally one week, which required RSUs to contact the SCMS on a weekly basis. Some entities have equipment installed in the field that does not have access to the internet – making it more difficult to support certificate refresh. It is important to consider how many devices will be installed in locations without cellular connection or access to backhaul. Another consideration is whether the RSUs can directly communicate with the SCMS, or if these communications must be proxied through the TMC. The agency security requirements will need to be considered when planning for the RSU (and OBU) access to the SCMS.

- **Design 12: Consider where connected vehicle messages will be signed – at the RSU, TMC, or by a Third Party.** The New York City DOT CV Pilot Site is taking an approach to centrally sign some of the messages (e.g., MAP and TIM) at the TMC while the THEA CV Pilot Site is signing all messages at the

RSU. Originally, the CV Pilot Sites considered the option of developing separate security profiles, but it was later determined that it would be easier to develop a single MAP Security Profile that both sites could use. The RSU specification used did not support the remote signing of certificates. As a result, this was addressed in NTCIP 1202 version 3. New York City had to work with their RSU vendor to develop a temporary approach while the standards process continues. The approach used by New York City DOT is to assign a separate block (index above 100) to indicate a pre-signed message from the TMC. Users of CV Pilot Security Profiles may find it difficult to understand what the CV Pilot sites did because this was not addressed in the current development of the new standard NTCIP 1218: Object Definitions for Roadside Unit Standard (RSU).

- **Design 13: Ensure that agency staff or device vendors can support enrollment/bootstrapping.** Based on CV Pilot experiences from all three sites, it is recommended that agencies consider enrolling the devices themselves into the SCMS or having their connected vehicle device vendor conduct the enrollment/bootstrapping process. Both approaches are viable options. For the New York City CV Pilot, the device vendor enrolled the devices. Once devices came off the assembly line, they were ready for initializing. The vendor was able to enroll the devices before they were shipped. The Wyoming DOT conducted bootstrapping for some of their devices and had their vendor conduct enrollment for the other set of devices they deployed. While either approach can be used, agencies should consider the additional resources that may be needed by agency staff to enroll devices. If Agencies may want to work with their device vendors to understand if they have experience enrolling devices with an SCMS and include appropriate requirements in the device vendors' contracts to enroll the devices with their SCMS. Upon enrollment, the vendor will need to acquire operating certificates for factory testing and "burn-in"; these certificates will probably have expired by the time the devices are received and installed, thus, the "live" connection to the SCMS will be needed before the RSU will start normal operation.

Over-the-Air (OTA) Considerations

- **Design 14: Leverage Over-the-Air (OTA) updates for software/firmware patches and other updates.** Over-the-air (OTA) updates allow software and firmware updates to be rolled out to a connected vehicle remotely and eliminates the need to require a technician to physically install them in the vehicle. Such implementation is expected to be a game-changer for future CV deployers' vehicle fleet management. Enabling OTA updates was particularly critical for all three CV Pilot sites' deployment concepts due to: (1) the number of vehicles involved in the projects, (2) the need to update software and application parameters during the operational phase, and (3) many of the Pilot participant vehicles (e.g., taxis, buses, semi-trucks) have schedule and operational constraints that restrict them from coming into the maintenance shop for manual software updates. The sites thus performed extensive research, design, and testing of their individual OTA mechanisms to accommodate these needs.

- **Design 15: Recognize that while OTA updates provide opportunities, it is not without challenges.** For example, it may be difficult for a vehicle OBU to download 100 megabytes of data over a 1.5-megabyte channel where the vehicle is only within a range of the RSU for a few seconds. The THEA CV Pilot calculated the length of time needed for OBUs to download firmware updates and realized the average OBU might not be within reach of the existing RSUs long enough for successful download. As a result, the THEA CV Pilot added RSUs for over-the-air updates. The New York CV

Pilot ended up installing two RSUs at the airport taxi-holding lot. Each RSU was configured to either download or upload via multi-channel, dual-radio mechanism. RSUs would be uploading OTA majority of the time based on OBUs uploading their logs while their download will be infrequent during the initial part of the deployment phase. The New York City CV Pilot found that the OTA update process (download) for a 20 MB file takes from 2-8 minutes and has strategically placed the RSUs to optimize the probability that they will be within range of an RSU with the download service. It was also discovered that the OBUs did not retain their accumulated downloads through an ignition cycle – hence, although they will accumulate the download packets from multiple RSUs as they travel through the network, they must collect the entire image during one ignition cycle. It is recommended that others require that the images be accumulated from multiple RSUs and that accumulation continue through ignition cycles. It was also discovered that the download operation could not be performed as intended – because of limitations with the RSU's use of continuous and alternating channels within the same device.

Other Design Considerations

- **Design 16: Ensure that RSUs have sufficient computing power.** To support SCMS functionality, connected vehicle devices require processing signatures and validations of certificates. Early deployers need to ensure that their device hardware can support the load to handle the number of signatures and validations that need to be processed every tenth of a second (the rate at which BSMs are broadcast). Deployers should have a good understanding of the load requirements on their connected vehicle devices and ensure that their hardware is not under-powered. Understanding the load requirement becomes particularly important when additional functions such as BSM zone processing, OTA uploading, and OTA downloading are included in the device operation. The Wyoming CV Pilot did encounter problems with computing power from their vendors. They were able to address any challenges by optimizing their code in the RSU. Since code base since could not change CPU libraries for signing/verification. As a result, the team experienced challenges when there were large batches of TIMs in a queue. It should be noted that a full security implementation has serious impact on processing – and may impact what can be done with the devices. Deployers need to understand that the RSU can be a dumb radio, or it can do some pre-processing. Deployers need to be clear what they are asking the device to do.

- **Design 17: Augment connected vehicle solutions with more traditional ITS technologies where necessary.** For some use cases and specific applications, traditional ITS devices can be highly useful in supporting connected vehicle applications. For example, in the case of pedestrian detection for including the pedestrian in crosswalk warning in the SPaT message – the New York City CV Pilot used traditional ITS video technology to detect pedestrians in the cross walk. The THEA CV Pilot also deployed traditional ITS devices as part of their project – including cameras to determine queue length, thermal cameras for detecting wrong way drivers, and lidar to detect pedestrians. These devices were deployment to augment the connected vehicle technologies.

- **Design 18: Design RSUs to continue broadcasting through jamming activities.** The New York City CV Pilot observed GPS jamming activity that prevented the RSU from operating and broadcasting connected vehicle messages. Jamming devices include radio frequency transmitters that intentionally block, jam, or interfere with lawful communications, such as cell phone calls, text messages, GPS systems, and Wi-Fi networks. To mitigate the impacts, deployers should ensure that

the RSU has a feature that allows it to continue broadcasting for a short period of time if a GPS jammer drives by its location.

- **Design 19: Secure a significant amount of time to review design documentation.** Reviews, updates, and discussion with vendors on System Design Documents (SDDs) and System Architecture Documents (SADs) take a significant amount of time. Time and effort are needed to nail down details about algorithms and integration points for wireless communication, OBUs, and RSUs. Since emerging technologies may not be well defined or tested, documentation is critical to fall back on to ensure vendors deliver products that meet user needs. A general design meeting with all of the vendors (RSU, OBU, TMC, Traffic Controller) and the agency and system manager. Such an open session makes sure that all parties understand their roles, contacts, and it is an opportunity for everyone to see the overall end to end design, requirements, and deal with such issues as network connectivity, interfaces, integration and testing program and security.
- **Design 20: Include extensibility requirements for "future proofing".** Beyond the USDOT RSU Requirements Specification v 4.1, RSU requirements developed in 2015 added all wireless technologies of OEM cars at the time and software-controlled radios for remote updates. For example, a spare slot was later used to add a C-V2X radio without need to replace the RSU.
- **Design 21: Coprocessors or another secondary processing unit is not needed and creates security holes.** Based on THEA CV Pilot experiences, multiple concurrent applications run within the RSU tamper-resistant housing, with messages signed using security keys stored in a hack-proof hardware security module rather than external co-processor with unknown security measures. The co-processors or another secondary processing unit are not needed and creates a single point of failure when plugged into the signal controller, whereas the RSUs and the signal controllers operate independently.

Design-Related Resources

The following are documents that provide additional information related to design lessons learned and best practices:

- New York CV Pilot: Application Design Stage Webinar (June 26, 2018): https://www.its.dot.gov/pilots/pdf/New York City _AppDev.pdf and https://itsa.adobeconnect.com/_a932559885/p3vlfyj9e8ko/?proto=true
- New York CV Pilot: System Design Document: Document Forthcoming
- THEA CV Pilot: Application Design Stage Webinar (January 19, 2018): https://www.its.dot.gov/pilots/pdf/CVP_SiteAppWebinarTHEA_Final.pdf and https://itsa.adobeconnect.com/_a932559885/p3dxm9ox8zml/?proto=true
- THEA CV Pilot: System Design Document: Document Forthcoming
- Wyoming CV Pilot: FHWA-JPO-17-468: https://rosap.ntl.bts.gov/view/dot/36241
- Wyoming CV Pilot: System Design Webinar (September 13, 2017): https://www.its.dot.gov/pilots/pdf/CVP_WYDOTSystemDesign_Webinar.pdf and https://itsa.adobeconnect.com/_a932559885/pwb8z0kj1h97/?proto=true

Section 4: RSU Installation Lessons Learned and Best Practices

This section documents lessons learned and best practices for the installation of RSUs.

General Installation Considerations

- **Installation 01: Develop installation checklists and procedures.** Instruct the installers not to leave the RSU installation site until thorough verification of the installation checklist and procedure and end to end connectivity is confirmed. After RSU installation, not all cables were found to be connected to the correct ports. This prevented remote monitoring of the installed RSUs using software and warranted a follow-up visit to manually check and reconnect the cables to their correct ports. Add to installation guide/procedure and follow up during and after installation.
- **Installation 02: Consider the location of existing ITS devices and line of sight for RSU antennas when selecting sites for the installation of RSUs.** Wherever feasible, CV equipment should be collocated at closed-circuit television (CCTV), dynamic message sign (DMS) or traffic signal locations sites to take advantage of the existing roadside infrastructure, power, and communications equipment. RSU mounting locations should also be optimized to achieve clear line of sight free of radio frequency (RF) signal path interference from trees, bridges, overpasses, and other structures. In New York City, many signal poles and mast arms lay behind the building face line, therefore limiting the line-of-site. Field inventories identified 15% of the installations would require additional infrastructure changes (e.g. additional communications gear, new mast/luminaire arms, controller relocation) to place the RSU antenna with adequate line-of-site.
- **Installation 03: Optimize RSU installations to prevent damage to RSU's antennas and improve RF propagation.** Site visits to the installed RSUs confirmed that several RSU antennas had been damaged and required adjustments. Generate installation guide for ensuring proper installation of RSUs on mast arms. In New York City, this included a vertical mount post to position the RSU above signal heads.
- **Installation 04: Verify optimal RSU height and resolve discrepancies in RSU elevation.** Ensure that the RSU is installed at an optimal height for applications to provided DSRC coverage and GPS location. The CV Pilot sites determined the optimal height using a sniffer. In addition to finding an optimal height for coverage, make sure the height of the RSU to prevent destruction of the equipment. The New York City CVP found that attaching the RSU on vertical mount post to position the RSU above the signal prevented damage to the hardware. In order to eliminate discrepancies between the measured elevation of the RSU using LiDAR and field-measurements, measure the heights more than once using each method. This then allows you to only configure the WSA once.
- **Installation 05: Ensure that RSUs are properly grounded.** During one year of continuous testing, the THEA Pilot found that four of the forty-four RSUs were not communicating with the Master server. After a series of investigations, THEA concluded that some RSUs were not grounded properly and that lightning strikes were causing damage to the RSUs. Each RSU was found to be installed and bonded to the mast arms correctly according to the vendor installation instructions. Lightning damage from direct hits to antennas or to the RSU itself was ruled out, as no damage to any electronic subassemblies attached to exposed antennas was observed. Next, the metal structures supporting the RSUs as well as nearby metal structures, such as poles, were examined. Some were

found to be bonded to the ground, while some were not. Based on the analysis, the investigation concluded the root cause to be lightning strikes to ungrounded metal structures where the arc introduces a voltage surge entering the RSU at the Ethernet connector. The Ethernet connector is attached directly to the PoE Splitter electronic subassembly mounted inside the RSU. When damaged, the PoE Splitter ceases communications to the Master Server, which initially reported that condition. Upon realizing this, THEA replaced the PoE splitter for all four RSUs – resulting in the RSUs returning to normal functionality again. The figure below graphically depicts the issue. Cloud-to-ground lightning strikes seek the path of least resistance (i.e., the ground connection on each structure). When grounded (no green "X"), the strike is contained. When left ungrounded as shown by the green "X", the next least path of resistance to earth ground is through 120VAC servicing the PoE Injector, continuing through the PoE Splitter of the RSU while seeking the ground of the RSU. That path of least resistance from the ungrounded structure through the RSU is shown as the two red arrows of the figure, likely an air-gap arc shown.

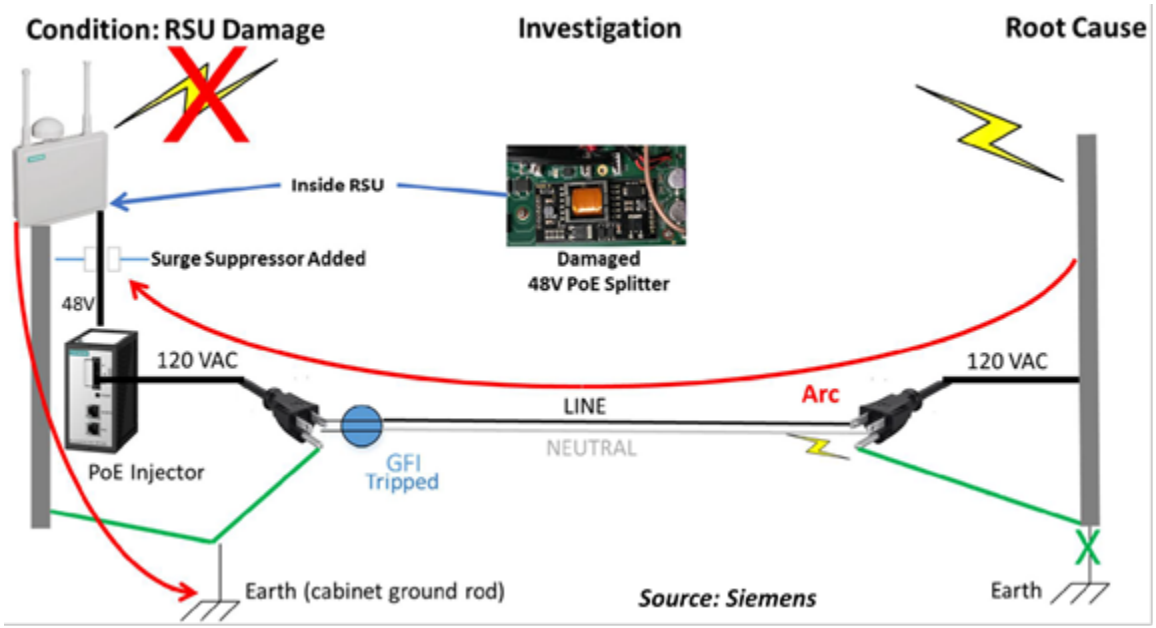

Figure 3. Depiction of THEA's Issue and Solution for Grounding an RSU.

Installation 06: Short-haul Wireless connections may be needed to bridge the gap between the RSU and the cabinet. When installing RSUs, deployers may encounter situations where conduit may not be able to run from the cabinet to the RSU. For deployments in New York City, the team experienced that due to intersection configurations, approximately 15% of RSU locations could not support a conduit run from the cabinet to the RSU. As a result, installers had to use short-haul wireless ethernet connections communications to the RSU to serve as a bridge to the cabinet.

Installation 07: Signage on structures may disrupt RSU antennas. When installing RSUs on structures, installers should be mindful that other signs and devices on the structure may impact the RSU. The New York City CV Pilot team experienced RSU failures when high winds whipped around signage on the pole, taking out RSU antennas.

Installation Timing/Scheduling Considerations

- **Installation 08: Start the permitting process early.** To prevent delays in the installation of hardware into existing infrastructure, begin the permitting process early. In many cases, it takes a while to get permission to add the RSUs to existing infrastructure. The permit process for connected vehicle devices will likely be similar to permit process for other ITS devices (e.g., CCTV cameras). both conventional devices and connected vehicle devices require permits for electrical, conduits, etc. While there is nothing unique to permitting for connected vehicles, agencies should consider the timing a process to obtain permits to install devices along the roadside.

- **Installation 9: Conduct site visits and account for a slower rate of installation of RSUs than OBUs, as they require dispatch crews.** To ensure that the proper equipment is used, site visits where RSUs will be installed should take place early on. When installing RSUs, there is always the potential that additional hardware may be needed. For the New York City pilot, the RSU installations were performed by New York City DOT field crews at a rate of about two per day per crew, a slower rate than what the New York City CV Pilot team had anticipated. The installation consisted of installing the surge suppressor on the ethernet to the RSU, adding the PoE inserter, bolting on the RSU, installing the ethernet through the pole and mast arm to the bottom of the RSU – and finally powering up the units and letting the system configure and start operation. Configuring the RSU is currently a manual process and prone to errors, however that process will eventually be automated and managed by the TMC so that it will be truly plug-and-play.

Other Installation Considerations

- **Installation 10: Ensure that RSU information from the asset management system is readily available on the RSU for device management and tracking.** To ensure information is included in the asset management system, the installer needs to enter inventory information including ownership (DOT property), type, model, year, and contact information for returning the RSU in case it is lost. The installer should be required to enter device information into the asset management system, print out the label, and put it on the RSU.

Installation-Related Resources

The following are documents that provide additional information related to installation lessons learned and best practices:

- New York CV Pilot: FHWA-JPO-17-455, https://rosap.ntl.bts.gov/view/dot/36389
- New York CV Pilot: Device Acquisition and Installation Experiences Webinar (July 30, 2018): https://www.its.dot.gov/pilots/pdf/New York City _CVP_SiteAcquisitionInstallation.pdf, https://itsa.adobeconnect.com/_a932559885/pkdk4gxzgjcu/?proto=true and https://www.its.dot.gov/pilots/New York City _acquisition_qa.htm
- THEA CV Pilot: FHWA-JPO-17-463, https://rosap.ntl.bts.gov/view/dot/36240
- THEA CV Pilot: Device Acquisition and Installation Experiences Webinar (August 7, 2018): https://www.its.dot.gov/pilots/pdf/CVP_Acquisition_InstallationWebinarTHEA.pdf, https://itsa.adobeconnect.com/_a932559885/pdymo99buz1e/?proto=true and https://www.its.dot.gov/pilots/thea_device_qa.htm
- Wyoming CV Pilot: FHWA-JPO-17-471, https://rosap.ntl.bts.gov/view/dot/35425

- Wyoming CV Pilot: Device Acquisition and Installation Experiences Webinar (July 23, 2018): https://www.its.dot.gov/pilots/pdf/WYDOT_CVP_Acquisition.pdf, https://itsa.adobeconnect.com/_a932559885/ppm3ozwdeknj/?proto=true and https://www.its.dot.gov/pilots/wydot_installation_qa.htm

Section 5: RSU Testing Lessons Learned and Best Practices

This section documents lessons learned and best practices for the testing of RSUs.

Overarching Testing Considerations

- **Testing 01: Ensure detailed testing is conducted for RSU software and hardware.** Connected vehicle software are immature. As such, it is important to account for detailed testing of all software, and even the hardware. For mature, existing applications, agencies should consider purchasing proof of concept devices to begin testing early in the process and notify and work with vendors to address shortcomings. If new applications are being developed, it will be difficult to prototype and test. As with any similar device, it is important that the testing include the "edge" conditions and "corner cases" – to make sure that the device does not take inappropriate action when confronted with such situations. Testing of the RSU should include interference between RSUs, flooding with many BSMs, and various error conditions such as too large MAP messages. Testing should also make sure that the RSU is not transmitting faulty packets; checksum of zero is not allowed for IPv6.

- **Testing 02: Ensure rigorous requirements verification and acceptance testing.** Systematic acceptance testing and requirements verifications should be performed throughout development, integration, installation, and deployment. Systems readiness (at each level of development and integration) should be measured by completion and internal approval of:

    - Test cases and procedures
    - Requirements verification
    - Passing of acceptance test
    - Test results report

- **Testing 03: Conduct testing early with actual infrastructure.** Conduct testing early with real-life, actual infrastructure to verify end-to-end system/application performance (over-the-air updates, data management, security, etc.). New development efforts such as over-the-air updates and connected vehicle security need to be piloted/tested early in the program. Actual infrastructure should include multiple devices as many issues are not immediately visible with one or two RSUs but become evident only when 8-10 are within the same area. In addition, deployers should monitor longer term operation. Testing for throughput should be several days and it should be subjected to interference conditions, power cycles, and GPS issues to see that it reacts properly.

- **Testing 04: Complete testing of individual components of the system prior to system-level testing.** Testing the individual components and verifying the messages coming in and out of each unit provides a better understanding of the failures in the system, if any arise during use case testing. Define procedures for testing individual components prior to those for system-level testing. It is important to test with the traffic controller and proper MAP messages and with security enabled. Configuring the RSU can be complex and it is important that the agency understand how to configure the traffic controller and the RSU for compatible and secure operation.

- **Testing 05: Rigorous testing will likely be needed before devices can be ready for operations.** To ensure the safe operation of connected vehicle technologies, the CV Pilot sites conducted rigorous

testing – including an Operational Readiness Test – prior to the technologies becoming operational. The purpose of this rigorous testing was to ensure that devices operated safely and performed in accordance to the requirements. For Example, New York City testing included:

  - Validating data collection (travel time and RF levels)
  - Configuration of operation
  - Functional SPaT, MAP and TIM
  - Operational Stability – Failsafe recovery
  - Security support
  - RF receiver and transmitter
  - OTA – Uploading Tests
  - OTA – Downloading Tests
  - Startup-shutdown – Power interruption
  - Time management
  - Routine Environmental, Shock, and Vibration Tests

- **Testing 06: Test for security relating to communication.** To ensure secure communication, deployers should consider testing the following items for security vulnerabilities:

  - Traffic Management Center (TMC) to the Advanced Traffic Controller (ATC): DTLS, TLS, VPN
  - ATC to RSU: DTLS – SNMP v1
  - TMC to RSU: DTLS – SNMP v3
  - Encryption requirements (OBS software completion)
  - X.509 certificate management
  - Where the messages "signed" (1609.2) – RSU (SPaT), TMC (MAP, TIM)
  - Hardware Security Module (HSM) at TMC

- **Testing 07: Understand that testing for *Pilot* does not equal testing for *Scale*.** There can be gaps between testing and operating at scale. Examples are summarized below:

  - As data volumes increase (e.g., more BSMs are sent to devices), devices may not operate properly or as expected.
  - Agencies need to consider RSU's failing at scale (e.g., numerous deployed devices requiring updates) as this may require a large number of either hardware or firmware updates.
  - Technical challenges exist in ensuring a secure network—e.g., SCMS integration and firewall compatibility.
  - Consider that having a few RSUs and a few vehicles is very different than seeing 20-30 RSUs all broadcasting various WSAs and SPaT and MAP messages along with 100 vehicles within range. Several issues of overloading the OBU were discovered as the data logging and number of messages arriving for processing caused problems for the OBU.

- **Testing 08: Perform multiple/regression testing to verify that a previously tested system still performs the same way after changes were made in the field to another component.** Some fine tuning may make one part (one RSU type) of the system work, but this can result in other elements (other RSU types) failing. Make sure to test other parts of the system again after changes are made. Conduct multiple tests to show system stability.

- **Testing 09: Test the RSUs resiliency and ability to recover from failure.** Ensure that devices are able to recover from any failures during service and operate in fail-safe mode if needed. The device needs to be able to detect and handle faults and operate in fail-safe mode if needed. Make sure to test the device ability to recover from failure and resume OTA download/upload process. The THEA CV Pilot team learned that their system was able to withstand a weather event with power failure to the RSU as well as outage of the central system for several days. The OBUs accumulated data until the RSUs regained power within a few hours. The RSUs accumulated data from the OBUs until the central came back online. The central accumulated data from the RSUs until uploaded by the researchers without data loss. This would apply to a widespread emergency, the cars and OBUs still operate, for example emergency vehicles and transit. When testing devices, every "anomaly" counts; remember, it requires a crew and a bucket to replace and RSU. Deployers should also consider a mechanism to be able to remotely reset/reboot the RSU and to remotely update firmware and operating parameters.

- **Testing 10: Continually test systems and check their requirements.** Software and hardware might not be fully compliant with the requirements at the beginning of the development process. It is important to track closely their improvement, and make sure to test any updates against requirements.

- **Testing 11: Examine all possible root causes before power-cycle/reset/reboot of the device.** As part of device and network troubleshooting, devices were power cycled/reset/rebooted in order to minimize the down time. However, the determination of root causes and resolution/mitigation measures were not immediately considered. Log and monitor all possible root causes and resolution/mitigation measures for each device in the system. In some cases, if the vendor debug log is not downloaded before the next time the vehicle is used, it will be lost. The vendor should be required to describe ***why*** the unit failed – i.e. exactly what happened to cause it to fail. Simply rebooting is not a solution – the cause of the failure is still there.

Testing Location Considerations

- **Testing 12: Arrange a testing location that can accommodate the necessary test runs.** Testing should occur in a closed environment that is sufficiently large. A large, closed environment is needed to support safe testing of V2V and V2I safety applications. New York City DOT made available a test location within the Aqueduct Racetrack parking lot to demonstrate their connected vehicle applications. Through partnerships, WYDOT was able to perform testing on tracks owned by the Office of Emergency Management. THEA was able to close its Reversible Express Lanes for the testing and demonstration of their connected vehicle technology. The New York City CV Pilot team was also able to establish a test rack with 60 OBUs and a couple of RSUs for some of the testing which proved very valuable in troubleshooting OTA issues.

Tools Considerations for Testing

- **Testing 13: Leverage Radio Frequency (RF) tools to support testing.** It is important to obtain RF tools (interference detection, protocol analyzers, GPS repeaters, etc.) early for testing. Test Tools should be required from each vendor. The "Sniffer" or equivalent was the main device used by all of the pilots to evaluate operation and troubleshooting. A sniffer hardware designed to monitor

network traffic by examining data packets flowing through the air over radio frequencies. This device can be used to evaluate and verify the message content RSUs and OBUs are broadcasting.

- **Testing 14: If using licensed spectrum, consider purchasing equipment to detect potential interference from other users in the 5.9 GHz band that can affect operations.** Though the FCC originally allocated the 5.9 GHz band for DSRC-based ITS applications, in 2013 the FCC proposed allowing unlicensed devices to share the spectrum with primary users as long as they were not found to be interfering with the primary DSRC users. During the deployment period, THEA detected and tracked down an interference on their DSRC communication channels coming from a local amateur radio operator. While the ham radio could not receive DSRC radio messages due to the far lesser range of DSRC, THEA's DSRC radio would receive the ham radio messages, causing the DSRC radio to consider the channel "busy" and not "clear to send". The additional signal on THEA's channels impacted the performance of their equipment in terms of data exchange and back haul speed, with testing indicating a degradation in data uploads by up to 50%. Upon review of these findings, Florida Department of Transportation (acting as the enforcement agency) ordered the amateur radio operator to vacate the channel. Due to the scale of the New York City CV Pilot deployment, the New York City team invested in the purchase of sophisticated interference checking and RF spectrum analysis equipment. This equipment will allow them to locate and quantify field interference with GNSS and DSRC and to confirm the failures of the OBU and RSUs in the event of a suspected failure.

Other Testing Considerations

- **Testing 15: Test the OTA download and upload mechanisms before extensive installation of the OBUs and RSUs.** OTA download and upload were tested through several scenarios including stationary vehicles, moving vehicles in contact with single or multiple RSUs, and interrupted data connection. File sizes were varied to evaluate the expected application/media performance in consideration of the contact time between OBU and RSU that will vary by location. It was concluded that the New York City CV Pilot project's objectives for managing the vehicle fleet's firmware, configuration files, and data logs can be met at the proposed RSU support locations in the pilot area. The New York City CV Pilot team worked with the OBU and RSU vendors to conduct the OTA testing in Atlanta's test environment. They will use the test results for RSU installations under various operating scenarios for deployment throughout the New York City CV Pilot area.

- **Testing 16: Test for RSU Traveler Information Message (TIM) transmission range.** During testing, the Wyoming CV Pilot site encountered some range issues with sending TIMs to vehicles. It is important to test the range of RSU to OBU communication. It is recommended that agencies work with their vendor to test and verify configuration to ensure successful transmission range.

- **Testing 17: Ensure that RSUs will run 24/7/365 without problems.** The RSU should be just as reliable as a traffic controller. It is important to track the reliability of the devices by examining their system logs and monitoring their availability. Such Band-Aid solutions as rebooting daily/weekly is indicative of design flaws that need to be corrected

- **Testing 18: Ensure RSUs can collect and forward all participant data.** Test to ensure that RSUs can collect and forward all participant data. The THEA CV Pilot was able to show that the RSUs were able

to collect all BSMs, alerts and warnings from all participant vehicles and forward to the central. RSUs were able to process all incoming data from their connected vehicle system.

- **Testing 19: Ensure that Security is Considered from the Beginning and Testing is Conducted on a Secure System.** The CV Pilot Sites noted that they were surprised at how much adding security added complexity and impacted the overall system. Future deployers should not make the mistake to spend a huge amount of time validating a non-secured system and trying to add security at a later date. Security should be considered from the origin. Once security is added, it is hard to go backward.

Testing-Related Resources

- New York CV Pilot: https://www.its.dot.gov/pilots/pdf/New York City VP_SiteOperationalReadinessWebinar.pdf (March 11, 2019)
- THEA CV Pilot: Update at the Operational Readiness Milestone (March 11, 2019): https://www.its.dot.gov/pilots/pdf/THEA_Connected_Vehicle.pdf and https://connectdot.connectsolutions.com/puwudda264sx/?proto=true
- Wyoming CV Pilot: Update at the Operational Readiness Milestone (July 18, 2019): https://www.its.dot.gov/pilots/pdf/WYDOT_CV_SiteOperationalReadinessWebinar.pdf and https://itsa.adobeconnect.com/_a932559885/p7p1w7vnxrvl/?proto=true

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-20-804

U.S. Department of Transportation