# Connected Vehicle Pilot Deployment Program Phase 1

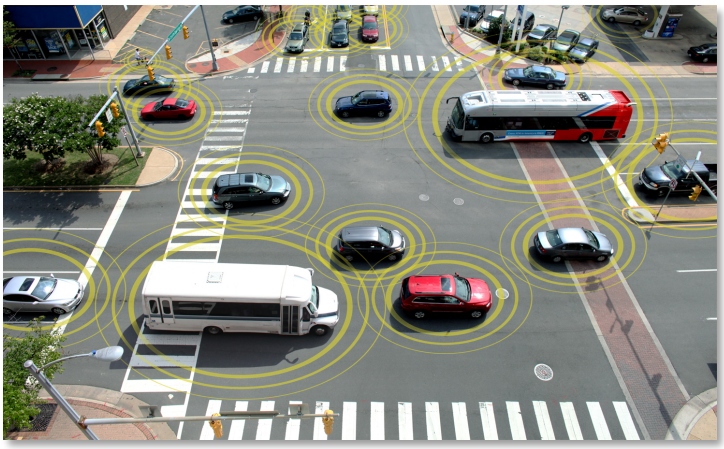
## Systems Requirements Specification (SyRS) – New York City

www.its.dot.gov/index.htm

**Final Report — September 11, 2017**

**Updated – August 5, 2021**

**Publication Number: FHWA-JPO-16-303**



U.S. Department of Transportation

Produced by Connected Vehicle Pilot Deployment Program Phase 1
New York City Department of Transportation
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

# Notice



---

Cover photo courtesy of ITS JPO Resources, Connected Vehicle Basics 2016

## Technical Report Documentation Page

| 1. Report No. | 2. Government Accession No. | 3. Recipient's Catalog No. |
|---|---|---|
| FHWA-JPO-16-303 | | |

| 4. Title and Subtitle | 5. Report Date |
|---|---|
| Connected Vehicle Pilot Deployment Program Phase 1, System Requirements Specification (SyRS) – New York City | August 4, 2021 |
| | 6. Performing Organization Code |

| 7. Author(s) | 8. Performing Organization Report No. |
|---|---|
| Steve Galgano, NYCDOT; Mohamad Talas, NYCDOT; David Benevelli, TransCore; Robert Rausch, TransCore; Samuel Sim, TransCore; Keir Opie, Cambridge Systematics; Mark Jensen, Cambridge Systematics; Chris Stanley, Battelle; Denny Stephens, Battelle; Doug Pape, Battelle | |

| 9. Performing Organization Name And Address | 10. Work Unit No. (TRAIS) |
|---|---|
| New York City Department of Transportation (NYCDOT)<br>Bureau of Traffic Operations<br>34-02 Queens Boulevard<br>Long Island City, NY 11101 | 11. Contract or Grant No.<br>DTFH6115C00036 |

| 12. Sponsoring Agency Name and Address | 13. Type of Report and Period Covered |
|---|---|
| U.S. Department of Transportation<br>ITS-Joint Program Office<br>1200 New Jersey Avenue, S.E.,<br>Washington, DC 20590 | Final SyRS |
| | 14. Sponsoring Agency Code<br>HOIT-1 |

**15. Supplementary Notes**
Program Manager: Kate Hartman
Contracting Officer's Representative (COR): Jonathan Walker

**16. Abstract**
This document describes the System Requirements Specification (SyRS) for the New York City Department of Transportation (NYC) Connected Vehicle Pilot Deployment (CVPD) Project. This SyRS describes the results of the definition of need, the operational concept, and system analysis tasks. It also conveys the requirements that are geared towards satisfying the needs of the users and stakeholders of the system. It is the second of several planning documents for the CVPD Program, Phase 1 project funded by the United States Department of Transportation (USDOT). Other planning documents, developed under this project phase, that influence this SyRS include the Concept of Operations (ConOps), Security Management Operational Concept, Performance Measurement and Evaluation Plan, Safety Management Plan, and Human Use Approval.

| 17. Key Words | 18. Distribution Statement |
|---|---|
| connected vehicles, DSRC, V2V, V2I, safety, system requirements, CV Pilots, development guide, New York City | |

| 19. Security Classif. (of this report) | 20. Security Classif. (of this page) | 21. No. of Pages | 22. Price |
|---|---|---|---|
| Unclassified | Unclassified | 177 | |

# Acknowledgements

The New York City Department of Transportation (NYCDOT) System Requirements Specification (SyRS) team thanks the participating fleet owners and stakeholders in the New York City (NYC) Connected Vehicle Pilot Deployment (CVPD) project. These organizations have provided information needed for establishing the user needs and requirements of the NYC CVPD system. Also, the team acknowledges the guidance and support from USDOT and Noblis during the SyRS Walkthrough sessions, which were instrumental in developing and refining the system requirements.

# Table of Contents

# List of Figures



# List of Tables

# Chapter 1. Introduction

This document describes the System Requirements Specification (SyRS) for the New York City Department of Transportation (NYC) Connected Vehicle Pilot Deployment (CVPD) Project. This SyRS describes the results of the definition of need, the operational concept, and system analysis tasks. It also conveys the requirements that are geared towards satisfying the needs of the users and stakeholders of the system.

It is the first of several planning documents for the CVPD Program, Phase 1 project funded by the United States Department of Transportation (USDOT). Other planning documents, developed under this project phase, that influence this SyRS include the Concept of Operations (ConOps), Security Management Operational Concept, Performance Measurement and Evaluation Plan, Safety Management Plan, and Human Use Approval.

Two other project phases are scheduled following the successful completion of Phase 1. Phase 2 consists of the design, deployment, and test activities occurring over a 20-month period. A maintain and operate period comprises Phase 3 of the project over an 18-month period.

The document is organized to meet the requirements of the USDOT System Engineering Process and IEEE 1233-1998 as required by the USDOT Broad Agency Announcement (BAA) dated January 30, 2015 amended.

## 1.1 System Purpose

The fundamental message of the New York City (NYC) Vision Zero initiative is that death and injury on City streets is not acceptable. These tragedies happen in every community within NYC, to families from every walk of life – from the Upper East Side to the Lower East Side; from Park Slope to Edenwald. They happen to people who drive and to those who bike, but overwhelmingly, the deadly toll is highest for pedestrians – especially children and seniors. The goal of Vision Zero is to eliminate traffic deaths by 2024. The NYC CVPD project will focus on safety improvements for both motorists and non-motorists. In particular, the crash risks increase during nighttime hours when vehicle speeds tend to be higher and it becomes more difficult for vehicle drivers to see pedestrians crossing the roadway.

As the safety statistics indicate, surface improvements on city streets alone will not mitigate the number of crashes, fatalities, and severe injuries long-term. While no “Silver Bullet” will end all crashes, multiple supplemental tools are needed that can work together to attain Vision Zero’s goal. The connected vehicle (CV) technology is one of these tools and it presents a systematic approach in alerting vehicles of unsafe roadway conditions and prevents collisions with other vehicles and pedestrians. It will provide numerous safety benefits that facilitate Vision Zero's goals and initiatives.

## 1.2 System Scope

NYC is implementing the CV technology as another tool in its quest for Vision Zero. It is anticipated that the CV technology will reduce the number of and severity of crashes in the deployment area. In addition to deploying the technology, New York City will assess its impacts and potential for attaining the Vision Zero goal of zero crashes/fatalities/injuries. Figure 1-1. NYC CVPD System Concept in Section 1.5, System Overview, provides a conceptual view of the system to be deployed. It also provides insight to whether a component exists or will be newly deployed within the project.

The NYC CVPD project is one of three initial CV deployment projects that establish a base for growing a nation-wide connected vehicle system. As such, its focus is on utilizing standards to build basic infrastructure in a manner that provides a foundation for future deployments of connected vehicle technology.

The NYC CVPD project provides a real demonstration and evaluation of the benefits of the CV technology in a dense urban environment. NYC has deployed a robust infrastructure with advanced traffic controllers (ATC), an advanced adaptive traffic signal control system which currently uses travel times as part of its operational algorithms, an aggressive maintenance program, and a ubiquitous high speed wireless network (NYCWiN). By deploying Aftermarket Safety Devices (ASD) and Roadside Units (RSU), our team can bring the benefits of the CV paradigm to NYC's Vision Zero initiative and provide the opportunity to evaluate the benefits with a significant number of vehicles that are regularly driving in the area.

This project will also provide the Federal Highway Administration (FHWA) the opportunity to showcase the benefits of CV technology without replacing the vehicle fleet – which is likely to be the situation for many years to come. At the same time, the NYC CVPD will be used to demonstrate the benefits to vulnerable road users who suffer the most from roadway fatalities in NYC.

In the ConOps, the system needs were developed for the following users: traffic manager, fleet owners, roadway users, and system manager. They are presented using two perspectives – the NYCDOT traffic management needs and the stakeholders (i.e. fleet owners, driver/operators) needs for deploying, maintaining, and operating connected vehicle technology to be installed on their vehicles. Other needs for operating and maintaining the infrastructure (i.e. core services) are also identified. Each system need is identified with a unique number for tracing through the system development life cycle (SDLC). For each need, a set of system requirements are developed to provide the needed services for the users and stakeholders of the NYC CVPD.

The improvements provided by this project are summarized in the following list:

- Vehicle fleets equipped with ASDs for Dedicated Short Range Communications (DSRC).
- Initial intersections equipped with RSU for DSRC communications.
- Initial curves, entrance/exit ramps, and work zones equipped with RSUs.
- Fleet terminal facility areas equipped with RSU for DSRC communications.
- Significant deployment of CV safety applications.
- New applications for managing DSRC devices from over-the-air (OTA) updates to radio frequency link monitoring.

The original scope of NYC CV Pilot deployment project included deploying ASDs to 10,000 vehicles, RSUs at 300 locations, and PIDs for 100 visually-impaired pedestrian users. However, many of the initial stakeholder organizations that had expressed interest in the NYC CV pilot program did not continue their support. Hence, organizations such as TLC, taxi fleets, UPS, and DSNY ended up deciding not to participate. MTA allowed installation in eleven (11) of its buses, but ultimately it also chose to discontinue allowing further ASD installations in its buses.

This led to NYCDOT choosing NYC or DCAS fleets for partnering with other agencies to bring in more vehicles for installation. Therefore, the total number of ASD deployments became 3,000 vehicles while the number of RSU deployments increased to 450. In addition, the pedestrian application for the PID to be used by visually-impaired pedestrians encountered many issues that led to delays as well. The PID deployment number was also decreased from 100 devices to 10 prototype PIDs to be used for testing and evaluation of the technology.

Also, procuring turnkey devices proved to be challenging. This led to delays in release, testing, and validation of prototype and production devices. The amount of time and effort expended into procurement, testing, and validation has been well above the original expectations made during planning stages of the NYC CV pilot project. Additional details can be found in the As-Built Addendum section at the end of this document.

## 1.3 Definitions, Acronyms, and Abbreviations

Table 1-1 defines selected project-specific terms used throughout this System Requirements Specification (SyRS) document.

**Table 1-1. Glossary of Terms**

| Term | Definition |
|---|---|
| Access Control | Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories. |
| Adjacent (A) | Data that is hyper local (relevant to a geographic area within ~1 minute travel distance) |
| Adjacent (A) | Data that is hyper local (relevant to a geographic area within ~1 minute travel distance) |
| Administrator | These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed. |
| Aggregation | The process of combining data elements of similar format into a single data element that is a statistical representation of the original elements. |
| Analysis | The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other. |
| Anonymity | Lacking individuality, distinction, and “recognizability” within message exchanges. |

| Term | Definition |
|---|---|
| Anonymous Certificate | A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority. |
| APDU | Application Protocol Data Unit. This is a defined data structure that is transferred at a peer level between two applications. |
| Application | One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task. |
| Application User | A user who interfaces with Application Layer software for a desired function or feature. |
| Assumption | A judgment about unknown factors and the future which is made in analyzing alternative courses of action. |
| Authenticate | The process of ensuring that an APDU originated from a source identified within the message |
| Authenticate-ability | The ability of the receiver of information to authenticate the sender's identity or trustworthiness to send data within the domain. If required, this can be accomplished by verifying the incoming message has been digitally 'signed' by the sender. |
| Authentication | The process of determining the identity of a user that is attempting to access a network. |
| Authenticity | The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source. |
| Authorization | The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service. |
| Available | Ready or able to be used |
| Backup | The ability of one System Element replacing another System Element's functionality upon the failure of that System Element. |
| Bad Actor | A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope. |
| Boundaries | The area of management and control for a System or Object. It could be by latitude/longitude or by county or by regional jurisdictions. |
| Broadcast | A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog. |
| Cardinality | The characterization of the relationship between the number of sender(s) and receiver(s) of a data exchange. (e.g. broadcast (one-to-many) unicast (one to one)) |

| Term | Definition |
|---|---|
| Center | An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of this ConOps Specification these are considered the same. |
| Concept of Operations (ConOps) | A user-oriented document that describes a system's operational characteristics from the end user's viewpoint. |
| Confidentiality | The property of being unable to read PDU contents by any listener that is not the intended receiver |
| Configurable Parameter | Non-static data that can be adjustable and updated when needed. |
| Configuration | Data that is used to customize the operational environment for a System Element or System User, or the System as a whole |
| Configure | The process of selecting from a set of option(s) or alternative values in order to create a specific operational environment. |
| Constraint | An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors. |
| Continental (C) | Data that is continental in scope. |
| Contract | In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project. |
| Control | To exercise influence over. |
| Coverage Area | A geographic jurisdiction within which the System provides services. |
| Cyber Address | The cyber or network address of a Unified Implementation of the Reference Architecture object. |
| Data Consumer | A user or system that is receiving or using data from another user or system.<br>Any Unified Implementation of the Reference Architecture object that registers with and subsequently requests and receives delivery of data from a data warehouse. |
| Data Provider | Any Unified Implementation of the Reference Architecture object that registers with and subsequently deposits data into a data warehouse<br>A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data. |
| Data Warehouse | A data storage facility that supports the input (deposit) and retrieval (delivery) of clearly defined data objects. This can be design and implemented in a variety of ways, including publish/subscribe and a traditional query based database. |
| Decrypt | To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access. See Encryption. |
| Deployment Benefits | This term refers to the measures of effectiveness used by the NYCDOT and the Independent Evaluator on a periodic basis to assess the benefits realized from the utilization of connected vehicle technology and applications within the project's deployment areas. |

| Term | Definition |
|---|---|
| Digital Certificate or Signature | A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute website - www.sans.org. |
| DNS (Domain Name System) | The internet protocol for mapping host names, domain names, and aliases to IP addresses. |
| Encryption | Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key. |
| End-User | The ultimate user of a product or service, especially of a computer system, application, or network. |
| Environment | The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it. |
| Extensibility | The ability to add or modify functionality or features with little or no design changes. |
| Field | These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSU and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure. |
| Forwarding | The process of forward sending data onto another entity (system user) without modifying or storing the data for any substantial length of time. |
| Functionality | The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product. |
| Geo-Fence | An electronic set of geo reference points that form a bounded geographic region. |
| Geo-Referencing | The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space. |
| Hardware | Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners. |
| Historic (H) | Transient Data that is historical (relevant at the time of reporting for an indefinite interval). |
| Identity Certificate | A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. |

| Term | Definition |
|---|---|
| Integrity | To maintain a system that is secure, complete, and conforming to an acceptable conduct without being vulnerable and corruptible.<br>The property of being certain that a message's contents are the same at the receiver as at the sender. |
| Interconnect | The communications link between two architectural objects. |
| Internet | An interconnected system of networks that connects computers around the world via the TCP/IP protocol. |
| Issuance | For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA).<br>For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA).<br>Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms. |
| Jurisdictional Scope | The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised. |
| Link | A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port. |
| Local (L) | Data that is local (relevant to a geographic area within 10 minute travel distance) |
| Logical Security | Safeguards that include user identification and password access, authentication, access rights and authority levels. |
| Misbehaving User | A user who exhibits misbehavior. |
| Misbehavior | The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages. etc.; either purposeful or unintended |
| Misbehavior Information | Includes Misbehavior Reports from System Users, as well as other improper System User acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages, and other inappropriate System User behavior. |
| Misbehavior Report | Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior. |
| Mobile | These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information |
| National (N) | Data that is national in scope. |

| Term | Definition |
|---|---|
| Non-repudiation | The property whereby a PDU is constructed in such a way that the PDU sender cannot effectively deny having been the sender of that PDU; and the PDU receiver cannot effectively deny having received a particular PDU. |
| Now (N) | Transient Data that is hyper current (relevant at the time of reporting for applications that require sub-second response). |
| On-Board Equipment (OBE) | Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment. |
| Operational Data Environment | The ODE consist of several different USDOT developed smart data routers brokering processed data between various data sources, including the Unified Implementation of the Reference Architecture, and a variety of data users (e.g. RDE, TMCs). As a smart data router, the ODE routes data from disparate data sources to software applications (including CV applications) that have placed data subscription requests to the ODE. The ODE also performs necessary security / credential checks and, as needed, data valuation, aggregation, integration and propagation functions. |
| Operators | These are the day-to-day users of the System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system. |
| Permission | Authorization granted to do something. From the System's perspective, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the System. |
| Persistent Connection | A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection. |
| Physical Security | Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. This can range from simply a locked door to badge entry. with armed security guards |
| Priority | A rank order of status, activities, or tasks. Priority is particularly important when resources are limited. |
| Privacy | The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively. |
| Process | A series of actions, changes, or functions bringing about a result. |
| Protocol Data Unit (PDU) | A defined data structure that is transferred at a peer level between corresponding software entities functioning at the same layer in the OSI standard model which are operating on different computing platforms that are interconnected via communications media . |
| Public Key | In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI). |
| Recent (R) | Transient Data that is current (relevant at the time of reporting for applications that do not require sub-second response). |

| Term | Definition |
|---|---|
| Regional (R) | Data that is regional (relevant to a geographic area within ~30 minute travel distance) |
| Registry | A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc. |
| Reliability | Providing consistent and dependable system output or results. |
| Repackage Data | Data that is broken down for aggregation, parsing, or sampling. |
| Requirement | (A) A condition or capability needed by a user to solve a problem or achieve an objective. (B) A condition or capability that must be met or possessed by a system component to satisfy a contract, standard, specification, or other formally imposed document. (C) A documented representation of a condition or capability as in definition (A) or (B). (IEEE Std 610.12-1990) |
| Research Data Exchange | A web-based data resource provided by the USDOT ITS-JPO's Real-Time Data Capture and Management (DCM) program which collects, manages, and provides archived and real-time multi-source and multi-modal data to support the development and testing of ITS applications. |
| Scalability | The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign. |
| Scenario | A step-by-step description of a series of events that may occur concurrently or sequentially. |
| Secure Storage | Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off. |
| Secure Transmission | To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications. |
| Secure/Securely | Referring to storage, which consists of both logical and physical safeguards |
| Session-oriented Connection | A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection. |
| Software | Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software. |
| States | A distinct system setting in which the same user input will produce different results than it would in other settings. The System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby. |
| Static (S) | Data that is permanent (relevant at the time of reporting for an indefinite interval). |
| Status | Anomalies, actions, intermittent and other conditions used to inform the System Operator for reparation or maintenance. |
| Subsystem | An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses. |
| Synchronization | the act or results of occurrence or operating at the same time or rate |

| Term | Definition |
|---|---|
| System | A collection of interacting elements organized to accomplish a specified function or set of functions within a specified environment. Typically the System Elements within the System are operationally self- contained but are interconnected and collaborate to meet the needs of the System and its Users.<br>A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. |
| System Element | A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment.<br>An object and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system element includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses. |
| System Need | A capability that is identified and supported within the System to accomplish a specific goal or solve a problem |
| System Performance | This term refers to the measures of effectiveness used by NYCDOT traffic management operations staff on a periodic basis to manage the on-going operation of the system. |
| System Personnel | This represents the staff that operates and maintains the System. In addition to network managers and operations personnel, System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployment teams, and Testers. |
| System Requirements Specification (SyRS) | A structured collection of information that embodies the requirements of the system. |
| System User | System Users refers to Mobile, Field, and Center Systems. |
| Testers | These users verify the System's operation when any changes are made to its operating hardware or software. |
| Time | A measurable period during which an action, process or condition occurs. |
| Time Synchronization | Calibration adjustment of date, hour, minutes, and seconds for keeping the same time within a system. |
| Time-of-Day | Current hours, minutes, and seconds within a day. |
| Traceability | The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test. |
| Transition | A passage from one state, stage, subject, or place to another |
| Trust Credentials | A user's authentication information which determines permissions and/or allowed actions with a system and other users. |

| Term | Definition |
|---|---|
| Unicast | The sending of a message to a single network destination identified by a unique address. |
| User | An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions. |
| User Need | A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system. |
| Valid | When data values within a message are acceptable and logical (e.g., numbers fall within a range, numeric data are all digits). |
| Validate | To establish or confirm the correctness of the structure, format and/or contents of a data object. |

Table 1-2 defines selected project-specific acronyms used throughout this System Requirements Specification (SyRS) document.

**Table 1-2. Acronym List**

| Acronym / Abbreviation | Definition |
|---|---|
| 3G | Third Generation |
| 3P | Third Party |
| 4G | Fourth Generation |
| A | Adjacent |
| ACL | Access Control List |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| ASD | Aftermarket Safety Device |
| ASN.1 | Abstract Syntax Notation.1 |
| ASTC | Advanced Solid-state Traffic Controller (NYC standard traffic signal controller device) |
| ATC | Advance Traffic Controller (see ASTC) |
| ATIS | Advanced Traveler Information System |
| BAA | Basic Agency Agreement |
| BSM | Basic Safety Message |
| C | Continental |
| C2C | Center to Center |
| C2F | Center to Field |
| CA | Certificate Authority |
| CAMP | Crash Avoidance Metrics Partnership |
| CIA | Confidentiality/Integrity/Availability |
| ConOps | Concept of Operations |
| CRL | Certificate Revocation List |

| Acronym / Abbreviation | Definition |
|---|---|
| CV | Connected Vehicle |
| CVPD | Connected Vehicle Pilot Deployment |
| CVRIA | Connected Vehicle Reference Implementation Architecture |
| DCAS | Department of Citywide Administrative Services |
| DCM | Device Configuration Manager |
| DD | Data Distribution |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DSNY | New York City Department of Sanitation |
| DOT | Department of Transportation |
| DSRC | Dedicated Short Range Communications |
| EVSD | Enhance Vehicle Situation Data |
| Gbps | Gigabits per second |
| GHz | Gigahertz |
| GID | Geographic Intersection Description |
| GNSS | Global Navigation Satellite System |
| GPS | Global Positioning System |
| H | Historic |
| HMI | Human Machine Interface |
| HSM | Hardware Security Module |
| HTTPS | Hypertext Transfer Protocol (Secured) |
| I2V | Infrastructure to Vehicle |
| IEEE | Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| ISD | Intersection Situation Data |
| ITS | Intelligent Transportation System |
| JPO | Joint Program Office |
| KSI | Killed or Severally Injured |
| L | Local |
| MAP | Map Data Message (a DSRC message) |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MTA | Metropolitan Transportation Authority |
| N | Now (context: temporal data distribution) |
| N | National (context: geographical data distribution) |
| NHTSA | National Highway Traffic Safety Administration |
| NOC | Network Operations Center |

| Acronym / Abbreviation | Definition |
|---|---|
| NTP | Network Time Protocol |
| NYC | New York City |
| NYCDOT | New York City Department of Transportation |
| NYCWiN | New York City Wireless Network |
| O&M | Operations & Maintenance |
| OBD | On-board Diagnostics |
| OBE | On-Board Equipment |
| OCMC | Office of Construction Mitigation and Coordination |
| ODE | Operational Data Environment |
| OEM | Office of Emergency Management |
| OER | Office of Emergency Response |
| ORDS | Object Registration & Recovery Service |
| OS | Operating System |
| OST-R | Office of the Assistant Secretary of Transportation for Research and Technology |
| OTA | Over-the-Air |
| P2P | Peer-to-Peer |
| PDU | Protocol Data Unit |
| PID | Personal Information Device (e.g. SmartPhone) |
| PII | Personally Identifiable Information |
| PKI | Public Key Infrastructure |
| POC | Proof of Concept |
| R | Recent (context: time domain) |
| R | Regional (context: geographic domain) |
| RA | Registration Authority |
| RDE | Research Data Exchange |
| RF | Radio Frequency |
| RSA | Roadside Alert |
| RSE | Roadside Equipment |
| RSU | Roadside Unit |
| S | Static |
| SAE | Society of Automotive Engineers International |
| SCM | Security & Credential Management |
| SCMS | Security Credential Management System/Service |
| SDC | Situation Data Clearinghouse |
| SDLC | System Development Life Cycle |
| SDW | Situation Data Warehouse |
| SET-IT | System Engineering Tool – Intelligent Transportation |

| Acronym / Abbreviation | Definition |
|---|---|
| SM | Service Monitor |
| SMS | Service Monitor System |
| SPaT | Signal Phase and Timing (a DSRC message) |
| SPMD | Safety Pilot Model Deployment |
| SSL | Secure Sockets Layer |
| SyRS | System Requirements Specification |
| TAI | International Atomic Time (French: Temps atomique international) |
| TBD | To Be Determined |
| TCP | Transmission Control Protocol |
| TIC | <Region> Transportation Information Center |
| TLS | Transport Layer Security |
| TMC | Traffic Management Center |
| TPAC | Third Party Application Center |
| TSD | Traveler Situation Data |
| UDP | User Datagram Protocol |
| USDOT | United States Department of Transportation |
| UTC | Coordinated Universal Time (French: Temps universal coordonné) |
| V2I (I2V) | Vehicle-to-Infrastructure (Infrastructure-to-Vehicle) |
| V2V | Vehicle-to-Vehicle |
| VPN | Virtual Private Network |
| VRU | Vulnerable Road User |
| WAID | Wide Area Information Distributor |
| WAVE | Wireless Access in Vehicular Environments |
| Wi-Fi | Wireless Fidelity (short to mid-range wireless network) |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WSA | WAVE Service Advertisement |
| WSM | WAVE Short Messages |
| WSMP | WAVE Short Message Protocol |
| XML | eXtensible Markup Language |

## 1.4 References

Table 1-3 lists the references used to develop the concepts in this document. As some of the base standards referred to in the list are currently evolving, their identifiers have been temporarily highlighted to indicate that the version may change.

**Table 1-3. References**

| # | Document (Title, source, version, date, location) |
|---|---|
| 1 | *Initiatives - Vision Zero*, New York City Department of Transportation. http://www.nyc.gov/html/visionzero/pages/home/home.shtml |
| 2 | *Traffic Fatalities Fall in 2014, but Early Estimates Show 2015 Trending Higher*, National Highway Transportation Safety Administration (NHTSA). https://www.transportation.gov/briefing-room/traffic-fatalities-fall-2014-early-estimates-show-2015-trending-higher |
| 3 | *Borough Pedestrian Safety Action Plans*, New York City Department of Transportation. http://www.nyc.gov/html/dot/html/pedestrians/ped-safety-action-plan.shtml |
| 4 | *Vision Zero Action Plan*, New York City Department of Transportation. http://www.nyc.gov/html/visionzero/assets/downloads/pdf/nyc-vision-zero-action-plan.pdf |
| 5 | *Principles for a Connected Vehicle Environment*, U.S. Department of Transportation ITS Joint Program Office-HOIT, April 18, 2012 http://www.its.dot.gov/connected_vehicle/pdf/ConnectedVehiclePrinciples_final4-18-2012.pdf |
| 6 | *Connected Vehicle Reference Implementation Architecture Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. http://www.iteris.com/cvria/ |
| 7 | *Core System Concept of Operations*, US Department of Transportation, Research and Innovative Technology Administration, October24, 2011 http://www.its.dot.gov/docs/CoreSystemConOpsRevE2.pdf |
| 8 | *Core System Architecture Document*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011 http://www.its.dot.gov/docs/CoreSystemArchitectureDoc_revC.pdf |
| 9 | *Core System Requirements Specification*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011 http://www.its.dot.gov/docs/CoreSystem_SE_SyRS_RevF.pdf |
| 10 | *Core System Deployment Critical Risk Assessment Report*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011 http://www.its.dot.gov/docs/CoreSystem_RiskReport_RevB.pdf |
| 11 | *Core System Standards Recommendations*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011 http://www.its.dot.gov/docs/CoreSystem_StdsRecommendations_RevA.pdf |
| 12 | *Connected Vehicle Technology - Test Bed Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. http://www.its.dot.gov/testbed.htm |
| 13 | Safety Pilot Model Deployment – "5.9GHz DSRC Aftermarket Safety" Device Specification, US Department of Transportation, Research and Innovative Technology Administration, Version 3.1, March 22, 2014 |
| 14 | Safety Pilot Model Deployment – *"5.9GHz DSRC Vehicle Awareness Device" Specification*, US Department of Transportation, Research and Innovative Technology Administration, Version 3.5, December 12, 2011 http://www.its.dot.gov/safety_pilot/pdf/Vehicle_Awareness_Device_Specification-r3-5--20111202.pdf |
| 15 | *IEEE 1233 1998 – IEEE Guide for Developing System Requirements Specifications E-ISBN: 978-0-7381-1723-2* |

| # | Document (Title, source, version, date, location) |
|---|---|
| 16 | *1609.0-2013 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture* http://standards.ieee.org/findstds/standard/1609.0-2013.html |
| 17 | *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages* http://standards.ieee.org/findstds/standard/1609.2-2013.html |
| 18 | *1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, 2016* http://standards.ieee.org/findstds/standard/1609.3-2016.html |
| 19 | *1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation, 2016* http://standards.ieee.org/findstds/standard/1609.4-2016.html |
| 20 | *SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary*™, SAE International, January 19, 2016 http://standards.sae.org/j2735_201601/ |
| 21 | *SAE J3067 - Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods*, August 26, 2014 http://standards.sae.org/j3067_201408/ |
| 21 | *SAE J2945/1_201603 - Dedicated Short Range Communication (DSRC) Minimum Performance Requirements*™, March, 2016 http://www.sae.org/technical/standards/J2945/1_201603 |
| 22 | *USDOT Security Credential Management System*, US Department of Transportation, Research and Innovative Technology Administration, April 13, 2012. http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf |
| 23 | *USDOT's Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015-2019*, December, 2014 http://www.its.dot.gov/strategicplan.pdf |
| 24 | *ITU-R TF.460-4: Standard-frequency and time-signal emissions*, International Telecommunication Union. 1986. Annex I http://www.cl.cam.ac.uk/~mgk25/volatile/ITU-R-TF.460-4.pdf |
| 25 | *USDOT Broad Agency Announcement with New York City*, New York City Department of Transportation, September, 2015 |
| 26 | *DSRC Roadside Unit (RSU) Specifications Document*, USDOT, Version 4.0, April 15, 2014 http://www.its.dot.gov/testbed/PDF/USDOT_RSUSpecification4%200_Final.pdf |
| 27 | *Initiatives - Vision Zero*, New York City Department of Transportation. http://www.nyc.gov/html/visionzero/pages/home/home.shtml |
| 28 | U.S. DOT Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communication Technology (NHTSA 34-14; dated Aug. 18, 2014) |
| 29 | *Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications Concept of Operations Document*, Final Report —May 29, 2012 FHWA-JPO-13-058, www.its.dot.gov/index.htm |
| 30 | *Collision avoidance timing analysis of DSRC-based vehicles*, Accident Analysis and Prevention,2009, www.elsevier.com |
| 31 | *Security Credential Management System Proof–of–Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.0,* CAMP |

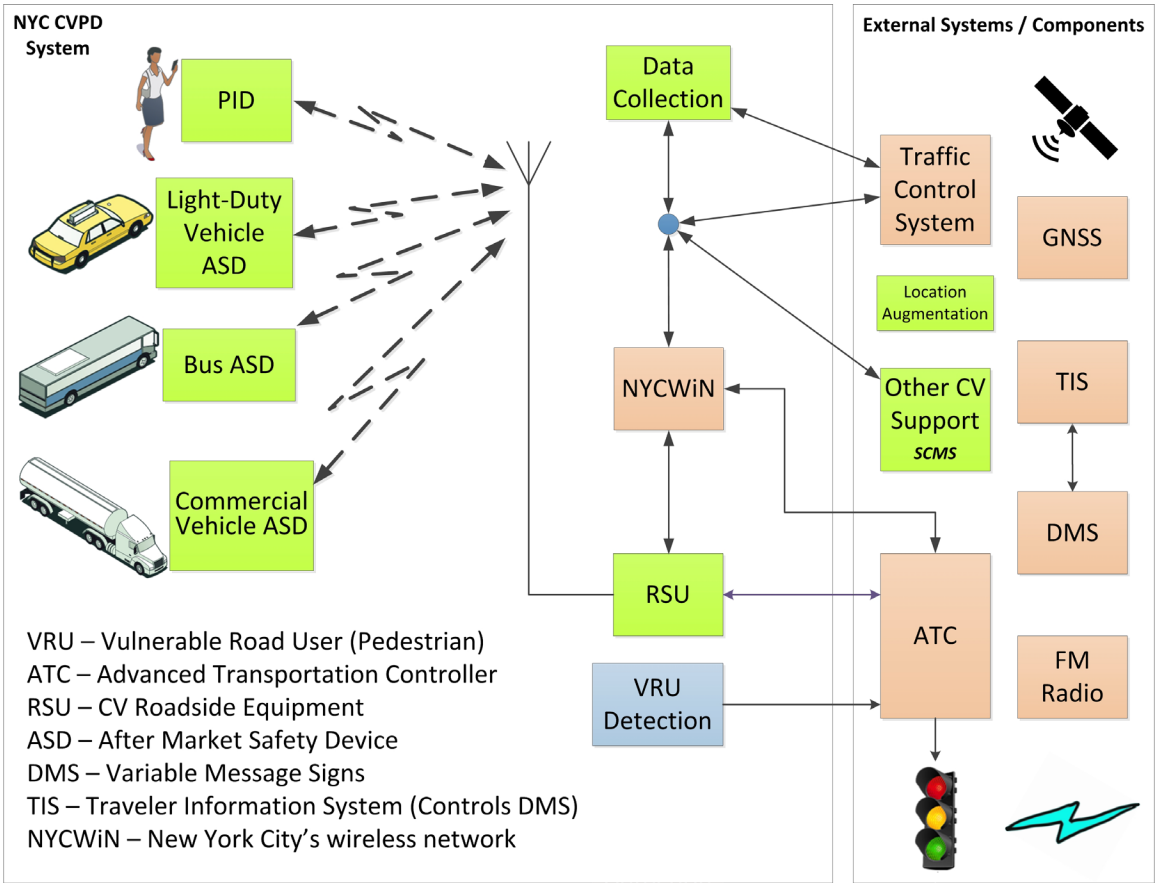
| # | Document (Title, source, version, date, location) |
|---|---|
| **32** | *Connected Vehicle Pilot Deployment Program Phase 1,Concept of Operations (ConOps) - New York* City, USDOT, FHWA-JPO-16-299, Final, 2016, |
| **33** | *Manual on Uniform Traffic Control Devices for Streets and Highways*, USDOT, 2009. http://mutcd.fhwa.dot.gov/pdfs/2009/pdf_index.htm |
| **34** | *Human Factors Design Guidelines for Advanced Traveler Information Systems (ATIS) and Commercial Vehicle Operations (CVO)*, USDOT, FHWA-RD-98-057. http://www.fhwa.dot.gov/publications/research/safety/98057/toc.cfmk |
| **35** | *In-Vehicle Display Icons and Other Information Elements: Volume 1*, USDOT, FHWA-RD-03-06503-065. http://www.fhwa.dot.gov/publications/research/safety/03065/index.cfm |
| **36** | *Crash Warning System Interfaces: Human Factors Insights and Lessons Learned*, National Highway Traffic Safety Administration, HS 810 697. http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2007/CWS_HF_Insights_Task_5_Final_Rpt.pdf |
| **37** | *Driver Vehicle Interface (DVI) Design Assistance for Advanced Technology Applications*, National Highway Traffic Safety Administration, (in press). (Battelle Final Report to Virginia Tech Transportation Institute and National Highway Traffic Safety Administration). |
| **38** | ISO 15628 "Road transport and traffic telematics -- Dedicated Short Range Communication (DSRC) -- DSRC application layer" (MIB Contents for DSRC Application Layer) |
| **39** | *ISO TS 19091 Intelligent transport systems — Cooperative ITS — Using V2I and I2V communications for applications related to signalized intersections, In Ballot* |
| **40** | *Vehicle Safety Communications 0 Applications (VSC-A), USDOT National Highway Safety Administration, DOT HS 811 492 Volumes A-D, September, 2011* |
| **41** | *VPN over TLS references* |
| **42** | *Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications -System Requirements Document, Final Report – July 18, 2012 FHWA-JPO-13-059*, www.its.dot.gov/index.htm |
| **43** | *SNMP v3 references* |
| **44** | *TCP/IP references* |
| **45** | *Network Time Protocol* Internet Engineering Task Force RFC 5905-5908 |

## 1.5 System Overview

This project brings New York City (NYC) another step ahead towards reaching the Vision Zero goal of eliminating the injuries and fatalities due to traffic crashes. The project's concept is simple - it introduces CV technology and communications into the NYC travel environment by equipping several large vehicle fleets with the technology and equips several areas with the corresponding connected vehicle infrastructure.

It is important to understand the implications of the connected vehicle technology deployment in New York City. A small portion of NYC roadway network will have connected vehicle infrastructure installed (i.e. 450 Roadside Unit (RSU) locations). Vehicle-to-Infrastructure (V2I) applications such as Red Light Violation Warning, Speed Compliance, and Curve Speed Compliance will support connected vehicles operating in these areas. However, the geographic reach of the connected vehicle technology is much broader. Vehicles equipped with connected vehicle technology (i.e. ASDs) will travel in this infrastructure equipped area *and throughout the City's transportation network*. Thus the connected vehicle technology that supports Vehicle-to-Vehicle (V2V) applications will function anywhere two equipped vehicles are within range of one another. Equipped vehicle encounters may occur on the surface streets, in the tunnels and bridges crossing the rivers, at the airports, and on the City's higher speed facilities such as the FDR Drive and the Long Island Expressway. The large fleet size means that there will be many opportunities for the connected vehicle technology to perform over a large geographic area and diverse roadway environments.

Figure 1-1 depicts the envisioned NYC CVPD system and the boundary between the internal system and the external systems and components that interface with the NYC CVPD environment. The ASDs, RSUs, PIDs, data collection/processing system, NYCWiN, and VRU detection system are in the NYC CVPD system. The TCS, ATC, GNSS, TIS, DMS, FM Radio, and other CV support systems including the SCMS are the external systems and components.




Source: NYCDOT 2016

**Figure 1-1. NYC CVPD System Concept[1]**

The existing system elements, critical to the operation of the pilot system, are illustrated with beige backgrounds. These existing elements include the traffic control system (TCS), traffic controller (ATC), Global Navigation Satellite System (GNSS), Traveler Information System (TIS), Dynamic Message Signs (DMS), FM radio, and supporting New York City's wireless network (NYCWiN) communications infrastructure. The new system elements which exist and will be reused, modified, or integrated into the NYC CVPD system contain green backgrounds. They comprise of the ASDs in light-duty vehicle, bus, and commercial vehicle, RSUs, PIDs, data collection/processing system, and other CV support systems including the Security Credential Management System (SCMS). The Vulnerable Road User (VRU) detection devices are shown with a blue background. They are relatively new and will be deployed to the system on a very limited basis.

NYC's initial system deployment is anticipated to be the largest CV technology deployment to date. It is anticipated that approximately 281 intersections in Manhattan and 28 intersections along Flatbush Avenue in Brooklyn will be instrumented with RSUs to communicate with up to 3,000 vehicles equipped with ASDs. These devices will monitor communications with other connected vehicles and the infrastructure and provide alerts to vehicle drivers/operators. Other RSUs will be installed at locations to support system management functions such as providing security credentials, managing

[1] Note that the assumption is that the bicyclist uses the same application as the pedestrian to obtain similar system services and user notifications.

application and parameter configurations, and uploading logged information. These locations consist of fleet terminal facilities, airports, and river crossings (bridges and tunnels) where vehicles frequently travel.

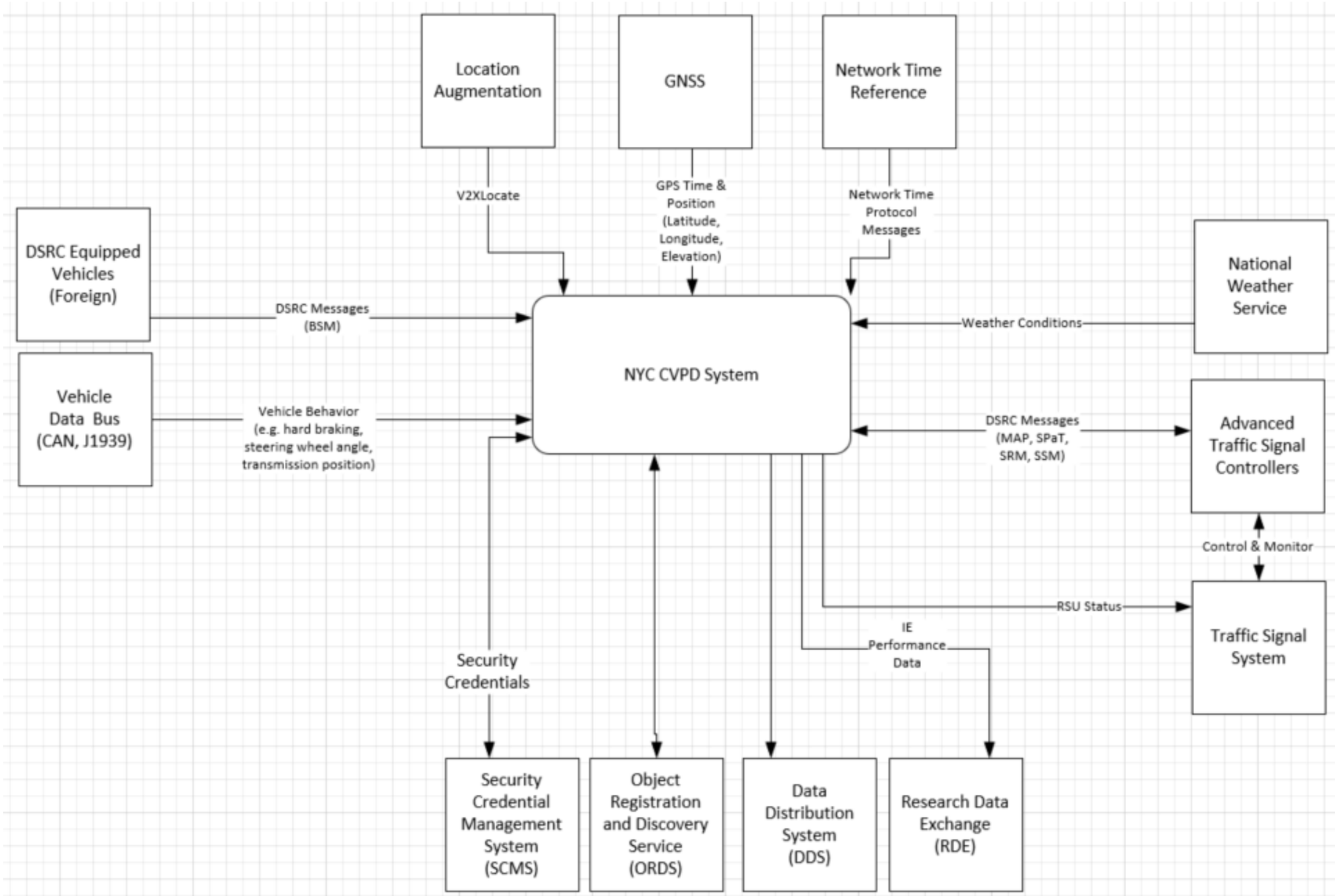
# Chapter 2. General System Description

The NYC CVPD system will consist of the specific subsystems in Figure 1-1 in the previous section. It will also interact with external components, interfaces, and systems shown in Figure 2-1. While some external systems are being developed at this time by USDOT, they will become fully functional as the NYC CVPD project phase is completed. The Security Credential Management System (SCMS), Operational Data Environment (ODE), and Object Registration Discovery Service (ORDS) are expected to be developed and provided by the USDOT. The Location and Time Source (LTS), Service Monitor (SM) System, and Wide Area Information Disseminator (WAID) will be provided by NYCDOT as the owner of the NYC CVPD system.

## 2.1 System Context

Figure 2-1 provides a detailed context of the NYC CVPD system. It defines the technical subsystems and interfaces that cross the system boundaries and the high-level interactions among the various components.

The left side of the context diagram represents the vehicles equipped with ASD and DSRC communication and their internal data bus. The right side identifies the traffic signal system, the advanced traffic signal controllers, and the National Weather Service (NWS) that will feed external data and DSRC messages to the NYC CVPD system. The top part of the diagram shows the location augmentation for maintaining the V2XLocate positioning system via RSU triangulation/trilateration, the GNSS for synchronizing the GPS time and position data (latitude, longitude, elevation), and the Network Time Reference for transmitting the Network Time Protocol (NTP) messages. The bottom portion of the diagram presents the SCMS for maintaining the security credentials, the Object Registration and Discovery Service (ORDS) for object registration and search, Operational Data Environment (ODE) for distribution of CV data, and Research Data Exchange (RDE) for exchange of Independent Evaluator (IE) performance data with USDOT. The ODE has replaced the Data Distribution System (DDS) as the platform for routing the data from multiple data sources to a common, integrated format for subscribers to software applications such as CV applications. However, at this time the USDOT ODE is not expected to play a role and interact directly with the NYC CVPD system.




Source: NYCDOT 2016

**Figure 2-1. NYC CVPD System Context Diagram**

### 2.1.1 DSRC Communication with Vehicles

All vehicles participating in the NYC CVPD will be equipped with ASDs. The ASDs will communicate with the Vehicle Communications Bus (CAN, J1939) and obtain vehicle behavior information (i.e. hard braking, steering wheel angle, transmission position, etc.). Based on the data collected, the DSRC-equipped vehicles will transmit messages in the form of BSMs to nearby RSUs, which will then forward it to the NYCDOT TMC for initial post-processing.

### 2.1.2 Location and Time

In the NYC CVPD system, location augmentation will occur through corrections via V2XLocate technology that uses RSU triangulation/trilateration. As shown in Figure 2-1, the ASD and RSU will depend on the Global Navigation Satellite System (GNSS) or Global Positioning System (GPS) time source for determining their time and position (latitude, longitude, and elevation). The Network Time Protocol (NTP) messages will serve as an external time source for synchronizing the location and time of non-CV equipment (i.e. Advanced Solid-State Traffic Controllers (ASTC), Traffic Control System (TCS), National Weather Service (NWS)) with the NYC CVPD infrastructure.

### 2.1.3 Existing External Systems

The National Weather Service (NWS) data on existing weather conditions will be captured and tied to the recorded CV application event data. To further remove the possibility of unusual weather events to particular dates, the precise nature of the weather events may be summarized as sunny, cloudy, light rain, heavy rain, light snow, heavy snow (or similar) instead of precise precipitation amounts or rates.

ASTC is the standard traffic signal controller device used in NYC. The controllers will be provisioned with CV capabilities to be able to exchange DSRC messages (i.e. SPaT, MAP,) with the NYC CVPD system. They will be monitored and controlled by Traffic Control System (TCS) which also will communicate with the RSUs and monitor their operational status.

### 2.1.4 Performance Measurement

The USDOT ODE will be responsible for collecting, processing, and distributing near real-time CV data such as BSM, MAP, SPaT, and TIM messages. It will link the data produced by the roadway users with the USDOT situation data clearinghouse and warehouse facilities. In the NYC CVPD system, the NYCDOT TMC will post-process and obfuscate the time, date, and location data in the BSMs received by the vehicles and SPaT, MAP, and TIM messages broadcasted by the RSUs. It will utilize its own algorithm to aggregate, sanitize, and strip the data of any PII. At this time, the USDOT ODE is not expected to play a role and interact directly with the NYC CVPD.

The Research Data Exchange (RDE) is USDOT ITS-JPO's web-based data resource for its real-time Connected Data Systems (CDS) program which collects, manages, and provides archived and real-time multi-source and multi-modal data to support the development and testing of ITS applications. The post-processed data from the NYC CVPD system will be sent to USDOT's Independent Evaluator (IE) for additional performance measurement analysis. After this process, the IE may elect to share the data on the ODE.

### 2.1.5 Security

The USDOT SCMS represents the interconnected NYC CV system that enable trusted communications between the ASDs, RSUs, and the TMC to protect the system and its data from unauthorized access. It will support the secure distribution, use, and revocation of security credentials in the NYC CVPD. Currently, it is being developed by USDOT for utilization in the three pilot sites.

The back office facilities at NYCDOT Traffic Management Center (TMC) will not be used for the security credentials management system (SCMS) functions, security enrollment certificates signing, and DSRC messages (BSM, SPaT, MAP, TIM) signing. Instead, these operations will be allocated to the field RSUs as supported by the latest USDOT RSU specification. Another option for consideration entailed utilizing a separate RSU within the TMC in lieu of the back office proxy server for managing the SCMS and signing of the enrollment certificates, pseudonym certificates, and safety messages transmitted by the devices. However, the method of allowing individual RSUs to sign the data has been selected to mitigate risks on schedule and cost.

The ORDS will provide registration and look-up services for allowing objects to locate other objects in the CV environment for communication purposes. It will be used to provide registration and discovery services for enabling the secure data transfer applications in the NYC CVPD.

## 2.2 System Modes and States

### 2.2.1 Operational Modes

The NYC CVPD system will operate in either online or offline mode as shown in Table 2-1 below.

**Table 2-1. NYC CVPD System Operational Modes**

| Mode | Description |
|---|---|
| Online | All subsystems and interfaces in the NYC CVPD system are operational.<br>All external systems and components are operational |
| Offline | One or more subsystems and interfaces in the NYC CVPD system have failed.<br>A critical external system (e.g. GNSS) has failed or a significant number of external units (e.g. ASTC) have failed. (Note that the significant number value will be established during the detailed design.) |

The NYC CVPD system devices will operate in the DSRC modes shown in Table 2-2 to Table 2-4.

**Table 2-2. RSU Operational Modes**

| State | Description |
|---|---|
| Online | The RSU communicates with other CV devices and subsystems. |
| Offline | The RSU no longer communicates with other CV devices and subsystems. |

**Table 2-3. ASD Operational Modes**

| State | Description |
|---|---|
| Online | The ASD communicates with other CV devices and subsystems. |
| Offline | The ASD no longer communicates with other CV devices and subsystems. |

**Table 2-4. PID Operational Modes**

| State | Description |
|---|---|
| Online | The PID communicates with other CV devices and subsystems. |
| Offline | The PID no longer communicates with other CV devices and subsystems. |

### 2.2.2 Operational States

During NYC CVPD's normal operation, the CV device will be able to communicate via DSRC to and/or from the device. For performance evaluation purposes, it will operate in either active or silent state as shown in Table 2-5.

**Table 2-5. NYC CVPD System Operational States**

| State | Description |
|---|---|
| Active | The device transmits and/or receives DSRC messages while event records are collected. |
| Silent | The device transmits and/or receives DSRC messages but no event records are collected. |

### 2.2.3 Operational Configuration

The NYC CVPD system devices will operate with the following parameter types:

- Control parameter: determines when to operate a particular device
- Configuration parameter: determines how to operate (e.g. time delays, distances) a particular device
- Recording parameter: determines what information for how long a particular device will record

Specific details about each parameter can be found in Section 2.3.1.2.

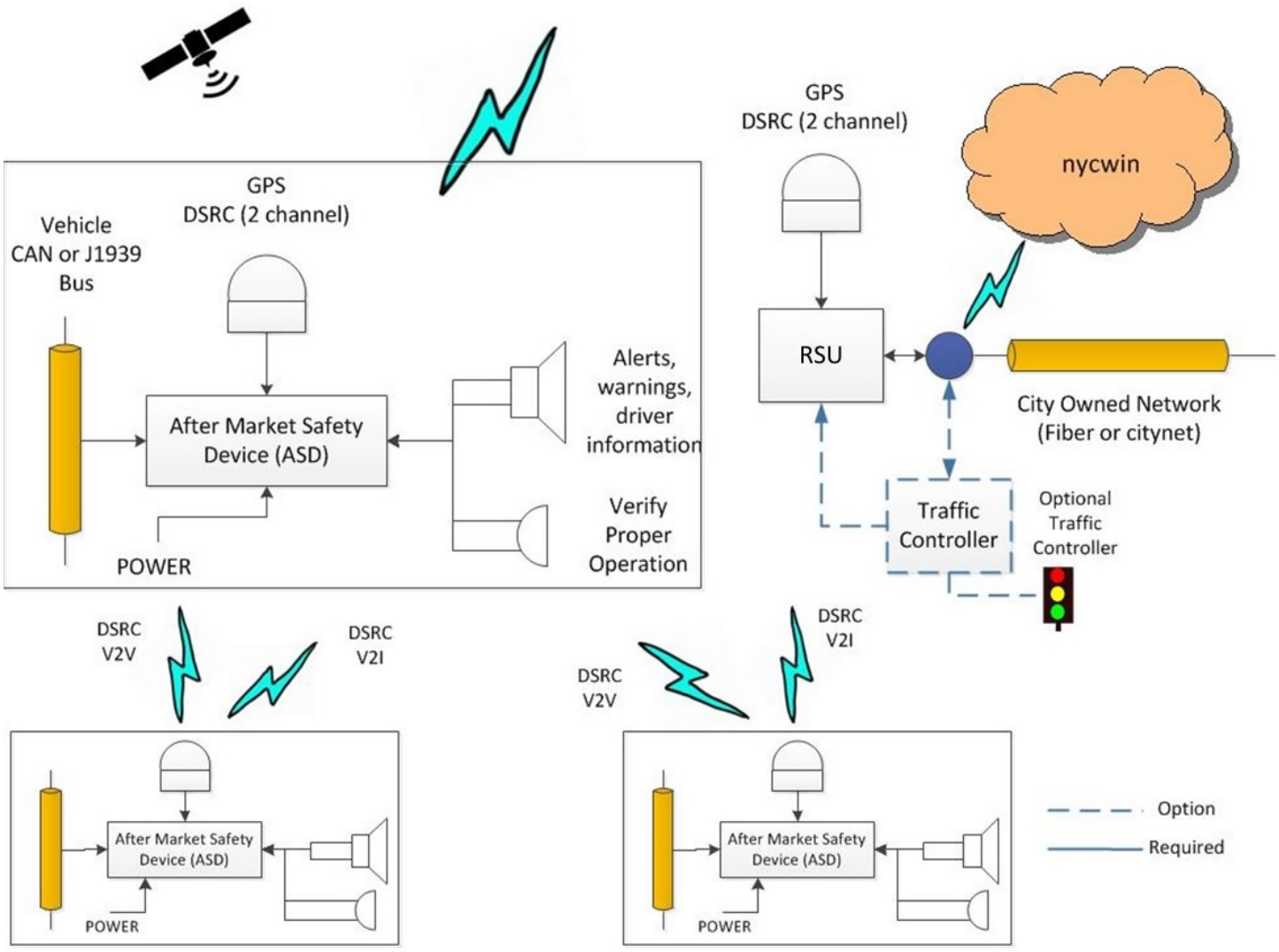
## 2.3 Major System Capabilities

This section provides an overview of the major capability groupings for the NYC CVPD system requirements. Based on Figure 2-1 above, it describes the contextual components of the NYC CVPD system.

### 2.3.1 ASD Context

In the NYC CVPD system, the ASDs will send and receive DSRC safety messages through multiple V2V and V2I safety applications. They will be equipped with a speaker for warning the driver, an Ethernet port for maintenance, and power button. They will communicate with the Vehicle Data Bus (CAN, J1939) for gathering the vehicle behavior information and GPS for time and location source.

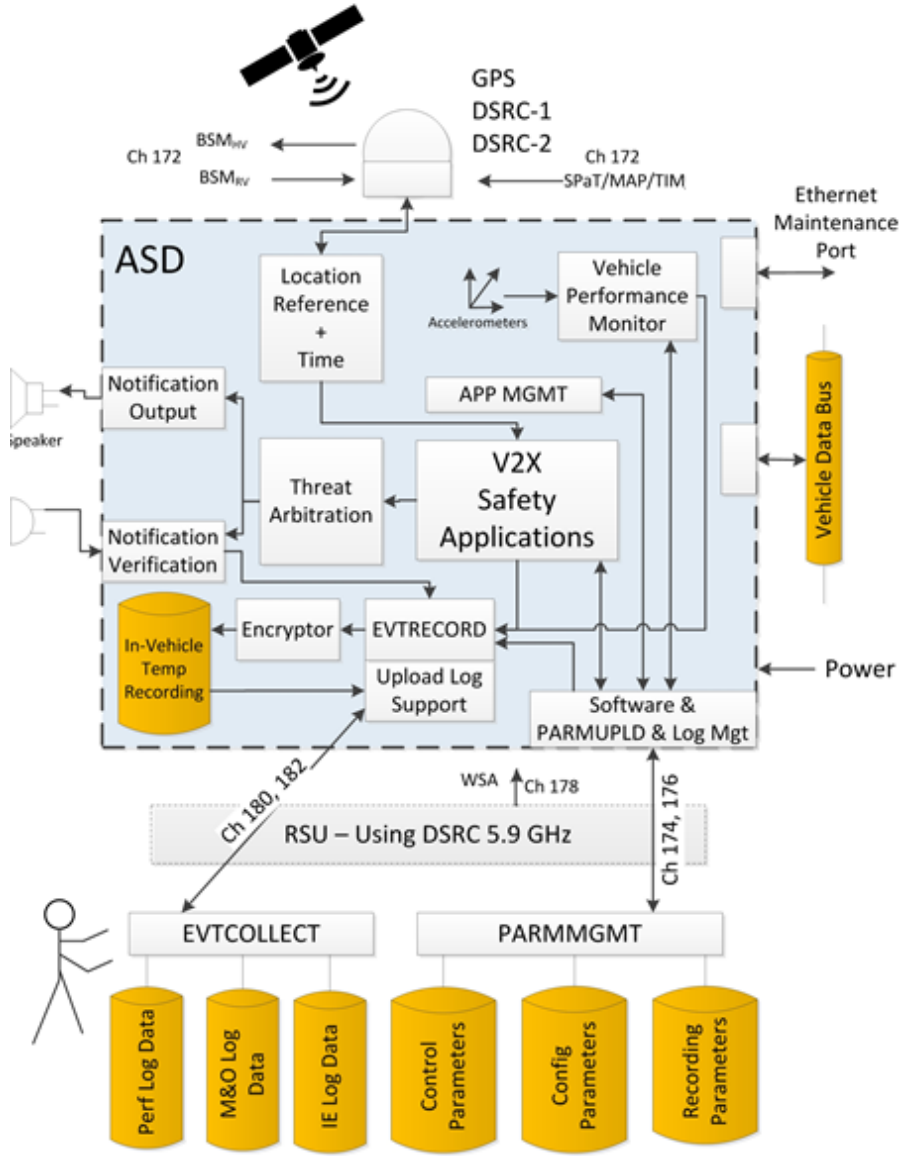
Figure 2-2 shows three (3) ASD units and their interfaces to the vehicle driver, GNSS, vehicle data bus (CAN or J1939), and DSRC connection to other ASDs, subsystems, and external systems. In the NYC CVPD system, the ASDs will send and receive DSRC safety messages through multiple V2V and V2I safety applications. They will be equipped with a speaker for warning the driver, an Ethernet port for maintenance, and power button. They will communicate with the vehicle data bus for gathering the vehicle behavior information and GPS time and location source.




Source: NYCDOT 2016

**Figure 2-2. ASD Concept Diagram**

Figure 2-3 presents a detailed view of the ASD system architecture and its connections to other ASDs, subsystems, and external systems via DSRC. The host vehicle's ASD will transmit BSMs to and from other vehicle ASDs and receive SPaT, MAP, and TIM messages through DSRC channel 172. For tuning the safety applications to the NYC traffic environment, the control, configuration, and recording parameters will be downloaded from the Parameter Management application to the ASD via DSRC channels 174 and 176. As it collects event logs based on warnings from safety applications, it will upload them to the Event Collect application in the designated RSUs via DSRC channels 180 and 182. This exchange will occur as the ASDs enter the range of a particular RSU and receive the WAVE Service Advertisement (WSA) message from the RSU via DSRC channel 178 at 5.9 GHz. The Event Collect application will manage performance data, maintenance and operation data, and IE log data.




Source: NYCDOT 2016

**Figure 2-3. ASD Context Diagram**

The ASD will run multiple V2X safety applications, and threat arbitration will determine which application takes priority over others instead of allowing multiple applications to be triggered and notify the driver at once. The Event Record application will log event records from the safety application triggers, including the BSM, location reference and time, and accelerometer information from the Vehicle Performance Monitor application. It will send the event records to the In-Vehicle Temporary Recording module then to the Upload Log Support function for transmitting the log data to the designated RSUs.

#### *2.3.1.1 Event Collection*

The ASD will log the information before and after a particular event. The number of seconds before and after each event is to be determined, and it may depend on the type of warning generated by the ASD. What data is recorded will be subject to whether OBD-II/CAN bus is accessible and what data is produced by the ASD. This performance log data is expected to include time and location information from the BSMs, the warning issued by the ASD, any SPaT, TIM, and MAP messages from any RSU it can hear, and the vehicle maneuver as a result of that warning. As the vehicle returns to its fleet terminal, the recorded data will be uploaded to the RSU at the terminal.

When the vehicle operator begins normal duties by turning on the ASD-equipped vehicle, the ASD will confirm whether it is ready for operation. If the ASD experiences a fault, it will generate a maintenance & operation (M&O) log data that contains the start-up event and the fault. When the vehicle returns to its fleet barn after normal operating hours, the ASD will communicate with the RSU to verify its firmware version against the advertised available version. If the ASD's version is outdated, then it will initiate the over-the-air (OTA) software and firmware update transaction from the RSU at the vehicle's fleet barn.

As the driver returns the vehicle to its respective fleet barn, the event data log will be transmitted from the ASD to the RSU at the barn. Then, the RSU will receive the data, acknowledge the transaction, and send it to NYCDOT TMC's back office CV data processing center. The event log data will be processed for analyzing the safety benefits of the NYC CVPD. Then, it will undergo extensive post-processing and normalization (i.e., cleansing) before being transmitted to the USDOT. As it is aggregated, the types of event counts will be incremented by time-of-day, location, and event type into collection bins. Any traceable and private information will be discarded. Once all errors are addressed and checked, the raw data will be purged. This independent evaluator (IE) log data will be used by the USDOT IE for additional evaluation and uploading onto its Research Data Exchange (RDE) portal.

#### *2.3.1.2 Parameter Management*

During installation, the ASD will be programmed with control parameters for tuning the safety applications to the NYC traffic environment. The software parameters will be uploaded via DSRC channels 174 and 176. Configuration parameters will also be downloaded to the ASD to determine minimum thresholds for each application prior to the operation. For example, the vehicle kinematics including but not limited to center of gravity, speed, and curve radius will be set before the ASD is deployed in the field. Also, recording parameters will be set to establish threat arbitration. This will prevent multiple safety applications from warning the driver and prioritize which application trigger will be activated before others.

## 2.3.2 Event Recording Context

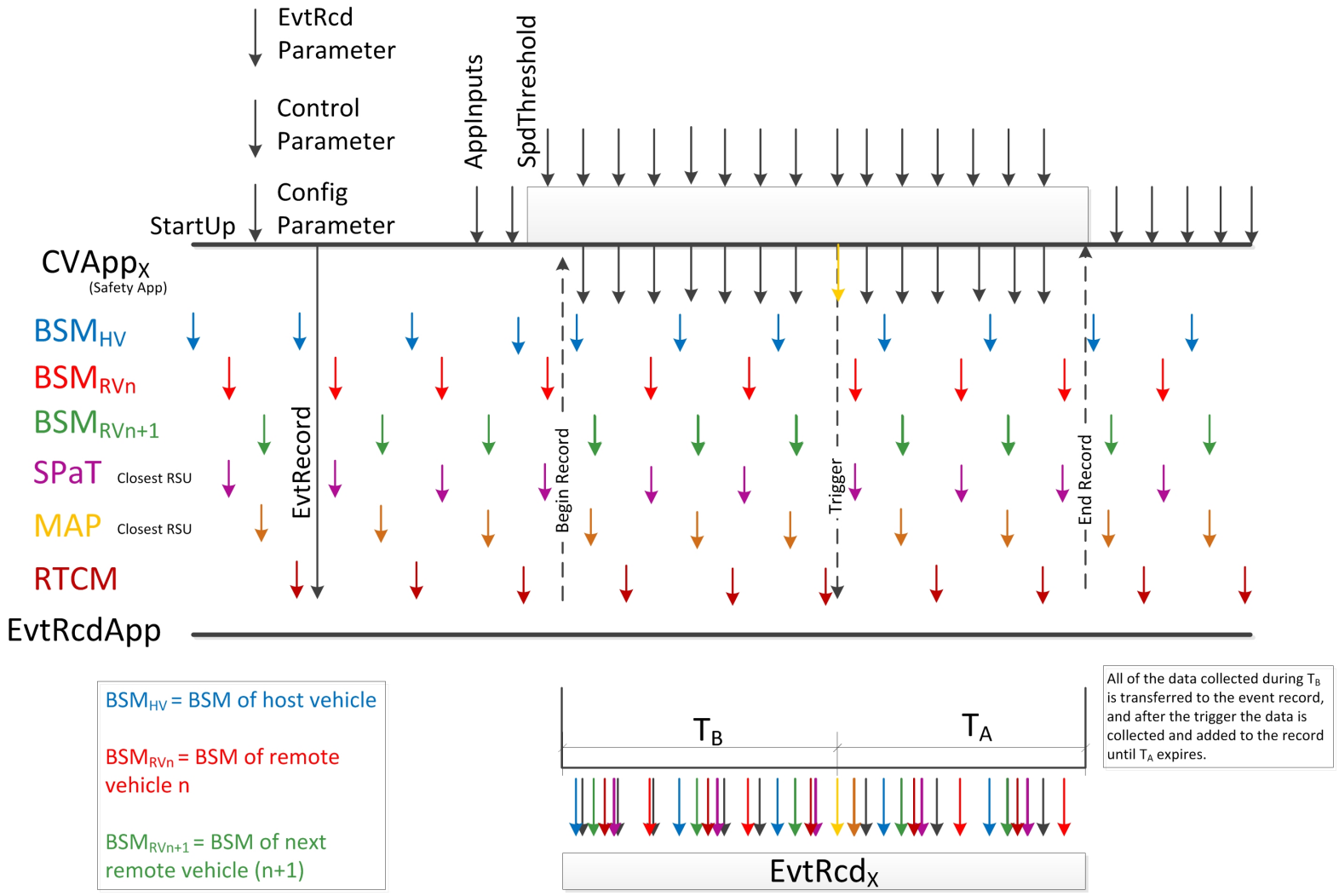
The ASDs will log relevant information surrounding a triggered event as shown in Figure 2-4. The trigger will be configurable and will include the CV application warnings, acceleration criteria, brake system status, etc. The time periods for collecting data before and after the trigger event will be configurable for each event trigger. These periods will consist of a few seconds (e.g., 10-20) prior to and a few seconds (e.g., 30-40) following the trigger's activation. The relevant information (data) will be limited to what the ASD provides, and it may include vehicle data when the ASD is connected to the vehicle's data bus (i.e., CAN, J1939). For instance, each event log entry will include location (i.e., latitude, longitude, elevation, 3-axis acceleration), indicated warnings, and the action (i.e., lights, wipers, turn signals, steering angles, brakes) of the vehicle. More importantly, this event log will be stored on the vehicle for later retrieval when the vehicle returns to its fleet terminal where the data will be offloaded.

Note that the definition of an event will be configurable so it can be used to collect short-term driver behavioral data (hard break, steering turns, accelerations, etc.) for aggregation and performance measures. However, such data will be cleansed of any traceable personal data (exact location and time) to prevent from being correlated to other records such as police reports.

## 2.3.3 CV Application Terminology

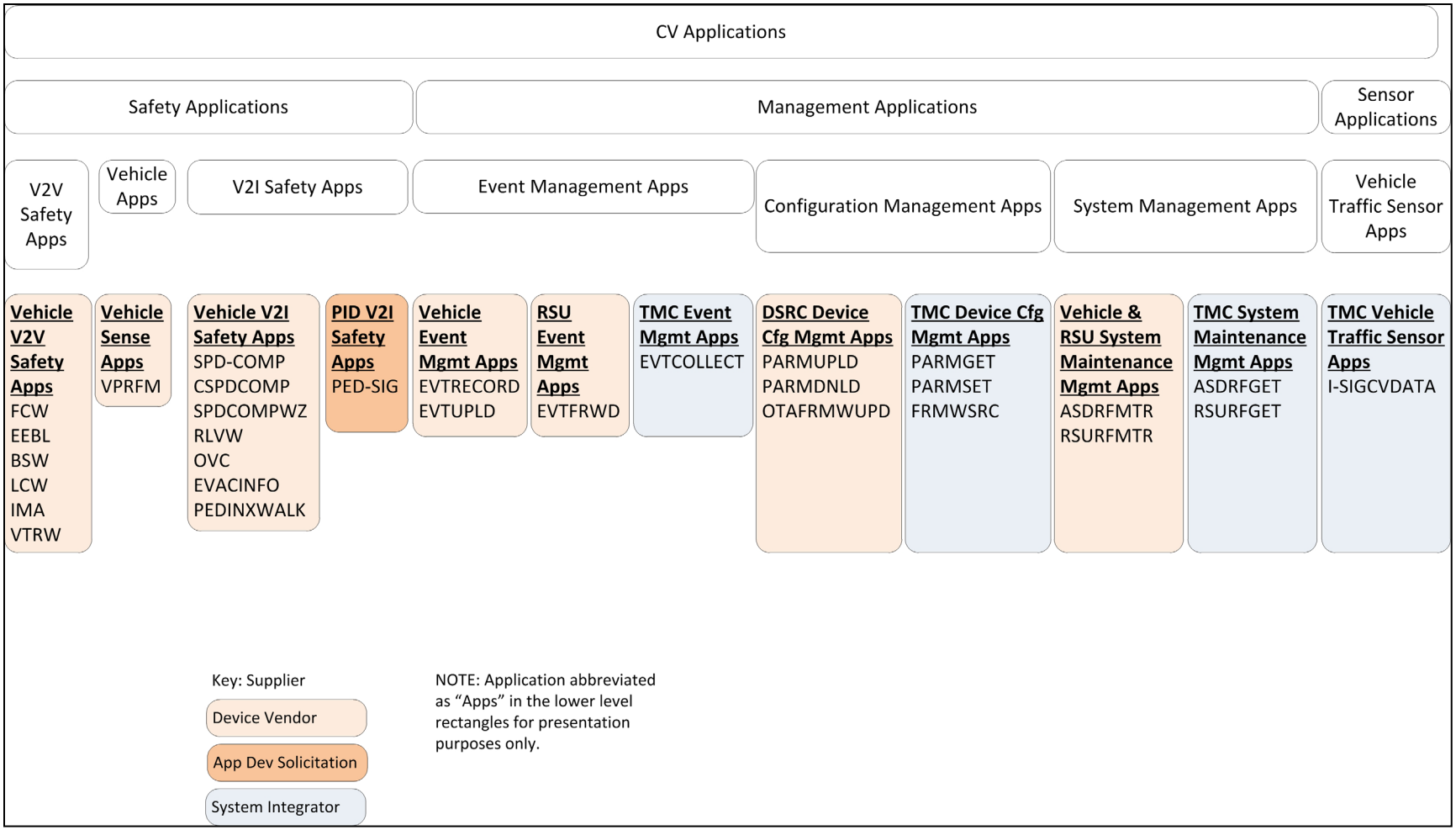
Figure 2-5 outlines the classification of all applications to be deployed in the NYC CVPD system. As the ASDs communicate with other ASDs and RSUs, they will send and receive DSRC safety messages through multiple safety applications. These consist of V2V, Vehicle Performance Radio Frequency (RF) Monitoring, V2I, and I2P applications. The ASDs will also utilize a set of management applications that support the communication and data management functions of the system. Event management applications will record, upload, and forward the event records at the ASD, RSU, and TMC. Configuration management applications will upload and download the parameters and over-the-air (OTA) firmware to and from the DSRC devices. System management applications will monitor the RF levels of the ASDs and RSUs and maintain the NYC CVPD system performance. Sensor application via the I-SIGCVDATA will utilize vehicle traffic sensors to provide CV data feeds to NYC's existing adaptive signal control system.

.




Source: NYCDOT 2016

**Figure 2-4. Event Recording Context Diagram**




Source: NYCDOT 2016

**Figure 2-5. NYC CVPD Applications Context Diagram**

### *2.3.3.1 Safety Applications*

#### 2.3.3.1.1 V2V Safety Applications

Six of the CV applications are intended to be utilized unchanged from their initial concept of operations. These applications are listed in the SAE J2794/1 standard for V2V communications and the USDOT's publication FHWA-JPO-13-058. These applications do not need to be re-engineered as components of this project as this work has already been completed. The applications and references for them are listed in Table 2-6 below.

**Table 2-6. CV Application ConOp References**

| CV Application | Concept of Operations Reference |
|---|---|
| Forward Crash Warning (FCW) | NHTSA DOT HS 811 492A |
| Emergency Electronic Brake Lights (EEBL) | NHTSA DOT HS 811 492A |
| Blind Spot Warning (BSW) | NHTSA DOT HS 811 492A |
| Lane Change Warning (LCW) | NHTSA DOT HS 811 492A |
| Intersection Movement Assist (IMA) | NHTSA DOT HS 811 492A |
| Vehicle Turning Right in Front of Bus Warning (VTRW) | Transit Safety Retrofit Package Development<br>TRP Concept of Operations<br>Final Report – May 28, 2014 FHWA-JPO-14-117 |

#### 2.3.3.1.2 Vehicle Applications

The Vehicle Performance RF Monitoring (VPRFM) application will collect and log the vehicle operational data (i.e. hard breaking, steering wheel turns, acceleration).

#### 2.3.3.1.3 V2I Safety Applications

Speed Compliance (SPDCOMP) application will provide warnings to drivers when they exceed the posted regulatory speed limit. If the vehicle is approaching a curve, the Curve Speed Compliance (CSPD-COMP) application will activate and warn the driver. Similarly, if the vehicle is approaching a designated work or school zone, the Speed Compliance in Work Zone (SPDCOMPWZ) application will be triggered.

Red Light Violation Warning (RLVW) application will warn drivers when the ASD determines that they will run the red light. It will utilize the SPaT message from the RSU at the signalized intersection.

Oversize Vehicle Compliance (OVC) application will warn the driver of impending height-restricted infrastructure such as bridge or tunnel entrance. Each vehicle's size information will be configured into its ASD. Using the pre-configured vehicle height information, the ASD will determine whether the vehicle is able to pass through the bridge or tunnel.

Emergency Communications and Evacuation Information (EVAC) application will support NYC's emergency communications and dissemination of evacuation traveler information. Centers including

the Traffic Management Center (TMC), Office of Emergency Response (OER), and weather service will partake in the emergency operations and management functions.

Pedestrian in Signalized Crosswalk (PEDINXWALK) application will utilize the pedestrian detection information to warn drivers about the presence of pedestrians in a crosswalk at a signalized intersection. As a pedestrian passes through a crosswalk at a signalized intersection with additional pedestrian detection equipment installed, the pedestrian's presence will be detected by the traffic control system. The traffic control system will notify the vehicle of a pedestrian's presence in the crosswalk.

Mobile Accessible Pedestrian Signal System (PED-SIG) application will support the visually impaired (blind) crossing the street. The NYC CVPD project assumes that a portable personal information device (PID) such as a smartphone with both normal cellular and DSRC communication will be used. The traffic signal controller will communicate with the RSU at the same intersection which will transmit SPaT and MAP messages to the PID in a similar way to the ASD.

#### *2.3.3.2 Management Applications*

##### 2.3.3.2.1 Event Management

The Vehicle Event Management applications include Event Recording (EVTRECORD) and Event Uploading (EVTUPLD). As the ASD receives BSMs, the EVTRECORD application will collect event logs before and after the warnings. Then, the EVTUPLD application will transmit the event record data to designated RSUs as the vehicle passed by them.

The RSU Event Management application is Event Forwarding (EVTFRWD). As the RSU collects the event record data from the ASDs, it will send the data to the TMC's back-office CV data processing center.

The TMC Event Management application is Event Collection (EVTCOLLECT). As the TMC's CV back-office receives the event record data, it will post-process and obfuscate the data to eliminate personally identifiable information (PII) and time and location breadcrumb information.

##### 2.3.3.2.2 Configuration Management

The DSRC Device Configuration Management applications consist of Parameter Upload (PARMUPLD), Parameter Download (PARMDNLD), and Over-the-Air Firmware Upload (OTAFRMWUPLD). The PARMUPLD and PARMDNLD applications will be used to install the necessary parameters to the ASD for each application before deployment. The OTAFRMWUPLD will be used for remote firmware upgrades from the RSU at each fleet barn to the ASDs.

The TMC Device Configuration Management applications are Parameter Get (PARMGET), Parameter Set (PARMSET), and Firmware Service (FRMWSRC). The PARMGET and PARMSET applications will be used to transmit the parameter configurations from the TMC to the RSUs for installing into the ASDs. The FRMWSRC application will be used to provide the RSU at each fleet barn with the necessary firmware updates for uploading into the individual ASDs.

##### 2.3.3.2.3 System Management

The Vehicle and RSU System Maintenance Management applications are the ASD RF Monitoring (ASDRFMTR) and RSU RF Monitoring (RSURFMTR). The ASDRFMTR application will be used to

detect the presence or absence of ASDs in the NYC CVPD. It will trace the radio frequency (RF) radiation issues to a specific vehicle, and the information collected will be given to the fleet owners for arranging repairs or adjustments to be made to the vehicle. The RSURFMTR application will address any temporary occlusion by a vehicle from issues such as vehicle ID change and the vehicle operator stopping or turning off the ASDs.

The TMC System Maintenance Management applications are the ASD RF Get (ASDRFGET) and RSU RF Get (RSURFGET). Both applications will be used to post-process and analyze the RF logs from the ASDRFMTR and RSURFMTR applications. Similar to the EVTCOLLECT application, the ASDRFGET and RSURFGET applications will purge the raw data of any PIIs and time and location information.

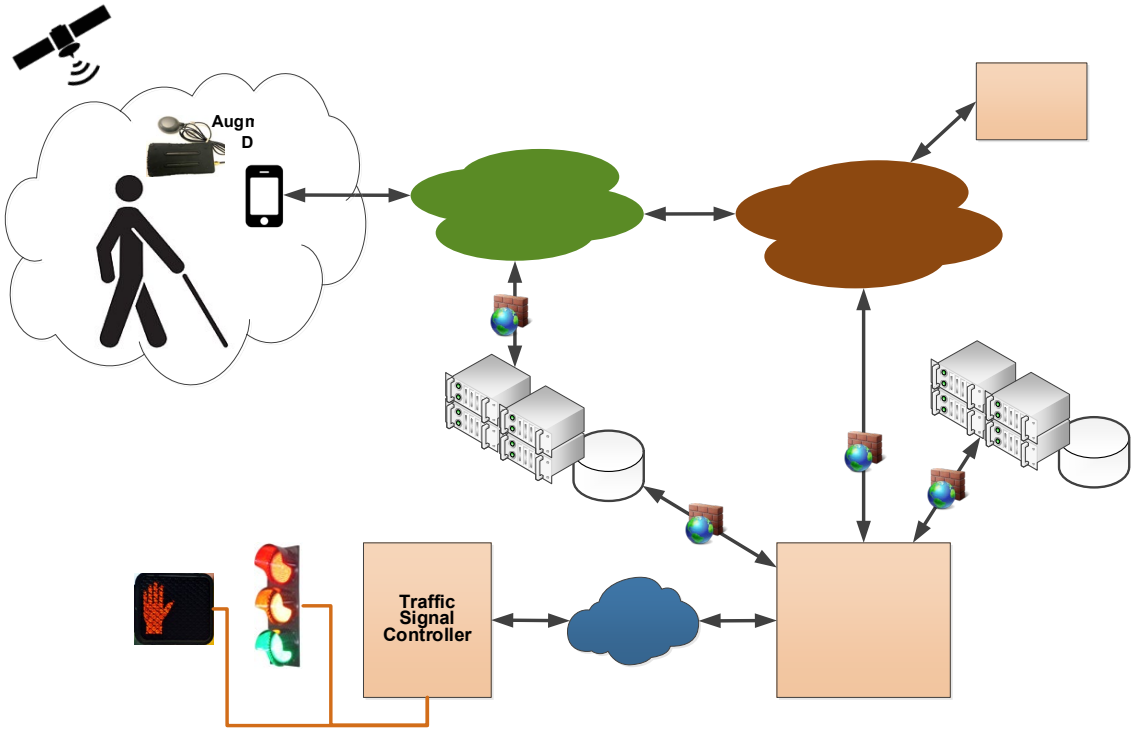
#### *2.3.3.3 Sensor Applications*

The TMC Vehicle Traffic Sensor application will be Intelligent Signal System CV Data (I-SIGCVDAT). It will utilize the NYC CVPD data as an input to NYC's existing Adaptive Control Decision Support System (ACDSS). This data will augment or replace the existing data from the toll tag reader system that provides travel time and speed information. This is intended to compare the two datasets and determine if ACDSS can rely on only the CV data collected from the pilot deployment project.

## 2.3.4 PID Context

At first, the intent of the project was to use the localized Signal Phase and Timing (SPaT) and Map Data (MAP) messages broadcast over Dedicated Short Range Communication (DSRC) to provide assistance for visually impaired pedestrians while navigating the crosswalks at connected vehicle (CV) instrumented intersections. It was recognized that this was experimental and would be a pilot trial of the use of the technology for this application. When DSRC enabled smartphones were no longer available, per the vendor's suggestion the project scope was modified to use cellular communications (4G, LTE) to the smartphone instead of the DSRC media from the local Roadside Unit (RSU). Since the SPaT information includes "time points", the latencies involved in providing the SPaT information via cellular service for this type of application were expected to have minimal effect on the performance of the application.

Figure 2-6 displays the architecture of the PED-SIG or PED application. The advanced solid-state traffic controllers (ASTC) were modified to transmit SPaT information to the Traffic Management Center (TMC) for processing in preparation for use by the PID applications. This data is transmitted to the TMC from the ASTC "on change", such as when the values in the SPaT message changed. At the TMC, the information is time corrected to use Coordinated Universal Time (UTC) rather than Line Frequency Time and sent to the Amazon Web Services (AWS) cloud along with the MAP message content which is stored at the TMC. Thus, the AWS cloud is provided with the same data as the RSU so that the application can process this information and provide it to the PID to support intersection navigation assistance for a visually-impaired pedestrian.




Source: NYCDOT 2020

**Figure 2-6. Pedestrian Support Application Architecture**

The MAP message contents were developed using the USDOT "tool", updated with the sidewalk descriptions and augmented with the use of the Cyclomedia high resolution database to improve the accuracy of the location information for the crosswalks and landing zones. It should also be noted that the MAP message used by the PIDs is not size constrained in the same manner as the MAP message transmitted by the RSU such that the TMC sends more detailed information to the AWS cloud than is transmitted by the RSU. The TMC exports the MAP and SPaT information to the AWS cloud where it is used by the PED application as described in their design specification.

In addition, the vendor developed a "Location Augmentation Device" for use by the visually-impaired pedestrian to improve the overall accuracy of the location information when coupled with the smartphone to support the SC application. The location accuracy of a smartphone in the urban environment is inadequate for such applications. The Location Augmentation Device (LAD) is coupled to the smartphone using Bluetooth and the SC application uses both the smartphone location and compass coupled with the location information from the augmentation device to provide the assistance to the visually impaired pedestrian.

When the SC application is active, evaluation data is supposed to be collected and sent to New York University (NYU) servers where it will be used for the performance evaluation for the PID program. If the operation of the prototypes is acceptable, the plan is for NYU to acquire the smartphones, solicit participants, obtain consent from the users, and then distribute the smartphones to those users. The data collected along with survey information is to be evaluated to determine the overall utility, value, and issues associated with the PID and SC application for the user community. The project team

worked with the NYU Independent Review Board (IRB) to ensure safety, and privacy of the participants.

The subsequent requirements section assumes that the MAP and SPaT messages are transmitted as described above. The following assumptions are made in developing the pedestrian application requirements:

- Enrollment will download the security credentials, if the application is connecting to the signal.
- There will be no signal actuation.
- The application will connect with the cloud.
- There will be no personal data collected.
- The mobile device will be easily managed by visually-impaired users.
- There will be data from the signal to the mobile device.

## 2.4 Major System Conditions

The CV system is expected to always be in operation. Management provisions are made to monitor the operation of the system's devices in order to identify failures and resolve them. These fall into two areas – one for the infrastructure devices and their communications links with the other being the vehicle resident ASDs.

Driver/operators need to be informed when vehicles start that their vehicle resident ASD is operating properly. Failed ASDs will not prevent the safe operation of the vehicle by the driver/operator – the driver will not receive alerts/alarms from the device in when it is failed. Support personnel will have to be notified by the driver/operator in order to begin the repair process.

When RSUs fail, vehicle drivers/operators will not be notified and will operate their vehicles normally without alerts/alarms from the ASDs for V2I applications. In this state, the V2V applications will continue to function and provide alerts/alarms when in the presence of other connected vehicles (assuming that their ASDs are also functioning properly).

Such fail conditions in the CV devices will result in safety-related implications such as inability to issue alerts. Furthermore, this will lead to insufficient or inaccurate data and safety benefit analysis of the system. The types of potential fail modes are defined in Table F-2 in the Appendix.

## 2.5 Major System Constraints

In New York City (NYC), the speed limit is 25 mph unless signed otherwise. This speed restriction has been recently implemented under the objectives of the Vision Zero program. In New York City, turns on red signals are treated differently than the remainder of the nation. Right-turn-on-red (RTOR) after stop is prohibited within New York City unless signed to indicate otherwise. This operational restriction has existed since the traffic laws were modified during the 1970s in response to fuel shortages. NYC has unique definitions for commercial vehicles and trucks that differ from New York State Department of Motor Vehicles classifications. It encourages drivers to check their vehicle's classification information before making trips and to review the City's truck route map to avoid problematic issues such as driving on the area's parkways.

From the beginning of the CV program, ensuring individual privacy has been a key to adoption of the CV technology. In order to produce these safety benefits consistent with the goals of the USDOT's connected vehicle program, the project will adopt the USDOT objective to "not collect or store any data on individuals or individual vehicles, or will it enable the government to do so[37]." Throughout all meetings with the project stakeholders, the stakeholders expressed that this objective must be met to continue their participation.

The stakeholder's concern is that time and location information constitutes potentially Personally Identifiable Information (PII) because it could be merged with other records (e.g., police crash reports) and used in legal proceedings, disciplinary proceedings, or insurance negotiations. Keeping data with this time/location information is a potential infringement of an individual's privacy. Concerns have also been expressed by the labor unions and legal departments that if such records were known to exist, they would be subpoenaed for criminal and/or civil suits and would be subject to FOIA requests – which are very frequent in NYC.

The goal of privacy poses a formidable challenge for the deployment of the NYC CVPD project. While privacy is a fundamental concept embedded in the CV system design, the need to measure deployment benefits necessitates knowing details regarding the vehicle and its whereabouts. To balance these competing objectives, the NYC CVPD will provide detailed vehicle operational information after it has been aggregated and normalized (i.e., scrubbed) of time and location details. This approach satisfies the detailed information needs for evaluation while protecting the privacy of the vehicle drivers/operators.

Another constraint is a result of the project's focus on safety. The NYC legal staff is concerned about the deployment of safety focused applications that may not provide warnings to the drivers/operators. On one hand, the concern is about a warning not being given to the driver/operator that could have mitigated a crash/injury/fatality situation. This also applies to participants who are visually-impaired or audibly-impaired. In addition to maintaining safety during the system operation, the memorandum of understanding (MOU), financial, and legal/regulatory terms and conditions will be established to protect the safety of all participants in the NYC CVPD.

The other concern is that for the purposes of data collection for a before/after evaluation, the system will operate in silent mode for a time period in order to gather data. While the previous concern exists during this silent period, there is another regarding toggling the system between silent and active mode. This mode difference has the potential to impact drivers' decisions should they become secure in knowing the system will generate warnings when in fact it is in silent mode. To address these concerns, the NYC project team proposes using a single transition from silent to active mode for the fleets.

## 2.6 User Characteristics

This section defines the users and stakeholders and their roles and responsibilities of the NYC CVPD system. The expected users represent various maintenance and operational functions, location, and type of utilized CV devices. The users are classified based on their perception of the system and the needs to be satisfied by the system. Also, some of the key personnel may serve in multiple roles based on the user needs and functions.

## 2.6.1 Traffic Manager

As the roadway infrastructure owner, NYCDOT consists of multiple traffic managers in the NYC CVPD system. In supporting the goals of Vision Zero, the traffic managers' responsibilities include managing the speed on surface streets to 25 mph regulatory speed limit; reducing crashes between vehicles, vehicles and infrastructure, vehicles and pedestrians, and vehicles and visually/audibly-impaired pedestrians; informing drivers of serious incidents; and providing mobility information in heavily congested areas.

#### *2.6.1.1 NYCDOT ASD Monitoring Personnel*

The NYCDOT ASD monitoring personnel is responsible for checking the health status and RF footprint of the communication to and from ASDs in the NYC CVPD. The ASD will collect log information on its operational status and sent for review. When equipment faults are detected, the monitoring personnel will notify and dispatch the maintenance personnel to the vehicle fleet barn, where troubleshooting and repair works will be performed.

#### *2.6.1.2 NYCDOT RSU Monitoring Personnel*

The NYCDOT RSU monitoring personnel is responsible for checking the health status and RF footprint of the communication to and from RSUs in the NYC CVPD. When equipment failures are detected, they will notify and dispatch the maintenance personnel to the RSU. The proposed RSU locations consist of signalized intersection, vehicle fleet terminal, bridge/tunnel crossings, and other designated locations that may be outside the NYC CVPD pilot area.

#### *2.6.1.3 NYCDOT TMC Operators*

The NYCDOT Traffic Management Center (TMC) operators are responsible for operating the citywide TMC. They interact with the traffic control system (TCS) and provide operator data and command inputs to the system operations. Status on field equipment such as wired and wireless communication networks and traffic signal controller (ASTC) upgrades will be communicated with other NYC CV system users.

The TMC operators will also communicate with the RSUs in the NYC CVPD to monitor and manage traffic flow and roadway conditions. For minor traffic accidents and work zone activities, they will work with the City's traffic surveillance system, traffic information system, work zone management system to monitor traffic in and around the areas of influence. In the event of major disasters, they will coordinate incident management activities and exchange information with NYCDOT Office of Emergency Response (OER).

## 2.6.2 Fleet Manager

In the NYC CVPD, the fleet manager will be responsible for overseeing the vehicle equipment installation, coordinating maintenance activities, and daily operation of the vehicles. Their roles include managing equipment maintenance, and daily operations of the vehicle fleets. Also, their major concern on potential use of the data for enforcement or driver performance assessment will be addressed by establishing the need to have privacy of vehicles and drivers in the CV system.

#### *2.6.2.1 NYCDOT Fleets*

NYCDOT Fleets represent the fleet owners that manage maintenance vehicles, trucks, and passenger cars from NYCDOT for its daily operation. They include light-duty and heavy vehicles such as inspector's cars, passenger trucks, asphalt trucks, and other construction vehicles. Approximately 1230 NYCDOT vehicles are expected to be deployed in the NYC CVPD program.

#### *2.6.2.2 Department of Citywide Administrative Services (DCAS)*

DCAS in NYC is the agency that provides shared services to support City operations. It administers citywide fleet management including maintenance and operation of motor vehicle pool. Due to TLC/taxi fleets, UPS, and DSNY no longer deciding to participate in NYC CVPD, NYCDOT has been able to coordinate with DCAS fleet owners in obtaining additional vehicles for ASD installation and deployment. About 1759 DCAS fleet vehicles are expected to be deployed in the NYC CVPD program.

#### *2.6.2.3 Metropolitan Transportation Authority (MTA)*

MTA is the agency responsible for operation and maintenance of local and express buses in NYC's five boroughs. It manages about a total of 5,900 buses that belong to ~16 different bus models. In the NYC CVPD project, eleven (11) buses have been deployed.

### 2.6.3 Roadway Users

The roadway users in the NYC CVPD include vehicle drivers/operators, pedestrians, and performance management users. Based on stakeholder meetings with the participating fleet owners, the need for privacy and management of the CV applications for the traffic environment will apply to both fleet owners and roadway users.

#### *2.6.3.1 Drivers*

Drivers represent the vehicle operators from each participating fleet owner in the NYC CVPD. With the project plan to instrument 3,000 vehicles, the project will be dealing with a potentially much larger pool of driver/operators. This is due to the nature of the fleets and that multiple drivers may be used to operate the vehicles. Many of the fleet vehicles will be in service more than five days a week and for periods well beyond an eight (8)-hour shift. If the ASD in the vehicle experiences a fault, the driver will be responsible for reporting to the fleet owner who will then notify the NYCDOT and coordinate maintenance activities.

Vehicle driver/operators will also be responsible for identifying issues with their vehicles and bringing those issues to the attention of the vehicle owners for repair. In the case of the vehicle fleets, some fleet owners have internal organizations for vehicle maintenance. Other fleet owners utilize third-party maintenance providers for vehicle maintenance on a contract basis.

#### *2.6.3.2 Pedestrians*

Pedestrians represent the people that walk along the roadways. In the NYC CVPD system, they are classified into two distinct groups. The first group includes the visual impaired pedestrians who are participating in the NYC CV pilot and equipped with personal information devices (PID). Each

participant will carry the PID which will be used for the Mobile Accessible Pedestrian Signal System (PED-SIG) application in assisting the visually-impaired pedestrian to cross the intersection safely. Pedestrians for Accessible and Safe Streets (PASS) is the coalition that works to promote safe access to sidewalks and streets for the visually-impaired and audibly-impaired pedestrians in NYC. PASS is expected to be a stakeholder that will aid in recruiting the visually-impaired pedestrians for the NYC CV pilot.

The second group consists of pedestrians who are not participants and not carrying any PIDs. They may be crossing intersections that are proposed to be equipped with new pedestrian detection equipment. These intersections are listed in see Table 35 in NYC CVPD Phase 1 ConOps, FHWA-JPO-16-299. This pedestrian detection data will be used for the Pedestrian in Signalized Crosswalk (PEDINXWALK) application and alerting the driver of the pedestrian crossing.

#### *2.6.3.3 Performance Measurement Users*

Performance measurement users will be responsible for viewing the daily event log history, the log uploading process, and batch processing of the data. They will be able to see and understand how much data and how many events are generated and recorded. Also, they will be the first point people for noticing any anomalies in the CV device operation, such as errors in time synchronization in the ASDs via Global Navigation Satellite System (GNSS) devices.

## 2.6.4 System Manager

The system manager in NYC CVPD will be responsible for the roadway and traffic control devices in the project areas. It uses internal and external third-party resources to maintain the roadway infrastructure. There are well established relationships and procedures within the NYCDOT for these maintenance activities. These processes include reporting facilities (e.g. 511, web sites), work order generation and tracking, and management oversight.

NYCDOT and DoITT share responsibility for communications infrastructure. Both organizations utilize a combination of internal staff as well as third-party contractors to maintain this equipment. The lines of demarcation between the organizations and their responsibilities are well-known and managed through existing systems and processes.

#### *2.6.4.1 NYC Department of Information Technology & Telecommunications (DoITT)*

As NYC's communication infrastructure owner/operator, the NYC DoITT will be responsible for the back-office environment through NYCWiN. It will also work with NYCDOT in resolving compatibility issues with NYCWiN's existing IPv4 network backhaul with NYC CVPD system's IPv6 infrastructure. In conjunction with NYCDOT, NYC DoITT will maintain the security and reliability of NYC's communications infrastructure for the NYC CVPD system operation.

#### *2.6.4.2 NYCDOT Traffic Management Center (TMC) Back Office*

The back-office in the NYCDOT TMC will provide the following management functions:

- Managing RSU performance (failure identification, repair, maintenance)
- Managing RSU radio frequency (RF) footprints

- Managing CV application configuration
- Distributing obfuscated data externally to USDOT Independent Evaluator (IE)
- Collecting data from the RSU/ASD
- Aggregating, normalizing, and obfuscating the CV data
- Assessing the NYC CVPD system performance and safety benefits

The support environment for the CV system's core services will include the following elements:

- USDOT Production Security Credentials Management System (SCMS)
- Operational Data Environment (ODE)
- Object Registration and Discovery Service (ORDS)
- Location and Time Source (LTS)
- Service Monitor System (SMS)
- Wide Area Information Disseminator (WAID)

The Security Credential Management System (SCMS), Operational Data Environment (ODE), and Object Registration Discovery Service (ORDS) are expected to be developed and provided by the USDOT. The ODE has replaced the Data Distribution System (DDS) as the platform for routing the data from multiple data sources to a common, integrated format for subscribers to software applications such as CV applications. The Location and Time Source (LTS), Service Monitor (SM) System, and Wide Area Information Disseminator (WAID) will be provided by NYCDOT as the owner of the NYC CVPD system.

The back office facilities at NYCDOT Traffic Management Center (TMC) will not be used for the security credentials management system (SCMS) functions, security enrollment certificates signing, and DSRC messages (BSM, SPaT, MAP, TIM) signing. Instead, these operations will be allocated to the field RSUs as supported by the latest USDOT RSU specification. Another option for consideration entailed utilizing a separate RSU within the TMC in lieu of the back office proxy server for managing the SCMS and signing of the enrollment certificates, pseudonym certificates, and safety messages transmitted by the devices. However, the method of allowing individual RSUs to sign the data has been selected to mitigate risks on schedule and cost.

#### *2.6.4.3 NYCDOT Maintenance Personnel*

The NYCDOT maintenance personnel will be responsible for troubleshooting and repairing faults in the CV equipment software and hardware. The RSUs' operation will be checked for issues by the NYCDOT monitoring personnel who will determine whether site visits and field repairs will be required. Once the issues are diagnosed, the maintenance technicians will be dispatched to the RSU locations, perform the repairs, and report back to the monitoring staff.

The maintenance technician will also monitor the RF footprint of the communication to and from the device. When new firmware version becomes available, the technician will makes sure the firmware update is transmitted from the RSU and installed in the ASD. Also, the CV application configurations will be downloaded and tweaked as needed from the vehicle's OBD II/CAN bus port.

For software and firmware updates, the NYCDOT maintenance staff will work with the TMC to install them via the RSU at each vehicle fleet barn. Once the vehicle returns to its garage after normal operation, the RSU will communicate with the ASD to check its firmware version. When an upgrade is needed, the ASD will request the over-the-air (OTA) firmware upgrade package which will be installed via the RSU.

#### *2.6.4.4 Performance Measurement Manager*

Performance measurement managers will be responsible for checking and validating the daily event log history, the log uploading process, and batch processing of the data. They will be able to determine how much data and how many events are generated and recorded. Also, they will receive the data transmitted from the ASDs and the RSUs and run batch processing to scrub them of any personally identifiable information (PII) including but not limited to time and location.

For establishing and quantifying the NYC performance targets, the NYC performance measurement managers will utilize field observed data and traffic microsimulation software such as Aimsun to model and estimate traffic operations. This allows the calculation of performance metrics from both field data where possible and also from simulated operations of vehicles where that collection of field data is not possible or exceedingly difficult or expensive.

## 2.6.5 Independent Evaluator

Performance measurement users will be responsible for viewing the daily event log history, the log uploading process, and batch processing of the data. They will be able to see and understand how much data and how many events are generated and recorded. Also, they will be the first point people for noticing any anomalies in the CV device operation, such as errors in time synchronization in the ASDs via Global Navigation Satellite System (GNSS) devices.

#### *2.6.5.1 NYCDOT IRB*

NYU will be the IRB and perform the initial assessment of the vehicle and pedestrian data and the ensuing safety benefits. The CV application performance will also be analyzed in consideration of the dense urban environment where intersections are tightly clustered together (e.g. ~250 feet) and location referencing will be a technical challenge due to the “urban canyon effect” from tall buildings and limited views of the GNSS devices.

#### *2.6.5.2 USDOT IE*

The USDOT will engage Texas Transportation Institute (TTI) as the independent evaluator (IE) to analyze the project’s performance with respect to USDOT's goals that may or may not include goals identified by the NYC pilot site. TTI will be responsible for analyzing the processed event data and the safety benefits of the NYC CVPD program. In addition to the safety benefits, the USDOT is interested in exploring what additional benefits such as mobility, environmental, and public agency efficiency are attained with the NYC CVPD. To measure the CV application’s benefits, the project will incorporate a before/after evaluation using the CV equipment installed in fleet vehicles. The ASD equipment will be used to collect information regarding the performance of the CV applications in the project’s geographic and traffic environment.

## 2.7 Assumptions and Dependencies

The fundamental message of the NYC Vision Zero initiative is that death and injury on city streets is not acceptable. These tragedies happen in every community within NYC, to families from every walk of life – from the Upper East Side to the Lower East Side; from Park Slope to Edenwald. They happen to people who drive and to those who bike; but overwhelmingly, the deadly toll is highest for pedestrians – especially children and seniors. The goal of Vision Zero is to eliminate traffic deaths by 2024. The NYC CV Pilot Deployment project will focus on safety improvements for both motorists and non-motorists. In particular, the crash risks increase during nighttime hours when vehicle speeds tend to be higher and it becomes more difficult for vehicle drivers to see pedestrians crossing the roadway.

As the safety statistics indicate, surface improvements on city streets alone will not mitigate the number of crashes, fatalities, and severe injuries long-term. While no Silver Bullet will end all crashes, multiple supplemental tools are needed that can work together to attain Vision Zero's goal. The CV technology is one of these tools and it presents a systematic approach in alerting vehicles of unsafe roadway conditions and prevents collisions with other vehicles, pedestrians, and bicyclists. It will provide numerous safety benefits that facilitate Vision Zero's goals and initiatives.

The following assumptions represent a risk to the project that will affect the ability to meet the schedule or performance goals.

(a.) The *Security Credential Management System* version 1.1 will need to be available and stable by November 1, 2016. USDOT will need to define the specific protocols for all users to incorporate and the certification processes required to ensure equipment meets the standards for security and interoperability.

The protocols and their implementation will need to be able to handle messages at the rate needed for the traffic density in New York City. The response times for the SCMS will have an impact on the system design as to whether credentials need to be managed as store and forward due to the demands for service. Note that this is an important consideration based on the future of the use of the SCMS.

This is a deployment with actual **users in revenue service**; the security must be in place before testing moves to drivers outside the project team.

(b.) How well the DSRC and GNSS will perform in the urban canyon. The team already knows some of the issues from prior projects and preliminary testing. The early acquisition of ASDs will enable continued testing and development throughout Phase 2.

It is also clear that the location "tracking" mechanism needs to continue in an active mode in the urban environment where possible – or many of the freeway applications will be turned off. There are large areas of NYC where there is "something" overhead – it is unfortunate that every time GPS is lost, they all become inactive?

(c.) The Schedule will be met by the selected vendors. The demands on the hardware and the complexity of the software will be unprecedented for connected vehicle equipment. The team will work with vendors to establish realistic schedules and enable as much work in parallel as possible. After development is complete, manufacturing and installing the units will take time.

(d.) The contracting delays and schedule will require that the vendors start much of their work "at risk"; if the city takes 6 months after announcement of award, the vendors will need to

proceed with the development and hardware design “at risk” in order to even come close to meeting the proposed schedule. That is – much of the development, certification, and testing must, of necessity, begin before the City issues a billable contract. It is also likely that the prototypes will be delivered and installed before the contract is issued! Will all of the vendors accept such conditions?

(e.) Review & approval by USDOT of all aspects of the Phase 2 work must be done very quickly and the existing “approvals” of the ConOps, requirements, performance evaluations, SMOC must be used to jump start the development and procurement specifications.

(f.) Data collection in the “Before” period begins May 2018 at the start of Phase 3.

(g.) There is inadequate time [schedule] and budget to deal with a vendor pre-qualification phase and bake-off. We will rely on the responses to the RFEI; the vendor chosen may not be the low bid as we will require further demonstrations prior to award. However, once the vendors have been chosen, the project is at significant risk until the completion of the 100 ASD/10 RSU pre-pilot installation and testing program is successfully completed; if the vendor is ultimately unable to complete this phase successfully, the schedule is at serious risk because of the time required to start with an additional vendor. If we move forward with 2 vendors, the risk is mitigated, but the development costs and integration costs may as much as double.

(h.) USDOT completes its promised tools and utilities – especially for the development of the MAP message (including PED crossings) by the end of 2016.

(i.) The FCC does not change the use patterns for the DSRC band – as this could necessitate a re-design and re-engineering of both the hardware and software.

## 2.8 Operational Scenarios

The operational scenarios are documented in Section 6 of the FHWA-JPO-16-299, Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations (ConOps) - New York City.

# Chapter 3. System Capabilities, Conditions, and Constraints

## 3.1 Physical

The following lists describe the requirements for the physical aspects of NYC CVPD:

### 3.1.1 Construction

The CV device will meet all of the indicated quality requirements listing within this section. Note that mechanical security requirements are covered in the System Security section.

#### *3.1.1.1 Mechanical Requirements*

| ReqID | Requirement Text |
|---|---|
| 203.7.1 | The RSU shall provide evidence of tampering (e.g. opening of the case) through tamper-evident seals on media ports (e.g. USB) and screw holes. |
| 203.7.2 | The ASD shall provide evidence to detect tampering (e.g. opening of the case) through tamper-evident seals on all media ports and screw holes. |
| 203.22.1 | Connected Vehicle equipment mounted externally to the vehicle shall be contained within the envelope defined by the ASD vendor specification. |
| 203.7.3 | The RSU size dimensions shall not exceed 13” h x 13” w x 4” d exclusive of mounting hardware. |

#### *3.1.1.2 Electrical Requirements*

| ReqID | Requirement Text |
|---|---|
| 203.4.1 | The ASD shall operate on the voltage supplied by the host vehicle. |
| 203.16.1 | The current drawn by the ASD shall not exceed with the maximum allowable amperage specified by the ASD vendor. |
| 203.16.2 | The RSU shall not overload the power supplies provided by the RSU vendor based on maximum allowable power consumption. (During operation, turn off, turn on, etc. per NEMA TS2 environmental testing.) |
| 203.17.2 | All connections to the RSU shall be protected from lightening and power surges on the Ethernet. |
| 203.18.1 | The ASDs shall withstand electromagnetic interference (EMI) from external sources and electrical distribution. |

| ReqID | Requirement Text |
|---|---|
| 203.18.2 | The ASD shall withstand electrostatic discharge (ESD) from external sources and electrical distribution. |
| 203.18.3 | The RSU shall withstand electrostatic discharge (ESD) from external sources and electrical distribution. (Provide ESD definitions/specifications.) |
| 203.19.1 | The ASD design shall prevent battery drain. |
| 402.2.2 | The RSU shall be able to resume normal function within 2 minutes of restoration of power. |

## 3.1.2 Durability

The CV device will meet all of the indicated durability requirements listing within this section.

#### *3.1.2.1 Back-up Power*

| ReqID | Requirement Text |
|---|---|
| 203.31.1 | Back office servers shall have their power source augmented by an Uninterruptable Power Supply (UPS). |

#### *3.1.2.2 Repair*

| ReqID | Requirement Text |
|---|---|
| 203.1.1 | The NYC CVPD maintenance personnel shall replace the ASD damaged by improper maintenance, tampering, or mishap. |
| 203.1.2 | The NYC CVPD maintenance personnel shall replace the RSU damaged by improper maintenance, tampering, or mishap. |
| 203.2.1 | The NYC CVPD maintenance personnel shall be able to reboot the ASD after a disruptive software glitch. |
| 203.2.2 | The NYC CVPD maintenance personnel shall be able to reboot the RSU after a disruptive software glitch. |

## 3.1.3 Adaptability

The CV devices will meet all of the indicated adaptability requirements listing within this section. They address how the NYC CVPD system will continue to operate after Phase 3 which may entail system expansion and explain how the system will continue to evolve as new standards, software, and hardware are developed.

| ReqID | Requirement Text |
|---|---|
| 202.2.1 | The NYC CVPD applications shall have modifiable algorithms and software parameters for tuning the system's operation. |
| 202.3.1 | The ASD shall have upgradable hardware components for improving the device performance upon expansion of the NYC CVPD system. |
| 202.3.2 | The RSU shall have upgradable hardware components for improving the device performance upon expansion of the NYC CVPD system. |

### 3.1.4 Environmental conditions

The CV devices will meet all the defined requirements in this section. They will be capable of operating without failure under all environmental conditions experienced in the United States and its territories.

| ReqID | Requirement Text |
|---|---|
| 204.3.1 | The audible message volume in the ASD shall be distinguishable from other sounds. |
| 204.3.2 | The audible message volume in the ASD shall be developed and tested in a real traffic environment. |
| 203.17.1 | The RSU shall be designed to operate properly in the outdoor environment. (e.g. temperature, humidity, rain, fog, sun, snow, shock, vibration, etc.) {Ref augmented NEMA TS2-20XX} |

## 3.2 System Performance Characteristics

The CV device will meet all the defined system performance requirements in this section. Note that the performance requirements will be based on measures of performance collected and analyzed from the NYC CVPD.

| ReqID | Requirement Text |
|---|---|
| 110.2.3 | All NYC CVPD ASDs shall utilize the same GPS time source and common accuracy configuration as the NYC CVPD Infrastructure. |
| 201.5.1 | The ASD shall provide the alerts to the driver without ambiguity. |
| 202.7.1 | The ASD shall process all radio messages at a minimum rate of 10 Hz. |

## 3.2.1 Vehicle Performance Monitoring

| ReqID | Requirement Text |
|---|---|
| 110.2.2 | The ASD shall broadcast the BSM of host vehicles per SAE standards J2945/1 and J2735. |
| 110.2.3 | All NYC CVPD ASDs shall utilize the same GPS time source and common accuracy configuration as the NYC CVPD Infrastructure. |
| 202.4.2 | The Vehicle Performance Monitoring application shall collect/log vehicle operational data (e.g. hard break, steering turns, accelerations based on accelerometers). |
| 202.4.3 | The fleet manager shall be able to solicit and collect feedback from the anonymous vehicle operators on the operation of the system. |
| 202.8.1 | The ASD shall monitor the delivery of the audio alert and any audio instructions to the driver.<br>(Clarification: the monitoring system [internal to the ASD] shall confirm that the actual audio information [sound] was produced in the vehicle and that the audio information matches what the alert was intended to deliver. The purpose of this requirement is detect faulty speaker wiring and damaged speakers that prevent the alert from being delivered to the driver. It is not intended to be an accurate voice to text conversion system, but sufficient to determine that an alert message was delivered.)<br>By way of example, a microphone located at or near the speaker can verify that the specific audio word(s) or tone was presented to the driver; contrarily, simply measuring the voltage output sent to the speaker is not sufficient since the speaker could be damaged or sabotaged. |
| 202.9.1 | The ASD shall include an accelerometer for each of the three axes. |
| 203.26.1 | The ASD shall be able to process (and authenticate and/or encrypt) the DSRC messages at a minimum rate of 10 Hz. This includes all messages on all channels: BSM, TIM, MAP, SPaT, etc. in addition to IP communications traffic for management applications. |
| 204.5.1 | The Host Vehicle ASD shall begin aural alerts within 250 milliseconds of being triggered by the application. |
| 401.1.2 | The ASD shall have sufficient computing power to authenticate messages on the Safety Applications defined in Table C-1 in time for the individual Safety Applications to meet their individual performance requirements. |
| 401.12.1 | The RSU shall interface with signal controllers, NYCWiN, and DSRC messages from vehicles and pedestrians. (Note: this will be expanded into multiple requirements for each interface.) |

## 3.2.2 IE Performance Monitoring

| ReqID | Requirement Text |
|---|---|
| 510.2.1 | The NYC CVPD performance monitoring subsystem shall normalize, obfuscate, aggregate, and analyze the performance measurement data specified in the Task 5 Performance Measurement Plan. |

| ReqID | Requirement Text |
|---|---|
| 510.5.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed data and transmit it to the RDE. |
| 510.6.1 | The NYC CVPD performance monitoring subsystem shall collect and post-process the volume counts from temporary automatic traffic recording (ATR) machines. |
| 510.7.1 | The NYC CVPD performance monitoring subsystem shall compare and post-process the travel time from MiM RFID tag readers. |
| 510.7.3 | The NYC CVPD performance monitoring subsystem shall compare and post-process the travel time from MTA bus GPS datasets. |
| 510.8.1 | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the number of active, inactive, and offline ASDs and RSUs in the field by time of day. |
| 510.8.2 | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the number of CV applications in operation and warnings produced by time of day. |
| 510.8.3 | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the network-wide system safety and mobility measurements. (Note: the reports shall include the crash frequencies and average speeds by peak period.) |
| 510.9.1 | The NYC CVPD performance monitoring subsystem shall provide obfuscated datasets without PII to the USDOT Independent Evaluator for additional evaluation. |
| 510.10.2 | The ASD shall have the capability of operating in active mode and recording normal driver behaviors and reactions while notifying the user of the perceived warnings. |

## 3.2.3 Event Data Recording

As noted above, the ASD is responsible for notifying the driver when there is a threat that is detected by the ASD applications; such threats include those posed by the V2V applications as well as those described by the V2I applications. The requirements listed below are based on the concept of ongoing logging of situational status which is then collected and stored as an encrypted event record that will provide a snapshot of data collected before and after the “event” as outlined herein. The event record is encrypted on the ASD and sent to the analysis server which is part of the NYC CVPD back office systems.

| ReqID | Requirement Text |
|---|---|
| 501.2.1 | The ASD shall include a general purpose event recording application. |
| 501.2.1.1 | The ASD shall include a rotating 5 minute log of the raw data listed in Table G-4. |
| 501.2.1.2 | Once the log has accumulated 5 minutes of data, it shall replace the oldest data with new data such that it always keeps the most recent 5 minutes of data to a 100 ms accuracy. |
| 501.2.1.3 | Each log entry shall include a UTC time stamp accurate to 10 milliseconds. |
| 501.2.1.4 | Each log entry shall include the BSM data for the host vehicle regardless of whether the data has changed. |

| ReqID | Requirement Text |
|---|---|
| 501.2.1.5 | Each log entry shall include the peak accelerometer values since last entry. Clarification: accelerometer entries are added to the log whenever the value changes or at 1 second intervals whichever is shorter but not more rapidly than 10 times per second. Thus, the accelerometer entries show the times at which the value changed with a time stamp but no values are lost to the resolution of 1 second. |
| 501.2.1.6 | Each log entry shall include the BSM data for all vehicles that are within a configurable distance (VDIS) from the host vehicle. (Clarification: typical values are expected to be 0-50 meters.) |
| 501.2.1.7 | A log entry shall be made for each SPaT and MAP message received from two nearest RSUs. |
| 501.2.2 | The ASD shall continuously monitor the location of the host vehicle as described in SAE J2945/1. |
| 501.3.1 | The ASD shall collect log entries into an event record to describe vehicle actions surrounding a CV application event. |
| 501.3.2 | The ASD shall log the SAE J2735 BSMs received at 100 millisecond interval before and after an event. |
| 501.3.3 | The ASD shall log the information 5-300 seconds (configurable by type of event, time period, and resolution) before and 20-50 after the event. |
| 501.3.4 | The ASD shall collect less detailed CV probe data for mobility data collection. (See ASD Demonstration Procurement Specification Version 2.2 Appendix L Mobility Data Section b for clarification.) |
| 501.3.5 | The durations shall have the capability of being modified by the CV application that triggers the warning. |
| 501.3.6 | The safety applications listed in Table C-1 shall implement the most recent event recording parameters supplied externally to the application based on their own recording criteria in Table E-3. |
| 501.4.1 | A safety application shall record events based on the most recently received recording parameters set. |
| 501.4.2 | An application shall trigger an event recording when an alert is triggered. |
| 501.4.3 | The event recording application shall collect pre- and post- trigger information using the host application's trigger recording times. |
| 501.4.4 | The safety applications shall collect trigger information (event recording data) listed in Table G-1. |

## 3.2.4 Event Data Collection

| ReqID | Requirement Text |
|---|---|
| 502.1.1 | When the event recording receives a triggering input, it shall start the creation of an event record. |
| 502.1.2 | Each event record shall indicate the application and the reason that the alarm was created; (Clarification: each triggering event (alarm) will notify the ASD logging system to initiate the creation of an event record and will provide some application specific (e.g. application ID, value which caused the trigger) information (up to XX bytes indicating the reason for the event); this data shall be included in the “header” for the event record.) |
| 502.1.2.1 | The event record data shall be included in the “header” for the event record. |
| 502.1.4 | The before and after times shall be configurable for each different application ID.<br>(Note: different applications may request that the pre and post incident collection times be different from the default.) |
| 502.1.5 | The ASD shall accept downloaded parameters to specify the number of seconds to be included in the event record prior to and after the occurrence of the event for each application ID. (Note that the pre-event and post-event collection times may be different values). |
| 502.1.6 | The event recording application shall be able to simultaneously create and collect event records for up to 10 concurrent or staggered events. Clarification: as one event is concluded, it makes space for additional events. |
| 502.1.7 | The ASD shall be able to upload the event records to (through) an RSU when the service is available. (Clarification: this is expected to use IP communications – but is not specified at this time. The RSU’s located in the barn and at choke points are intended to accomplish this upload process, although this could also be added to any or all of the RSU’s.) |
| 502.1.9 | Event records shall be automatically purged whenever the power is applied to the ASD and the time last log entry is more than a configurable number of hours (example: 96 hours).<br>(Clarification: all of the vehicles for the NYC CVPD are fleet vehicles and hence normally return to their “barn” on a daily basis. However, in some cases, if a fleet vehicle is driven “home” and not returned to a location where an RSU can access its logs, the project would like to recover that data when the vehicle returns to the City if possible without compromising privacy.) |
| 502.1.10 | Log entries shall be inserted in the event log whenever the vehicle engine is running. |
| 510.1.1 | The NYC CVPD performance monitoring subsystem shall count the number of events after the events of applications listed in Table C-1 in the Before and After periods. |

## 3.2.5 Performance Data Collection and Processing

| ReqID | Requirement Text |
|---|---|
| 106.1.1 | The NYC CVPD performance monitoring subsystem shall post-process the mobility data from the I-SIGCVDATA application Before and After periods. |
| 106.1.1.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speed from NYC CVPD for comparison to the legacy detection system. |
| 106.1.1.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average travel time from NYC CVPD for comparison to the legacy detection system. |
| 502.2.1 | The RSUs shall collect the selected mobility data in accordance with Appendix I, section I.3.2 in the NYC CVPD RSU Procurement Specification shall be collected and transmit this data to the TMC for traffic signal timing plan optimization and analysis for new timing plan development. |
| 502.2.2 | The RSU shall record the BSM data from the Host Vehicle (HV) in accordance with Appendix I, Section I.3.1, Number 12, in the NYC CVPD RSU Procurement Specification. |
| 502.2.3 | The BSM data shall be recorded based on distance traveled and time in accordance with Appendix I, Section I.3.1, Number 12, in the NYC CVPD RSU Procurement Specification. |
| 502.2.4 | The BSM data time and distance parameters shall be configurable in accordance with Appendix I, Section I.3.2 in the NYC CVPD RSU Procurement Specification. |
| 503.1.1.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average number of stops. |
| 503.1.1.3 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speeds of the vehicles. |
| 503.1.1.4 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the reduction in speed limit violations Before and After periods. |
| 503.1.1.5 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the speed variations of the vehicles. |
| 503.1.1.6 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the driver actions in response to warnings and vehicle trajectories. |
| 503.1.2 | The NYC CVPD performance monitoring subsystem shall evaluate the change in speed limit adherence, speed variability, and the average segment speed for each vehicle fleet on a given roadway segment for a given time period (cycle length basis) from the Before period to the After period. |
| 503.2.7.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the crash counts and rates of speed-related crashes from police crash databases. |
| 503.2.7.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the lateral collision. |

| ReqID | Requirement Text |
|---|---|
| 503.2.7.3 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the vehicle speeds at curve entry from the Host Vehicle BSM in the event records. |
| 503.2.7.4 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of warnings generated Before and After period. |
| 503.2.8 | The NYC CVPD performance monitoring subsystem shall evaluate whether the number of curve speed violations on each applicable studied roadway segment decreases from the Before period to the After period. |
| 503.3.4.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speed of triggered events at work zone compared to posted speeds. |
| 503.3.4.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the vehicle speed limit violations in variable speed zone areas Before and/or After periods or with/without CV. |
| 503.3.4.3 | The NYC CVPD performance monitoring subsystem shall utilize the data from the crash databases and measure the work zone related crash counts and rates in reduced speed zones. |
| 503.3.4.4 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure time to collision for instantaneous safety in reduced speed zones. |
| 503.3.5 | The NYC CVPD performance monitoring subsystem shall evaluate whether the number of work zone speed violations on each applicable studied roadway segment decrease from the Before period to the After period and with/without CV. |
| 504.1.1 | The NYC CVPD performance monitoring subsystem shall post-process the data surrounding the V2V application events. |
| 504.1.1.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the fatality, injury, and property damage only (PDO) crash rates from external crash database sources. |
| 504.1.2 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reportable vehicle-to-vehicle crashes from the Before period to the Pilot period. |
| 504.2.5.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the bus / right-turn related crash counts and rates. |
| 504.2.5.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure right-turn related conflicts between a bus and another vehicle. |
| 504.2.6 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of bus / right-turn vehicle crashes from the Before period to the Pilot period. |
| 504.3.4.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the red light violation counts and rates. |
| 504.3.4.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the crash counts and rates related to red light violation. |

| ReqID | Requirement Text |
|---|---|
| 504.3.5 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number and severity of red light violations at each studied intersection from the Before period and the Pilot period. |
| 505.1.5.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the pedestrian related crash counts and rates. |
| 505.1.5.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure pedestrian-related conflicts/hard braking events. |
| 505.1.6 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported vehicle-to-pedestrian crashes from the Before period to the Pilot period. |
| 505.2.1.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of pedestrian crossing violation reductions. |
| 505.2.1.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the visually-impaired pedestrian-related crash counts and rates. |
| 505.2.1.3 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the conflicts with visually-impaired pedestrians. |
| 505.2.1.4 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the wait time for crossing at the intersections. |
| 505.2.2 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported crashes involving visually-impaired pedestrians from the Before period to the Pilot period. |
| 506.1.1.1 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the reduction in truck route violations Before and After period. |
| 506.1.2 | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported crashes decrease from the Before period to the Pilot period. |

# 3.3 System Security

The CV device will meet all the defined security requirements in this section.

## 3.3.1 Security Management and Operations

The ***Security Management and Operations Concept*** describes how the NYC CVPD will be employing the SCMS for the applications and the applicable physical security requirements. The project will use [interface to] the SCMS to obtain enrollment certificates for each RSU and each ASD.

As of this writing, there are no established certification requirements and test procedures for the use of the SCMS and for the installation of the enrollment certificate in the devices (RSU, ASD).

Vendors shall be required to certify that their devices conform to the applicable standards for the DSRC communications (IEEE 1609.x, and IEEE 802.11p) and that their message sets conform to the

SAE J2735 and J2945/x for the BSM, SPaT, MAP, and TIM. Since these standards are still in development, the NYC CVPD shall require that the RSU and ASD conform to the standards as adopted by 10/31/2016.

| ReqID | Requirement Text |
|---|---|
| 203.5.2 | If the ASD determines that it has no valid certificates, it shall cease transmission of BSMs. |
| 203.20.1 | The ASD shall prevent incoming messages with invalid conditions per criteria in the IEEE 1609.2 from being acted on. |
| 401.1.1 | The ASD Vehicle Communications wireless link shall have communications security to ensure the authenticity of all its messages in accordance to the standards prescribed by the overall USDOT connected vehicle program. |
| 401.3.1 | The ASD shall carry out plausibility checking on the remote vehicle BSM data. (Definition of plausibility checking needs to be determined.) |
| 401.3.2 | The ASD shall sign its event log file entries using its BSM signing keys. |
| 401.3.3 | The ASD operating system (OS) shall prevent the log file signing application from sending messages on any channel other than those that are identified by by the PSID or WSA for particular service. |
| 401.3.4 | The ASD shall indicate successful receipt of the pseudonym certificates. |
| 401.3.5 | The SCMS supplier shall track the expected expiry times of ASD enrollment certificates. |
| 401.3.7 | When the ASD has no valid BSM signing certificates, it shall store the log file entries as IEEE 1609.2 data of type unsecured. |
| 401.3.8 | The ASD vendor shall replace the ASDs that need to be re-enrolled with newer ASDs. |
| 401.4.4 | The RSU supplier shall provide the serial number and its enrollment certificate for each RSU. |
| 401.4.6 | The RSU-SCMS interface shall allow the RSU to request application certificates with different contents from the current ones during the lifetime of the current ones. |
| 401.6.2 | If a device misbehaves, the SCMS shall blacklist the device and its enrollment certificates and prevent it from obtaining more authorization certificates. |
| 401.7.1 | The ASD shall obtain certificates via IPv6 connectivity through the RSU. |
| 401.7.2 | The RSU shall broadcast the WSA for certificate download on control channel 178 and indicate IPv6 connectivity and the IP address on a service channel other than channel 172 or 178. |
| 401.7.3 | The RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications. |
| 401.7.5 | The RSUs shall support IPv6 tunneling over IPv4. |
| 401.7.6 | Communication between the ASD and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface. (Note: The SCMS interface should not need any further security.) |
| 401.7.7 | The information security manager shall investigate and monitor the data traffic usage to detect unapproved use of the IP connection. |

| ReqID | Requirement Text |
|---|---|
| 401.7.8 | Communication between the RSU and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface. (Note: The SCMS interface should not need any further security.) |
| 401.8.1 | The NYCDOT IT shall address any denial of service (DoS) attacks within each NYC network using its existing practices. (Note: the networks include NYCWiN, CityNet, DOTNet, any network that DoITT is responsible for.) |
| 401.8.2 | The information security manager shall monitor the DSRC communications performance to detect DoS attacks. |
| 401.8.3 | The RSU shall report over a management interface if channel busy ratios go above a configurable threshold. |
| 401.8.4 | The ASD shall log an event report every second for which channel busy ratios go above a configurable threshold. |
| 401.9.1 | The RSU shall operate client-side transport layer security (TLS) and accept only TLS server certificates with specific URLs. |
| 401.9.2 | The RSU shall protect root certificates for client-side TLS against modification and provide other certificates in the chain, which shall not make a separate query to the internet to obtain the entire chain. |
| 401.14.1 | Devices shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS. |
| 401.14.2 | Devices shall support establishment of a standard TLS-based VPN with client authentication for communication to the TMC, with a long-term client cert and a single CA cert trusted to authorize connections from the TMC. |
| 401.14.3 | Devices shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application. |
| 401.14.4 | Devices shall store RF Monitoring log file entries encrypted with an encryption key belonging to the TMC. |
| 401.14.5 | The host processor on the device shall perform and pass integrity checks as specified in requirements 401.14.6 - 401.14.9. |
| 401.14.6 | The integrity checks performed at boot shall use a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified. |
| 401.14.7 | Until all integrity checks on the software and firmware configuration of the host have passed, the device shall not allow a privileged application (as defined in Security Management Operating Concept section 6.1.1) to sign a message. |
| 401.14.8 | If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any application to have access to locally stored private keys. |
| 401.14.9 | If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any privileged application (as defined in Security Management Operating Concept section 6.1.1) to operate. |
| 401.14.10 | The OS on the device shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the HSM. |

| ReqID | Requirement Text |
|---|---|
| 401.14.11 | The OS shall not permit keys designated as private to be read from the HSM. |
| 401.14.12 | The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device. |
| 401.14.13 | All cryptographic software and firmware for the HSM shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification. |
| 401.14.14 | The HSM operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not. |
| 401.14.15 | The HSM operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary. |
| 401.14.16 | The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case). |
| 401.14.17 | All unused media ports (e.g. USB) shall be sealed. |
| 401.14.18 | There shall be no removable media. |
| 401.14.19 | The certificate management service shall start requesting a new certificate or batch of pseudonym certificates a day before the expiry of the current certificate or batch. |
| 401.14.20 | When verifying, the device shall require that 1609.2 signed messages are signed by a certificate that is protected from modification by, or chains back to a certificate that is protected from modification by, the secure boot process. |
| 401.14.22 | A device shall not create or transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it does not currently have valid certificates for that usage scenario |
| 401.14.23 | A device shall verify a DSRC message when any of the following conditions is met:<br>a) A device identifies the message as containing a new DE_TemporaryID value.<br>b) The message results in the issuance of issue either advisory, warning, or alert.<br>c) The remote vehicle constitutes a potential threat (define potential threat as a vehicle that may collide with the host vehicle based on the both vehicle's speeds and trajectories)<br>d) The host vehicle constitutes a threat to a pedestrian using a DSRC equipped Personal Information Device.<br>e) Other potential threat situations such as infrastructure size restrictions, speed compliance, red light violations, and other safety applications.<br>f) Other situations as identified during the Phase 2 Design.<br>Note: Verification consists of meeting the IEEE 1609.2 requirements specified herein this document and the associated message's Security Profile (to be provided in Phase 2). |

| ReqID | Requirement Text |
|---|---|
| 403.2.1 | The ASD shall support a secure session protocol through VPN over TLS to the TMC for protecting the firmware download. |
| 403.2.2 | The RSU shall support a secure session protocol through VPN over TLS to the TMC for protecting the firmware download. |
| 403.3.1 | The ASD shall partition enough storage space for its current and new firmware images. |
| 403.4.1 | The ASD shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted. |
| 403.4.2 | The RSU shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted. |

## 3.4 Information Management

The CV device will meet all the defined information management requirements in this section. These requirements address how the data and information will be protected and encrypted.

| ReqID | Requirement Text |
|---|---|
| 201.1.1 | The ASD event recording shall encrypt each event record. (Clarification: this prevents vehicle identity and determination of whether the vehicle is from the control group or the treatment group.) |
| 502.1.12 | Event records shall only be decrypted by the central performance analysis software. |

## 3.5 System Operations

The CV device will meet all the defined system operations requirements in this section. These requirements describe the limits, ergonomics, usability, and other factors that can affect the operation of the NYC CVPD system.

### 3.5.1 System Human Factors

| ReqID | Requirement Text |
|---|---|
| 204.6.1 | The system administrator shall be able to change the volume level of the audio output (e.g. speakers). |
| 510.10.1 | The ASD shall have the ability to operate in either silent mode or active mode. |
| 510.10.1.1 | The ASD shall record events* without audibly notifying the driver when operating in silent mode. |
| 510.10.1.2 | The ASD shall record events* while audibly notifying the driver when operating in active mode. |

| ReqID | Requirement Text |
|---|---|
| 510.10.1.3 | The ASD shall set the application alert mode to silent mode or active mode per the most recent parameters downloaded. |

## 3.5.2 System Maintainability

| ReqID | Requirement Text |
|---|---|
| 201.4.2 | The TMC staff shall be able to monitor the NYC CVPD system-wide RSU malfunctions. |
| 201.5.2 | The ASD shall have configurable parameters for tuning alert thresholds. |
| 202.6.1 | The Parameter Control functional entity at the TMC shall sign the Parameter Control messages per IEEE 1609.2. |
| 202.6.3 | The Parameter Control functional entity shall meet the highest security requirements for a device of the appropriate class. (Note: this shall be derived via the Confidentiality/Integrity/Availability (CIA) analysis once the application specification is developed in detail.) |
| 202.6.5 | The Parameter Control functional entity shall update the parameter control message signatures daily. |
| 202.6.7 | The Parameter Control message version shall be based on the message payload. |
| 202.6.8 | The ASDs from all suppliers shall implement the same Parameter Control protocol. (Note: Parameter Control protocol will be defined by SAE or by NYC CVPD.) |
| 203.11.1 | The ASD software components shall accommodate failures in hardware or in adjacent software modules in a way that does not pose hazards. |
| 203.28.1 | The TMC staff shall be able to monitor the NYC CVPD system-wide ASD malfunctions. |
| 401.5.1 | All devices shall carry no more than two weeks' worth of operating certificates. |
| 401.5.2 | The day before a new week becomes valid; the devices shall download the next week's worth of certificates. |
| 401.7.4 | Mobile devices in need of certificate update shall switch to the advertised channel. |
| 401.11.1 | A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages received.<br>(Note: the only exception to this is a firmware update in which case faulty software could violate this requirement.) |
| 401.11.2 | A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages transmitted. |
| 402.3.1 | The NYC CVPD performance monitoring subsystem shall measure the RF received range of each ASD. |
| 402.3.2 | The NYC CVPD performance monitoring subsystem shall measure the RF monitoring range of the RSU. |
| 404.1.1 | The ASD shall include a threat arbitrator for advisories and alerts presented to the driver in cases where multiple safety advisories are indicated simultaneously. |

| ReqID | Requirement Text |
|---|---|
| 405.1.1 | The ASD shall allow recording of the RF signal level for any message received. (For example, clarification: when the ASD hears a BSM from another vehicle, it will measure and record the RF level of the received message.) |
| 405.1.2 | The ASD shall record the first BSM it hears from each unique ASD ID along with its own location (X,Y,Z) and RF level information. |
| 405.1.3 | The ASD shall record the first MAP message it hears from each RSU ID along with the contents of its own location (X,Y,Z) at the time and the RF level. |
| 405.1.4 | The ASD shall record the first SPaT message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time and the RF level. |
| 405.1.5 | The ASD shall record the last MAP message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time and the RF level. |
| 405.1.6 | The ASD shall record the last SPaT message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time of receipt and the RF level. |
| 405.1.7 | The ASD RF Log Entries shall be stored in the ASD local memory. |
| 405.1.8 | The ASD RF log entries shall be purged after 7 days. |
| 405.1.9 | The ASD RF log space shall be sufficient to store 7 days of interactions with 3,000 ASDs and 450 RSUs, equivalent to about 2,000 entries per day. |
| 405.1.10 | If the ASD RF log files exceed the space allocated (Req 405.1.9), then the oldest data shall be written over without damaging newer log files. (Note: the ASD Ethernet port will be fully blocked after certification testing.) |
| 405.1.11 | The following requirements shall apply to the ASD RF data monitoring, uploading, and purging. |
| 405.1.11.1 | The ASD shall monitor the control channel (178) when the ASD encounters an RSU that supports the RF data upload. |
| 405.1.11.2 | The ASD shall upload the contents of the RF logs to the back office systems. |
| 405.1.11.3 | The ASD shall purge the logs after they have been acknowledged by the RSU. |
| 405.1.12 | The ASD shall authenticate all transactions to retrieve the RF logs. |
| 405.2.1 | The static RSU shall record the first BSM message it hears from each ASD along with the time and the RF level. |
| 405.2.2 | The static RSU shall record the last BSM message it hears from each ASD along with the time and the RF level. |
| 405.2.3 | The RSU shall upload the data to the back office system whenever its buffers are full or more than 60 minutes old. |
| 405.2.4 | Once the RF log data is received and acknowledged by the back office system, it shall be purged from the RSU. |
| 405.2.5 | The RSU shall authenticate all transactions to retrieve its RF logs. |
| 405.2.6 | The RSU shall allow recording of the RF signal level for any message received. (For example, clarification: when the RSU hears a BSM from any vehicle, it shall be able to measure and record the RF level of the received message.) |

| ReqID | Requirement Text |
|---|---|
| 405.2.7 | The mobile RSU shall record the first BSM message it hears from each ASD along with the time and the RF level only when it is stopped. |
| 405.2.8 | The mobile RSU shall record the last BSM message it hears from each ASD along with the time and the RF level only when it is stopped. |

#### *3.5.2.1 Functional Safety Requirements*

The following requirements are based on the functional safety requirements listed in Appendix C of the ***Safety Management Plan***. Maintainability requirements from measures of effectiveness that reflect mean time, mean time to failure, etc. are defined.

| ReqID | Requirement Text |
|---|---|
| 102.5.33 | The ASD shall have access to Intersection IDs where the Pedestrian Detection equipment exists. |
| 201.5.1 | The ASD shall provide the alerts to the driver without ambiguity. |
| 201.6.1 | The RSU shall broadcast the regulatory speed information to the ASD. |
| 203.6.3 | The RSU shall broadcast the location of a curve and other details to support the CSPD-COMP application. |
| 203.6.4 | The RSU shall broadcast the location of a static work zone to support the SPDCOMPWZ application. |
| 203.6.5 | The RSU shall broadcast the location of a moving work zone to support the SPDCOMPWZ application. |
| 203.6.6 | The RSU shall broadcast the location of a school zone to support the SPDCOMPWZ application. |
| 203.6.7 | The RSU shall broadcast the location of a roadway's vehicle size restriction to support the OVC application. |
| 204.4.1 | The NYC CVPD HMI shall communicate alerts to the driver through auditory devices. |
| 204.4.4 | The NYC CVPD HMI shall communicate evacuation information to the driver through auditory alerts. |
| 404.1.2 | The ASD shall incorporate a prioritization scheme as defined in the current version of J2735 for messages such that safety-enhancing messages will have priority over non-safety-enhancing messages. |
| 404.2.1 | The CV applications in the ASD shall run concurrently. |
| 404.2.2 | The CV applications shall prioritize alerts based on GPS location accuracy to prevent false and missed alarms from being triggered. |
| 404.3.1 | The ASD shall determine the threat arbitration rules for addressing multiple events occurring nearly simultaneously by the specific vehicle type (light-duty, bus, truck/commercial vehicle). |

### 3.5.3 System Reliability

| ReqID | Requirement Text |
|---|---|
| 402.1.1 | The ASD shall revert to a fail-safe mode as specified in Table F-2 when unable to perform its normal operations. |
| 402.1.2 | The RSU shall revert to a fail-safe mode as specified in Table F-2 when unable to perform its normal operations. |
| 402.1.3 | The ASD shall report a self-diagnosed failure of itself or one of its software modules (1) to an RSU attempting to install new firmware or parameters and (2) to a device connected to the ASD's maintenance port. |
| 402.1.4 | The RSU shall report a self-diagnosed failure through NYCWiN at the TMC. |

## 3.6 Policy and Regulation

The CV device will meet all the defined policy and regulation requirements in this section.

### 3.6.1 Maintenance

| ReqID | Requirement Text |
|---|---|
| 203.14.1 | The ASD interface design and test before production shall address poor choice of color, icon shape, location, or sound. |
| 203.15.2 | The ASD installation procedure shall stipulate wire routing. |
| 401.2.7 | The RSU shall meet the USDOT certification requirements as defined in TBD prior to September 15, 2016. (Note: this will be detailed in the design phase.) |

## 3.7 System Life Cycle Sustainment

The CV device will meet all the defined system life cycle sustainment requirements in this section.

| ReqID | Requirement Text |
|---|---|
| 401.2.6 | The ASD shall meet pre-determined certification criteria based on procurement documents. |

## 3.8 Application Requirements

The CV device will meet all the defined application requirements in this section.

## 3.8.1 Common Application

| ReqID | Requirement Text |
|---|---|
| 110.1.1 | The Safety Application shall function in vehicle classes in which it is to be installed in the NYC CVPD. (Note: NYC CVPD vehicles are specified in the USDOT ASD Design Specification v3.1.) |
| 110.1.2 | The Safety Application shall function in weather (pavement and atmospheric) and lighting conditions anticipated for the NYC CVPD. (Note: NYC CVPD operational weather conditions are specified in the USDOT ASD Design Specification v3.1.) |
| 110.1.3 | The Safety Application shall function on NYC CVPD roadways. (Note: NYC CVPD roadways are identified in the NYC CVPD ConOps.) |
| 110.1.4 | The Safety Application shall obtain vehicle position data whose accuracy supports the application's calculations for issuing advisories and alerts. |
| 110.1.5 | The Safety Application shall not interfere with other in-vehicle safety systems. |
| 110.1.6 | The Safety Application shall use advisories and alerts that conform to human factors guidelines issued by the FHWA, NHTSA, and SAE. |
| 110.1.7 | The Safety Application shall perform self-diagnostics upon power up and at TBD intervals when the vehicle is operating. (Note: Self-Diagnostics refers to the ability of the Safety Application to determine whether it is capable of performing its intended function. This will be detailed in the design phase.) |
| 110.1.8 | The Safety Application shall determine the operating level/mode of operational, degraded, or failure based on the results of a self-diagnostic test. |
| 110.1.9 | The Safety Application shall set the operational status corresponding to the operational level mode as follows:<br>1. Operational – online<br>2. Degraded – online<br>3. Failure – offline |
| 110.1.10 | The Safety Application shall log self-diagnostic test failure which contains, at a minimum, the following information:<br>1. Date and time of test failure<br>2. Additional information to the nature of a failed test |
| 110.1.11 | The Safety Application shall maintain historical information of self-diagnostic test failures for a predetermined period in non-volatile storage. (Note: Non-volatile storage refers to storage that remains intact even when there is no power. It is left up to the implementer to determine if the retention of data is a fixed window of time, if it is based on a fixed amount of storage, or if it is until cleared.) |
| 110.1.12 | The Safety Application shall take itself off-line when the operating level/mode is failure. |
| 110.1.13 | The Safety Application shall restore or maintain itself on-line when the operating level/mode is either operational or degraded. |
| 110.1.14 | The Safety Application shall perform effectively for all defined NYC CVPD functional classes of roadway and levels of service (LOS) where the application is installed or is being used. (Note: NYC CVPD functional classes of roadway and levels of service are specified in the NYC CVPD ASD Specification.) |

| ReqID | Requirement Text |
|---|---|
| 110.1.15 | The Safety Application shall be able to receive and decode messages broadcast by NYC CVPD RSU. (Note: NYC CVPD RSU is specified in the NYC CVPD RSU Specification.) |
| 110.1.16 | The V2I Safety Application alerts shall only be issued when the current inputs to the application warrants an advisory or alert. |
| 110.1.17 | Safety Application Driver Training shall conform to human factors guidelines issued by the FHWA, NHTSA, and SAE. |
| 110.1.18 | The Safety Application shall not provide information to the driver that conflicts with infrastructure roadside signage. |
| 110.1.19 | The safety application shall provide its operational status (online, offline) to the ASD management system. |
| 110.1.20 | An application shall receive intersection geometry information, e.g. Geometric Intersection Design (GID), from the closest MAP message based on the host vehicle's current location. |
| 110.1.21 | The application shall obtain vehicle speed from one of the sources available to the ASD. These sources include the CAN interface, GNSS interface, derivation from sequential GNSS location readings. |
| 110.3.1 | The safety applications listed in Table C-1 shall acquire vehicle position accuracy, speed, and heading to the ASD. |
| 110.3.2 | The safety application listed in Table C-1 shall determine if the ASD Position, speed and heading information provided is sufficiently accurate to support the ASD's advisory and alert calculations. |
| 110.3.3 | The safety applications listed in Table C-1 shall only issue advisories and alerts if the ASD Position, speed and heading information provided is sufficiently accurate to support the ASD's advisory and alert calculations. |
| 110.3.4 | The safety applications listed in Table C-1 shall acquire roadway geometry information for the roadway ahead from the ASD. (Note: roadway geometry information is expected to come from MAP messages acquired by the ASD from NYC CVPD DSRC Infrastructure.) |
| 110.3.4.1 | The V2I safety applications listed in Table C-1 except for CSPD-COMP and SPDCOMPWZ applications shall acquire the roadway geometry information through the MAP message from the RSUs. |
| 110.3.4.2 | The CSPD-COMP and SPDCOMPWZ applications listed in Table C-1 shall acquire the roadway geometry information through the TIM message from the RSUs. |
| 110.3.5 | The safety applications listed in Table C-1 shall acquire the posted speed for the roadway ahead, including upcoming curve(s). (Note: Posted speed information is expected to come from MAP messages acquired by the ASD from NYC CVPD DSRC Infrastructure.) |
| 110.3.5.1 | The V2I safety applications listed in Table C-1 except for CSPD-COMP and SPDCOMPWZ applications shall acquire the posted speed information through the MAP message from the RSUs. |

| ReqID | Requirement Text |
|---|---|
| 110.3.5.2 | The CSPD-COMP application listed in Table C-1 shall acquire the posted speed for the upcoming curved section of a roadway through the TIM message from the RSU. |
| 110.3.5.3 | The SPDCOMPWZ application listed in Table C-1 shall acquire the posted speed for the upcoming work zone through the TIM message from the RSU. |
| 110.3.6 | Issuance of the CSPD-COMP and SPDCOMPWZ application advisory of a reduced speed curve ahead to the driver shall coincide with driver visibility of roadside curve ahead signage. (Note: Location of roadside signage and sign visibility distances are described in the MUTCD.) |
| 110.3.7 | The safety application shall acquire data from the ASD which includes the following:<br>1. Vehicle positioning information<br>2. Vehicle position accuracy<br>3. Vehicle speed<br>4. Vehicle acceleration<br>5. Vehicle heading |
| 201.2.1 | The V2V safety applications shall set the message threshold at the proper level. |
| 201.2.2 | The V2V safety applications shall formulate the decision algorithm properly to recognize the threat. |
| 201.2.3 | The V2V safety applications shall ensure that all components of the system are functioning as intended. |
| 201.3.2 | The V2I safety applications shall operate on correct, timely information. |
| 201.4.1 | The NYC CVPD safety management subsystem shall verify the initial data entry from the V2I safety applications. |
| 202.1.3 | The safety applications listed in Table C-1 shall implement the most recent application control parameters supplied externally to the application as described in Table E-1. |
| 202.1.4 | The safety application shall allow the central system to modify the control parameters as defined in Table E-1. |

## 3.8.2 V2V Application

#### *3.8.2.1 Forward Crash Warning*

| ReqID | Requirement Text |
|---|---|
| 102.1.1 | The FCW safety application shall warn drivers of impending rear-end collisions with other DSRC-equipped vehicles. |

#### *3.8.2.2 Emergency Electronic Brake Light*

| ReqID | Requirement Text |
|---|---|
| 102.2.1 | The EEBL safety application shall warn drivers about DSRC-equipped vehicles braking. |

#### *3.8.2.3 Blind Spot Warning*

| ReqID | Requirement Text |
|---|---|
| 102.3.1 | The BSW safety application shall warn drivers about DSRC-equipped vehicles in their blind spots. |

#### *3.8.2.4 Lane Change Warning*

| ReqID | Requirement Text |
|---|---|
| 102.3.2 | The LCW safety application shall warn drivers about DSRC-equipped vehicles changing lanes in the same direction. |

#### *3.8.2.5 Intersection Movement Assist*

| ReqID | Requirement Text |
|---|---|
| 102.4.1 | The IMA safety application shall warn drivers about DSRC-equipped vehicles that cross the intersection. |

#### *3.8.2.6 Vehicle Turning Right in Front of a Transit Vehicle*

| ReqID | Requirement Text |
|---|---|
| 102.5.4 | The VTRW application shall detect whether a vehicle is turning right in front of transit vehicle via the position and heading data received in a basic safety message (from a remote vehicle) based on the PVT accuracy for positioning. |
| 102.5.5 | The application alert mode in the VTRW application shall be active when the transit vehicle stops within a bus stop geographic zone. |
| 102.5.6 | The application alert mode shall terminate when the transit vehicle stops within a bus stop geographic zone. |
| 102.5.7 | The VTRW application shall only issue alerts to the driver when the transit vehicle indicates an impending crash. |
| 102.5.8 | A VTRW application shall advise if a remote vehicle which originates directly behind the transit vehicle at a bus stop begins to pass to the left of the transit vehicle as the transit vehicle is departing a bus stop. |

| ReqID | Requirement Text |
|---|---|
| 102.5.9 | A VTRW alert shall alert the driver if a remote vehicle which originates directly behind the transit vehicle at a bus stop passes to the left of the transit vehicle as the transit vehicle is departing a bus stop and the remote vehicle's position and heading indicates an intent to return to or cross the lane of the transit vehicle. |
| 102.5.17 | The VTRW application shall present the alerts regardless of traffic signal status. |
| 102.5.26 | The VTRW application shall have access to the transit vehicle's gear position. |

## 3.8.3 V2I Application

### *3.8.3.1 Speed Compliance*

| ReqID | Requirement Text |
|---|---|
| 101.1.2 | The SPDCOMP application shall obtain regulatory speed limits from the MAP message per SAE J2735-201603 based on the host vehicle's current location. |
| 101.1.4 | The SPDCOMP application shall trigger an alert when either the vehicle speed exceeds the recommended speed by a configured amount or for a configured period of time by time of day. (Note: configurable speed (Excessive Speed Amount Threshold), configurable time (Excessive Speed Time) are defined in Table E-1 and time of day is defined in Table D-1 in the Appendix). |

### *3.8.3.2 Curve Speed Compliance*

| ReqID | Requirement Text |
|---|---|
| 101.2.10 | The CSPD-COMP application shall determine if there is a curve with reduced speed ahead. |
| 101.2.11 | The CSPD-COMP application shall advise the driver of a curve with reduced speed ahead. |
| 101.2.14 | The CSPD-COMP application shall determine the difference between the posted speed on the upcoming curve and the vehicle's current speed. |
| 101.2.15 | If the vehicle speed is greater than the posted curve speed, the Vehicle CSPD-COMP Application shall advise the driver in time for the driver to reduce vehicle speed to the posted speed limit before the vehicle enters the curve. |
| 101.2.16 | While the vehicle is in the curve, the CSPD-COMP application shall trigger a driver alert when the host vehicle speed exceeds the posted speed plus the Excessive Curve Speed Amount Threshold for a time period exceeding the Excessive Curve Speed Time Threshold. |

#### *3.8.3.3 Speed Compliance / Work Zone*

| ReqID | Requirement Text |
|---|---|
| 101.3.9 | The SPDCOMPWZ application shall acquire the following from Speed Zone information for use in SPDCOMPWZ advisory and alert calculations:<br>1. Posted Reduced Speed Zone Speed Limit<br>2. Work Zone geometric information |
| 101.3.10 | The SPDCOMPWZ application shall determine if there is a reduced speed zone ahead. |
| 101.3.11 | The SPDCOMPWZ application shall advise the driver of a reduced speed zone ahead. |
| 101.3.13 | The SPDCOMPWZ application shall determine the speed of the host vehicle based on accuracy and (configurable) threshold per J2945/1. |
| 101.3.14 | The SPDCOMPWZ application shall determine the difference between the posted speed on the upcoming reduced speed zone and the vehicle's current speed. |
| 101.3.15 | If the vehicle speed is greater than the reduced speed zone, the SPDCOMPWZ application shall advise the driver in time for the driver to reduce vehicle speed to the posted speed limit before the vehicle enters the zone. |
| 101.3.16 | The SPDCOMPWZ application shall determine if the vehicle exceeds the Work Zone Posted Speed plus the Excessive Zone Speed Amount Threshold, for a period exceeding the Excessive Zone Speed Time Threshold. |
| 101.3.17 | While the vehicle is in the speed zone, the SPDCOMPWZ application shall trigger a driver alert when the vehicle speed exceeds the Work Zone Posted Speed plus the Excessive Zone Speed Amount Threshold, for a period exceeding the Excessive Zone Speed Time Threshold. |

#### *3.8.3.4 Red Light Violation Warning*

| ReqID | Requirement Text |
|---|---|
| 102.6.1 | The RLVW Application shall receive the SPaT and MAP data sent by the RSUs to the vehicles deployed along the NYC CVPD corridors as per J2735. |
| 102.6.2 | The RLVW application shall use the same time source as infrastructure SPaT applications. |
| 102.6.9 | The RLVW application shall acquire SPaT information, through the Host Vehicle ASD, from the intersection RSU and signal controller at a signalized intersection within RSU's DSRC range and in the vehicle's direction of travel. |
| 102.6.10 | The RLVW application shall acquire the location of the stop bars at signalized intersections at which RLVW is operating from the intersection MAP Message. |

| ReqID | Requirement Text |
|---|---|
| 102.6.11 | The RLVW application shall acquire the following from Intersection SPaT messages for use in RLVW advisory and alert calculations:<br>1. Intersection geometric information<br>2. Signal Phase and Timing information of the traffic signal at the Intersection<br>3. Intersection status of the traffic controller<br>4. Traffic law restrictions for the intersection |
| 102.6.12 | The Vehicle RLVW Application shall be inactive if one or more of the following conditions occur:<br>1. Vehicle position and accuracy information is not available<br>2. Vehicle Speed is not available<br>3. Communication failure between Vehicle and Infrastructure<br>4. SPaT information is not available<br>5. MAP information is not available<br>6. Vehicle Heading information is not available |
| 102.6.13 | The RLVW application shall calculate if a vehicle will violate the Red Light stop bar at a signalized intersection based on its current speed, heading, acceleration, location, location of stop bars, stop bar tolerance and yellow duration tolerance. |
| 102.6.14 | The RLVW application shall trigger a driver alert for a vehicle approaching a signalized intersection when it determines that a stop is required and the vehicle will violate the Red Light stop bar at a signalized intersection based on its current speed, heading, acceleration, location and the location of stop bars. |
| 102.6.15 | The RLVW application shall alert drivers in time for the driver to take action for a required stop at a signalized intersection. |
| 102.6.16 | The RLVW Application shall not alert the driver if the vehicle has safely stopped at the intersection and subsequently accelerates such that a violation occurs. |
| 102.6.18 | The RLVW application shall acquire the following from Intersection MAP messages for use in RLVW advisory and alert calculations:<br>1. Intersection geometric information<br>2. Signal Phase and Timing information of the traffic signal at the Intersection<br>3. Intersection status of the traffic controller<br>4. Traffic law restrictions for the intersection |

#### *3.8.3.5 Oversize Vehicle Compliance*

| ReqID | Requirement Text |
|---|---|
| 103.1.1 | The ASD shall advise the driver of a potential crash before the bridge, overpass, or tunnel to exit the restricted roadway and find an alternate route. (Note: Advisory Distance Threshold Parameter is defined in Table E-1 in the Appendix.) |
| 103.1.2 | The ASD shall warn the driver of an impending crash before the over-height bridge, overpass, or tunnel to stop the vehicle completely and avoid the crash. (Note: Warning Distance Threshold Parameter is defined in Table E-1 in the Appendix.) |

| ReqID | Requirement Text |
|---|---|
| 103.2.1 | The OVC application shall calculate whether or not the vehicle is at risk of crash by comparing the vehicle's height and the height of the roadway restriction. |
| 103.3.1 | The OVC application shall utilize the host vehicle's pre-established height in determining whether to alert the driver. |
| 103.3.2 | The OVC application shall determine the location of the vehicle relative to the location of the size-restricted or weight restricted roadway. |
| 103.3.3 | The RSU shall contain the roadway's clearance height and communicate it to the ASD via DSRC. |

#### *3.8.3.6 Emergency Communications and Evacuation Information*

| ReqID | Requirement Text |
|---|---|
| 105.1.2 | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of vehicles receiving emergency information Before and After periods. |

#### *3.8.3.7 Pedestrian in Signalized Intersection Warning*

| ReqID | Requirement Text |
|---|---|
| 104.1.5 | A PEDINXWALK alert shall be displayed if a pedestrian has been detected in a crosswalk that intersects the Transit Vehicle’s planned forward, left or right turn route at the intersection. |
| 104.1.7 | The Pedestrian Detector shall send a pedestrian detected signal when a pedestrian is present in the crosswalk it monitors. |
| 104.1.8 | The Pedestrian Detectors shall be pole mountable. |
| 104.1.10 | The PEDINXWALK System Latency for pedestrian detection shall be no more than 2 seconds from detecting pedestrian to alert. |
| 104.1.12 | The PEDINXWALK application shall receive Signal Phase and Timing for Pedestrian Lanes and Pedestrian presence detection from the SPaT system. |

## 3.8.4 I2P Application

#### *3.8.4.1 Mobile Accessible Pedestrian Signal System*

| ReqID | Requirement Text |
|---|---|
| 104.2.3 | The PED-SIG application shall correctly discern the pedestrian's position and intended crossing direction. |
| 104.2.4 | The PED-SIG application shall provide status of the walk signal in the intended direction. |

| ReqID | Requirement Text |
|---|---|
| 104.2.7 | The PED-SIG application shall advise (via audio) the pedestrian how to use the application. |
| 104.3.1 | The PED-SIG application shall receive intersection geometry information from the RSU based on J2735-201603. |
| 104.3.2 | The PED-SIG application shall use the intersection geometry information to determine the pedestrian's orientation. |
| 104.3.3 | The PED-SIG application shall use the intersection geometry information provided by the MAP message to determine the crosswalk geometry of the intended crossing. |
| 104.3.8 | The PED-SIG Application shall determine the intended crossing time from the intersection geographic information (distance) and the expected pedestrian travel rate (configurable). |
| 104.3.9 | The PED-SIG application shall collect data on the map error status notification. (partial, unable to detect). (Note: this is intended to assist the system in troubleshooting problems; the quality of the MAP data is critical to the application and this requirements ensures that such issues are made known to the central system for correction. This assumes that the application notifies the PED whenever it encounters a geographic computation error.) |
| 104.4.6 | The PED-SIG application on the PID shall acquire credentials from the SCMS that will allow it to authenticate the SPaT and MAP messages received. |
| 104.4.8 | The SCMS shall be able to set service specific permissions associated with the future support of pedestrian requests from the PID. |
| 104.4.10 | Applications on the PID shall be able to sign messages transmitted to the RSU. |
| 104.4.11 | Applications shall be capable of including a unique ID which shall remain stable (unchanged) throughout the PID's interaction with a single intersection. |
| 104.5.1 | The PED-SIG application shall provide information to the pedestrian based on the content of the SPaT and MAP message at the nearest intersection. |
| 104.5.2 | The Application on the PID shall assist the pedestrian in determining his/her orientation. (Note: Definition of orientation: to understand which street crossing the pedestrian is facing.) |
| 104.5.3 | The PID application shall provide information to the pedestrian regarding the availability of PED support services at the intersection. (If there is an RSU) |
| 104.5.4 | Application shall provide information to the pedestrian indicating the status of the pedestrian signal for the intended crossing including walk time remaining, clearance time remaining, and time until the next walk signal is expected. |
| 104.5.6 | The PED Applications shall allow the pedestrian to configure selected parameters and characteristics such as sound volume, voice commands, and walking speeds. |
| 104.5.8 | The application shall notify the pedestrian if there is a preemption or priority change (TSP) operation taking place which may disrupt the signal timing. |
| 104.5.9 | The PED application shall collect DSRC RF receive levels. (Note: this is for analysis of the reliability of the RSU to PED messages and the PED to RSU messages.) |

| ReqID | Requirement Text |
|---|---|
| 104.5.10 | The Application shall calculate intersection crossing information based on pedestrian's origin, destination, departure range, arrival range. (Note: this is for coordination of signal timing phase.) |
| 104.5.11 | The PED-SIG Application shall collect the performance data listed in Table G-3. |
| 104.5.13 | The Application shall collect metadata that includes the date and time when system information was generated. |
| 104.5.14 | The PED-SIG application shall receive signal timing and controller status from the RSU through the SPaT message. |
| 104.5.18 | Every PID shall be able to change signing keys per SAE J2945/9 Section 6.6. (Note: the signing will be static during interactions with a single intersection.) |
| 104.6.2 | The PED-SIG application shall continuously notify the user that it is operating. |
| 104.6.3 | The PED-SIG application shall be able to provide requested information within 10 seconds. |
| 104.6.3.1 | If the delay will be longer than 10 seconds, then the PED-SIG application shall provide information indicating how long it is expected to complete the operation. |
| 104.6.4 | The applications shall be able to measure and log the time required to provide the pedestrian the information. |
| 104.6.11 | The PID device shall be able to function in a communication-saturated environment. |
| 104.8.4 | The PID system shall ensure geo-location information is used for PED-SIG application only. |
| 104.8.9 | All data transmitted between the PID and the NYU server shall be encrypted to protect any personal information. |
| 104.8.10 | Data stored by the NYU server or exported for independent evaluation shall be processed to remove any personal information and any attributes including exact location and exact time such that the data cannot be associated with a particular person or event. |
| 104.9.4 | The PID shall use the channel assignments defined in Table F-1. |

# Chapter 4. System Interfaces

This section contains the interface requirements of the NYC CVPD components and their external capabilities.

## 4.1 Global Navigation Satellite System (GNSS)

| ReqID | Requirement Text |
|---|---|
| 401.17.1 | Each DSRC device shall obtain its time and position from the GNSS per the requirements of J2945/1 Section 6.2. |

## 4.2 Location Correction

### 4.2.1 Triangulation for ASD Location Accuracy

| ReqID | Requirement Text |
|---|---|
| 401.15.3 | RSUs shall exceed 802.11 ACK requirements in the following manner: Antenna referenced ACK turnaround time must be in (SIFS-12.5, SIFS+12.5) ns 95% for cable tested non-CSD signals. Note that any RSU employing the NXP based SAF5200 will support this by default. The position provided by the WSA shall be provided by the central system based on the 3D surveyed position. |

## 4.3 Network Time Reference

| ReqID | Requirement Text |
|---|---|
| 401.16.1 | Devices unable to receive timing information per J2945/1 Section 6.2 shall set their time from an authenticated time reference using the Network Time Protocol Version 4 per Internet Engineering Task Force RFC 5905-5908. |

## 4.4 Security Credential Management System (SCMS)

Note that other security requirements are listed in Section 3.3 System Security.

| ReqID | Requirement Text |
|---|---|
| 401.2.1 | The device supplier shall provide devices provisioned with valid enrollment certificates. |
| 401.2.2 | The device supplier shall provide devices that meet the interface requirements of the USDOT's certification program. |
| 401.6.3 | The SCMS shall maintain the blacklist internally. |
| 401.6.4 | The back office system shall acquire one SCMS certificate from each installed DSRC device and associate this certificate with the installed DSRC device. (Note: this requirement is temporary and will become obsolete after the SCMS deploys misbehavior detection and reporting features.) |
| 401.6.5 | The back office system administrator shall provide a DSRC device's acquired SCMS certificate when requesting that the SCMS registration authority add the associated DSRC device to the Certificate Revocation List (CRL). (Note: this requirement is temporary and will become obsolete after the SCMS deploys misbehavior detection and reporting features.) |
| 401.14.21 | Devices shall implement certificate download per the SCMS Interface (detailed requirements to be derived during Phase 2 as the final interface document is not yet published) |
| 403.1.1 | The device supplier shall sign the firmware images and manage the certificate management process for the firmware images. |
| 403.1.1.1 | The SCMS certificate shall have a lifespan of 3 years instead of weeks. |
| 403.1.1.2 | The SCMS signature scheme shall provide at least 128-bit security. |

## 4.5 Object Registration and Discovery Service (ORDS)

As stated in Chapter 2, the ORDS is expected to be developed and provided by the USDOT. Its requirements will be detailed in the design phase.

## 4.6 Data Distribution System (DDS)

As stated in Section 2.1, the ODE has replaced the Data Distribution System (DDS) as the platform for routing the data from multiple data sources to a common, integrated format for subscribers to software applications such as CV applications. However, at this time the USDOT ODE is not expected to play a role and interact directly with the NYC CVPD system. Its requirements will be detailed in the design phase.

## 4.7 Research Data Exchange (RDE)

| ReqID | Requirement Text |
|---|---|
| 510.11.1 | The interface for transferring performance measurement information to the USDOT Research Data Exchange (RDE) shall be negotiated by the NYC CVPD project team and the USDOT RDE operators during the detailed design of the system in Phase 2. |

## 4.8 National Weather Service

| ReqID | Requirement Text |
|---|---|
| 510.5.1 | The NYC CVPD performance monitoring subsystem shall collect hourly weather data observations from the following National Weather Service (NWS) stations in NYC:<br>• Central Park (KNYC)<br>• Kennedy International Airport (KJFK)<br>• LaGuardia Airport (KLGA) |
| 510.5.1.1 | The NYC CVPD performance monitoring subsystem shall obtain the weather data listed in Table G-2. |

## 4.9 Foreign Dedicated Short Range Communications Devices

| ReqID | Requirement Text |
|---|---|
| 110.4.1 | Foreign light-duty vehicles shall transmit DSRC BSM messages in accordance with the J2945/1 standard. |
| 110.4.2 | Foreign trucks shall transmit DSRC BSM messages in accordance with the J2945/1 and shall contain the following Part II SupplementalVehicleExtensions objects: classification, and vehicleData (height and mass) as defined in J2735 Section 6.133. |

## 4.10 Vehicle Data Bus

| ReqID | Requirement Text |
|---|---|
| 102.5.27 | The ASD shall have access to the host vehicle's brake status. |
| 202.4.1 | The ASD shall monitor the items in Table E-5 on the in-vehicle network. |
| 203.12.1 | The ASD shall utilize the OBD-II port, J-bus, or CAN bus. |

| ReqID | Requirement Text |
|---|---|
| 203.12.2 | The ASD shall conform to the associated SAE interface requirements for OBD-II port, J-bus, or CAN bus. (Clarification: the intent of this requirement is to prevent the ASD from interfering with other in-vehicle systems.) |
| 203.12.3 | The application in the ASD shall collect and process vehicle-related information through a direct connection or a splitter cable. (Note: individual application data needs will be addressed through each application's requirement.) |
| 203.25.1 | The ASD interface to the CAN bus shall not degrade or interfere with vehicle's normal operation. |
| 203.25.2 | The ASD's interface to the CAN bus shall not interfere with the vehicle's passenger's safety systems (e.g., restraints and extrication). |
| 401.3.6 | The ASD shall carry out plausibility checking on the internal CAN/J-Bus data. |

## 4.11 Advanced Traffic Signal Controllers

| ReqID | Requirement Text |
|---|---|
| 405.3.1 | Advanced Traffic Signal Controllers shall use TAI time to issue security credentials. |
| 405.3.2 | Advanced Traffic Signal Controllers shall issue messages to DSRC devices with security credentials that meet this document’s IEEE 1609.2 requirements. |
| 405.3.3 | Advanced Traffic Signal Controllers shall maintain an authenticated NTP based time reference. |
| 405.3.4 | Advanced Traffic Signal Controllers shall export their UTC times (Line Frequency referenced from the traffic signal system) as UTC times referenced from their authenticated NTP based time reference. |

## 4.12 Traffic Signal System

| ReqID | Requirement Text |
|---|---|
| 405.4.1 | The CV system shall export RSU status to the traffic signal system for display on the traffic signal system map. |
| 405.4.2 | The CV system shall export RSU RF signal range information to the traffic signal system for display on the traffic signal system map. |

# APPENDIX A User Needs

Table A-1 below lists the user needs described in the NYC CVPD ConOps (FHWA-JPO-16-299).

**Table A-1. User Needs**

| Need ID | System Needs | System Concept (CV Application) | Support for Vision Zero |
|---|---|---|---|
| 101.1 | Need to manage speed on surface streets – 25 MPH regulatory speed limit | Speed Compliance | Notify drivers when their speed exceeds the speed limit |
| 101.2 | Need to manage speeds on curves –regulatory speed limit | Curve Speed Compliance | Advise drivers to comply with the speed limit in curves, thus reducing the potential of a rollover and subsequent major traffic incident |
| 101.3 | Need to manage speed in work zones –speed limit | Speed Compliance / Work Zone | Facilitate widespread adherence to the NYC speed limit. Additional time-of-day reductions, such as those associated with a school zones or moving construction (e.g. pothole repair) zones |
| 102.1 | Need to reduce crashes between vehicles | Forward Crash Warning (FCW) | Warn drivers in case of an impending rear-end crash with another vehicle ahead in the same lane and direction of travel |
| 102.2 | Need to reduce crashes between vehicles | Emergency Electronics Brake Light (EEBL) | Notify drivers when a vehicle ahead generates an emergency brake event |
| 102.3 | Need to reduce crashes between vehicles | Blind Spot Warning (BSW) + Lane Change Warning/Assist (LCA) | Warn the driver of the vehicle if the blind-spot zone is occupied by another vehicle traveling in the same direction during a lane change attempt and when it is not attempted |
| 102.4 | Need to reduce crashes between vehicles | Intersection Movement Assist (IMA) | Warn the driver of a vehicle when it is not safe to enter an intersection because of high crash probability with other vehicles at stop-controlled and uncontrolled intersections |

| Need ID | System Needs | System Concept (CV Application) | Support for Vision Zero |
|---|---|---|---|
| 102.5 | Need to reduce crashes between vehicles | Vehicle Turning Right in Front of Bus Warning | Warn bus drivers of vehicles pulling up behind a stopped bus, making a lane changes to pass around the bus, and exhibiting a path to cross directly in front of the bus |
| 102.6 | Need to reduce crashes between vehicles | Red Light Violation Warning | Advise drivers if a vehicle is on an approach that is likely to result in the vehicle violating the red light |
| 103 | Need to reduce crashes between vehicles and infrastructure | Oversize Vehicle Warning | Provides warnings to vehicle drivers to avoid entering a height restricted facility and imminent low clearance location |
| 104.1 | Need to reduce crashes between vehicles and pedestrians / bicyclists | Pedestrian in Signalized Crosswalk Warning | Provide in-vehicle indication of pedestrian / bicyclists at intersections equipped with CV technologies |
| 104.2 | Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | Mobile Accessible Pedestrian Signal System (PED-SIG) | Allows for an automated call from the smartphone of a visually impaired pedestrian to the traffic signal and notify approaching drivers of the pedestrian's presence |
| 105 | Need to inform drivers of serious incidents | Evacuation Notification | Provides notification that an area is to be avoided and why (subset of Emergency Communications and Evacuation concepts) |
| 106 | Need to provide mobility information in heavily congested areas | Intelligent Traffic Signal System (I-SIGCVDATA) | Integration of CV movements with NYC's award winning Mid-town In Motion (MIM) adaptive traffic signal system |
| 201 | Need to have privacy | Data Normalization | Re-anchor time/location data to protect driver/operator while preserving vehicle trajectory details |
| 202 | Need to manage CV application for the traffic environment | CV Application Parameter Control | Manage parameters so that applications can be tuned for the traffic environment |
| 203 | Need to manage CV equipment maintenance | NYCDOT to provide equipment and maintain it | Establish a process for managing the installation of equipment and managing the inventory |
| 204 | Need to limit additional vehicle cab devices that have the potential to distract drivers | Provide audio warnings for the driver-vehicle interface | Provide either auditory sounds or short voice messages when warnings are triggered |

| Need ID | System Needs | System Concept (CV Application) | Support for Vision Zero |
|---|---|---|---|
| 303 | Need to notify vehicles of pedestrians | Pedestrian in Signalized Crosswalk | Visually impaired pedestrians want vehicle driver/operator notified due to limited deployment of the technology |
| 401 | Need to have trusted communications | Dedicated Short Range Communications and Security Credential Management System | Utilize existing standards and external systems to provide secure information exchanges |
| 402 | Need to manage equipment health | RF Monitoring | Equipped vehicles and infrastructure collect first/last contact with other equipped vehicles and infrastructure |
| 403 | Need to manage CV application life-cycle | Over-the-Air Firmware Updates | Provide an infrastructure to verify firmware versions and update when necessary |
| 404 | Need to manage CV application interrelationship | Configurable threat arbitration level for the CV applications | A configurable arbitration technique will be employed to ensure that the warning with the highest immediate threat is the warning presented to the driver. The arbitration algorithm will be configurable such that additional applications can be added to the ASD. |
| 501 | Need to collect detailed information when a warning is issued | Event Recording | Vehicles record the previous X seconds of Basic Safety Message (BSM) data and the next Y seconds of BSM data for evaluation when a CV application issues a warning |
| 502 | Need to collect event recordings | Upload Event Recordings | Vehicles initiate uploads of their event recordings when the service is available |
| 503 | Need to assess speed compliance | Before/After Speed Compliance Comparison | Record speed compliance warnings events and analyze them |
| 504 | Need to assess vehicle-vehicle crashes | Before/After Vehicle-Vehicle Crash Comparison | Record V2V application warning events and analyze them |
| 505 | Need to assess vehicle-pedestrian crashes | Before/After Vehicle-Pedestrian Crash Comparison | Record pedestrian crossing warning events and analyze them |
| 506 | Need to assess vehicle-infrastructure crashes | Before/After Vehicle-Infrastructure Crash Comparison | Record oversize vehicle warnings and analyze them |

| Need ID | System Needs | System Concept (CV Application) | Support for Vision Zero |
|---|---|---|---|
| 510 | Need to assess all CV applications | System Performance and Benefits Evaluation | Assess and post-process the data records before sending them to USDOT IE |

# APPENDIX B Needs-to-Requirements Traceability Matrix (NRTM)

The Needs-to-Requirements Traceability Matrix (NRTM) in Table B-1 below provides the means to demonstrate a requirement has been designed, developed, and tested. The detailed requirements in the subsequent tables record the Quality, Data, Security, Content, Architecture, Environment, Service Introduction, and all other project needs and constraints that define project scope and provide the foundation for design and subsequently, development.

**Table B-1. Needs-to-Requirements Traceability Matrix (NRTM)**

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 101.1 | 101.1.2 | Speed Compliance | The SPDCOMP application shall obtain regulatory speed limits from the MAP message per SAE J2735-201603 based on the host vehicle's current location. | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | NYC CVPD ConOps | Test |
| 101.1 | 101.1.4 | Speed Compliance | The SPDCOMP application shall trigger an alert when either the vehicle speed exceeds the recommended speed by a configured amount or for a configured period of time by time of day. (Note: configurable speed (Excessive Speed Amount Threshold), configurable time (Excessive Speed Time) are defined in Table E-1 and time of day is defined in Table D-1) | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | NYC CVPD ConOps | Test |
| 101.2 | 101.2.10 | Curve Speed Compliance | The CSPD-COMP application shall determine if there is a curve with reduced speed ahead. | Need ID 101.2: Need to manage speeds on curves – regulatory speed limit | CVRIA Curve Speed Warning | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 101.2 | 101.2.11 | Curve Speed Compliance | The CSPD-COMP application shall advise the driver of a curve with reduced speed ahead. | Need ID 101.2: Need to manage speeds on curves – regulatory speed limit | CVRIA Curve Speed Warning; MUTCD Table 2C-4 | Test |
| 101.2 | 101.2.14 | Curve Speed Compliance | The CSPD-COMP application shall determine the difference between the posted speed on the upcoming curve and the vehicle's current speed. | Need ID 101.2: Need to manage speeds on curves – regulatory speed limit | CVRIA Curve Speed Warning | Demo |
| 101.2 | 101.2.15 | Curve Speed Compliance | If the vehicle speed is greater than the posted curve speed, the Vehicle CSPD-COMP Application shall advise the driver in time for the driver to reduce vehicle speed to the posted speed limit before the vehicle enters the curve. | Need ID 101.2: Need to manage speeds on curves – regulatory speed limit | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-342] | Demo |
| 101.2 | 101.2.16 | Curve Speed Compliance | While the vehicle is in the curve, the CSPD-COMP application shall trigger a driver alert when the host vehicle speed exceeds the posted speed plus the Excessive Curve Speed Amount Threshold for a time period exceeding the Excessive Curve Speed Time Threshold. | Need ID 101.2: Need to manage speeds on curves – regulatory speed limit | Revised from CVRIA Curve Speed Warning | Test |
| 101.3 | 101.3.9 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall acquire the following from Speed Zone information for use in SPDCOMPWZ advisory and alert calculations:<br>1. Posted Reduced Speed Zone Speed Limit<br>2. Work Zone geometric information | Need ID 101.3: Need to manage speed in work zones –speed limit | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-625] | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 101.3 | 101.3.10 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall determine if there is a reduced speed zone ahead. | Need ID 101.3: Need to manage speed in work zones –speed limit | | Demo |
| 101.3 | 101.3.11 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall advise the driver of a reduced speed zone ahead. | Need ID 101.3: Need to manage speed in work zones –speed limit | | Demo |
| 101.3 | 101.3.13 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall determine the speed of the host vehicle based on accuracy and (configurable) threshold per J2945/1. | Need ID 101.3: Need to manage speed in work zones –speed limit | | Demo |
| 101.3 | 101.3.14 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall determine the difference between the posted speed on the upcoming reduced speed zone and the vehicle's current speed. | Need ID 101.3: Need to manage speed in work zones –speed limit | | Demo |
| 101.3 | 101.3.15 | Speed Compliance / Work Zone | If the vehicle speed is greater than the reduced speed zone, the SPDCOMPWZ application shall advise the driver in time for the driver to reduce vehicle speed to the posted speed limit before the vehicle enters the zone. | Need ID 101.3: Need to manage speed in work zones –speed limit | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-628] | Test |
| 101.3 | 101.3.16 | Speed Compliance / Work Zone | The SPDCOMPWZ application shall determine if the vehicle exceeds the Work Zone Posted Speed plus the Excessive Zone Speed Amount Threshold, for a period exceeding the Excessive Zone Speed Time Threshold. | Need ID 101.3: Need to manage speed in work zones –speed limit | Revised; CVRIA Reduced Speed Zone Warning | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 101.3 | 101.3.17 | Speed Compliance / Work Zone | While the vehicle is in the speed zone, the SPDCOMPWZ application shall trigger a driver alert when the vehicle speed exceeds the Work Zone Posted Speed plus the Excessive Zone Speed Amount Threshold, for a period exceeding the Excessive Zone Speed Time Threshold. | Need ID 101.3: Need to manage speed in work zones –speed limit | Revised; CVRIA Reduced Speed Zone Warning | Test |
| 102.1 | 102.1.1 | Forward Crash Warning | The FCW safety application shall warn drivers of impending rear-end collisions with other DSRC-equipped vehicles. | Need ID 102.1: Need to reduce crashes between vehicles | NYC CVPD ConOps | Test |
| 102.2 | 102.2.1 | Emergency Electronic Brake Light | The EEBL safety application shall warn drivers about DSRC-equipped vehicles braking. | Need ID 102.2: Need to reduce crashes between vehicles | NYC CVPD ConOps | Test |
| 102.3 | 102.3.1 | Blind Spot Warning | The BSW safety application shall warn drivers about DSRC-equipped vehicles in their blind spots. | Need ID 102.3: Need to reduce crashes between vehicles | NYC CVPD ConOps | Test |
| 102.3 | 102.3.2 | Lane Change Warning | The LCW safety application shall warn drivers about DSRC-equipped vehicles changing lanes in the same direction. | Need ID 102.3: Need to reduce crashes between vehicles | NYC CVPD ConOps | Test |
| 102.4 | 102.4.1 | Intersection Movement Assist | The IMA safety application shall warn drivers about DSRC-equipped vehicles that cross the intersection. | Need ID 102.4: Need to reduce crashes between vehicles | NYC CVPD ConOps | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 102.5 | 102.5.4 | Vehicle Turning Right in Front of a Transit Vehicle | The VTRW application shall detect whether a vehicle is turning right in front of transit vehicle via the position and heading data received in a basic safety message (from a remote vehicle) based on the PVT accuracy for positioning. | Need ID 102.5: Need to reduce crashes between vehicles | Modified from FHWA-JPO-14-118 (Battelle) [SYSREQ_042] | Demo |
| 102.5 | 102.5.5 | Vehicle Turning Right in Front of a Transit Vehicle | The application alert mode in the VTRW application shall be active when the transit vehicle stops within a bus stop geographic zone. | Need ID 102.5: Need to reduce crashes between vehicles | Editorial; FHWA-JPO-14-118 (Battelle) [SYSREQ_043] | Demo |
| 102.5 | 102.5.6 | Vehicle Turning Right in Front of a Transit Vehicle | The application alert mode shall terminate when the transit vehicle stops within a bus stop geographic zone. | Need ID 102.5: Need to reduce crashes between vehicles | Name Change; FHWA-JPO-14-118 (Battelle) [SYSREQ_044] | Demo |
| 102.5 | 102.5.7 | Vehicle Turning Right in Front of a Transit Vehicle | The VTRW application shall only issue alerts to the driver when the transit vehicle indicates an impending crash. | Need ID 102.5: Need to reduce crashes between vehicles | Editorial; FHWA-JPO-14-118 (Battelle) [SYSREQ_045] | Demo |
| 102.5 | 102.5.8 | Vehicle Turning Right in Front of a Transit Vehicle | A VTRW application shall advise if a remote vehicle which originates directly behind the transit vehicle at a bus stop begins to pass to the left of the transit vehicle as the transit vehicle is departing a bus stop. | Need ID 102.5: Need to reduce crashes between vehicles | Name Change, Editorial ; FHWA-JPO-14-118 (Battelle) [SYSREQ_046] | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 102.5 | 102.5.9 | Vehicle Turning Right in Front of a Transit Vehicle | A VTRW alert shall alert the driver if a remote vehicle which originates directly behind the transit vehicle at a bus stop passes to the left of the transit vehicle as the transit vehicle is departing a bus stop and the remote vehicle's position and heading indicates an intent to return to or cross the lane of the transit vehicle. | Need ID 102.5: Need to reduce crashes between vehicles | Name Change, Editorial ; FHWA-JPO-14-118 (Battelle) [SYSREQ_047 ] | Test |
| 102.5 | 102.5.17 | Vehicle Turning Right in Front of a Transit Vehicle | The VTRW application shall present the alerts regardless of traffic signal status. | Need ID 102.5: Need to reduce crashes between vehicles | FHWA-JPO-14-118 SWREQ_014 | Demo |
| 102.5 | 102.5.26 | Vehicle Turning Right in Front of a Transit Vehicle | The VTRW application shall have access to the transit vehicle's gear position. | Need ID 102.5: Need to reduce crashes between vehicles | | Demo |
| 102.5 | 102.5.27 | Aftermarket Safety Device | The ASD shall have access to the host vehicle's brake status. | Need ID 102.5: Need to reduce crashes between vehicles | | Demo |
| 102.6 | 102.6.1 | Red Light Violation Warning | The RLVW Application shall receive the SPaT and MAP data sent by the RSUs to the vehicles deployed along the NYC CVPD corridors as per J2735. | Need ID 102.6: Need to reduce crashes between vehicles | Revised from FHWA-JPO-13-059 [SYS-REQ-145]. ISO 19091 referenced per reviewers | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 102.6 | 102.6.2 | Red Light Violation Warning | The RLVW application shall use the same time source as infrastructure SPaT applications. | Need ID 102.6: Need to reduce crashes between vehicles | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-102] | Demo |
| 102.6 | 102.6.9 | Red Light Violation Warning | The RLVW application shall acquire SPaT information, through the Host Vehicle ASD, from the intersection RSU and signal controller at a signalized intersection within RSU's DSRC range and in the vehicle's direction of travel. | Need ID 102.6: Need to reduce crashes between vehicles | Modified from CVRIA Red Light Violation Warning, ISO 19091 | Demo |
| 102.6 | 102.6.10 | Red Light Violation Warning | The RLVW application shall acquire the location of the stop bars at signalized intersections at which RLVW is operating from the intersection MAP Message. | Need ID 102.6: Need to reduce crashes between vehicles | Modified from CVRIA Red Light Violation Warning | Demo |
| 102.6 | 102.6.11 | Red Light Violation Warning | The RLVW application shall acquire the following from Intersection SPaT messages for use in RLVW advisory and alert calculations:<br>1. Intersection geometric information<br>2. Signal Phase and Timing information of the traffic signal at the Intersection<br>3. Intersection status of the traffic controller<br>4. Traffic law restrictions for the intersection | Need ID 102.6: Need to reduce crashes between vehicles | Revised and split; FHWA-JPO-13-059 (Battelle) [SYS-REQ-137] | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 102.6 | 102.6.12 | Red Light Violation Warning | The Vehicle RLVW Application shall be inactive if one or more of the following conditions occur:<br>1. Vehicle position and accuracy information is not available<br>2. Vehicle Speed is not available<br>3. Communication failure between Vehicle and Infrastructure<br>4. SPaT information is not available<br>5. MAP information is not available<br>6. Vehicle Heading information is not available | Need ID 102.6: Need to reduce crashes between vehicles | FHWA-JPO-13-059 [SYS-REQ-138] | Test |
| 102.6 | 102.6.13 | Red Light Violation Warning | The RLVW application shall calculate if a vehicle will violate the Red Light stop bar at a signalized intersection based on its current speed, heading, acceleration, location, location of stop bars, stop bar tolerance and yellow duration tolerance. | Need ID 102.6: Need to reduce crashes between vehicles | Revised from CVRIA Red Light Violation Warning | Test |
| 102.6 | 102.6.14 | Red Light Violation Warning | The RLVW application shall trigger a driver alert for a vehicle approaching a signalized intersection when it determines that a stop is required and the vehicle will violate the Red Light stop bar at a signalized intersection based on its current speed, heading, acceleration, location and the location of stop bars. | Need ID 102.6: Need to reduce crashes between vehicles | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-139] | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 102.6 | 102.6.15 | Red Light Violation Warning | The RLVW application shall alert drivers in time for the driver to take action for a required stop at a signalized intersection. | Need ID 102.6: Need to reduce crashes between vehicles | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-147] | Test |
| 102.6 | 102.6.16 | Red Light Violation Warning | The RLVW Application shall not alert the driver if the vehicle has safely stopped at the intersection and subsequently accelerates such that a violation occurs. | Need ID 102.6: Need to reduce crashes between vehicles | Editorial; FHWA-JPO-13-059 (Battelle) [SYS-REQ-142] | Demo |
| 102.6 | 102.6.18 | Red Light Violation Warning | The RLVW application shall acquire the following from Intersection MAP messages for use in RLVW advisory and alert calculations:<br>1. Intersection geometric information<br>2. Signal Phase and Timing information of the traffic signal at the Intersection<br>3. Intersection status of the traffic controller<br>4. Traffic law restrictions for the intersection | Need ID 102.6: Need to reduce crashes between vehicles | Revised and split; FHWA-JPO-13-059 (Battelle) [SYS-REQ-137] | Inspect |
| 103 | 103.1.1 | Oversize Vehicle Compliance | The ASD shall advise the driver of a potential crash before the bridge, overpass, or tunnel to exit the restricted roadway and find an alternate route. (Note: Advisory Distance Threshold Parameter is defined in Table E-1 (pg. 157) in the Appendix.) | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 103 | 103.1.2 | Oversize Vehicle Compliance | The ASD shall warn the driver of an impending crash before the over-height bridge, overpass, or tunnel to stop the vehicle completely and avoid the crash. (Note: Warning Distance Threshold Parameter is defined in Table E-1 (pg. 157) in the Appendix.) | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |
| 103 | 103.2.1 | Oversize Vehicle Compliance | The OVC application shall calculate whether or not the vehicle is at risk of crash by comparing the vehicle's height and the height of the roadway restriction. | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |
| 103 | 103.3.1 | Oversize Vehicle Compliance | The OVC application shall utilize the host vehicle's pre-established height in determining whether to alert the driver. | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 103 | 103.3.2 | Oversize Vehicle Compliance | The OVC application shall determine the location of the vehicle relative to the location of the size-restricted or weight restricted roadway. | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |
| 103 | 103.3.3 | Oversize Vehicle Compliance | The RSU shall contain the roadway's clearance height and communicate it to the ASD via DSRC. | Need ID 103: Need to warn potential violators of size-restricted roadways (e.g. bridges, overpasses or tunnels) in time for the driver to take appropriate action | | Demo |
| 104.1 | 104.1.5 | Pedestrian in Signalized Intersection Warning | A PEDINXWALK alert shall be displayed if a pedestrian has been detected in a crosswalk that intersects the Transit Vehicle's planned forward, left or right turn route at the intersection. | Need ID 104.1: Need to reduce crashes between vehicles and pedestrians / bicyclists | FHWA-JPO-14-118 | Demo |
| 104.1 | 104.1.7 | Pedestrian in Signalized Intersection Warning | The Pedestrian Detector shall send a pedestrian detected signal when a pedestrian is present in the crosswalk it monitors. | Need ID 104.1: Need to reduce crashes between vehicles and pedestrians / bicyclists | FHWA-JPO-14-118 [HWREQ_030] | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.1 | 104.1.8 | Pedestrian in Signalized Intersection Warning | The Pedestrian Detectors shall be pole mountable. | Need ID 104.1: Need to reduce crashes between vehicles and pedestrians / bicyclists | FHWA-JPO-14-118 [SYSREQ_006] | Inspect |
| 104.1 | 104.1.10 | Pedestrian in Signalized Intersection Warning | The PEDINXWALK System Latency for pedestrian detection shall be no more than 2 seconds from detecting pedestrian to alert. | Need ID 104.1: Need to reduce crashes between vehicles and pedestrians / bicyclists | FHWA-JPO-14-118 [HWREQ_008] | Test |
| 104.1 | 104.1.12 | Pedestrian in Signalized Intersection Warning | The PEDINXWALK application shall receive Signal Phase and Timing for Pedestrian Lanes and Pedestrian presence detection from the SPaT system. | Need ID 104.1: Need to reduce crashes between vehicles and pedestrians / bicyclists | FHWA-JPO-14-118 [SYSREQ_048] | Demo |
| 104.2 | 104.2.3 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall correctly discern the pedestrian's position and intended crossing direction. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYC CVPD Safety Management Plan | Demo |
| 104.2 | 104.2.4 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall provide status of the walk signal in the intended direction. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYC CVPD Safety Management Plan | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.2.7 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall advise (via audio) the pedestrian how to use the application. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYC CVPD Safety Management Plan | Demo |
| 104.2 | 104.3.1 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall receive intersection geometry information from the RSU based on J2735-201603. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYC Team Review | Inspect |
| 104.2 | 104.3.2 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall use the intersection geometry information to determine the pedestrian's orientation. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Geospatial Requirement | Inspect |
| 104.2 | 104.3.3 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall use the intersection geometry information provided by the MAP message to determine the crosswalk geometry of the intended crossing. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Geospatial Requirement | Inspect |
| 104.2 | 104.3.8 | Mobile Accessible Pedestrian Signal System | The PED-SIG Application shall determine the intended crossing time from the intersection geographic information (distance) and the expected pedestrian travel rate (configurable). | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Geospatial Requirement | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.3.9 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall collect data on the map error status notification. (partial, unable to detect). (Note: this is intended to assist the system in troubleshooting problems; the quality of the MAP data is critical to the application and this requirements ensures that such issues are made known to the central system for correction. This assumes that the application notifies the PED whenever it encounters a geographic computation error.) | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Geospatial Requirement | Inspect |
| 104.2 | 104.4.6 | Mobile Accessible Pedestrian Signal System | The PED-SIG application on the PID shall acquire credentials from the SCMS that will allow it to authenticate the SPaT and MAP messages received. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Security Requirement | Inspect |
| 104.2 | 104.4.8 | Mobile Accessible Pedestrian Signal System | The SCMS shall be able to set service specific permissions associated with the future support of pedestrian requests from the PID. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Security Requirement | Inspect |
| 104.2 | 104.4.10 | Mobile Accessible Pedestrian Signal System | Applications on the PID shall be able to sign messages transmitted to the RSU. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Security Requirement | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.4.11 | Mobile Accessible Pedestrian Signal System | Applications shall be capable of including a unique ID which shall remain stable (unchanged) throughout the PID's interaction with a single intersection. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Security Requirement | Inspect |
| 104.2 | 104.5.1 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall provide information to the pedestrian based on the content of the SPaT and MAP message at the nearest intersection. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.2 | Mobile Accessible Pedestrian Signal System | The Application on the PID shall assist the pedestrian in determining his/her orientation. (Note: Definition of orientation: to understand which street crossing the pedestrian is facing.) | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.3 | Mobile Accessible Pedestrian Signal System | The PID application shall provide information to the pedestrian regarding the availability of PED support services at the intersection. (If there is an RSU.) | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.4 | Mobile Accessible Pedestrian Signal System | Application shall provide information to the pedestrian indicating the status of the pedestrian signal for the intended crossing including walk time remaining, clearance time remaining, and time until the next walk signal is expected. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.5.6 | Mobile Accessible Pedestrian Signal System | The PED Applications shall allow the pedestrian to configure selected parameters and characteristics such as sound volume, voice commands, and walking speeds. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.8 | Mobile Accessible Pedestrian Signal System | The application shall notify the pedestrian if there is a preemption or priority change (TSP) operation taking place which may disrupt the signal timing. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.10 | Mobile Accessible Pedestrian Signal System | The Application shall calculate intersection crossing information based on pedestrian's origin, destination, departure range, arrival range. (Note: this is for coordination of signal timing phase.) | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.11 | Mobile Accessible Pedestrian Signal System | The PED-SIG Application shall collect the performance data listed in Table G-3. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.13 | Mobile Accessible Pedestrian Signal System | The Application shall collect metadata that includes the date and time when system information was generated. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.5.14 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall receive signal timing and controller status from the RSU through the SPaT message. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.5.18 | Mobile Accessible Pedestrian Signal System | Every PID shall be able to change signing keys per SAE J2945/9 Section 6.6. (Note: the signing will be static during interactions with a single intersection.) | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Functional Requirement | Inspect |
| 104.2 | 104.6.2 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall continuously notify the user that it is operating. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Non-Functional Requirement | Demo |
| 104.2 | 104.6.3 | Mobile Accessible Pedestrian Signal System | The PED-SIG application shall be able to provide requested information within 10 seconds. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Non-Functional Requirement | Inspect |
| 104.2 | 104.6.3.1 | Mobile Accessible Pedestrian Signal System | If the delay will be longer than 10 seconds, then the PED-SIG application shall provide information indicating how long it is expected to complete the operation. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Non-Functional Requirement | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.6.4 | Mobile Accessible Pedestrian Signal System | The applications shall be able to measure and log the time required to provide the pedestrian the information. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Non-Functional Requirement | Inspect |
| 104.2 | 104.6.11 | Mobile Accessible Pedestrian Signal System | The PID device shall be able to function in a communication-saturated environment. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Non-Functional Requirement | Inspect |
| 104.2 | 104.8.4 | Mobile Accessible Pedestrian Signal System | The PID system shall ensure geo-location information is used for PED-SIG application only. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Privacy Requirement | Inspect |
| 104.2 | 104.8.9 | Mobile Accessible Pedestrian Signal System | All data transmitted between the PID and the NYU server shall be encrypted to protect any personal information. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Privacy Requirement | Inspect |
| 104.2 | 104.8.10 | Mobile Accessible Pedestrian Signal System | Data stored by the NYU server or exported for independent evaluation shall be processed to remove any personal information and any attributes including exact location and exact time such that the data cannot be associated with a particular person or event. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Privacy Requirement | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 104.2 | 104.9.4 | Mobile Accessible Pedestrian Signal System | The PID shall use the channel assignments defined in Table F-1. | Need ID 104.2: Need to reduce crashes between vehicles and visually / audibly-impaired pedestrians | NYCDOT Pedestrian Mobility Requirement | Inspect |
| 105 | 105.1.2 | Emergency Communications and Evacuation Information | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of vehicles receiving emergency information Before and After periods. | Need ID 105: Need to inform drivers of serious incidents | NYC CVPD Performance Measurement Plan | Demo |
| 106 | 106.1.1 | Mobility Data Collection | The NYC CVPD performance monitoring subsystem shall post-process the mobility data from the I-SIGCVDATA application Before and After periods. | Need ID 106: Need to provide mobility information in heavily congested areas | NYC CVPD Performance Measurement Plan | Demo |
| 106 | 106.1.1.1 | Mobility Data Collection | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speed from NYC CVPD for comparison to the legacy detection system. | Need ID 106: Need to provide mobility information in heavily congested areas | NYC CVPD Performance Measurement Plan | Demo |
| 106 | 106.1.1.2 | Mobility Data Collection | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average travel time from NYC CVPD for comparison to the legacy detection system. | Need ID 106: Need to provide mobility information in heavily congested areas | NYC CVPD Performance Measurement Plan | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.1.1 | Common Safety Applications | The Safety Application shall function in vehicle classes in which it is to be installed in the NYC CVPD. (Note: NYC CVPD vehicles are specified in the USDOT ASD Design Specification v3.1.) | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-002] | Demo |
| 110 | 110.1.2 | Common Safety Applications | The Safety Application shall function in weather (pavement and atmospheric) and lighting conditions anticipated for the NYC CVPD. (Note: NYC CVPD operational weather conditions are specified in the USDOT ASD Design Specification v3.1.) | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-003] | Demo |
| 110 | 110.1.3 | Common Safety Applications | The Safety Application shall function on NYC CVPD roadways. (Note: NYC CVPD roadways are identified in the NYC CVPD ConOps.) | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-004] | Demo |
| 110 | 110.1.4 | Common Safety Applications | The Safety Application shall obtain vehicle position data whose accuracy supports the application's calculations for issuing advisories and alerts. | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-005] | Demo |
| 110 | 110.1.5 | Common Safety Applications | The Safety Application shall not interfere with other in-vehicle safety systems. | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-006] | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.1.6 | Common Safety Applications | The Safety Application shall use advisories and alerts that conform to human factors guidelines issued by the FHWA, NHTSA, and SAE. | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-061 (Battelle) [SYS-REQ-009] | Test |
| 110 | 110.1.7 | Common Safety Applications | The Safety Application shall perform self-diagnostics upon power up and at TBD intervals when the vehicle is operating. (Note: Self-Diagnostics refers to the ability of the Safety Application to determine whether it is capable of performing its intended function. This will be detailed in the design phase.) | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.8 | Common Safety Applications | The Safety Application shall determine the operating level/mode of operational, degraded, or failure based on the results of a self-diagnostic test. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.9 | Common Safety Applications | The Safety Application shall set the operational status corresponding to the operational level mode as follows:<br>1. Operational – online<br>2. Degraded – online<br>3. Failure – offline | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.10 | Common Safety Applications | The Safety Application shall log self-diagnostic test failure which contains, at a minimum, the following information:<br>1. Date and time of test failure<br>2. Additional information to the nature of a failed test | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.1.11 | Common Safety Applications | The Safety Application shall maintain historical information of self-diagnostic test failures for a predetermined period in non-volatile storage. (Note: Non-volatile storage refers to storage that remains intact even when there is no power. It is left up to the implementer to determine if the retention of data is a fixed window of time, if it is based on a fixed amount of storage, or if it is until cleared.) | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.12 | Common Safety Applications | The Safety Application shall take itself off-line when the operating level/mode is failure. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.13 | Common Safety Applications | The Safety Application shall restore or maintain itself on-line when the operating level/mode is either operational or degraded. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.14 | Common Safety Applications | The Safety Application shall perform effectively for all defined NYC CVPD functional classes of roadway and levels of service (LOS) where the application is installed or is being used. (Note: NYC CVPD functional classes of roadway and levels of service are specified in the NYC CVPD ASD Specification.) | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.15 | Common Safety Applications | The Safety Application shall be able to receive and decode messages broadcast by NYC CVPD RSU. (Note: NYC CVPD RSU is specified in the NYC CVPD RSU Specification.) | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |
| 110 | 110.1.16 | Common Safety Applications | The V2I Safety Application alerts shall only be issued when the current inputs to the application warrants an advisory or alert. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.1.17 | Common Safety Applications | Safety Application Driver Training shall conform to human factors guidelines issued by the FHWA, NHTSA, and SAE. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Analysis |
| 110 | 110.1.18 | Common Safety Applications | The Safety Application shall not provide information to the driver that conflicts with infrastructure roadside signage. | Need ID 102: Need to reduce crashes | FHWA-JPO-13-061 | Analysis |
| 110 | 110.1.19 | Common Safety Applications | The safety application shall provide its operational status (online, offline) to the ASD management system. | Need ID 102: Need to reduce crashes | NYC CVPD Safety Management Plan | Test |
| 110 | 110.1.20 | Common Safety Applications | An application shall receive intersection geometry information, e.g. Geometric Intersection Design (GID), from the closest MAP message based on the host vehicle's current location. | Need ID 102: Need to reduce crashes | NYC CVPD ConOps, SAE J2735 201601 | Demo |
| 110 | 110.1.21 | Common Safety Applications | The application shall obtain vehicle speed from one of the sources available to the ASD. These sources include the CAN interface, GNSS interface, derivation from sequential GNSS location readings. | Need ID 102: Need to reduce crashes | NYC CVPD ConOps, SAE J2735 201601 | Test |
| 110 | 110.2.2 | Aftermarket Safety Device | The ASD shall broadcast the BSM of host vehicles per SAE standards J2945/1 and J2735. | Need ID 102: Need to reduce crashes | CVRIA; SAE J2945/1 | Test |
| 110 | 110.2.3 | Aftermarket Safety Device | All NYC CVPD ASDs shall utilize the same GPS time source and common accuracy configuration as the NYC CVPD Infrastructure. | Need ID 102: Need to reduce crashes | CVRIA | Inspection |
| 110 | 110.3.1 | Common Safety Applications | The safety applications listed in Table C-1 shall acquire vehicle position accuracy, speed, and heading to the ASD. | Need ID 102: Need to reduce crashes | | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.3.2 | Common Safety Applications | The safety application listed in Table C-1 shall determine if the ASD Position, speed and heading information provided is sufficiently accurate to support the ASD's advisory and alert calculations. | Need ID 102: Need to reduce crashes | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-318] | Test |
| 110 | 110.3.3 | Common Safety Applications | The safety applications listed in Table C-1 shall only issue advisories and alerts if the ASD Position, speed and heading information provided is sufficiently accurate to support the ASD's advisory and alert calculations. | Need ID 102: Need to reduce crashes | CVRIA Curve Speed Warning | Test |
| 110 | 110.3.4 | Common V2I Safety Applications | The safety applications listed in Table C-1 shall acquire roadway geometry information for the roadway ahead from the ASD. (Note: roadway geometry information is expected to come from MAP messages acquired by the ASD from NYC CVPD DSRC Infrastructure.) | Need ID 102: Need to reduce crashes | Revised from CVRIA Curve Speed Warning | Test |
| 110 | 110.3.4.1 | Common V2I Safety Applications | The V2I safety applications listed in Table C-1 except for CSPD-COMP and SPDCOMPWZ applications shall acquire the roadway geometry information through the MAP message from the RSUs. | Need ID 102: Need to reduce crashes | | Test |
| 110 | 110.3.4.2 | Common V2I Safety Applications | The CSPD-COMP and SPDCOMPWZ applications listed in Table C-1 shall acquire the roadway geometry information through the TIM message from the RSUs. | Need ID 102: Need to reduce crashes | | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.3.5 | Common Safety Applications | The safety applications listed in Table C-1 shall acquire the posted speed for the roadway ahead, including upcoming curve(s). (Note: Posted speed information is expected to come from MAP messages acquired by the ASD from NYC CVPD DSRC Infrastructure.) | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | TBD, pending further discussion and coordination with all 3 CVPD sites | Test |
| 110 | 110.3.5.1 | Common V2I Safety Applications | The V2I safety applications listed in Table C-1 except for CSPD-COMP and SPDCOMPWZ applications shall acquire the posted speed information through the MAP message from the RSUs. | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | | Test |
| 110 | 110.3.5.2 | Common V2I Safety Applications | The CSPD-COMP application listed in Table C-1 shall acquire the posted speed for the upcoming curved section of a roadway through the TIM message from the RSU. | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | | Test |
| 110 | 110.3.5.3 | Common V2I Safety Applications | The SPDCOMPWZ application listed in Table C-1 shall acquire the posted speed for the upcoming work zone through the TIM message from the RSU. | Need ID 101.1: Need to manage speed on surface streets – 25 MPH regulatory speed limit | | Test |
| 110 | 110.3.6 | Common Safety Applications | Issuance of the CSPD-COMP and SPDCOMPWZ application advisory of a reduced speed curve ahead to the driver shall coincide with driver visibility of roadside curve ahead signage. (Note: Location of roadside signage and sign visibility distances are described in the MUTCD.) | Need ID 102: Need to reduce crashes | | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 110 | 110.3.7 | Common Safety Applications | The safety application shall acquire data from the ASD which includes the following:<br>Vehicle positioning information<br>Vehicle position accuracy<br>Vehicle speed<br>Vehicle acceleration<br>Vehicle heading | Need ID 102: Need to reduce crashes | Editorial; FHWA-JPO-13-059 (Battelle) [SYS-REQ-114] | Test |
| 110 | 110.4.1 | Aftermarket Safety Device | Foreign light-duty vehicles shall transmit DSRC BSM messages in accordance with the J2945/1 standard. | Need ID 102: Need to reduce crashes | SAE J2945/1 | Test |
| 110 | 110.4.2 | Aftermarket Safety Device | Foreign trucks shall transmit DSRC BSM messages in accordance with the J2945/1 and shall contain the following Part II SupplementalVehicleExtensions objects: classification, and vehicleData (height and mass) as defined in J2735 Section 6.133. | Need ID 102: Need to reduce crashes | SAE J2945/1 | Test |
| 201 | 201.1.1 | Aftermarket Safety Device | The ASD event recording shall encrypt each event record. (Clarification: this prevents vehicle identity and determination of whether the vehicle is from the control group or the treatment group.) | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Test |
| 201 | 201.2.1 | Common Safety Applications | The V2V safety applications shall set the message threshold at the proper level. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan [ID 001] | Test |
| 201 | 201.2.2 | Common Safety Applications | The V2V safety applications shall formulate the decision algorithm properly to recognize the threat. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 201 | 201.2.3 | Common Safety Applications | The V2V safety applications shall ensure that all components of the system are functioning as intended. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Test |
| 201 | 201.3.2 | Common Safety Applications | The V2I safety applications shall operate on correct, timely information. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Test |
| 201 | 201.4.1 | Common Safety Applications | The NYC CVPD safety management subsystem shall verify the initial data entry from the V2I safety applications. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Demo |
| 201 | 201.4.2 | Roadside Unit | The TMC staff shall be able to monitor the NYC CVPD system-wide RSU malfunctions. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Test |
| 201 | 201.5.1 | Aftermarket Safety Device | The ASD shall provide the alerts to the driver without ambiguity. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Demo |
| 201 | 201.5.2 | Aftermarket Safety Device | The ASD shall have configurable parameters for tuning alert thresholds. | Need ID 201: Need to have privacy | NYC CVPD Safety Management Plan | Inspect |
| 201 | 201.6.1 | Roadside Unit | The RSU shall broadcast the regulatory speed information to the ASD. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 202 | 202.1.3 | CV Application Parameter Control | The safety applications listed in Table C-1 shall implement the most recent application control parameters supplied externally to the application as described in Table E-1. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Test |
| 202 | 202.1.4 | CV Application Parameter Control | The safety application shall allow the central system to modify the control parameters as defined in Table E-1. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Test |
| 202 | 202.2.1 | Adaptability | The NYC CVPD applications shall have modifiable algorithms and software parameters for improving the system performance. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Inspect |
| 202 | 202.3.1 | Adaptability | The ASD shall have upgradable hardware components for improving the device performance upon expansion of the NYC CVPD system. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Inspect |
| 202 | 202.3.2 | Adaptability | The RSU shall have upgradable hardware components for improving the device performance upon expansion of the NYC CVPD system. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Inspect |
| 202 | 202.4.1 | Aftermarket Safety Device | The ASD shall monitor the items in Table E-5 on the in-vehicle network. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Performance Measurement Plan | Inspect |
| 202 | 202.4.2 | Vehicle Performance Monitoring | The Vehicle Performance Monitoring application shall collect/log vehicle operational data (e.g. hard break, steering turns, accelerations based on accelerometers). | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Performance Measurement Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 202 | 202.4.3 | IE Performance Monitoring | The fleet manager shall be able to solicit and collect feedback from the anonymous vehicle operators on the operation of the system. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Performance Measurement Plan | Inspect |
| 202 | 202.6.1 | CV Application Parameter Control | The Parameter Control functional entity at the TMC shall sign the Parameter Control messages per IEEE 1609.2. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Inspect |
| 202 | 202.6.3 | CV Application Parameter Control | The Parameter Control functional entity shall meet the highest security requirements for a device of the appropriate class. (Note: this shall be derived via the Confidentiality/Integrity/Availability (CIA) analysis once the application specification is developed in detail.) | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Demo |
| 202 | 202.6.5 | CV Application Parameter Control | The Parameter Control functional entity shall update the parameter control message signatures daily. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Inspect |
| 202 | 202.6.7 | CV Application Parameter Control | The Parameter Control message version shall be based on the message payload. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Inspect |
| 202 | 202.6.8 | Aftermarket Safety Device | The ASDs from all suppliers shall implement the same Parameter Control protocol. (Note: Parameter Control protocol will be defined by SAE or by NYC CVPD.) | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 202 | 202.7.1 | Aftermarket Safety Device | The ASD shall process all radio messages at a minimum rate of 10 Hz. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD Security Management Operating Concept | Test |
| 202 | 202.8.1 | Vehicle Performance Monitoring | The ASD shall monitor the delivery of the audio alert and any audio instructions to the driver.<br>(Clarification: the monitoring system [internal to the ASD] shall confirm that the actual audio information [sound] was produced in the vehicle and that the audio information matches what the alert was intended to deliver. The purpose of this requirement is detect faulty speaker wiring and damaged speakers that prevent the alert from being delivered to the driver. It is not intended to be an accurate voice to text conversion system, but sufficient to determine that an alert message was delivered.)<br>By way of example, a microphone located at or near the speaker can verify that the specific audio word(s) or tone was presented to the driver; contrarily, simply measuring the voltage output sent to the speaker is not sufficient since the speaker could be damaged or sabotaged. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Demo |
| 202 | 202.9.1 | Vehicle Performance Monitoring | The ASD shall include an accelerometer for each of the three axes. | Need ID 202: Need to manage CV application for the traffic environment | NYC CVPD ConOps | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 203 | 203.1.1 | Durability: Repair | The NYC CVPD maintenance personnel shall replace the ASD damaged by improper maintenance, tampering, or mishap. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.1.2 | Durability: Repair | The NYC CVPD maintenance personnel shall replace the RSU damaged by improper maintenance, tampering, or mishap. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.2.1 | Durability: Repair | The NYC CVPD maintenance personnel shall be able to reboot the ASD after a disruptive software glitch. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.2.2 | Durability: Repair | The NYC CVPD maintenance personnel shall be able to reboot the RSU after a disruptive software glitch. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.4.1 | Aftermarket Safety Device | The ASD shall operate on the voltage supplied by the host vehicle. | Need ID 203: Need to manage CV equipment maintenance | | Test |
| 203 | 203.5.2 | | If the ASD determines that it has no valid certificates, it shall cease transmission of BSMs. | | | |
| 203 | 203.6.3 | Roadside Unit | The RSU shall broadcast the location of a curve and other details to support the CSPD-COMP application. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 203 | 203.6.4 | Roadside Unit | The RSU shall broadcast the location of a static work zone to support the SPDCOMPWZ application. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.6.5 | Roadside Unit | The RSU shall broadcast the location of a moving work zone to support the SPDCOMPWZ application. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.6.6 | Roadside Unit | The RSU shall broadcast the location of a school zone to support the SPDCOMPWZ application. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.6.7 | Roadside Unit | The RSU shall broadcast the location of a roadway's vehicle size restriction to support the OVC application. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.7.1 | Aftermarket Safety Device | The RSU shall provide evidence of tampering (e.g. opening of the case) through tamper-evident seals on media ports (e.g. USB) and screw holes. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.7.2 | Roadside Unit | The ASD shall provide evidence to detect tampering (e.g. opening of the case) through tamper-evident seals on all media ports and screw holes. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.7.3 | Roadside Unit | The RSU size dimensions shall not exceed 13” h x 13” w x 4” d exclusive of mounting hardware. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 203 | 203.12.1 | Aftermarket Safety Device | The ASD shall utilize the OBD-II port, J-bus, or CAN bus. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.12.2 | Aftermarket Safety Device | The ASD shall conform to the associated SAE interface requirements for OBD-II port, J-bus, or CAN bus. (Clarification: the intent of this requirement is to prevent the ASD from interfering with other in-vehicle systems.) | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Test |
| 203 | 203.12.3 | Aftermarket Safety Device | The application in the ASD shall collect and process vehicle-related information through a direct connection or a splitter cable. (Note: individual application data needs will be addressed through each application's requirement.) | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.14.1 | Aftermarket Safety Device | The ASD interface design and test before production shall address poor choice of color, icon shape, location, or sound. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.15.2 | Aftermarket Safety Device | The ASD installation procedure shall stipulate wire routing. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.16.1 | Aftermarket Safety Device | The current drawn by the ASD shall not exceed with the maximum allowable amperage specified by the ASD vendor. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 203 | 203.16.2 | Roadside Unit | The RSU shall not overload the power supplies provided by the RSU vendor based on maximum allowable power consumption. (During operation, turn off, turn on, etc. per NEMA TS2 environmental testing.) | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.17.1 | Roadside Unit | The RSU shall be designed to operate properly in the outdoor environment. (e.g. temperature, humidity, rain, fog, sun, snow, shock, vibration, etc.) {Ref augmented NEMA TS2-20XX} | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.17.2 | Roadside Unit | All connections to the RSU shall be protected from lightening and power surges on the Ethernet. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.18.1 | Aftermarket Safety Device | The ASDs shall withstand electromagnetic interference (EMI) from external sources and electrical distribution. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.18.2 | Aftermarket Safety Device | The ASD shall withstand electrostatic discharge (ESD) from external sources and electrical distribution. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.18.3 | Roadside Unit | The RSU shall withstand electrostatic discharge (ESD) from external sources and electrical distribution. (Provide ESD definitions/specifications.) | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.19.1 | Aftermarket Safety Device | The ASD design shall prevent battery drain. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 203 | 203.22.1 | Aftermarket Safety Device | Connected Vehicle equipment mounted externally to the vehicle shall be contained within the envelope defined by the ASD vendor specification. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.25.1 | Aftermarket Safety Device | The ASD interface to the CAN bus shall not degrade or interfere with vehicle's normal operation. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.25.2 | Aftermarket Safety Device | The ASD's interface to the CAN bus shall not interfere with the vehicle's passenger's safety systems (e.g., restraints and extrication). | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Demo |
| 203 | 203.26.1 | Aftermarket Safety Device | The ASD shall be able to process (and authenticate and/or encrypt) the DSRC messages at a minimum rate of 10 Hz (10 times/sec). This includes all messages on all channels: BSM, TIM, MAP, SPaT, etc. in addition to IP communications traffic for management applications. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.28.1 | Aftermarket Safety Device | The TMC staff shall be able to monitor the NYC CVPD system-wide ASD malfunctions. | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |
| 203 | 203.31.1 | Durability: Power Disruption | Back office servers shall have their power source augmented by an Uninterruptable Power Supply (UPS). | Need ID 203: Need to manage CV equipment maintenance | NYC CVPD Safety Management Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 204 | 204.3.1 | Environmental conditions | The audible message volume in the ASD shall be distinguishable from other sounds. | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | NYC CVPD Safety Management Plan | Inspect |
| 204 | 204.3.2 | Environmental conditions | The audible message volume in the ASD shall be developed and tested in a real traffic environment. | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | NYC CVPD Safety Management Plan | Inspect |
| 204 | 204.4.1 | Human-Machine Interface | The NYC CVPD HMI shall communicate alerts to the driver through auditory devices. | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | NYC CVPD Safety Management Plan | Inspect |
| 204 | 204.4.4 | Human-Machine Interface | The NYC CVPD HMI shall communicate evacuation information to the driver through auditory alerts. | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | NYC CVPD Safety Management Plan | Inspect |
| 204 | 204.5.1 | Aftermarket Safety Device | The Host Vehicle ASD shall begin aural alerts within 250 milliseconds of being triggered by the application. | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | Revised; FHWA-JPO-13-059 (Battelle) [SYS-REQ-146] | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 204 | 204.6.1 | Aftermarket Safety Device | The system administrator shall be able to change the volume level of the audio output (e.g. speakers). | Need ID 204: Need to limit additional vehicle cab devices that have the potential to distract drivers | NYC CVPD Safety Management Plan | Demo |
| 401 | 401.1.2 | Aftermarket Safety Device | The ASD shall have sufficient power to authenticate messages on the Safety Applications defined in Table C-1 in time for the individual Safety Applications to meet their individual performance requirements. | Need ID 401: Need to have trusted communications | FHWA-JPO-13-061 | Test |
| 401 | 401.2.1 | SCMS Interface | The device supplier shall provide devices provisioned with valid enrollment certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.2.2 | SCMS Interface | The device supplier shall provide devices that meet the interface requirements of the USDOT's certification program. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.2.6 | Aftermarket Safety Device | The ASD shall meet pre-determined certification criteria based on procurement documents. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.2.7 | Roadside Unit | The RSU shall meet the USDOT certification requirements as defined in TBD prior to September 15, 2016. (Note: this will be detailed in the design phase.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.3.1 | Aftermarket Safety Device | The ASD shall carry out plausibility checking on the remote vehicle BSM data. (Definition of plausibility checking needs to be determined.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.3.2 | Aftermarket Safety Device | The ASD shall sign its event log file entries using its BSM signing keys. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.3.3 | Aftermarket Safety Device | The ASD operating system (OS) shall prevent the log file signing application from sending messages on any channel other than those that are identified by the PSID or WSA for particular service. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Test |
| 401 | 401.3.4 | Aftermarket Safety Device | The ASD shall indicate successful receipt of the pseudonym certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.3.5 | Aftermarket Safety Device | The SCMS supplier shall track the expected expiry times of ASD enrollment certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.3.6 | Aftermarket Safety Device | The ASD shall carry out plausibility checking on the internal CAN/J-Bus data. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.3.7 | Aftermarket Safety Device | When the ASD has no valid BSM signing certificates, it shall store the log file entries as IEEE 1609.2 data of type unsecured. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.3.8 | Aftermarket Safety Device | The ASD vendor shall replace the ASDs that need to be re-enrolled with newer ASDs. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.4.4 | Roadside Unit | The RSU supplier shall provide the serial number and its enrollment certificate for each RSU. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.4.6 | Roadside Unit | The RSU-SCMS interface shall allow the RSU to request application certificates with different contents from the current ones during the lifetime of the current ones. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.5.1 | Common CV Equipment | All devices shall carry no more than two weeks' worth of operating certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.5.2 | Common CV Equipment | The day before a new week becomes valid, the devices shall download the next weeks' worth of certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.6.2 | Common CV Equipment | If a device misbehaves, the SCMS shall blacklist the device and its enrollment certificates and prevent it from obtaining more authorization certificates. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.6.3 | Common CV Equipment | The SCMS shall maintain the blacklist internally. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.6.4 | Common CV Equipment | The back office system shall acquire one SCMS certificate from each installed DSRC device and associate this certificate with the installed DSRC device. (Note: this requirement is temporary and will become obsolete after the SCMS deploys misbehavior detection and reporting features.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.6.5 | Common CV Equipment | The back office system administrator shall provide a DSRC device's acquired SCMS certificate when requesting that the SCMS registration authority add the associated DSRC device to the Certificate Revocation List (CRL). (Note: this requirement is temporary and will become obsolete after the SCMS deploys misbehavior detection and reporting features.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.7.1 | Aftermarket Safety Device | The ASD shall obtain certificates via IPv6 connectivity through the RSU. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.7.2 | Roadside Unit | The RSU shall broadcast the WSA for certificate download on control channel 178 and indicate IPv6 connectivity and the IP address on a service channel other than channel 172 or 178. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.7.3 | Roadside Unit | The RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.7.4 | Common CV Equipment | Mobile devices in need of certificate update shall switch to the advertised channel. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.7.5 | Roadside Unit | The RSUs shall support IPv6 tunneling over IPv4. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.7.6 | DSRC Connectivity | Communication between the ASD and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface. (Note: The SCMS interface should not need any further security.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.7.7 | DSRC Connectivity | The information security manager shall investigate and monitor the data traffic usage to detect unapproved use of the IP connection. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.7.8 | DSRC Connectivity | Communication between the RSU and the SCMS shall operate in an encrypted, end-to-end connection in accordance with the published SCMS interface. (Note: The SCMS interface should not need any further security.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.8.1 | Denial of Service | The NYCDOT IT shall address any denial of service (DoS) attacks within each NYC network using its existing practices. (Note: the networks include NYCWiN, CityNet, DOTNet, any network that DoITT is responsible for.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.8.2 | Denial of Service | The information security manager shall monitor the DSRC communications performance to detect DoS attacks. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.8.3 | Denial of Service | The RSU shall report over a management interface if channel busy ratios go above a configurable threshold. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.8.4 | Denial of Service | The ASD shall log an event report every second for which channel busy ratios go above a configurable threshold. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.9.1 | Roadside Unit | The RSU shall operate client-side transport layer security (TLS) and accept only TLS server certificates with specific URLs. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.9.2 | Roadside Unit | The RSU shall protect root certificates for client-side TLS against modification and provide other certificates in the chain, which shall not make a separate query to the internet to obtain the entire chain. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Inspect |
| 401 | 401.11.1 | Common CV Equipment | A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages received.<br>(Note: the only exception to this is a firmware update in which case faulty software could violate this requirement.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.11.2 | Common CV Equipment | A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages transmitted. | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.12.1 | Roadside Unit | The RSU shall interface with signal controllers, NYCWiN, and DSRC messages from vehicles and pedestrians. (Note: this will be expanded into multiple requirements for each interface.) | Need ID 401: Need to have trusted communications | NYC CVPD Security Management Operating Concept | Demo |
| 401 | 401.14.1 | SMOC - Common CV Equipment: Security | Devices shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS. | Ensure that devices can be securely managed | Security Management Operating Concept section 5.2.3 | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.14.2 | SMOC - Common CV Equipment: Security | Devices shall support establishment of a standard TLS-based VPN with client authentication for communication to the TMC, with a long-term client cert and a single CA cert trusted to authorize connections from the TMC. | Ensure end-to-end security for bulk data upload | Security Management Operating Concept section 5.2.4 | Demo |
| 401 | 401.14.3 | SMOC - Common CV Equipment: Security | Devices shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application. | Protect receivers from false messages | Security Management Operating Concept section 5.3.2 | Demo |
| 401 | 401.14.4 | SMOC - Common CV Equipment: Security | Devices shall store RF Monitoring log file entries encrypted with an encryption key belonging to the TMC. | Protect privacy of drivers | Security Management Operating Concept section 5.3.12 | Demo |
| 401 | 401.14.5 | SMOC - Device security classes: common requirements | The host processor on the device shall perform and pass integrity checks as specified in requirements 401.14.6 - 401.14.9. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.2 | Demo |
| 401 | 401.14.6 | SMOC - Device security classes: common requirements | The integrity checks performed at boot shall use a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.2 | Test |
| 401 | 401.14.7 | SMOC - Device security classes: common requirements | Until all integrity checks on the software and firmware configuration of the host have passed, the device shall not allow a privileged application (as defined in Security Management Operating Concept section 6.1.1) to sign a message. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.2 | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.14.8 | SMOC - Device security classes: common requirements | If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any application to have access to locally stored private keys. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.2 | Test |
| 401 | 401.14.9 | SMOC - Device security classes: common requirements | If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any privileged application (as defined in Security Management Operating Concept section 6.1.1) to operate. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.2 | Test |
| 401 | 401.14.10 | SMOC - Device security classes: common requirements | The OS on the device shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the HSM. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.3 | Test |
| 401 | 401.14.11 | SMOC - Device security classes: common requirements | The OS shall not permit keys designated as private to be read from the HSM. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.3 | Test |
| 401 | 401.14.12 | SMOC - Device security classes: common requirements | The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.3.4 | Test |
| 401 | 401.14.13 | SMOC - Device security classes: common requirements | All cryptographic software and firmware for the HSM shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.4.1 | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.14.14 | SMOC - Device security classes: common requirements | The HSM operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.4.1 | Demo |
| 401 | 401.14.15 | SMOC - Device security classes: common requirements | The HSM operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.1.4.1 | Demo |
| 401 | 401.14.16 | SMOC - Device security classes: common requirements | The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case). | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.2 | Inspect |
| 401 | 401.14.17 | SMOC - Device security classes: common requirements | All unused media ports (e.g. USB) shall be sealed. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.2 | Inspect |
| 401 | 401.14.18 | SMOC - Device security classes: common requirements | There shall be no removable media. | Ensure appropriate level of security for operations | Security Management Operating Concept section 6.2 | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.14.19 | SMOC - 1609.2 security management | The certificate management service shall start requesting a new certificate or batch of pseudonym certificates a day before the expiry of the current certificate or batch. | Protect receivers from false messages | Security Management Operating Concept section 8.2.1.1 | Test |
| 401 | 401.14.20 | SMOC - 1609.2 verification | When verifying, the device shall require that 1609.2 signed messages are signed by a certificate that is protected from modification by, or chains back to a certificate that is protected from modification by, the secure boot process. | Protect receivers from false messages | Security Management Operating Concept section 5.2.2.2, 6.1.3.2 | Test |
| 401 | 401.14.21 | SMOC - ASD: ASD Certificate Update | Devices shall implement certificate download per the SCMS Interface (detailed requirements to be derived during Phase 2 as the final interface document is not yet published) | Need to enable secure, reliable credential update | Security Management Operating Concept section 7.2.6 | Test |
| 401 | 401.14.22 | SMOC - Secure message transmission | A device shall not create or transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it does not currently have valid certificates for that usage scenario. | Enable secure, reliable credential update | Security Management Operating Concept section 7.2.6 | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.14.23 | SMOC - 1609.2 verification | A device shall verify a DSRC message when any of the following conditions is met:<br>A) A device identifies the message as containing a new DE_TemporaryID value.<br>B) The message results in the issuance of issue either advisory, warning, or alert.<br>C) The remote vehicle constitutes a potential threat (define potential threat as a vehicle that may collide with the host vehicle based on the both vehicle's speeds and trajectories)<br>D) The host vehicle constitutes a threat to a pedestrian using a DSRC equipped Personal Information Device.<br>E) Other potential threat situations such as infrastructure size restrictions, speed compliance, red light violations, and other safety applications.<br>F) Other situations as identified during the Phase 2 Design.<br>Note: Verification consists of meeting the IEEE 1609.2 requirements specified herein this document and the associated message's Security Profile (to be provided in Phase 2). | Protect receivers from false messages | Security Management Operating Concept section 5.3.4 | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 401 | 401.15.3 | Roadside Unit | RSUs shall exceed 802.11 ACK requirements in the following manner: Antenna referenced ACK turnaround time must be in (SIFS-12.5, SIFS+12.5) ns 95% for cable tested non-CSD signals. Note that any RSU employing the NXP based SAF5200 will support this by default. The position provided by the WSA shall be provided by the central system based on the 3D surveyed position. | Need ID 401: Need to have trusted communications | | Demo |
| 401 | 401.16.1 | Common CV Equipment | Devices unable to receive timing information per J2945/1 Section 6.2 shall set their time from an authenticated time reference using the Network Time Protocol Version 4 per Internet Engineering Task Force RFC 5905-5908. | Need ID 401: Need to have trusted communications | SAE J2945/1 | Demo |
| 401 | 401.17.1 | Common CV Equipment | Each DSRC device shall obtain its time and position from the GNSS per the requirements of J2945/1 Section 6.2. | Need ID 401: Need to have trusted communications | SAE J2945/1 | Demo |
| 402 | 402.1.1 | Durability: DSRC Device Mode | The ASD shall revert to a fail-safe mode as specified in Table F-2 when unable to perform its normal operations. | Need ID 402: Need to manage equipment health | NYC CVPD Safety Management Plan | Test |
| 402 | 402.1.2 | Durability: DSRC Device Mode | The RSU shall revert to a fail-safe mode as specified in Table F-2 when unable to perform its normal operations. | Need ID 402: Need to manage equipment health | NYC CVPD Safety Management Plan | Test |
| 402 | 402.1.3 | Durability: DSRC Device Mode | The ASD shall report a self-diagnosed failure of itself or one of its software modules (1) to an RSU attempting to install new firmware or parameters and (2) to a device connected to the ASD's maintenance port. | Need ID 402: Need to manage equipment health | NYC CVPD Safety Management Plan | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 402 | 402.1.4 | Durability: DSRC Device Mode | The RSU shall report a self-diagnosed failure through NYCWiN at the TMC. | Need ID 402: Need to manage equipment health | NYC CVPD Safety Management Plan | Demo |
| 402 | 402.2.2 | Durability: Power Disruption | The RSU shall be able to resume normal function within 2 minutes of restoration of power. | Need ID 402: Need to manage equipment health | NYC CVPD Safety Management Plan | Inspect |
| 402 | 402.3.1 | RF Monitoring System Performance | The NYC CVPD performance monitoring subsystem shall measure the RF received range of each ASD. | Need ID 402: Need to manage equipment health | NYC CVPD ConOps | Inspect |
| 402 | 402.3.2 | RF Monitoring System Performance | The NYC CVPD performance monitoring subsystem shall measure the RF monitoring range of the RSU. | Need ID 402: Need to manage equipment health | NYC CVPD ConOps | Inspect |
| 403 | 403.1.1 | Over-the-Air Firmware Updates | The device supplier shall sign the firmware images and manage the certificate management process for the firmware images. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |
| 403 | 403.1.1.1 | Over-the-Air Firmware Updates | The SCMS certificate shall have a lifespan of years instead of weeks. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |
| 403 | 403.1.1.2 | Over-the-Air Firmware Updates | The SCMS signature scheme shall provide at least 128-bit security. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 403 | 403.2.1 | Over-the-Air Firmware Updates | The ASD shall support a secure session protocol through VPN over TLS to the TMC for protecting the firmware download. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |
| 403 | 403.2.2 | Over-the-Air Firmware Updates | The RSU shall support a secure session protocol through VPN over TLS to the TMC for protecting the firmware download. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |
| 403 | 403.3.1 | Over-the-Air Firmware Updates | The ASD shall partition enough storage space for its current and new firmware images. This is further amplified to ensure that the ASD has sufficient memory to allow the update of all firmware (OS and all applications) and all logs present – such that it can continue to operate properly prior to the changeover to the new version. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Inspect |
| 403 | 403.4.1 | Over-the-Air Firmware Updates | The ASD shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Test |
| 403 | 403.4.2 | Over-the-Air Firmware Updates | The RSU shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted. | Need ID 403: Need to manage CV application life-cycle | NYC CVPD Security Management Operating Concept | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 404 | 404.1.1 | Aftermarket Safety Device | The ASD shall include a threat arbitrator for advisories and alerts presented to the driver in cases where multiple safety advisories are indicated simultaneously. | Need ID 404: Need to manage CV application interrelationship | FHWA-JPO-13-061 | Test |
| 404 | 404.1.2 | Aftermarket Safety Device | The ASD shall incorporate a prioritization scheme as defined in the current version of J2735 for messages such that safety-enhancing messages will have priority over non-safety-enhancing messages. | Need ID 404: Need to manage CV application interrelationship | FHWA-JPO-13-059, SAE J2735 (current version) | Inspect |
| 404 | 404.2.1 | Aftermarket Safety Device | The CV applications in the ASD shall run concurrently. | Need ID 404: Need to manage CV application interrelationship | NYC CVPD Safety Management Plan, ASD specification (current version) | Test |
| 404 | 404.2.2 | Aftermarket Safety Device | The CV applications shall prioritize alerts based on GPS location accuracy to prevent false and missed alarms from being triggered. | Need ID 404: Need to manage CV application interrelationship | NYC CVPD Safety Management Plan, ASD specification (current version) | Test |
| 404 | 404.3.1 | Aftermarket Safety Device | The ASD shall determine the threat arbitration rules for addressing multiple events occurring nearly simultaneously by the specific vehicle type (light-duty, bus, truck/commercial vehicle). | Need ID 404: Need to manage CV application interrelationship | NYC CVPD Safety Management Plan | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 405 | 405.1.1 | ASD RF Monitoring | The ASD shall allow recording of the RF signal level for any message received. (For example, clarification: when the ASD hears a BSM from another vehicle, it will measure and record the RF level of the received message.) | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Demo |
| 405 | 405.1.2 | ASD RF Monitoring | The ASD shall record the first BSM it hears from each unique ASD ID along with its own location (X,Y,Z) and RF level information. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.3 | ASD RF Monitoring | The ASD shall record the first MAP message it hears from each RSU ID along with the contents of its own location (X,Y,Z) at the time and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.4 | ASD RF Monitoring | The ASD shall record the first SPaT message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.5 | ASD RF Monitoring | The ASD shall record the last MAP message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.6 | ASD RF Monitoring | The ASD shall record the last SPaT message it hears from each RSU along with the contents of its own location (X,Y,Z) at the time of receipt and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 405 | 405.1.7 | ASD RF Monitoring | The ASD RF Log Entries shall be stored in the ASD local memory. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Inspect |
| 405 | 405.1.8 | ASD RF Monitoring | The ASD RF log entries shall be purged after 7 days. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Demo |
| 405 | 405.1.9 | ASD RF Monitoring | The ASD RF log space shall be sufficient to store 7 days of interactions with 3,000 ASDs and 450 RSUs, equivalent to about 2,000 entries per day. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Analysis |
| 405 | 405.1.10 | ASD RF Monitoring | If the ASD RF log files exceed the space allocated (Req 405.1.9), then the oldest data shall be written over without damaging newer log files. (Note: the ASD Ethernet port will be fully blocked after certification testing.) | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Inspect |
| 405 | 405.1.11 | ASD RF Monitoring | The following requirements shall apply to the ASD RF data monitoring, uploading, and purging. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.11.1 | ASD RF Monitoring | The ASD shall monitor the control channel (178) when the ASD encounters an RSU that supports the RF data upload. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 405 | 405.1.11.2 | ASD RF Monitoring | The ASD shall upload the contents of the RF logs to the back office systems. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.11.3 | ASD RF Monitoring | The ASD shall purge the logs after they have been acknowledged by the RSU. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.1.12 | ASD RF Monitoring | The ASD shall authenticate all transactions to retrieve the RF logs. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.1 | RSU RF Monitoring | The static RSU shall record the first BSM message it hears from each ASD along with the time and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.2 | RSU RF Monitoring | The static RSU shall record the last BSM message it hears from each ASD along with the time and the RF level. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.3 | RSU RF Monitoring | The RSU shall upload the data to the back office system whenever its buffers are full or more than 60 minutes old. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 405 | 405.2.4 | RSU RF Monitoring | Once the RF log data is received and acknowledged by the back office system, it shall be purged from the RSU. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.5 | RSU RF Monitoring | The RSU shall authenticate all transactions to retrieve its RF logs. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.6 | RSU RF Monitoring | The RSU shall allow recording of the RF signal level for any message received. (For example, clarification: when the RSU hears a BSM from any vehicle, it shall be able to measure and record the RF level of the received message.) | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.7 | RSU RF Monitoring | The mobile RSU shall record the first BSM message it hears from each ASD along with the time and the RF level only when it is stopped. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.2.8 | RSU RF Monitoring | The mobile RSU shall record the last BSM message it hears from each ASD along with the time and the RF level only when it is stopped. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | NYC CVPD ConOps | Test |
| 405 | 405.3.1 | Advanced Traffic Signal Controller | Advanced Traffic Signal Controllers shall use TAI time to issue security credentials. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 405 | 405.3.2 | Advanced Traffic Signal Controller | Advanced Traffic Signal Controllers shall issue messages to DSRC devices with security credentials that meet this document's IEEE 1609.2 requirements. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |
| 405 | 405.3.3 | Advanced Traffic Signal Controller | Advanced Traffic Signal Controllers shall maintain an authenticated NTP based time reference. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |
| 405 | 405.3.4 | Advanced Traffic Signal Controller | Advanced Traffic Signal Controllers shall export their UTC times (Line Frequency referenced from the traffic signal system) as UTC times referenced from their authenticated NTP based time reference. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |
| 405 | 405.4.1 | Roadside Unit | The CV system shall export RSU status to the traffic signal system for display on the traffic signal system map. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |
| 405 | 405.4.2 | Roadside Unit | The CV system shall export RSU RF signal range information to the traffic signal system for display on the traffic signal system map. | Need ID 405: Need to support automatic diagnostics for the system devices (RSU, ASD) | | Test |
| 501 | 501.2.1 | Event Data Recording | The ASD shall include a general purpose event recording application. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1; NYC CVPD Performance Measurement Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 501 | 501.2.1.1 | Event Data Recording | The ASD shall include a rotating 5 minute log of the raw data listed in Table G-4. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Test |
| 501 | 501.2.1.2 | Event Data Recording | Once the log has accumulated 5 minutes of data, it shall replace the oldest data with new data such that it always keeps the most recent 5 minutes of data to a 100 ms accuracy. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Test |
| 501 | 501.2.1.3 | Event Data Recording | Each log entry shall include a UTC time stamp accurate to 10 milliseconds. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Demo |
| 501 | 501.2.1.4 | Event Data Recording | Each log entry shall include the BSM data for the host vehicle regardless of whether the data has changed. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Inspect |
| 501 | 501.2.1.5 | Event Data Recording | Each log entry shall include the peak accelerometer values since last entry. Clarification: accelerometer entries are added to the log whenever the value changes or at 1 second intervals whichever is shorter but not more rapidly than 10 times per second. Thus, the accelerometer entries show the times at which the value changed with a time stamp but no values are lost to the resolution of 1 second. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Demo |
| 501 | 501.2.1.6 | Event Data Recording | Each log entry shall include the BSM data for all vehicles that are within a configurable distance (VDIS) from the host vehicle. (Clarification: typical values are expected to be 0-50 meters.) | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 501 | 501.2.1.7 | Event Data Recording | A log entry shall be made for each SPaT and MAP message received from two nearest RSUs. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Demo |
| 501 | 501.2.2 | Event Data Recording | The ASD shall continuously monitor the location of the host vehicle as described in SAE J2945/1. | Need ID 501: Need to collect detailed information when a warning is issued | SAE J2945/1 | Demo |
| 501 | 501.3.1 | Event Data Recording | The ASD shall collect log entries into an event record to describe vehicle actions surrounding a CV application event. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Inspect |
| 501 | 501.3.2 | Event Data Recording | The ASD shall log the SAE J2735 BSMs received at 100 millisecond interval before and after an event. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Inspect |
| 501 | 501.3.3 | Event Data Recording | The ASD shall log the information 5-300 seconds (configurable by type of event, time period, and resolution) before and 20-50 after the event. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Demo |
| 501 | 501.3.4 | Event Data Recording | The ASD shall collect less detailed CV probe data for mobility data collection. (See ASD Demonstration Procurement Specification Version 2.2 Appendix L Mobility Data Section b for clarification.) | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Inspect |
| 501 | 501.3.5 | Event Data Recording | The durations shall have the capability of being modified by the CV application that triggers the warning. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 501 | 501.3.6 | Event Data Recording | The safety applications listed in Table C-1 shall implement the most recent event recording parameters supplied externally to the application based on their own recording criteria in Table E-3. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Test |
| 501 | 501.4.1 | Event Data Recording | A safety application shall record events based on the most recently received recording parameters set. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Test |
| 501 | 501.4.2 | Event Data Recording | An application shall trigger an event recording when an alert is triggered. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Test |
| 501 | 501.4.3 | Event Data Recording | The event recording application shall collect pre- and post- trigger information using the host application's trigger recording times. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Test |
| 501 | 501.4.4 | Event Data Recording | The safety applications shall collect trigger information (event recording data) listed in Table G-1. | Need ID 501: Need to collect detailed information when a warning is issued | NYC CVPD ConOps | Test |
| 502 | 502.1.1 | Event Record Data Collection | When the event recording receives a triggering input, it shall start the creation of an event record. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 502 | 502.1.2 | Event Record Data Collection | Each event record shall indicate the application and the reason that the alarm was created; (Clarification: each triggering event (alarm) will notify the ASD logging system to initiate the creation of an event record and will provide some application specific (e.g. application ID, value which caused the trigger) information (up to XX bytes indicating the reason for the event); this data shall be included in the “header” for the event record.) | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Test |
| 502 | 502.1.2.1 | Event Record Data Collection | The event record data shall be included in the “header” for the event record. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Test |
| 502 | 502.1.4 | Event Record Data Collection | The before and after times shall be configurable for each different application ID. (Note: different applications may request that the pre and post incident collection times be different from the default.) | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Inspect |
| 502 | 502.1.5 | Event Record Data Collection | The ASD shall accept downloaded parameters to specify the number of seconds to be included in the event record prior to and after the occurrence of the event for each application ID. (Note that the pre-event and post-event collection times may be different values). | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Demo |
| 502 | 502.1.6 | Event Record Data Collection | The event recording application shall be able to simultaneously create and collect event records for up to 10 concurrent or staggered events. Clarification: as one event is concluded, it makes space for additional events. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Test |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 502 | 502.1.7 | Event Record Data Collection | The ASD shall be able to upload the event records to (through) an RSU when the service is available. (Clarification: this is expected to use IP communications – but is not specified at this time. The RSU's located in the barn and at choke points are intended to accomplish this upload process, although this could also be added to any or all of the RSU's.) | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Demo |
| 502 | 502.1.9 | Event Record Data Collection | Event records shall be automatically purged whenever the power is applied to the ASD and the time last log entry is more than a configurable number of hours (example: 96 hours).<br>(Clarification: all of the vehicles for the NYC CVPD are fleet vehicles and hence normally return to their "barn" on a daily basis. However, in some cases, if a fleet vehicle is driven "home" and not returned to a location where an RSU can access its logs, the project would like to recover that data when the vehicle returns to the City if possible without compromising privacy.) | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Test |
| 502 | 502.1.10 | Event Record Data Collection | Log entries shall be inserted in the event log whenever the vehicle engine is running. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Demo |
| 502 | 502.1.12 | Event Record Data Collection | Event records shall only be decrypted by the central performance analysis software. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Analysis |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 502 | 502.2.1 | Mobility Data Collection | The RSUs shall collect the selected mobility data in accordance with Appendix I, section I.3.2 in the NYC CVPD RSU Procurement Specification and transmit this data to the RSU for traffic signal timing plan optimization and analysis for new timing plan development. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Inspection |
| 502 | 502.2.2 | Mobility Data Collection | The RSU shall record the BSM data from the Host Vehicle (HV) in accordance with Appendix I, Section I.3.1, Number 12, in the NYC CVPD RSU Procurement Specification. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Inspection |
| 502 | 502.2.3 | Mobility Data Collection | The BSM data shall be recorded based on distance traveled and time in accordance with Appendix I, Section I.3.1, Number 12, in the NYC CVPD RSU Procurement Specification. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Inspection |
| 502 | 502.2.4 | Mobility Data Collection | The BSM data time and distance parameters shall be configurable in accordance with Appendix I, Section I.3.2 in the NYC CVPD RSU Procurement Specification. | Need ID 502: Need to collect event recordings | NYC CVPD ConOps | Inspection |
| 503 | 503.1.1.2 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average number of stops. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.1.1.3 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speeds of the vehicles. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Inspect |
| 503 | 503.1.1.4 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the reduction in speed limit violations Before and After periods. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 503 | 503.1.1.5 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the speed variations of the vehicles. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Inspect |
| 503 | 503.1.1.6 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the driver actions in response to warnings and vehicle trajectories. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.1.2 | Speed Compliance | The NYC CVPD performance monitoring subsystem shall evaluate the change in speed limit adherence, speed variability, and the average segment speed for each vehicle fleet on a given roadway segment for a given time period (cycle length basis) from the Before period to the After period. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.2.7.1 | Curve Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the crash counts and rates of speed-related crashes from police crash databases. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.2.7.2 | Curve Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the lateral collision. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.2.7.3 | Curve Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the vehicle speeds at curve entry from the Host Vehicle BSM in the event records. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 503 | 503.2.7.4 | Curve Speed Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of warnings generated Before and After period. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.2.8 | Curve Speed Compliance | The NYC CVPD performance monitoring subsystem shall evaluate whether the number of curve speed violations on each applicable studied roadway segment decreases from the Before period to the After period. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.3.4.1 | Speed Compliance / Work Zone | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the average speed of triggered events at work zone compared to posted speeds. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.3.4.2 | Speed Compliance / Work Zone | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the vehicle speed limit violations in variable speed zone areas Before and/or After periods or with/without CV. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.3.4.3 | Speed Compliance / Work Zone | The NYC CVPD performance monitoring subsystem shall utilize the data from the crash databases and measure the work zone related crash counts and rates in reduced speed zones. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 503 | 503.3.4.4 | Speed Compliance / Work Zone | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure time to collision for instantaneous safety in reduced speed zones. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 503 | 503.3.5 | Speed Compliance / Work Zone | The NYC CVPD performance monitoring subsystem shall evaluate whether the number of work zone speed violations on each applicable studied roadway segment decrease from the Before period to the After period and with/without CV. | Need ID 503: Need to assess speed compliance | NYC CVPD ConOps | Demo |
| 504 | 504.1.1 | Common V2V Applications | The NYC CVPD performance monitoring subsystem shall post-process the data surrounding the V2V application events. | Need ID 504: Need to assess vehicle-vehicle crashes | NYC CVPD Performance Measurement Plan | Test |
| 504 | 504.1.1.1 | Common V2V Applications | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the fatality, injury, and property damage only (PDO) crash rates from external crash database sources. | Need ID 504: Need to assess vehicle-vehicle crashes | NYC CVPD Performance Measurement Plan | Test |
| 504 | 504.1.2 | Common V2V Applications | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reportable vehicle-to-vehicle crashes from the Before period to the Pilot period. | Need ID 504: Need to assess vehicle-vehicle crashes | NYC CVPD Performance Measurement Plan | Test |
| 504. | 504.2.5.1 | Vehicle Turning Right in Front of a Transit Vehicle | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the bus / right-turn related crash counts and rates. | Need ID 504: Need to assess vehicle-vehicle crashes | | Inspect |
| 504 | 504.2.5.2 | Vehicle Turning Right in Front of a Transit Vehicle | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure right-turn related conflicts between a bus and another vehicle. | Need ID 504: Need to assess vehicle-vehicle crashes | | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 504 | 504.2.6 | Vehicle Turning Right in Front of a Transit Vehicle | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of bus / right-turn vehicle crashes from the Before period to the Pilot period. | Need ID 504: Need to assess vehicle-vehicle crashes | | Inspect |
| 504 | 504.3.4.1 | Red Light Violation Warning | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the red light violation counts and rates. | Need ID 504: Need to assess vehicle-vehicle crashes | | Demo |
| 504 | 504.3.4.2 | Red Light Violation Warning | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the crash counts and rates related to red light violation. | Need ID 504: Need to assess vehicle-vehicle crashes | | Demo |
| 504 | 504.3.5 | Red Light Violation Warning | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number and severity of red light violations at each studied intersection from the Before period and the Pilot period. | Need ID 504: Need to assess vehicle-vehicle crashes | | Demo |
| 505 | 505.1.5.1 | Pedestrian in Signalized Intersection Warning | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the pedestrian related crash counts and rates. | Need ID 505: Need to assess vehicle-pedestrian crashes | | Inspect |
| 505 | 505.1.5.2 | Pedestrian in Signalized Intersection Warning | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure pedestrian-related conflicts/hard braking events. | Need ID 505: Need to assess vehicle-pedestrian crashes | | Inspect |
| 505 | 505.1.6 | Pedestrian in Signalized Intersection Warning | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported vehicle-to-pedestrian crashes from the Before period to the Pilot period. | Need ID 505: Need to assess vehicle-pedestrian crashes | | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 505 | 505.2.1.1 | Mobile Accessible Pedestrian Signal System | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the number of pedestrian crossing violation reductions. | Need ID 505: Need to assess vehicle-pedestrian crashes | NYC CVPD Performance Measurement Plan | Inspect |
| 505 | 505.2.1.2 | Mobile Accessible Pedestrian Signal System | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the visually-impaired pedestrian-related crash counts and rates. | Need ID 505: Need to assess vehicle-pedestrian crashes | NYC CVPD Performance Measurement Plan | Inspect |
| 505 | 505.2.1.3 | Mobile Accessible Pedestrian Signal System | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the conflicts with visually-impaired pedestrians. | Need ID 505: Need to assess vehicle-pedestrian crashes | NYC CVPD Performance Measurement Plan | Inspect |
| 505 | 505.2.1.4 | Mobile Accessible Pedestrian Signal System | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the wait time for crossing at the intersections. | Need ID 505: Need to assess vehicle-pedestrian crashes | NYC CVPD Performance Measurement Plan | Inspect |
| 505 | 505.2.2 | Mobile Accessible Pedestrian Signal System | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported crashes involving visually-impaired pedestrians from the Before period to the Pilot period. | Need ID 505: Need to assess vehicle-pedestrian crashes | NYC CVPD Performance Measurement Plan | Inspect |
| 506 | 506.1.1.1 | Oversize Vehicle Compliance | The NYC CVPD performance monitoring subsystem shall utilize the post-processed event data and measure the reduction in truck route violations Before and After period. | Need ID 506: Need to assess vehicle-infrastructure crashes | NYC CVPD Performance Measurement Plan | Test |
| 506 | 506.1.2 | Oversize Vehicle Compliance | The NYC CVPD performance monitoring subsystem shall evaluate the change in the number of reported crashes decrease from the Before period to the Pilot period. | Need ID 506: Need to assess vehicle-infrastructure crashes | NYC CVPD Performance Measurement Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 510 | 510.1.1 | Common Safety Applications | The NYC CVPD performance monitoring subsystem shall count the number of events after the events of applications listed in Table C-1 in the Before and After periods. | Need ID 510: Need to assess all CV applications | NYC CVPD ConOps | Demo |
| 510 | 510.2.1 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall normalize, obfuscate, aggregate, and analyze the performance measurement data specified in the Task 5 Performance Measurement Plan. | Need ID 510: Need to assess all CV applications | NYC CVPD ConOps | Demo |
| 510 | 510.5.1 | Weather Data | The NYC CVPD performance monitoring subsystem shall collect hourly weather data observations from the following National Weather Service (NWS) stations in NYC:<br>o Central Park (KNYC)<br>o Kennedy International Airport (KJFK)<br>o LaGuardia Airport (KLGA) | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.5.1.1 | Weather Data | The NYC CVPD performance monitoring subsystem shall obtain the weather data listed in Table G-2. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.5.2 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall utilize the post-processed data and transmit it to the RDE. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.6.1 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall collect and post-process the volume counts from temporary automatic traffic recording (ATR) machines. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 510 | 510.7.1 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall compare and post-process the travel time from MiM RFID tag readers. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.7.3 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall compare and post-process the travel time from MTA bus GPS datasets. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.8.1 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the number of active, inactive, and offline ASDs and RSUs in the field by time of day. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.8.2 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the number of CV applications in operation and warnings produced by time of day. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.8.3 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall generate system performance reports on the network-wide system safety and mobility measurements. (Note: the reports shall include the crash frequencies and average speeds by peak period.) | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.9.1 | IE Performance Monitoring | The NYC CVPD performance monitoring subsystem shall provide obfuscated datasets without PII to the USDOT Independent Evaluator for additional evaluation. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |

| NeedID | ReqID | ReqTitle | Requirement Text | Justification for the Requirement | Source for Justification | Verification Method |
|---|---|---|---|---|---|---|
| 510 | 510.10.1 | Aftermarket Safety Device | The ASD shall have the ability to operate in either silent mode or active mode. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Demo |
| 510 | 510.10.1.1 | Aftermarket Safety Device | The ASD shall record events* without audibly notifying the driver when operating in silent mode. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Demo |
| 510 | 510.10.1.2 | Aftermarket Safety Device | The ASD shall record events* while audibly notifying the driver when operating in active mode. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Demo |
| 510 | 510.10.1.3 | Aftermarket Safety Device | The ASD shall set the application mode to silent mode or active mode per the most recent parameters downloaded. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Demo |
| 510 | 510.10.2 | IE Performance Monitoring | The ASD shall have the capability of operating in active mode and recording normal driver behaviors and reactions while notifying the user of the perceived warnings. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |
| 510 | 510.11.1 | Research Data Exchange | The interface for transferring performance measurement information to the USDOT Research Data Exchange shall be negotiated by the NYC CVPD project team and the USDOT RDE operators during the detailed design of the system in Phase 2. | Need ID 510: Need to assess all CV applications | NYC CVPD Performance Measurement Plan | Inspect |

# APPENDIX C Safety Applications

Table C-1 below lists the V2V, V2I, and I2P safety applications installed and operated by the ASDs in the NYC CVPD system.

**Table C-1. NYC CVPD Safety Applications**

| Type | Application | Abbreviation |
|---|---|---|
| V2V | Forward Crash Warning | FCW |
| | Emergency Electronic Brake Light | EEBL |
| | Blind Spot Warning | BSW |
| | Lane Change Warning | LCW |
| | Intersection Movement Assist | IMA |
| | Vehicle Turning Right in Front of a Bus Warning | VTRW |
| V2I | Speed Compliance | SPDCOMP |
| | Curve Speed Compliance | CSPD-COMP |
| | Speed Compliance / Work Zone | SPDCOMPWZ |
| | Red Light Violation Warning | RLVW |
| | Oversize Vehicle Compliance | OVC |
| | Emergency Communications and Evacuation Information | EVACINFO |
| | Pedestrian in Signalized Intersection Warning | PEDINXWALK |
| I2P | Mobile Accessible Pedestrian Signal System | PED-SIG |

# APPENDIX D Definitions

Table D-1 below lists the definitions of key terms in the system requirements.

**Table D-1. Definitions**

| ReqID | Term | Description |
|---|---|---|
| 101.1.4 | Time of day | NYC CVPD system operating hours |
| 101.2.11, 101.3.11 | Ahead | See MUTCD Table 2C-4 |
| 101.2.15 | Curve alert distance (feet) | Distance required for a vehicle to decelerate from its current speed to the curve advisory speed at a deceleration rate [that is configurable by vehicle type], plus an allowance of <TBD> seconds for driver perception time (Note: this will be detailed in the design phase.) |
| 101.2.16 | Warning | Notification from the ASD to the driver once the ASD determines that the application threshold has been exceeded and violation or crash is imminent. |
| 101.2.16 | Alert | Trigger generated by the once the ASD determines that the application threshold has been exceeded. Once the alert is triggered, the ASD generates the corresponding warning to the driver. |
| 101.2.16 | Time period | Amount of time detected by the ASD in which the application threshold is exceeded by the vehicle |
| 101.2.6, 102.6.7 | Sufficiently accurate position | Road-level accuracy (which needs to be defined at the system level for use in other apps) |
| 101.2.6, 102.6.7 | Sufficiently accurate speed (mph) | Calculation of where to begin the alert use the lower end of the 90% confidence interval for speed. That way the app will issue an alert only if it is confident that one is warranted. |
| 101.2.6, 102.6.7 | Sufficiently accurate heading | First, confidence of the direction of travel on the road (again, needs a system-level determination). Second, projected path includes an instrumented curve. Ordinarily, that will be clear to project. When an exit is within range, we do not know whether the exit will be taken. So say that we know the heading only when the exit and the road have instrumented curves. |
| 101.3.11, 401.14. 23 | Advise, advisory | Initial notification from the ASD to the driver once the ASD determines that the application threshold will exceed and violation or crash is likely to occur. |
| 102.5.5, 102.5,6 | Geographic zone | Pre-defined radius around a point of interest (e.g. bus stop) stored in the MAP message. |

| ReqID | Term | Description |
|---|---|---|
| 102.5.6 | Application alert mode | The control mechanism for audible notifications in either Silent or Active mode, with the default being the Active mode. |
| 102.5.7, 103.1.2 | Impending crash | Crash that is imm<br>inent if the driver does not take action after receiving warning from the ASD. |
| 102.6.15 | In time | Time spent by the driver for processing the application alert from the ASD and taking action (e.g. slow down, divert to an alternate route). |
| 202.1.3, 501.3.6 | Externally | Parameter download process from the TMC to the applications in the ASD. |
| 202.9.2 | Sudden change of direction or speed, sudden stop, or impact | Road-level change in acceleration measured by the accelerometer in the ASD. (Note: this will be detailed in the design phase.) |
| 203.22.1, | Externally | CV equipment installation in the vehicle's exterior. |
| 404.3.1 | Nearly simultaneously | Alerts from multiple applications that occur almost at the same time by the same ASD. |
| 404.3.1 | Threat arbitration rules | Mechanism established by recording parameters for controlling simultaneous or nearly simultaneous alerts from multiple applications and preventing multiple applications from warning the driver, based on priority among the alerts as listed in Table E-2. |
| 501.2.1.1 | Rotating 5 minute log of raw data | Note: the event log entries are expected to be recorded at the frequency of the available data or 10 Hz, whichever is less.<br>For Example, SPaT messages may occur at 10 Hz while MAP messages may occur at 2 Hz, thus the number of each type will vary.<br>Clarification: Measurements shall be recorded whenever they change or at 1 second intervals, whichever is shorter. Each message received (BSM, SPaT, MAP, TIM) shall be recorded regardless of whether the data changes or not as described below. |
| 501.2.1.3 | Log entry | Collection of stored event logs in the ASDs |
| 501.4.2 | Event record | Collection of BSMs generated by the ASDs before and after the alert is triggered. |
| 503.1.2 | Speed variability | The range of vehicle speeds (e.g. 25th to 75th percentile) for each vehicle fleet on a given roadway segment for a given time period from the Before period to the After period. |

| ReqID | Term | Description |
|---|---|---|
| 510.10.1 | Active mode | Operational state in which the device transmits and/or receives DSRC messages while event records are collected. |
| 510.10.1 | Silent mode | Operational state in which the device transmits and/or receives DSRC messages but no event records are collected. |

# APPENDIX E Parameters

Table E-1 below identifies the control parameters for tuning the applications in the NYC CVPD system.

**Table E-1. Application Control Parameters**

| Term | Units | Description | Notes |
|---|---|---|---|
| Minimum Speed Threshold | MPH | The minimum host vehicle speed at which the application monitors vehicle speed and issues alerts. | Used by SPDCOMP. |
| Excessive Speed Amount Threshold | MPH | Increment in speed (mph) above the Posted Speed which the vehicle must exceed for a period exceeding the Excessive Speed Time Threshold before application issues Warning Alert. | Used by SPDCOMP. |
| Excessive Speed Time Threshold | Seconds | Length of time (seconds) the Posted Speed must exceed the Excessive Speed Amount Threshold before application issues Warning Alert. | Used by SPDCOMP. |
| Time To Crash | Seconds | The time-to-crash value calculated by the application to an accuracy of 0.01 seconds | Calculated by FCW. |
| Minimum Curve Speed Threshold | MPH | The minimum host vehicle speed in the curve at which the application monitors vehicle speed and issues alerts. | Used by CSPD-COMP. |
| Excessive Curve Speed Amount Threshold | MPH | Increment in speed (mph) above the Posted Curve Speed which the vehicle must exceed for a period exceeding the Excessive Curve Speed Time Threshold before application issues Warning Alert. | Used by CSPD-COMP. |
| Excessive Curve Speed Time Threshold | Seconds | Length of time (seconds) the Posted Curve Speed must exceed the Excessive Curve Speed Amount Threshold before application issues Warning Alert. | Used by CSPD-COMP. |
| Minimum Zone Speed Threshold | MPH | The minimum host vehicle speed in the zone at which the application monitors vehicle speed and issues alerts. | Used by SPDCOMPWZ. |

| Term | Units | Description | Notes |
|---|---|---|---|
| Excessive Zone Speed Amount Threshold | MPH | Increment in speed (mph) above the Posted Zone Speed which the vehicle must exceed for a period exceeding the Excessive Zone Speed Time Threshold before application issues Warning Alert. | Used by SPDCOMPWZ. |
| Excessive Zone Speed Time Threshold | Seconds | Length of time (seconds) the Posted Zone Speed must exceed the Excessive Zone Speed Amount Threshold before application issues Warning Alert. | Used by SPDCOMPWZ. |
| Stop Bar Tolerance | Feet | Tolerance in distance to stop bar (feet) used to adjust when application issues Red Light Violation Warnings. | Used by RLVW. |
| Yellow Duration Tolerance | Seconds | Tolerance in Yellow Duration (seconds) used to adjust when application issues Red Light Violation Warnings. | Used by RLVW. |
| Advisory Distance Threshold | Feet | The minimum distance before the driver can exit the restricted roadway and find an alternate route. | Used by OVC |
| Warning Distance Threshold | Feet | The minimum distance for the vehicle to completely stop and avoid crashing into the bridge, overpass, or tunnel entrance. | Used by OVC |
| Transit Bus Length | Feet | Length of the transit vehicle | Used by VTRW and PEDINXWALK |
| Transit Bus Width | Feet | Width of the transit vehicle | Used by VTRW and PEDINXWALK |

Table E-2 below lists the parameters needed by multiple safety applications. All applications need a parameter that can be used to stop the application from providing alerts. For most applications, this can be the minimum speed where the application is active. If the minimum speed for an application is set to 100 mph, the application is essentially disabled. The oversized vehicle compliance application does not have a minimum speed, but it can be disabled by broadcasting an expiration time for the Traveler Information Message (TIM) it is based on. The Emergency Communications and Evacuation Information (EVAC) app operates via TIM messages as well, and is essentially always inactive unless an EVAC TIM message has been received.

All vehicle safety applications also have a recorded sound that plays to present the alert to the driver. Audible messages for the Emergency Evacuation application are transmitted as needed, so the ability to download a sound is required for this application. Using that ability to change the alert sounds for other applications during the testing period will provide flexibility to experiment with buzzers and phrases.
A minimum confidence level parameter will enable the applications to be adjusted for accuracy. Exactly how that works will depend on the implementation.

Vehicle-specific values, notably size, are encoded in the ASD when it is installed in the vehicle. Whether these should be adjustable only with physical access to the vehicle is a question for discussion. Locating a vehicle known to have incorrect dimensions could be difficult. On the other hand, dimensions are best confirmed when the vehicle is present.

The vehicle-dependent maximum braking capability is a remotely tunable parameter needed by some applications. The vehicles do not sense whether they are loaded, so the braking capability will assume the vehicle is loaded. None of the applications account for surface conditions or other weather-related conditions

To support the performance evaluation, engineering data will be recorded whenever an application is triggered. Event recording parameters are the pre-trigger recording time and the post-trigger recording time, which may vary by application. Additional event recording parameters, such as recording resolution (e.g., percentage of BSMs to be recorded), may also be desired.

The top-level software on the ASD needs parameters to utilize threat arbitration and control simultaneous or nearly simultaneous alerts from multiple applications. The priority among the alerts is most simply stored as an order, 1-13, of the vehicle safety applications. There is also a minimum quiet time between two alerts, or alert spacing.

Note that Table E-2 provides an initial list of the parameters in the NYC CVPD system. Therefore, each application includes a number of free parameters to be considered for future decisions.

**Table E-2. Preliminary Summary of Adjustable Parameters by Application**

| Term | SPD-COMP | CSPD-COMP | SPDCOMP WZ | FCW | EEBL | LCW | IMA | VTRW | PEDIN XWALK | OVC | RLVW | EVAC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Minimum speed when active | maybe | maybe | maybe | maybe | maybe | maybe | ✓ | ✓ | maybe | | maybe | |
| Sound | ✓ | ✓ | ✓ | ✓ | ✓ | L & R | L & R | ✓ | F & L & R | turn & stop | ✓ | special |
| Minimum confidence level | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vehicle dimensions | | | | | | | | l w | | h | l | l w h |
| Braking capability | | | | maybe | maybe | | | | maybe | | maybe | |
| Event Recording Parameters | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| App priority | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Alert spacing | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Term | SPD-COMP | CSPD-COMP | SPDCOMP WZ | FCW | EEBL | LCW | IMA | VTRW | PEDIN XWALK | OVC | RLVW | EVAC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Free parameters for expansion | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 4 | 2 | 1 | 1 | 1 |
| Excessive speed amount | ✓ | ✓ | ✓ | | | | | | | | | |
| Excessive speed time | ✓ | ✓ | ✓ | | | | | | | | | |
| Day and night start hours | ✓ | | | | | | | | | | | |
| Maximum Distance | | | | ✓ | ✓ | | ✓ | | | | | |
| Minimum for unavoidable crash | | | | ✓ | | | | | | | | |
| Hard braking threshold (RV) | | | | | ✓ | | | | | | | |
| Whether to act on adjacent lanes | | | | | ✓ | | | | | | | |
| Whether to warn on turn signal | | | | | | ✓ | | | | | | |
| Whether to warn on movement | | | | | | ✓ | | | | | | |
| Maximum RV range for approach | | | | | | ✓ | | | | | | |
| Minimum acceleration | | | | | | | ✓ | | | | | |
| Closest permitted approach | | | | | | | ✓ | | | | | |
| Path prediction parameters | | | | | | | | ✓ | maybe | | | |
| Ped call detection | | | | | | | | | maybe | | | |
| Deceleration threshold | | | | | | | | | ✓ | | ✓ | |
| Maximum permitted rolling stop | | | | | | | | | | | ✓ | |
| Sufficient braking threshold | | | | | | | | | ✓ | | ✓ | |

Table E-3 below defines the event recording parameters for collecting the event records before and after warning is triggered.

**Table E-3. Event Recording Parameters**

| Term | Units | Description | Notes |
|---|---|---|---|
| Pre-trigger Recording Time | Seconds | The time period prior to the trigger from which DSRC messages (BSM, MAP, SPaT, TIM), application parameters, and vehicle performance data are to be incorporated into the event record as specified for the Safety Applications. | |
| Post-trigger Recording Time | Seconds | The time period after the trigger from which DSRC messages (BSM, MAP, SPaT, TIM), application parameters, and vehicle performance data are to be incorporated into the event record as specified for the Safety Applications. | |
| Recording Resolution | Seconds | Period used to record BSM. Use either 0.1, 1, or 5 seconds. | The applications have differing needs for recording the BSM information due to the driver response. Some applications need short time periods while others need longer time periods to verify driver reaction. Examples of applications with short period needs are Red Light Violation Warning. Examples of applications with long period needs are Oversize Vehicle Compliance and Speed Compliance / Work Zones. |
| Sphere of Influence Distance | Meters | The range around the connected vehicle in which the events from application triggers are recorded | |
| Hard Braking Threshold | Meters per Square Second | The deceleration rate of 0.4g as defined in J2945/1, section 3.1, which is considered to be the threat vehicle in the application. | Used by EEBL. The vehicle that generates the BMS indicating an EEBL has exceeded the hard braking threshold (decal > 0.4g). The threat vehicle transmits the hard breaking via BSM and the host vehicles that react to it are in the same or adjacent lane to the threat vehicle and behind the threat vehicle. |

| Term | Units | Description | Notes |
|---|---|---|---|
| Maximum Distance Threshold | Feet | The maximum distance allowed from a host vehicle to the threat vehicle for generating an EEBL alert. | Used by EEBL, FCW. This limits the host vehicle's generation of a trigger to within this distance of the threat vehicle. |
| Time To Crash | Seconds | The time-to-crash value calculated by the application to an accuracy of 0.01 seconds | Calculated by FCW. |

Table E-4 below presents the event recording data parameters needed for the ASD to collect the event records before and after warning is triggered.

**Table E-4. Event Recording Parameters by Application**

| Application | Event Recording Data Parameter |
|---|---|
| SPD-COMP | SPD-COMP Application Alert Mode<br>SPD-COMP Application Pre-trigger Recording Time<br>SPD-COMP Application Post-trigger Recording Time<br>SPD-COMP Application Recording Resolution<br>SPD-COMP Application Sphere of Influence Distance |
| CSPD-COMP | CSPD-COMP Application Alert Mode<br>CSPD-COMP Application Pre-trigger Recording Time<br>CSPD-COMP Application Post-trigger Recording Time<br>CSPD-COMP Application Recording Resolution<br>CSPD-COMP Application Sphere of Influence Distance |
| SPDCOMPWZ | SPDCOMPWZ Application Alert Mode<br>SPDCOMPWZ Application Pre-trigger Recording Time<br>SPDCOMPWZ Application Post-trigger Recording Time<br>SPDCOMPWZ Application Recording Resolution<br>SPDCOMPWZ Application Sphere of Influence Distance |
| VRTW | VTRW Application Alert Mode<br>VTRW Application Pre-trigger Recording Time<br>VTRW Application Post-trigger Recording Time<br>VTRW Application Recording Resolution<br>VTRW Application Sphere of Influence Distance |

| Application | Event Recording Data Parameter |
|---|---|
| RLVW | RLVW Application Alert Mode<br>RLVW Application Pre-trigger Recording Time<br>RLVW Application Post-trigger Recording Time<br>RLVW Application Recording Resolution<br>RLVW Application Sphere of Influence Distance |
| PEDINXWALK | PEDINXWALK Application Alert Mode<br>PEDINXWALK Application Pre-trigger Recording Time<br>PEDINXWALK Application Post-trigger Recording Time<br>PEDINXWALK Application Recording Resolution<br>PEDINXWALK Application Sphere of Influence Distance |

Table E-5 below lists the performance monitoring data parameters that will be collected from the vehicle bus and monitored on the in-vehicle network for the performance evaluation of the NYC CVPD system.

**Table E-5. Vehicle Performance Monitoring Parameters**

| Vehicle Performance Monitoring Parameter |
|---|
| Directional Signals |
| Hard Breaking |
| Steering Wheel Angle |
| Hard Break |
| Braking Status |
| Steering Turns |
| Turn-Signal Indicator |
| Acceleration |

# APPENDIX F DSRC Devices

Table F-1 below identifies the details of each DSRC channel to be used in the NYC CVPD system infrastructure.

**Table F-1. DSRC Channel Assignment**

| DSRC Channel | Purpose |
|---|---|
| 172 | For transmission of the DSRC messages: BSM, SPaT, MAP, and TIM |
| 174 | Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA software updates and application parameter changes and provide SCMS access |
| 176 | Service channel for WAVE Short Message Protocols (WSMP) that indicate OTA software updates and application parameter changes and provide SCMS access |
| 178 | Control channel for WAVE Service Advertisements that announce the device supports specific additional services for PED applications, parameter changes, OTA software updates, credential acquisition, and uploading of log files collected |
| 180 | Service channel for uploading event log files to the TMC |
| 182 | Service channel for uploading event log files to the TMC |

Table F-2 below describes the potential device fail modes in the NYC CVPD system.

**Table F-2. Device Fail Modes (Preliminary)**

| Fail Mode | Description |
|---|---|
| Mechanical | Corrosion, shock |
| Electrical | Electrostatic discharge, short circuit |
| Location Accuracy Loss | Device's location accuracy estimates exceeds the minimum performance ranges established by standards. |
| Certificates Unavailable | The device has been refused additional operational certificates. |

# APPENDIX G Data Tables

Table G-1 below presents the event recording data that the ASD collects before and after warning is triggered.

**Table G-1. Event Recording Data**

| Application | Event Recording Data |
|---|---|
| SPD-COMP | Event Type: SPD-COMP<br>Event Timestamp<br>Regulatory Speed<br>Vehicle Speed<br>Excessive Speed Amount Threshold<br>Excessive Speed Time Threshold<br>Excessive Criteria Exceeded (Time or Amount)<br>Host Vehicle BSM for pre-trigger and post-trigger time periods |
| CSPD-COMP | Event Type: CSPD-COMP<br>Event Timestamp<br>Posted Curve Speed<br>Vehicle Speed<br>Excessive Curve Speed Amount Threshold<br>Excessive Curve Speed Time Threshold<br>Excessive Criteria Exceeded (Time and/or Amount)<br>Host Vehicle BSM |
| SPDCOMPWZ | Event Type: SPDCOMPWZ<br>Event Timestamp<br>Posted Zone Speed<br>Vehicle Speed<br>Excessive Zone Speed Amount Threshold<br>Excessive Zone Speed Time Threshold<br>Excessive Criteria Exceeded (Time and/or Amount)<br>Host Vehicle BSM |
| VRTW | Event Type: VTRW<br>Event Timestamp<br>Host Vehicle BSM<br>Remote Vehicle BSM |
| RLVW | Event Type: RLVW<br>Event Timestamp<br>Vehicle Speed<br>Vehicle Deceleration<br>Distance to Stop Bar<br>Stop Bar Tolerance<br>Yellow Duration Tolerance<br>SPaT Messages<br>MAP Message<br>Host Vehicle BSMs (includes vehicle location) |

| Application | Event Recording Data |
|---|---|
| PEDINXWALK | Event Type: PEDINXWALK<br>Event Timestamp<br>Signal Phase and Timing Parameters<br>Pedestrian Detection Parameters<br>Host Vehicle BSM |

Table G-2 below shows the available weather measures from the NWS that will be collected by the NYC CVPD system.

**Table G-2. Weather Data**

| Weather Data Measure |
|---|
| observation_time |
| observation_time_rfc822 |
| weather |
| temperature_string |
| temp_f |
| temp_c |
| relative_humidity |
| wind_string |
| wind_dir |
| wind_degrees |
| wind_mph |
| wind_kt |
| pressure_string |
| pressure_mb |
| pressure_in |
| dewpoint_string |
| dewpoint_f |
| dewpoint_c |
| visibility_mi |

Table G-3 below lists the preliminary list of the performance data for the PED-SIG application as stated in Req 104.5.11 in Section 3.8.4.1.

**Table G-3. Preliminary PED-SIG Application Performance Data**

| PED-SIG Application Performance Data |
|---|
| Number of pedestrian crossing violation reductions |
| Visually-impaired pedestrian-related crash counts, by severity |
| Conflicts with visually-impaired pedestrians |
| Time to collision (vehicle to pedestrian) |
| Waiting time at intersection for crossing |

Table G-4 below defines the rotating 5-minute log of the raw data generated by the ASD as stated in Req 501.2.1.1.

**Table G-4. 5-Minute Log of the Raw Data**

| 5-Minute Log of the Raw Data |
|---|
| BSM (Host Vehicle) |
| BSM (each Remote Vehicle) |
| MAP |
| SPaT |
| TIM |
| Vehicle Performance Values |

# As-Built Addendum

This section highlights changes made to the overall SyRS due to the final deployment and the schedule of activity. Elements within this section supersede portions of the document not altered to reflect the details of the changes.

a. The PID application to assist the visually impaired pedestrian at CV equipped intersections has changed significantly. The SPaT information is received from the ASTC, combined with the MAP information stored at the TMC and sent to the AWS cloud where the SmartCross application process the data and distributes it to the appropriate PID using a cellular service. The data is then collected and exported to the NYU data collection system where it is evaluated. Instead of distributing PIDs to the user community for testing/trials and evaluation, the 10 prototypes will be used with selected participants who will test/trial the PID application in a protected and assisted environment. Evaluation of the preliminary results indicated that the application was not robust enough to be distributed without supervision in a protected environment. The detailed design is provided in a separate document. Section 2.3.4 and Figure 2-6 have been updated accordingly. In addition, the PID will not be enrolled with the SCMS as previously described.
b. Note that the communications between the TMC and the RSU uses 2 different protocols: SNMPv3 for management of the MIB objects supported by the RSU, and XFER a proprietary protocol developed by the RSU vendor for uploading and downloading files used for data collection, and RSU configuration. It should be noted that NTCIP 1218 had not been developed at the time of this project, and it was necessary to utilize the vendor's protocol to support these exchanges. The vendor has made this protocol readily and publicly available without restriction for use with their RSUs.
c. While there is some discussion of the use of UPS participation and the participation of the Taxi fleets/owners, both of these did not become active participants in the project, The fleet is primarily composed of various City fleets including DCAS, Parks, DOT, Department of Corrections (DOC), Department of Environmental Protection (DEP), Department of Health Services (DHS), and other service fleets operated by NYC. The City fleets are generally equipped with Geotab devices which monitors their general usage; this data has been available to the CVPD project to determine the general routes and locations frequented by the City fleets participating in the CVPD project. This data will be used to evaluate the accuracy of the data collected and to assist the project in monitoring the health of the CV equipped vehicles.
d. The HSM is a rack-mountable appliance installed at the TMC to expand TMC operations with direct-to-vehicle messaging over latest V2X network technology. Traveler Information, MAP, and other infrastructure messages are inspected and digitally signed to prevent hacking so TMC messages can be trusted. The HSM authenticates incoming messages and signs certificates for outgoing messages to and from the TMC. The HSM inspects and formats TMC messages for acceptance by V2X networked devices. Installed RSUs and ASDs do not require any additional components. In addition to the NYCDOT TMC back-office management functions, the HSM has been critical for maintaining the security of the data being transmitted. Also known as the TMC Authority, provides complete support for IEEE 1609.2 algorithms and protocols including SAE J2735, and J2945/x. It also provides FIPS 140-2 Level 3 protection for V2X signing keys. The TMC Authority checks and digitally signs traffic management center messages for instant verification and acceptance, compliant with IEEE 1609.2 standards and cryptography. Data is

secured inside and out with FIPS 140-2 Level 3 protection of keys and TLS v1.2 tunnels to TMC servers. High availability network failover is standard, including redundant power supplies and storage; the TMC Authority maintains trusted reliable operation, even in untrusted environments.

e. Achieving location augmentation has been critical especially in the urban canyon parts of the NYC CV Pilot area. To improve location accuracy for the DSRC devices in the NYC CV project, using the DSRC Radio Technical Commission for Maritime (RTCM) was considered first. As defined in SAE J2735, the RTCM messages would be transmitted along with the other DSRC messages over channel 172. However, the V2XLocate technology was chosen instead after multiple tests and demonstrations in the Manhattan grid section of the NYC CV pilot area.

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-16-303

U.S. Department of Transportation