Connected Vehicle Environment (CVE) System Requirements

for the Smart Columbus
Demonstration Program

UPDATED REPORT | May 20, 2021

Produced by City of Columbus

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Acknowledgement of Support

This material is based upon work supported by the U.S. Department of Transportation under Agreement No. DTFH6116H00013.

Disclaimer

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

This Systems Requirements Specification (SyRS) is intended to provide the requirements that drive the specification, design, development, implementation, integration and testing of the Smart Columbus Connected Vehicle Environment (CVE). The SyRS is a “black-box” description of what the CVE must do, but not how it will do it. The document contains descriptions of inputs, outputs, and required relationships between inputs and outputs.

1.1. DOCUMENT PURPOSE

This System Requirement Specification (SyRS) serves as the second in a series of engineering documents intended to describe the CVE, building upon the Concept of Operations (ConOps) Document. The SyRS describes a set of requirements that, when realized, will satisfy the expressed needs of the CVE. This document includes the identification, organization and presentation of the requirements for the CVE project, which is a system made up of Connected Vehicle (CV) infrastructure and applications. These requirements are derived from the user needs, constraints and interfaces that the CVE is expected to implement, and the work within leverages prior system requirements efforts for related projects and applications. This SyRS addresses conditions for incorporating operational concepts, design constraints, and design configuration requirements as well as the necessary characteristics and qualities of individual requirements and the set of all requirements.

This document was developed based on IEEE 1233-1998 IEEE Guidance for Developing System Requirements Specifications and contains the following chapters:

- **Chapter 1. Introduction** provides an overview of the CVE project and key elements that guide the development of this SyRS document, including an overview of the project, the stakeholders, requirements development process, and referenced materials.
- **Chapter 2. System Description** focuses on describing and extending the CVE system concepts established in the Concept of Operations (ConOps), including system capabilities, conditions, constraints, and decomposing the system into its functional groups for establishing requirements.
- **Chapter 3. System Requirements** contains the requirements for each functional group that make up the system.
- **Chapter 4. Engineering Principles** provides a description of engineering principles applied to the system and requirements definition process.

1.2. PROJECT SCOPE

In 2016, the U.S. Department of Transportation (USDOT) awarded $40 million to the City of Columbus, Ohio, as the winner of the Smart City Challenge. With this funding, Columbus intends to address the most pressing community-centric transportation problems by integrating an ecosystem of advanced and innovative technologies, applications, and services to bridge the sociotechnical gap and meet the needs of residents of all ages and abilities. In conjunction with the Smart City Challenge, Columbus was also awarded a $10 million grant from Paul G. Allen Family Foundation to accelerate the transition to an electrified, low-emissions transportation system.

With the award, the City established a strategic Smart Columbus program with the following vision and mission:

- **Smart Columbus Vision**: Empower residents to live their best lives through responsive, innovative, and safe mobility solutions
- **Smart Columbus Mission**: Demonstrate how Intelligent Transportation Systems (ITS) and equitable access to transportation can have positive impacts on every day challenges faced by cities

To enable these new capabilities, the Smart Columbus program is organized into three focus areas addressing unique user needs: enabling technologies, emerging technologies, and enhanced human services. The CVE primarily addresses needs in the enabling technologies focus area. The CVE project is one of the eight projects in the Smart Columbus program and is a significant enabler to other technologies delivered through the other seven projects. The CVE project will integrate smart traveler applications, automated vehicles, connected vehicles, and smart sensors into its transportation network by focusing on deploying CV infrastructure and CV applications.

- **CV Infrastructure** – The project will focus on building out the physical and logical CV infrastructure, which will consist of CV hardware and software (e.g. roadside units (RSUs), on-board equipment, front and backhaul communications, equipment interfaces, etc.). The CVE will generate the needed transportation-related data that are used by applications.
- **CV Applications and Data** – The project scope also consists of deploying CV-specific applications that will leverage the data generated by the infrastructure to deliver real-time safety and mobility services. Data will be collected, related, stored, and made available for use in other Smart Columbus project applications.

The CVE is expected to enhance safety and mobility for vehicle operators and improve pedestrian safety in school zones by deploying CV infrastructure on the roadside and CV equipment in vehicles. The CVE will also provide sources of high-quality data for traffic management and safety purposes.

The foundation for the CVE is the Columbus traffic-signal system (CTSS), which is an open-architecture, computerized traffic-signal system and communications network that allows the City to monitor many of the region's signalized intersections, traffic surveillance monitors, pavement weather sensors, and snow and ice crews using a high-speed network backbone. When complete, the CTSS will interconnect up to 1,250 traffic signals in the Columbus region and provide uniform signal coordination capability throughout the system. The existing CTSS network was leveraged to connect to CV equipment at intersections along four select corridors and to equipment at intersections along the Alum Creek corridor managed by Franklin County, the Village of Obetz, and Ohio Department of Transportation (ODOT). Deployment of in-vehicle devices target populations near frequently used infrastructure deployment corridors. **Table 1** lists the improvements associated with the CVE project.

Table 1: Connected Vehicle Environment Project Scope

Infrastructure		Applications and Data	
85+ RSUs The project will install RSUs and other CV-compatible equipment at signalized intersections in the project areas.	**1,000+ OBUs** The project will install onboard units (OBUs) on participating private, emergency, transit, and freight vehicles.	**11 CV Applications** The project will deploy vehicle-to-vehicle (V2V) safety, vehicle-to-infrastructure (V2I) safety, and V2I mobility applications.	**Data Capture** The project will capture, relate, store, and respond to data generated by the infrastructure, used by the applications for traffic management.

Source: City of Columbus

The intent of the CVE project is to improve safety and mobility of travelers by deploying CV technology as part of a larger initiative within the City to improve the overall transportation system. CV technology will also be deployed to support the improvement in freight operations, another of the City's goals.

Collectively, CV is just one component, but if it proves to be effective, other projects can also benefit from the positive outcomes. Because the CVE primarily intends to deploy CV technology (not the development of new applications or functionality), it is important for the reader to understand that the ability of the CVE to address the user needs captured in the ConOps depends on the availability of deployment-ready hardware and software solutions. Thus, the design and implementation of the CVE will draw on these previous development efforts. The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)[1] and its predecessor, the Connected Vehicle Reference Implementation Architecture (CVRIA)[2], are resources that provide descriptions of CV applications that have been researched in the context of the National ITS architecture. Furthermore, the USDOT ITS Joint Program Office's (JPO) ITS CodeHub, formally the Open Source Application Development Portal (OSADP), contains software for applications that have been developed.[3] When possible, applications on ARC-IT, CVRIA and OSADP will be used as-is or will have minimal modifications made to address user needs documented in the ConOps.

Given that the primary scope of the CVE is to realize the benefits of deploying CV technology into an operational environment, only applications that have demonstrated sufficient levels of development and testing are being considered for implementation. However, the CVE will be designed in such a way that added functionality concepts (that need further development) can be integrated with the CVE once development and testing have matured to a point where applications are deployment-ready. Additionally, due to the networked nature of devices in the CVE, several policies and constraints related to information technology (IT) and data security are expected to be developed as part of the deployment.

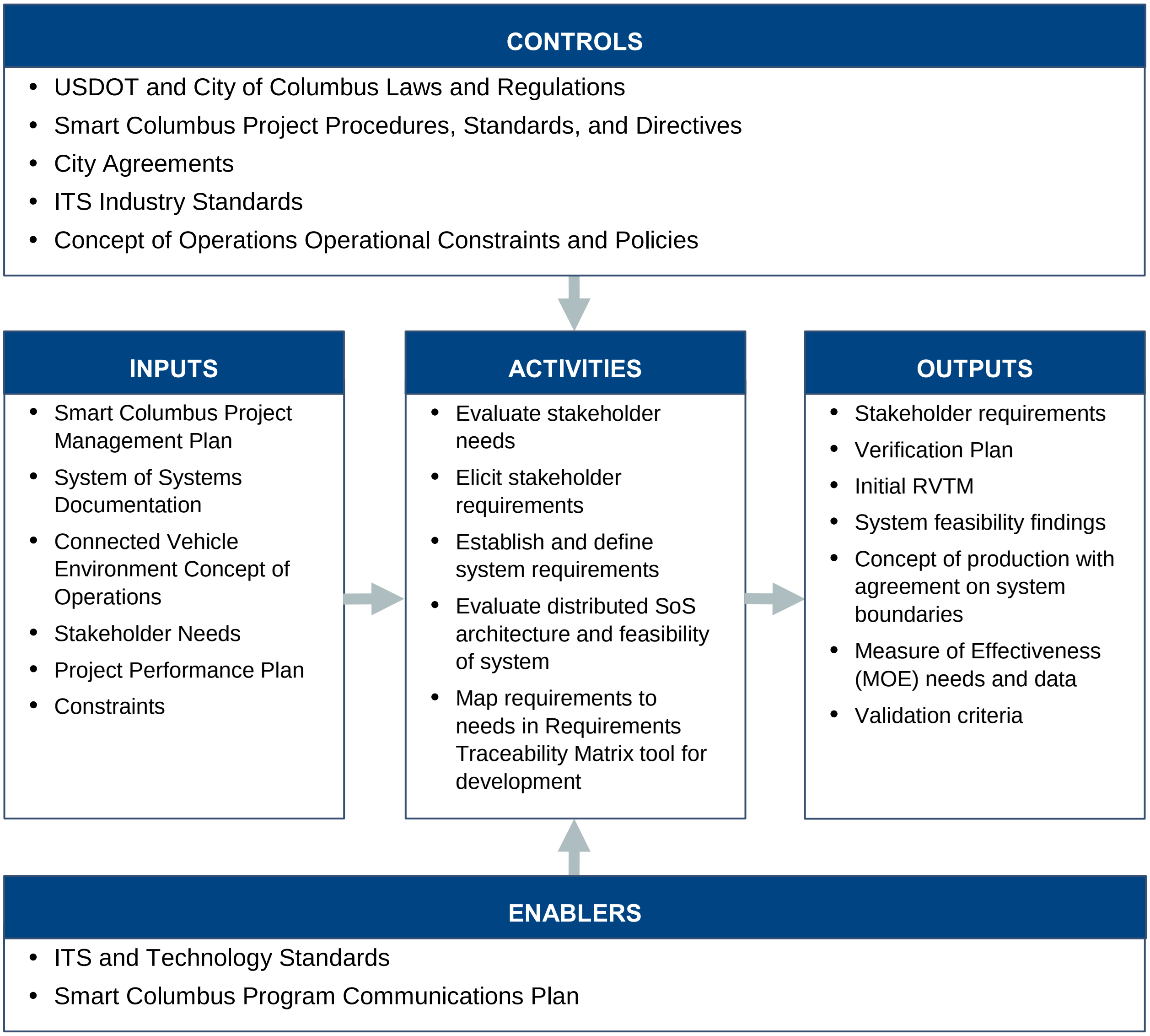
[1] https://local.iteris.com/arc-it/

[2] https://local.iteris.com/cvria/

[3] ITS Code Hub. https://its.dot.gov/code/

1.3. REQUIREMENTS PROCESS

The requirements established for this project will govern the CVE system's development cycle and are an essential factor in further defining and clarifying the scope and feasibility of development for the system. This process will also provide the basis for the technical description of deliverables in the form of a system-level specification and defined interfaces at the system boundaries. **Figure 1** provides a high-level view of the project's stakeholder requirements definition process. Once the project's requirements are established they will be formally placed under configuration control using the Helix software system.



CONTROLS

- USDOT and City of Columbus Laws and Regulations
- Smart Columbus Project Procedures, Standards, and Directives
- City Agreements
- ITS Industry Standards
- Concept of Operations Operational Constraints and Policies

INPUTS

- Smart Columbus Project Management Plan
- System of Systems Documentation
- Connected Vehicle Environment Concept of Operations
- Stakeholder Needs
- Project Performance Plan
- Constraints

ACTIVITIES

- Evaluate stakeholder needs
- Elicit stakeholder requirements
- Establish and define system requirements
- Evaluate distributed SoS architecture and feasibility of system
- Map requirements to needs in Requirements Traceability Matrix tool for development

OUTPUTS

- Stakeholder requirements
- Verification Plan
- Initial RVTM
- System feasibility findings
- Concept of production with agreement on system boundaries
- Measure of Effectiveness (MOE) needs and data
- Validation criteria

ENABLERS

- ITS and Technology Standards
- Smart Columbus Program Communications Plan

Source: City of Columbus

Figure 1: Connected Vehicle Environment Stakeholder Requirements Definition Process

1.4. REFERENCES

Table 2 contains documents, literature, and Working Group Sessions used to gather input for this document.

Table 2: References

Document Number	Title	Rev	Pub. Date
FHWA-JPO-17-518	Smart Columbus Systems Engineering Management Plan (SEMP) for Smart Columbus Demonstration Program https://d2rfd3nxvhnf29.cloudfront.net/2019-08/Smart%20Columbus%20Systems%20Engineering%20Management%20Plan_0.pdf	V3	January 16, 2018
–	Beyond Traffic: The Smart City Challenge – Phase 2 – Volume 1: Technical Application https://d3hzplpmmz6qe4.cloudfront.net/2019-07/Columbus%20Smart%20City%20Challenge%20Technical%20Application.pdf	–	July 29, 2016
–	Security Credential Management System Proof–of–Concept Implementation – EE Requirements and Specifications Supporting SCMS Software Release 1.0 http://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements20160111_1655.pdf	–	January 11, 2016
1233-1998	IEEE Guidance for Developing System Requirements Specifications	–	1998
INCOSE-TP-2003-002-03.2.2	INCOSE Systems Engineering Handbook	3.2.2	2011
–	Systems Engineering Guidebook for Intelligent Transportation Systems	3.0	2009
–	Concept of Operations for the Connected Vehicle Environment for the Smart Columbus Demonstration Program https://d2rfd3nxvhnf29.cloudfront.net/2021-05/SCC-B-CVE-ConOps-Update%205.14.21.pdf	Updated	May 14, 2021
–	SPaT Challenge Verification Document	1.2	October 30, 2017
FHWA-JPO-16-315	Connected Vehicle Pilot Deployment Program Phase 1, System Requirements Specification (SyRS) – Tampa (THEA)	–	August 2016
FHWA-JPO-16-303	Connected Vehicle Pilot Deployment Program Phase 1 Systems Requirements Specification (SyRS) – New York City	–	July 2016

Document Number	Title	Rev	Pub. Date
SAE J2735 _201603	Dedicated Short Range Communications (DSRC) Message Set Dictionary	_	March 2016
SAE J2945/1 _201603	On-Board System Requirements for V2V Safety Communications	_	March 2016
SAE J2945/4 (draft)	Road Safety Applications	_	–
SAE J2945/9 (draft)	Performance Requirements for Safety Communications to Vulnerable Road Users	_	–
IEEE 802.3	IEEE Standard for Ethernet	_	2015
IEEE 802.11p	Wireless Access in Vehicular Environments	_	–
IEEE 1609.2	IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages	_	2016
IEEE 1609.3	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services	_	2016
IEEE 1609.4	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation	_	2016
NTCIP 1202	NTCIP Object Definitions for Actuated Traffic Controllers	3	January 2005
NTCIP 1211	NTCIP Objects for Signal Control and Prioritization (SCP)	–	October 2014

Source: City of Columbus

1.5. PROJECT CHANGES DURING DEVELOPMENT

Since the initial release in the CVE Systems Requirements Document in November 2018, and during the subsequent deployment of the CVE system, several changes to system requirements have occurred. These changes have been accounted for in this document and are summarized in the list below. Note that this section does not include any clarifying details about system requirements, rather only the major items that changed during development.

The following requirements have been modified or added:

- The Roadside Safety Message (SAE J2945/4) has been replaced by the Traveler Information Message (SAE J2735:2016).
- Requirements associated with the RSU generating SPaT, SSM, RTCM, and other messages have been modified to indicate these messages are generated by roadside equipment.
    - The Message Handler generates SPaT, SSM, RTCM, etc., but since the Message Handler was part of the Design, “roadside equipment” is used as a generic term.

- Requirements associated with MAP and TIM messages being stored on the RSU have been modified to indicate these messages are stored on roadside equipment.
  - MAP and TIM messages are stored on the Message Handler, but since the Message Handler was part of the Design, “roadside equipment” is utilize as a generic term.
- Requirements associated with applications using MMITTS algorithms have been modified to use a “proven” algorithm.
  - The OBU provider supplied applications they developed for other deployments that were not based on MMITSS algorithms but had been proven and meet the specific application requirements.
- Requirements associated with applications using CAMP algorithms have been modified to use a “proven” algorithm.
  - The OBU provider supplied applications they developed for other deployments that were not based on CAMP algorithms but had been proven and meet the specific application requirements.
- Requirements associated with RTCM message types were modified to reflect the message types required by the OBU.
  - Message Types 1001 and 1005 were replaced with Types 1 and 2, respectively and Requirements were added for Message Types 3 and 9.
- The modifiable OBU ID list has been replaced with a list of SRM BasicVehicleRoles.
- RSUs broadcast V2I messages on Channel 180.
- WSA content Requirements were added.
- Requirements were added for RSUs to specifically support OBU firmware and certificate downloads.

The following requirements have been removed/deprecated:

- All requirements associated with Truck Platooning have been removed.
  - The Truck Platooning feature was not implemented.
- All requirements associated with HDV BSM Part II, Trailer information, have been removed
  - BSM Trailer information was not added to the BSM.
- All requirements associated with the RSU logging messages have been removed.
  - All messages are sent to the TCVMS as they are received by an RSU; messages are not logged at the roadside.
- All requirements associated with emergency vehicle and heavy-duty vehicle Human Machine Interface (HMI) have been removed.
  - HMIs were not installed in these vehicle types.
- All requirements associated with the TCVMS providing e-mail alerts have been removed

  - RSU related alerts are displayed on the TCVMS dashboard, e-mails are not sent to Traffic Management Staff.

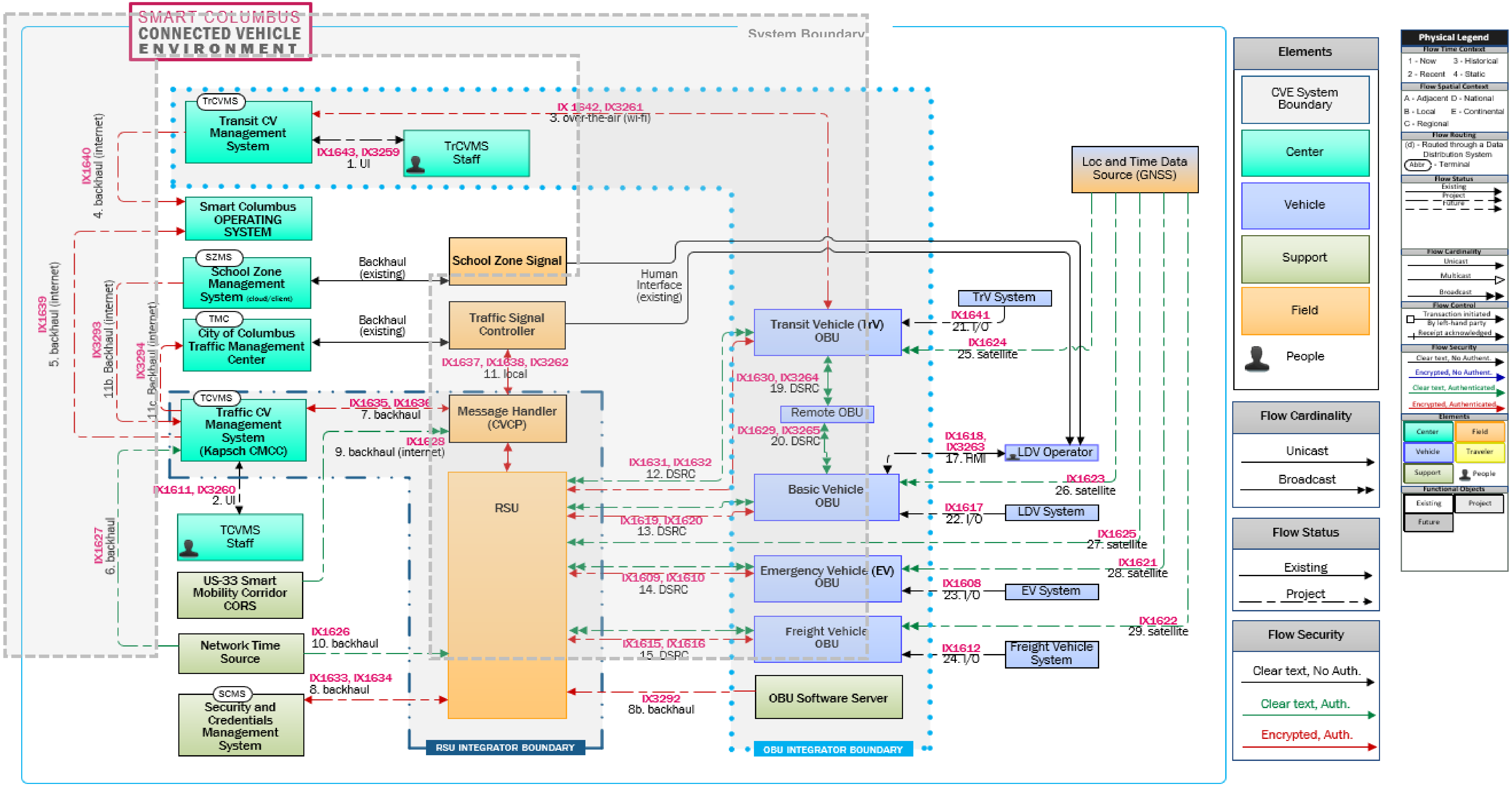
Chapter 2. System Description

2.1. SYSTEM CONTEXT

The CVE can be described as a combination of subsystems that work together: a system of roadside equipment, a system of in-vehicle equipment, and a system of backhaul networks for agency data. On the roadside, the fundamental functions of the RSUs are to obtain several types of status information from roadside ITS devices and broadcast this information to vehicles in the vicinity. Intersections identified for the deployment of roadside CV equipment presumably contain necessary physical cabinet and conduit space for the proposed CV equipment, and that the distance between the cabinet equipment and overhead RSU mounting locations conform to distance constraints for physical communication between locally networked devices. Necessary remedies will be addressed upon completion of detailed installation plans.

Subsequently, in a vehicle, the fundamental functions of On-board Units (OBUs) are to obtain various types of status information from the vehicle and broadcast this information to other vehicles and infrastructure in the vicinity. The OBU may utilize status information from the vehicle (this includes interfaces with other in-vehicle devices deployed as part of the Smart Columbus program), other vehicles, the roadside, and location and time data (obtained from a location and time source), such as Global Navigation Satellite System (GNSS) to support safety and mobility applications. Similarly, the RSU exchanges information with the roadside ITS equipment, vehicles, and location and time data to support mobility applications. OBUs will be comprised of DSRC radios, and depending on their applications, may include a HMI and/or connect to vehicle data systems. Both the OBU and RSU utilize the Security and Credentials Management System (SCMS) to make sure that it is working with data from trusted sources, and the roadside device saves operational data on the Smart Columbus Operating System (OS).

Figure 2 shows Vehicle-to-Infrastructure (V2I) communication between vehicles and roadside devices (via DSRC); communication between roadside devices and data management systems (via backhaul); and Vehicle-to-Vehicle (V2V) communication between onboard devices (via DSRC). **Table 3** summarizes the interfaces, hardware, facilities, communications and messages used in the system. The reader should reference these figures and table throughout this section to foster a better understanding of the system concept.



Source: City of Columbus as generated from ARC-IT

Figure 2: Connected Vehicle Environment System Breakdown Diagram

Table 3: Connected Vehicle Environment Proposed System Interfaces and Elements

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1643-V01 • CVE-IF1277-V01 • CVE-IF1473-V01	Interface 1.1	TrCVMS	TrCVMS Staff	• CV transit operational administrative coordination: ○ Archive data and query responses	User Interface
• CVE-IX3259-V01 • CVE-IF1277-V01	Interface 1.2	TrCVMS Staff	TrCVMS	• CV transit operational administrative coordination: ○ Transit vehicle interaction event data parameters ○ Archived data query	
• CVE-IX3260-V01 • CVE-IF3044-V01	Interface 2.1	TCVMS	TCVMS Staff	• CV traffic operations and administrative coordination: ○ RSU Status	User Interface
• CVE-IX1611-V01 • CVE-IF3044-V01	Interface 2.2	TCVMS Staff	TCVMS	• CV traffic operations and administrative coordination: ○ MAP Data ○ TIM Data ○ Signal Priority Parameters ○ RSU Status Query	
• CVE-IX3261-V01 • CVE-IF3214-V01	Interface 3.1	TrCVMS	Transit Vehicle System (via COTA Garage Communications)	• Transit Vehicle Interaction Event Data Parameters	Wi-Fi
• CVE-IX1642-V01 • CVE-IF3214-V01	Interface 3.2	Transit Vehicle System (via COTA Garage Communications)	TrCVMS	• Transit Vehicle Interaction Data	
• CVE-IX1640-V01 • CVE-IF1472-V01	Interface 4	TrCVMS	Smart Columbus Operating System	• Transit Vehicle Interaction Events	Backhaul
• CVE-IX1639-V01	Interface 5	TCVMS	Smart Columbus Operating System	• BSM, SRM, SSM, SPaT	Backhaul
• CVE-IX1627-V01	Interface 6	Network Time Source	TCVMS	• Network Time Data	Backhaul

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1635-V01	Interface 7.1	Message Handler	TCVMS	• BSM, SPaT, SRM, SSM • RSU Status	Backhaul
• CVE-IX1636-V01 • CVE-IF1342-V01 • CVE-IF1341-V01	Interface 7.2	TCVMS	Message Handler	• MAP • TIM • Signal priority parameters	
• CVE-IX1633-V01 • CVE-IF1354-V01 • CVE-IF1353-V01	Interface 8.1	RSU	SCMS	• RSU Enrollment Request • OBU Enrollment Request • RSU Application Certificate Request • OBU Pseudonym Certificate Request	Backhaul
• CVE-IX1634-V01 • CVE-IF1344-V01 • CVE-IF1354-V01	Interface 8.2	SCMS	RSU	• RSU Enrollment Certificate • OBU Enrollment Certificate • RSU Application Certificate • OBU Pseudonym Certificate	
• CVE-IX3292-V01	Interface 8b	OBU Software Server	RSU	• OBU Firmware Update	Backhaul
• CVE-IX1628-V01 • CVE-IF1339-V01	Interface 9	Ohio CORS	Message Handler	• RTCM data	Backhaul
• CVE-IX1626-V01	Interface 10	Network Time Source	RSU	• Network Time Data	Backhaul
• CVE-IX1637-V01 • CVE-IF1347-V01	Interface 11a.1	Message Handler	Traffic Signal Controller	• SRM data (signal preemption request data)	Local
• CVE-IX1638-V01 • CVE-IF1340-V01 • CVE-IF1345-V01 • CVE-IF1346-V01	Interface 11a.2	Traffic Signal Controller	Message Handler	• SPaT data • SSM Data	
• CVE-IX3293-V01	Interface 11b	School Zone Management System	TCVMS	• School Zone Schedule Data	Backhaul (Internet)
• CVE-IX3294-V01	Interface 11c	TCVMS	TMC	• CV traffic operations and administrative coordination: ▪ RSU Status	Backhaul (Internet)

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1631-V01 • CVE-IF3247-V01 • CVE-IF1231-V01 • CVE-IF1235-V01 • CVE-IF1227-V01 • CVE-IF1238-V01 • CVE-IF2985-V01 • CVE-IF2978-V01	Interface 12.1	RSU	Transit Vehicle OBU	• SPaT • MAP • RTCM • SSM • TIM	DSRC
• CVE-IX3262-V01 • CVE-IF3247-V01 • CVE-IF1250-V01 • CVE-IF1361-V01	Interface 12.2	Transit Vehicle OBU	RSU	• BSM • SRM	
• CVE-IX1631-V01 • CVE-IF3247-V01 • CVE-IF3210-V01	Interface 12.1	RSU	Transit Vehicle OBU	• OBU Enrollment Certificate • OBU Pseudonym Certificate[4]	DSRC
• CVE-IX1632-V01 • CVE-IF3247-V01 • CVE-IF1361-V01	Interface 12.2	Transit Vehicle OBU	RSU	• OBU Enrollment Request • OBU Pseudonym Certificate Request	
• CVE-IX1619-V01 • CVE-IF3247-V01 • CVE-IF1362-V01 • CVE-IF1361-V01	Interface 13.1	Basic Vehicle OBU	RSU	• BSM	DSRC

[4] *Pseudo certificates used for transit vehicles configured to request Transit Signal Priority include the PSID for SRM, in addition to BSMs and Misbehavior Reporting (not used) and expire after one (1) week. Further, these devices only contain two weeks of certificates.*

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1620-V01 • CVE-IF3247-V01 • CVE-IF1229-V01 • CVE-IF1240-V01 • CVE-IF1233-V01 • CVE-IF1225-V01 • CVE-IF1357-V01 • CVE-IF1358-V01 • CVE-IF1356-V01 • CVE-IF1360-V01	Interface 13.2	RSU	Basic Vehicle OBU	• SPaT • MAP • RTCM • TIM	
• CVE-IX1619-V01 • CVE-IF3247-V01 • CVE-IF1243-V01 • CVE-IF1361-V01	Interface 13.1	Basic Vehicle OBU	RSU	• OBU Enrollment Request • OBU Pseudonym Certificate Request	DSRC
• CVE-IX1620-V01 • CVE-IF3247-V01 • CVE-IF1243-V01 • CVE-IF3210-V01	Interface 13.2	RSU	Basic Vehicle OBU	• OBU Enrollment Certificate • OBU Pseudonym Certificate	
• CVE-IX1609-V01 • CVE-IF3247-V01 • CVE-IF1248-V01 • CVE-IF1251-V01 • CVE-IF1361-V01	Interface 14.1	EV OBU	RSU	• BSM • SRM	DSRC
• CVE-IX1610-V01 • CVE-IF3247-V01 • CVE-IF1232-V01 • CVE-IF1236-V01 • CVE-IF1228-V01 • CVE-IF1239-V01 • CVE-IF2986-V01	Interface 14.2	RSU	EV OBU	• SPaT • MAP • RTCM • SSM	

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1609-V01 • CVE-IF3247-V01 • CVE-IF1248-V01 • CVE-IF1361-V01	Interface 14.1	EV OBU	RSU	• OBU Enrollment Request • OBU Pseudonym Certificate Request •	DSRC
• CVE-IX1610-V01 • CVE-IF3247-V01 • CVE-IF3210-V01	Interface 14.2	RSU	EV OBU	• OBU Enrollment Certificate • OBU Pseudonym Certificate[5]	
• CVE-IX1615-V01 • CVE-IF3247-V01 • CVE-IF1249-V01 • CVE-IF1363-V01 • CVE-IF1361-V01	Interface 15.1	Freight Vehicle OBU	RSU	• BSM • SRM	DSRC
• CVE-IX1616-V01 • CVE-IF3247-V01 • CVE-IF1230-V01 • CVE-IF1234-V01 • CVE-IF1226-V01 • CVE-IF1237-V01 • CVE-IF1359-V01	Interface 15.2	RSU	Freight Vehicle OBU	• SPaT • MAP • SSM • RTCM	
• CVE-IX1615-V01 • CVE-IF3247-V01 • CVE-IF1361-V01	Interface 15.1	Freight Vehicle OBU	RSU	• OBU Enrollment Request • OBU Pseudonym Certificate Request[6]	DSRC
• CVE-IX1616-V01 • CVE-IF3247-V01 • CVE-IF3210-V01	Interface 15.2	RSU	Freight Vehicle OBU	• OBU Enrollment Certificate • OBU Pseudonym Certificate	

[5] *Pseudo certificates used for Emergency Vehicles configured to request Signal Pre-empt include the PSID for SRM, in addition to BSMs and Misbehavior Reporting (not used) and expire after one (1) week. Further, these devices only contain two weeks of certificates.*

[6] *Pseudo certificates used for freight vehicles configured to request Freight Signal Priority include the PSID for SRM, in addition to BSMs and Misbehavior Reporting (not used) and expire after one (1) week. Further, these devices only contain two weeks of certificates.*

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1618-V01 • CVE-IF3197-V01 • CVE-IF3019-V01 • CVE-IF1222-V01 • CVE-IF1246-V01	Interface 17.1	Basic Vehicle OBU	Basic Vehicle Operator	• Alert, Application Availability • System Status Information • Pending Updates • Power Status	User Interface
• CVE-IX3263-V01 • CVE-IF3019-V01	Interface 17.2	Basic Vehicle Operator	Basic Vehicle OBU	• OBU Start-Up Indication • Setting Adjustment	
• CVE-IX3264-V01	Interface 19.1	Transit Vehicle OBU	Remote OBU (LDV, HDV, EV, and Transit Vehicle OBU)	• BSM	DSRC
• CVE-IX1630-V01 • CVE-IF1224-V01	Interface 19.2	Remote OBU (Basic Vehicle, Freight Vehicle, EV, and Transit Vehicle OBU)	Transit Vehicle OBU	• BSM	
• CVE-IX3265-V01 • CVE-IF1218-V01	Interface 20.1	Basic Vehicle OBU	Remote OBU (Basic Vehicle, Freight Vehicle, EV, and Transit Vehicle OBU)	• BSM	DSRC
• CVE-IX1629-V01 • CVE-IF1220-V01 • CVE-IF1221-V01 • CVE-IF1219-V01 • CVE-IF1223-V01	Interface 20.2	Remote OBU (Basic Vehicle, Freight Vehicle, EV, and Transit Vehicle OBU)	Basic Vehicle OBU	• BSM	
• CVE-IX1641-V01 • CVE-IF1244-V01 • CVE-IF1245-V01	Interface 21	Transit Vehicle System	Transit Vehicle OBU	• Vehicle Data	Local
• CVE-IX1617-V01	Interface 22	Basic Vehicle System	Basic Vehicle OBU	• Vehicle Data	Local
• CVE-IX1608-V01	Interface 23	EV System	EV OBU	• Vehicle Data	Local
• CVE-IX1612-V01	Interface 24	Freight Vehicle System	Freight Vehicle OBU	• Vehicle Data	Local

Related Interface Requirements	Reference	Source Element	Destination Element	Data Flow	Communications Media
• CVE-IX1624-V01	Interface 25	GNSS	Transit Vehicle OBU	• Location and Time Data	Local
• CVE-IX1623-V01 • CVE-IF1242-V01	Interface 26	GNSS	Basic Vehicle OBU	• Location and Time Data	Local
• CVE-IX1625-V01 • CVE-IF1343-V01	Interface 27	GNSS	RSU	• Location and Time Data	Local
• CVE-IX1621-V01	Interface 28	GNSS	EV OBU	• Location and Time Data	Local
• CVE-IX1622-V01	Interface 29	GNSS	Freight Vehicle OBU	• Location and Time Data	Local

Source: City of Columbus

To establish an organizational framework for CVE requirements, the proposed system described in Section 5 of the ConOps was further refined, decomposed, and classified according to its functionality (i.e. functional groups) and its major system components, as illustrated on the context diagrams in **Figure 2**. **Table 4** details the list of the functional groups resulting from decomposing the CVE.

Table 4: Connected Vehicle Environment System Functional Groups

Ref #	Functional Group	High-Level Functionality
RSU	Roadside Unit	Relays CV data to/from vehicles and infrastructure elements
OBU	Onboard Unit	In-vehicle equipment that relays CV data to/from other vehicles and infrastructure and provides alerts/warnings to drivers (as applicable)
TSC	Traffic Signal Controller	Manages timing of traffic signals at intersections, reacting to requests for pre-empt/priority, as applicable
OS	Operating System	Data repository for all CV data captured. Source for Performance Measure calculations
TMC	Traffic Management Center	Centralized Management of all traffic signals. To be expanded to included management of CVE
TrMC	Transit Management Center	Repository for all Transit-related CV data as captured by OBU on transit vehicles
SCMS	Security Credential Management System	Manages Digital Certificates used to ensure authenticated message exchange
CORS	Continuously Operating Reference Station	Source of GPS position correction information used in conjunction with following
GNSS	Global Navigation Satellite System	Primary source of location services provided to CV-equipped vehicles
MAP	MapData Message	SAE J2735 2016:03 standard message for describing the geometry and layout of an intersection. Sent from RSU to OBU
SPAT	Signal Phase and Timing Message	SAE J2735 2016:03 standard message for conveying the current state and time remaining in a traffic signal phase.
SRM	Signal Request Message	SAE J2735 2016:03 standard message used by a vehicle to request preempt or priority service at a traffic signal.
SSM	Signal Status Message	SAE J2735 2016:03 standard message to provide current status of signal requests active or pending at a signalized location.
TIM	Traveler Information Message	SAE J2735 2016:03 standard message to provide traveler information such as changes in speed limit
RTCM	Radio Technical Commission for Maritime Services Corrections Message	SAE J2735 2016:03 standard message for conveying position correction information used by an OBU.
BSM	Basic Safety Message	SAE J2735 2016:03 standard message for conveying vehicle position, speed and trajectory info data

Ref #	Functional Group	High-Level Functionality
BSW	Blind Spot Warning Application	One of the suite of CV Applications to be employed in the CVE
EEBL	Emergency Electronic Brake Light Application	One of the suite of CV Applications to be employed in the CVE
EVP	Emergency Vehicle Preemption Application	One of the suite of CV Applications to be employed in the CVE
FCW	Forward Collision Warning Application	One of the suite of CV Applications to be employed in the CVE
FSP	Freight Signal Priority Application	One of the suite of CV Applications to be employed in the CVE
IMA	Intersection Movement Assist Application	One of the suite of CV Applications to be employed in the CVE
LCW	Lane Change Warning Application	One of the suite of CV Applications to be employed in the CVE
TSP	Traffic Signal Priority Applications	One of the suite of CV Applications to be employed in the CVE
TVIER	Transit Vehicle Interaction Event Recording	One of the suite of CV Applications to be employed in the CVE
VDTO	Vehicle Data for Traffic Operations	One of the suite of CV Applications to be employed in the CVE
RLVW	Red Light Violation Warning Application	One of the suite of CV Applications to be employed in the CVE
RSSZ	Reduced Speed School Zone Application	One of the suite of CV Applications to be employed in the CVE
TCVMS	Traffic CV Management System	Management Center for CV activities
TrCVMS	Transit CV Management System	Management Center for Transit activities
TSC	Traffic Signal Controller	Source of Signal Phase and Timing Data
APPS	CV Applications	CV Applications that use data generated in the CVE
RSE	Roadside Equipment	Other devices or equipment deployed at the roadside, not specifically defined

Source: City of Columbus

2.2. SYSTEM MODES AND STATES

Because it is composed of multiple devices and potentially hosting several applications, the system mode is viewed at a micro level. With devices deployed across the deployment area and outside the deployment area (i.e., vehicles), viewing the deployment as a single system is not considered for the purpose of defining modes. The mode will be composed of the status of a device, its ability to communicate, and the operational status of the installed applications.

Devices have three modes:

- **Normal mode:** A device and its applications are operating as required
- **Degradation mode:** Something unexpected occurred and part of the device may not be functioning as required
- **Error mode:** a complete failure of the device including communication failure

Each Roadside Unit (RSU) or Onboard Unit (OBU) (referred to simply as a device when considered generically as a DSRC-based unit) is considered to be in normal mode when the device is operating as designed and the applications are functioning as designed. A device enters Degradation mode when there is failure of one or more of the applications or a portion of the hardware fails. When an application fails, data is not being received, processed or transmitted for those application(s). The other applications continue to function as designed receiving, processing and transmitting data. When a portion of the device hardware fails, the application may or may not be able to perform its functions. When a device completely fails or loses the ability to communicate, it enters Error mode.

OBUs' modes cannot be determined in real time. Mode changes by these devices will be discovered only when the vehicle's data is downloaded and only for those OBUs that will capture data. If there is a complete failure of the device, then it will be apparent that the device is nonoperational. If the device is operating, but one of the applications has failed, this will be determined after the data has been downloaded and analyzed. OBU failures may be determined more efficiently as drivers may notice the OBU is not functioning properly and bring the vehicle in for OBU maintenance.

When determining the system state, the focus will be on the RSUs. These devices can provide a heartbeat to the TMC that can be monitored. The OBUs are not considered when modeling and determining the system state, as there is no reliable means to know if these devices are always operating as required.

The three RSU device states are: Operational, Partial Failure and Failed.

When the device is operational, an RSU is known to be up and operating and in communication with the TCVMS via the appropriate network. Partial failure of an RSU indicates that the RSU is not operating as required. An RSU is considered nonoperational when the communications with the RSU is down (interrupted) or the RSU itself has some failure preventing it from operating normally. The RSU is considered to be in a failed state when an RSU is inoperative.

2.3. MAJOR SYSTEM CHARACTERISTICS

2.3.1. System Capabilities

The primary outcome of the CVE is deployment of technology both roadside and in vehicles to enable communication between vehicles and between vehicles and roadside ITS equipment. The CV technology will provide information that will help to reduce crashes along the target corridors, improving safety for light-duty vehicle operators, transit vehicle operators, passengers, and public safety personnel.

The CVE will further maintain the safe and efficient movement of transit, freight, and emergency vehicles. Signal priority at intersections will allow a bus to receive early or extended green time to maintain its schedule. A freight priority capability at select signalized intersections will improve freight mobility and consequently deliver goods faster and more efficiently. Furthermore, a signal preemption strategy will provide right-of-way to emergency vehicles and allow safe, efficient passage through intersections.

The final capability is to provide the mechanisms to improve traffic management throughout the City of Columbus. Ideally, the CVE will enable state and local agencies to collect low-cost, comprehensive, high-quality data that can be used in conjunction with data collected from traditional and third-party sources to support enhanced traffic management activities. Archiving select data from the CVE into Operating System will further enhance the integration of transportation data into network management and long-term transportation planning.

2.3.2. System Conditions

The CVE is generally expected to perform under most conditions, securely and timely delivering data to/from and between vehicles, allowing for the stated objectives of the project to be met. Situations that may result in degraded or no performance include:

- **Loss of Power:** A power outage that impacts the infrastructure elements of the environment will prohibit the V2I applications from performing as expected.
- **Loss of Communications:** Localized communications will be employed to ensure that loss of communications will not adversely affect the interaction between the vehicles and infrastructure, albeit there may be conditions whereby data collected from the CVE will not be forwarded to the OS.
- **Device Failure:** Device failures fall into one of two classes, the roadside equipment, specifically the RSU, and the OBU.

Management provisions will be made to monitor the operation of the system’s infrastructure devices to identify failures and resolve them. When RSUs fail, vehicle operators will not be notified and will operate their vehicles normally without alerts or alarms from the OBUs for V2I applications. In this state, the V2V applications will continue to function and provide alerts or alarms in the presence of other CVs (if their OBUs are also functioning properly). Such fail conditions in the CV devices may result in safety-related implications such as inability to issue alerts. Furthermore, this may lead to insufficient or inaccurate data and safety benefit analysis of the system.

Light-Duty Vehicle (LDV) Operators with HMIs need to be informed when vehicles start that their vehicle resident OBU is operating properly. Failed OBUs will not prevent the safe operation of the vehicle by the LDV Operator; the LDV operator will not receive alerts or alarms from the device when it has failed. Support personnel will have to be notified by the LDV Operator to begin the repair process.

2.3.3. System Constraints

System constraints of the CVE can be grouped in several distinct categories which include equipment selection, network security and operations, user privacy and data collection, and impact to traffic operations.

Smart Columbus and the CVE serves as a deployment of CV technology. There is an expectation to maximize the implementation of commercial off-the-shelf hardware and software to meet the needs of users and stakeholders. Thus, the choice of devices to be deployed and the configuration of these devices are limited versus what might be expected for the CV Pilot projects – where detailed system design is required to meet project level goals. Specifically, and as noted in the ConOps, only applications which have met technology readiness level 6, or for which there is invaluable need were selected for inclusion.

It is fully expected that DSRC will be deployed as the wireless interface. RSUs will support bi-directional communications with vehicles via the DSRC interface, but are not required to include Wi-Fi, Bluetooth or any other wireless technology. Likewise, OBUs will be limited in the data they collect and the methods for both disseminating information to the LDV Operator, as well as capturing data from the Transit Vehicle OBU. Only LDVs are expected to have a HMI. Only Transit Vehicles belonging to the transit agency, COTA, are expected to log onboard events. All other data capture will be via the active J2735 messages, such as BSM, SPaT, MAP, TIM, SSM, SRM and RTCM.

The City has deployed several hundred miles of fiber and is in the process of connecting nearly every traffic signal controller in the Columbus region to this network. The CVE will be connected to many of these same traffic signal controllers. Presently, the traffic signal controller network is a private, internal DPS network. The CVE requires access to external, public resources, including SCMS, CORS and the Smart Columbus Operating System. Connecting the existing controller network to CVE will potentially expose the controller to security risks associated with a public facing interface. Thus, the CVE must implement an architecture that isolates it from the existing network, providing a reasonable assurance that the former will not compromise the latter. This may require upgrading field equipment, installing additional and possibly redundant equipment, and using spare communications links.

Throughout all meetings with the project stakeholders, the stakeholders expressed that privacy must be maintained. 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. The Smart Columbus Data Privacy Plan[7] and Data Management Plan[8] address specific methods to handle this, but given the limited data collection available, all data generated will be captured and handled accordingly.

Signal preemption and priority have potential impact on traffic operations and as it is not the goal of Smart Columbus to necessarily demonstrate that preempt or priority have an overall positive net effect to the transportation network. The CVE is focused on demonstrating that the technology can support this function. The City may decide to limit or eliminate specific locations or corridors planned to support priority/preemption; it may also require additional, conditional elements not presently specified.

[7] https://d2rfd3nxvhnf29.cloudfront.net/2020-09/SCC-D-DataPrivacyPlan-AnnualUpdate-V2.pdf

[8] https://d2rfd3nxvhnf29.cloudfront.net/2020-08/SCC-E-DataManagementPlan-Update-v1_0.pdf

2.4. USER CHARACTERISTICS

This section defines the stakeholders, user classes, and their roles and responsibilities for the CVE. Stakeholders refers to an individual or organization affected by the activities, inputs and outputs of the system being developed. They may have a direct or indirect interest in the system and their level of participation may vary. This includes public agencies, private organizations or the traveling public (end users) with a vested interest or "stake" in one or more aspects of the CVE as identified in **Table 5**. User Classes are classified based on their perception of the system and the needs identified. Note that some key personnel may serve in multiple roles based on the user needs and functions.

Table 5: Connected Vehicle Environment Stakeholders and User Classes

Target Stakeholders	User Classes						
	Light-Duty Vehicle Operator	Emergency Vehicle Operator	Heavy-Duty Vehicle Operator	Traffic Manager	Transit Vehicle Operator	Transit Manager	Network Manager
Private Vehicle Owners*	X	-	-	-	-	-	-
City of Columbus DPS Fleet Vehicle Operators, Car Share Vehicle Operators**	X	-	-	-	-	-	-
Dis-Tran (Freight Operator)	-	-	X	-	-	-	-
COTA Fixed-Route, Paratransit	-	-	-	-	X	X	-
COTA (Supervisor Vehicle and Police Response Unit)	X	-	-	-	-	-	-
City of Columbus Fire, Emergency Medical Services (EMS)	-	X	-	-	-	-	-
City of Columbus Police	-	X	-	-	-	-	-
City of Columbus Dept. of Public Service Traffic Managers	-	-	-	X	-	-	-
City of Columbus Department of Technology (DoT)	-	-	-	-	-	-	X

**Note: Linden residents are the target audience for privately-owned vehicles. Outreach can be done for other residents near CV corridors if additional participation is needed to satisfy in-vehicle installation objectives.*

*** Note: Car2Go, the only car-share entity operating in Columbus ended its service in the area on May 31, 2018. Should other carshare providers provide service in the area, they could be considered a potential stakeholder for the light-duty vehicle operator user class.*

Source: City of Columbus

2.4.1. Light-Duty Vehicle Operator

The Light-Duty Vehicle operator user class is comprised of Private Vehicle Owners, City of Columbus DPS Fleet Vehicle Operators, COTA Supervisor Vehicle Operators, and COTA Police Response Unit Operators. The City of Columbus light-duty fleet includes vehicles: construction inspection vehicles, DPS pool vehicles, infrastructure management vehicles, building and zoning inspections vehicle, signage and pavement supervisor vehicles, and traffic management vehicles. In the context of the CVE, light-duty vehicle operators are expected to use the Cleveland Avenue, High Street, and Morse Road corridors as part of their typical routines. As identified in the Justification for Changes in the ConOps, these three corridors are responsible for a large number of crashes and contain several of the most dangerous intersections in the Columbus area. While using these corridors, it is expected that light-duty vehicle operators are exercising awareness in the roadway environment to avoid unsafe situations.

2.4.2. Emergency Vehicle Operator

The Emergency Vehicle Operator user class is comprised of City of Columbus Fire, EMS and Police, and must navigate the roadway network to respond to emergencies throughout the city. When actively responding to calls, these vehicle operators engage flashing lights and sirens to make their presence known to other vehicles on the roadway. In response to the lights and sirens, other drivers are expected to yield to the emergency vehicles (and to provide a clear path by pulling over or stopping at intersections) so that the emergency vehicle operator can reach the destination as quickly as possible.

2.4.3. Heavy-Duty Vehicle Operator

The Heavy-Duty Vehicle Operator user class is comprised of drivers that operate heavy-duty freight vehicles for a local transportation company, Dist-Trans, a subsidiary of ODW Logistics. Dist-Trans moves freight along the Alum Creek Corridor, to I-270, to Morse Road, east of I-270. Moving freight in an expedient and efficient manner is very important for heavy-duty vehicle operators and the logistics companies they represent.

2.4.4. Traffic Manager

City of Columbus DPS Traffic Managers represents the Traffic Manager user class. The Traffic Manager is responsible for actively managing the transportation devices which allows them to modify the operations of traffic control devices (such as traffic signal timing) to improve network efficiency. DPS Traffic Managers currently use CCTV cameras to monitor traffic conditions. Based on conditions that are observed, one of several signal timing plans are implemented to alleviate the congestion that is occurring. The Traffic Manager is also responsible for the operations and maintenance of transportation network-connected devices. This includes, but is not limited to CCTVs, traffic signal controllers, and switches located in traffic signal cabinets.

2.4.5. Transit Vehicle Operator

The Transit Vehicle Operator user class is comprised of COTA fixed-route and paratransit vehicle operators. These operators are responsible for servicing COTA passengers along their designated routes.

2.4.6. Transit Manager

The Transit Manager user class is represented by COTA Transit Managers. The transit manager is responsible for making sure that transit vehicles run on-schedule, and for evaluating systems currently on-board transit vehicles and potential future on-board transit vehicle systems to determine if they can provide a benefit to the transit vehicle operator or to passengers. Because the transit vehicle operator must safely operate the vehicle, only a limited number of outputs from these systems can be provided to the transit vehicle operator without causing a distraction and reducing safety. The transit manager can evaluate the outputs that may be provided from a new system to determine if it should be implemented.

2.4.7. Network Manager

The Network Manager user class is represented by the City of Columbus DoT. They are responsible for operating and maintaining the fiber-optic network that is used to transmit data between networked devices. The current system uses fiber-optic backhaul to provide connectivity between the TMC and traffic signal controllers. The TMC uses the network to remotely specify modifications to traffic signal timing plans when congested conditions are noted. It is the responsibility of the Network Manager to establish network security protocols, enforce those protocols, and preserve connectivity or restore connectivity when outages are experienced.

2.5. ASSUMPTIONS AND DEPENDENCIES

Table 6 lists the known assumptions and dependencies that represent a risk to the CVE project or system and can affect the ability to meet the desired functionality, maintain the project schedule or meet performance goals.

Table 6: Assumptions and Dependencies

ID	Assumption	Corresponding Risk	Dependency	Degree
01	DSRC will be the medium for over-the-air message transmission.	DSRC will be replaced by competing technology	Continued availability of DSRC-based equipment	Medium
02	Position correction will be facilitated using RTCM v2.3 Type messages	RTCM may be insufficient to meet project needs	Quality of OBU GNSS hardware and use of RTCM	Med-High
03	The SPaT message will be generated by the TSC	TSC without capability is introduced into the CVE	SPaT Message broadcast	Low
04	SCMS will be available from DriveOhio	City may need to pivot to alternative source	SCMS is critical for secure operation of CVE	Medium
05	CV applications will be available from selected vendor	App selection was based, in part, on availability and readiness level.	Selection criteria must be clear with OBU vendors	Low-Med

Source: City of Columbus

2.6. SYSTEM CONSTRAINTS

Table 7 lists the constraints on the system as defined by the concept of operations, the contract or city/state policy. Requirements have been developed to support these constraints.

Table 7: System Constraints

Constraint ID	Reference	Constraint
CVE-CN1645-V01	Constraint 1	DPS will provide deployment support
CVE-CN1647-V01	Constraint 3	Equipment, software, processes, and interfaces shall be tested for interoperability before deployment to ensure they meet those standards for interoperability.
CVE-CN1648-V01	Constraint 4	All CVE components that utilize DSRC shall comply with IEEE, SAE, and USDOT standards, as follows: 1. SAE J2735_201603 - Dedicated Short Range Communications (DSRC) Message Set Dictionary. 2. SAE J 2945/1 - On-Board System Requirements for V2V Safety Communications. 3. SAE J 2945/4 (draft) - DSRC Messages for Traveler Information and Basic Information Delivery. 4. IEEE 802.11p - Wireless Access in Vehicular Environments. 5. IEEE 1609.2 - IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages. 6. IEEE 1609.3 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. 7. IEEE 1609.4 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. 8. NTCIP 1202 - NTCIP Object Definitions for Actuated Traffic Controllers. 9. NTCIP 1211 - NTCIP Objects for Signal Control and Prioritization (SCP) 10. DSRC Roadside Unit (RSU) Specifications Document v4.1 (October 2016)
CVE-CN1649-V01	Constraint 5	A DSRC-Enabled LDV OBU shall be installed in private vehicles
CVE-CN1650-V01	Constraint 6	A DSRC-Enabled LDV OBU shall be installed in DPS fleet vehicles
CVE-CN1651-V01	Constraint 7	A DSRC-Enabled LDV OBU shall be installed in COTA Supervisor vehicles
CVE-CN1652-V01	Constraint 8	A DSRC-Enabled HDV OBU shall be installed in HDVs
CVE-CN1653-V01	Constraint 9	A DSRC-Enabled Transit Vehicle OBU shall be installed in Transit Vehicles
CVE-CN1654-V01	Constraint 10	A DSRC-Enabled Transit Vehicle OBU shall be installed in Paratransit Vehicles
CVE-CN1655-V01	Constraint 11	A DSRC-Enabled OBU shall be installed on CEAVs

Constraint ID	Reference	Constraint
CVE-CN1656-V01	Constraint 12	A DSRC-Enabled Emergency Vehicle OBU shall be installed in Police Vehicles
CVE-CN1657-V01	Constraint 13	A DSRC-Enabled Emergency Vehicle OBU shall be installed in Fire Vehicles
CVE-CN1658-V01	Constraint 14	A DSRC-Enabled Emergency Vehicle OBU shall be installed in EMS Vehicles
CVE-CN1659-V01	Constraint 15	A DSRC-Enabled RSU will be installed at CVE intersections (identified in ConOps)
CVE-CN1660-V01	Constraint 16	Safety applications that output an alert from an OBU shall be commercial off the shelf software
CVE-CN1661-V01	Constraint 17	DPS will adhere to internal policies and best practices for executing signal priority and signal preemption strategies
CVE-CN1662-V01	Constraint 18	DPS will limit the ability to receive signal priority or preemption to select vehicles
CVE-CN1663-V01	Constraint 19	DPS will operate and maintain the CVE
CVE-CN1664-V01	Constraint 20	Performance measures will be used to assess the CVE
CVE-CN3088-V01	Constraint 22	Data that is used or stored in a center (e.g. TCVMS, TrCVMS) shall not contain PII
CVE-CN3106-V01	Constraint 23	A DSRC-Enabled LDV OBU shall be installed in COTA Police Response Unit vehicles

Source: City of Columbus

2.7. OPERATIONAL SCENARIOS

Chapter 6 of the *Concept of Operations for the Connected Vehicle Environment project for the Smart Columbus Demonstration Program – City of Columbus, Ohio* captures and documents the operational scenarios.

Chapter 3. System Requirements

This section of the document lists the identified requirements for the Connected Vehicle Environment. The requirements are organized first by requirement type, then by system and services (i.e. functional requirements (FR) for functional group 1, then FR for functional group 2, etc.).

The requirements tables in this section include a column for the requirement identifier, functional group, sub-component, description, a reference, and verification method. Each requirement type has a requirement identifier - **Appendix A. Document Terminology and Conventions** provides an overview of the method that is used to build the requirement identifier. The next two columns provide the functional group and sub-component. These are intended to organize the requirements in a manner that allows similar requirements to be grouped together. The requirements in the tables in this section are grouped by functional group and sub-component. The next column provides the requirement description, which is intended to be well-formed as specified by the Systems Engineering Guide for Intelligent Transportation Systems[9]: necessary, clear, complete, correct, feasible, and verifiable. The reference number identifies traceability to user needs, user scenarios, other (parent) requirements, and/or policies and constraints. The final column provides the verification method – the four fundamental verification methods considered include: inspection, demonstration, test, and analysis. Definitions of these methods are provided in **Section 4.1**. **Table 8** describes the classifications of the requirements in this document.

Table 8: List of Requirement Types

Type	Description
Functional (FN)	The Functional requirements specify actionable and qualitative behaviors (e.g. functions, tasks) of the core system of interest, which in the case of CVE includes the roadside infrastructure, including RSUs; as well as in-vehicle units.
Performance (PR)	The Performance requirements specify quantifiable characteristics of operations that define the extent, or how well, and under what conditions a function or task is to be performed (e.g. rates, velocities).
Interfaces (IF)	The Interface requirements define how the system will interact, communicate, or exchange data with external systems (external interface) and how core system elements interact with other parts of the system (internal interface).
Data (DR)	The Data requirements define the data collected, transformed, and stored from various sources as well as identifies new data that is expected to be generated.
Security (SR)	The Security requirements specify what is necessary to protect the integrity and operability of the system, its microservices, connections, and data. This includes physical security as well as cyber prevention, detection, identification, response and recovery requirements.
Policy and Regulation (RG)	The Policy and Regulation requirements specify relevant and applicable organizational policies or regulations that affect the development, operation or performance of the system (e.g. IT and labor policies, reports to regulatory agencies, health or safety criteria, etc.). This section also includes new policy and regulation imposed to realize the system.

[9] https://ops.fhwa.dot.gov/publications/seitsguide/seguide.pdf

Type	Description
Non-Functional (NF)	The Non-Functional requirements define the characteristics of the overall operation of the system, including the following: • Physical (PY) – specifies the construction, durability, adaptability and environmental characteristics of the system • Availability and Recovery (AR) – define the times of day, days of year, and overall percentage the system can be used and when it will not be available for use as well as recovery point and time objectives. • Maintainability (MT) – specify the level of effort required to locate and correct an error during operation. • Storage and Transport (ST) – specify the physical location and environment for the system, including designated storage facility, installation site, repair facility, requirements for transporting equipment, etc. • Disposal (DP) – specify the items related to the disposal of project/system components, due to either failure replacements, removal, end-of-life upgrade, or retirement.
Enabling (EN)	The Enabling requirements specify details concerning the management of information as well as the production of the system and its life cycle sustainment, including the following: • Information Management (IM) – specify the acquisition, management, and ownership of information from one or more sources, the custodianship and the distribution of that information to those who need it. • Life Cycle Sustainability (LC) – define what items the project or system will review, measure, and analyze as part of its commitment to quality during the life cycle of the system, including development, integration, verification, validation, and training.

Source: City of Columbus

3.1. FUNCTIONAL REQUIREMENTS

This section provides the high-level requirements for the system of interest (i.e. what the system will do). The requirements in **Table 9** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 9: Functional Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1113-V01	Roadside Equipment	Roadside Unit	An RSU shall obtain position correction information from a Continuously Operating Reference Station (CORS) for packaging and broadcasting as the RTCM message.	CVE-SN860-v02 CVE-IX1628-V01	Demonstration
CVE-FN1308-V01	Roadside Equipment	Roadside Unit	An RSU shall acquire time from the LTS interface in accordance with J2945/1 section 6.2.4.	CVE-SN850-v02 CVE-IX1625-V01 CVE-CN1648-V01 CVE-IX1626-V01	Demonstration
CVE-FN1309-V01	Roadside Equipment	Roadside Unit	An RSU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.	CVE-SN860-v02 CVE-IX1625-V01 CVE-CN1648-V01	Demonstration
CVE-FN1310-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast (school zone) TIMs to an LDV OBU when configured to perform this function.	CVE-UN140-v02 CVE-UN610-v02 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-FN1311-V01	Roadside Equipment	Roadside Unit	An RSU shall use Coordinated Universal Time (UTC) time for all logged data (e.g., events logs, probe vehicle data) based on the format defined in J2735 section 6.19 and epoch of January 1st, 1970.	CVE-CN1648-V01	Demonstration
CVE-FN1312-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SPaT messages from SPaT data inputs	CVE-UN130-v02 CVE-FN1557-V01 CVE-FN1558-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs	CVE-UN130-v02 CVE-UN220-v02 CVE-UN310-v02 CVE-UN510-v02 CVE-UN610-v02 CVE-FN1560-V01	Demonstration
CVE-FN1314-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SSM messages from SSM data inputs	CVE-UN220-v02 CVE-UN310-v02 CVE-UN510-v02	Demonstration
CVE-FN1316-V02	Roadside Equipment	Roadside Unit	Select RSUs in/around designated school zones (Linden STEM Academy and Our Lady of Peace School) shall broadcast TIMs only when the school zone flashing signal is flashing.	CVE-UN610-v02	Demonstration
CVE-FN1317-V01	Roadside Equipment	Roadside Unit	RSU functionality failure shall not affect the safe operation of the signal controller.	CVE-CN1659-V01	Demonstration
CVE-FN1318-V01	Roadside Equipment	Roadside Unit	All roadside equipment (including RSUs) shall support remote authenticated access.	CVE-IX1635-V01	Demonstration
CVE-FN3299-V01	Roadside Equipment	Roadside Unit	An RSU shall support over-the-air OBU 1609.2 Certificate updates through IPv6	CVE-SN870-V02 CVE-FN3228-V01	Demonstration
CVE-FN1319-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast the WSA on channel 180.	CVE-SN870-v02 CVE-IX1610-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-FN3297-V01	Roadside Equipment	Roadside Unit	RSU WSAs shall include PSIDs 0pE0-00-00-16 (SRM)\0pE0-00-00-15 (SSM) and 0pEF-FF-FF-FE (IPv6 Services)	CVE-SN870-v02 CVE-IX1610-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN3298-V01	Roadside Equipment	Roadside Unit	RSU WSAs shall contain a WAVE Routing Advertisement (WRA) that includes IPv6 Network information to be utilized by OBUs to join the RSU's IPv6 Network	CVE-SN870-v02 CVE-IX1610-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-FN1321-V01	Roadside Equipment	Roadside Unit	An RSU shall support IPv6 tunneling over IPv4.	CVE-UN710-v02 CVE-IX1626-V01 CVE-IX1628-V01 CVE-IX1633-V01 CVE-IX1637-V01	Demonstration
CVE-FN1325-V01	Roadside Equipment	Roadside Unit	It shall be possible for a system administrator with the appropriate permissions to configure the RSU to request application certificates with only designated geographic locations.	CVE-SN820-v02 CVE-CN1663-V01	Demonstration
CVE-FN1327-V01	Roadside Equipment	Roadside Unit	The CVE shall provide an interface to allow the system administrator to request new certificates bound to the new location if it moves from one location to another. (Note: its interface will allow requesting a new RSU application certificate with a site.)	CVE-IX1634-V01	Demonstration
CVE-FN1328-V01	Roadside Equipment	Roadside Unit	An RSU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.	CVE-IX1635-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1333-V01	Roadside Equipment	Roadside Unit	An RSU shall not create or transmit messages if the 1609.2 certificates do not contain the permissions for the corresponding PSID.	CVE-SN820-v02 CVE-CN1648-V01	Demonstration
CVE-FN1335-V01	Roadside Equipment	Roadside Unit	An RSU supplier shall provide the enrollment certificate for each RSU.	CVE-CN1645-V01	Demonstration
CVE-FN2972-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast (school zone) TIMs to a Transit Vehicle OBU when configured to perform this function.	CVE-IX1631-V01	Demonstration
CVE-FN2973-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU	CVE-IX1616-V01	Demonstration
CVE-FN2979-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU	CVE-IX1616-V01	Demonstration
CVE-FN2980-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU	CVE-IX1631-V01	Demonstration
CVE-FN2981-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU	CVE-IX1610-V01	Demonstration
CVE-FN2982-V01	Roadside Equipment	Roadside Unit	An RSU shall send SPaT messages generated from traffic signal controller output to an HDV OBU	CVE-IX1616-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN2983-V01	Roadside Equipment	Roadside Unit	An RSU shall send SPaT messages generated from traffic signal controller output to a Transit Vehicle OBU	CVE-IX1631-V01	Demonstration
CVE-FN2987-V01	Roadside Equipment	Roadside Unit	An RSU shall receive BSMs from an HDV OBU	CVE-IX1615-V01	Demonstration
CVE-FN2988-V01	Roadside Equipment	Roadside Unit	An RSU shall receive BSMs from a Transit Vehicle OBU	CVE-IX1632-V01	Demonstration
CVE-FN2989-V01	Roadside Equipment	Roadside Unit	An RSU shall receive BSMs from an Emergency Vehicle OBU	CVE-IX1609-V01	Demonstration
CVE-FN2990-V01	Roadside Equipment	Roadside Unit	An RSU shall receive SRMs from a Transit Vehicle OBU	CVE-IX1632-V01	Demonstration
CVE-FN2991-V01	Roadside Equipment	Roadside Unit	An RSU shall receive SRMs from an Emergency Vehicle OBU	CVE-IX1609-V01	Demonstration
CVE-FN3000-V01	Roadside Equipment	Roadside Unit	The RSU shall be able to send the SSM at a configurable rate	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1631-V01	Demonstration
CVE-FN3109-V01	Roadside Equipment	Roadside Unit	An RSU shall send SPaT messages generated from traffic signal controller output to an Emergency Vehicle OBU	CVE-IX1609-V01	Demonstration
CVE-FN3228-V01	Roadside Equipment	Roadside Unit	An RSU shall support over-the-air OBU firmware updates through IPv6	CVE-SN870-V02	Demonstration
CVE-FN3112-V01	Roadside Equipment	Roadside Unit	The RSU shall support OBU operating system updates that need to occur over the range of more than one RSU.	CVE-SN870-v02	Demonstration
CVE-FN1437-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall transmit performance metrics (as configured by traffic management staff and defined in the Performance Measurement Plan) to the Smart Columbus OS	CVE-UN410-v02 CVE-IX1639-V01 CVE-SN810-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1438-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send TIMs to the Smart Columbus OS	CVE-UN410-v02 CVE-IX1639-V01 CVE-SN810-v02 CVE-CN3088-V01	Demonstration
CVE-FN1439-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send MAP messages to the Smart Columbus OS	CVE-UN410-v02 CVE-IX1639-V01 CVE-SN810-v02	Demonstration
CVE-FN1440-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall enable loading of TIMs on roadside equipment	CVE-UN430-v02	Demonstration
CVE-FN1441-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall enable loading of MAP messages on roadside equipment	CVE-UN430-v02 CVE-IX1636-V02	Demonstration
CVE-FN1442-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for TIM messages from Traffic Management Staff	CVE-UN430-v02 CVE-IX1611-V02 CVE-UN420-v02	Demonstration
CVE-FN1443-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for MAP messages from Traffic Management Staff	CVE-UN430-v02 CVE-IX1611-V02 CVE-UN420-v02	Demonstration
CVE-FN1444-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for configurable parameters (for functions on the TCVMS and on roadside equipment) from Traffic Management Staff	CVE-UN430-v02 CVE-IX1611-V02 CVE-UN420-v02	Demonstration
CVE-FN1445-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall make the status of RSUs available to Traffic Management Staff	CVE-UN430-v02 CVE-IX1611-V02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1446-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide the VISA' functions of Validation, Integration, Sanitization (De-identification), and Aggregation of CV Data as defined in the U.S DOT SEMI ODE requirements (Reference TBR)	CVE-UN410-v02	Demonstration
CVE-FN1447-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate TIM messages	CVE-UN430-v02 CVE-UN420-v02	Demonstration
CVE-FN1448-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate MAP messages	CVE-UN430-v02 CVE-UN420-v02	Demonstration
CVE-FN1449-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the uptime status of RSUs	CVE-UN430-v02	Demonstration
CVE-FN1452-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall make the status of all RSUs available to Traffic Management Staff	CVE-UN430-v02	Demonstration
CVE-FN1453-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System should support the generation of performance metrics as defined in the Performance Management Plan	CVE-UN410-v02	Demonstration
CVE-FN1454-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System should use CV data made available through the CVE to generate performance metrics as defined in the Performance Management Plan	CVE-UN410-v02	Demonstration
CVE-FN1456-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall receive BSMs from the RSU	CVE-IX1635-V01	Demonstration
CVE-FN1463-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor tamper alert devices	CVE-PR1105-V01 CVE-FN1503-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1480-V01 CVE-UN430-v02 CVE-PR1105-V01	
CVE-FN2909-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate performance metrics (as configured by traffic management staff and as defined in the Performance Measurement Plan) from archived CV data	CVE-UN410-v02	Demonstration
CVE-FN2911-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall remove PII from BSMs that are received before further processing	CVE-CN3088-V01	Demonstration
CVE-FN3001-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept inputs for all required elements of a TIM message via a user interface.	CVE-IX1611-V02 CVE-CN1663-V01 CVE-UN420-v02	Demonstration
CVE-FN3002-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept inputs for all required elements of a MAP message via a user interface.	CVE-CN1663-V01 CVE-IX1611-V02 CVE-UN420-v02	Demonstration
CVE-FN3030-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide a means of allowing Traffic Management Staff to download archived CV data.	CVE-UN410-v02 CVE-UN440-v02 CVE-CN1663-V01	Demonstration
CVE-FN3032-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the archived CV data backup storage	CVE-UN410-v02 CVE-UN440-v02 CVE-CN1663-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN3041-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall allow traffic management staff to configure the generation of performance measures from archived CV data (e.g. a recurring database query).	CVE-UN440-v02 CVE-CN1663-V01 CVE-IX1611-V02	Demonstration
CVE-FN3045-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of a traffic signal controller cabinet that has been tampered with (based on the status of the tamper alert device)	CVE-UN430-v02 CVE-CN1663-V01 CVE-IX1611-V02	Demonstration
CVE-FN3047-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is not running normally (off, not responding, in safe mode, etc.)	CVE-IX1611-V02 CVE-UN430-v02 CVE-CN1663-V01	Demonstration
CVE-FN3049-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is offline	CVE-IX1611-V02 CVE-CN1663-V01 CVE-UN430-v02	Demonstration
CVE-FN3052-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall display different colored icons on the UI to indicate the real-time status of each RSU.	CVE-IX1611-V02 CVE-UN430-v02 CVE-CN1663-V01	Inspection
CVE-FN3053-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall allow Traffic Management Staff to select an RSU using the UI to reveal other RSU information (uptime percentage, tamper alert status, alert information, channel busy ratio, etc.)	CVE-IX1611-V02 CVE-UN430-v02 CVE-CN1663-V01	Demonstration
CVE-FN3054-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall maintain a log of all alerts issued to traffic management staff	CVE-UN430-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN3055-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall display an alert icon next to a given RSU icon on the UI to indicate that an alert has been issued for that RSU.	CVE-IX1611-V02 CVE-CN1663-V01 CVE-UN430-v02	Demonstration
CVE-FN3110-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept inputs from Traffic Management Staff for a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request Signal Priority or Preemption at each intersection.	CVE-CN1662-V01	Demonstration
CVE-FN3051-V01	Traffic Management System	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU (network entry vector) where unauthorized use has been detected and information regarding the unauthorized device.	CVE-IX1611-V02 CVE-CN1663-V01 CVE-UN430-v02	Demonstration
CVE-FN3039-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall provide a means of allowing Transit Management Staff to download archived Transit Vehicle Interaction Events.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3040-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the archived CV data backup storage	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3042-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall allow transit management staff to configure the generation of performance measures from archived CV data (e.g. a recurring database query).	CVE-CN1664-V01	Demonstration
CVE-FN3043-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall transmit performance metrics (as configured by transit management staff and defined in the Performance	CVE-IX1643-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			Measurement Plan) to the Smart Columbus OS		
CVE-FN1493-V01	V2I Mobility	Emergency Vehicle Preemption	An Emergency Vehicle OBU shall request to receive signal preemption at RSU-equipped intersections	CVE-UN220-v02	Demonstration
CVE-FN1497-V02	V2I Mobility	Emergency Vehicle Preemption	The EVP application should employ proven algorithms to enable emergency vehicle preemption	CVE-UN220-v02 CVE-CN1660-V01	Demonstration
CVE-FN1500-V01	V2I Mobility	Emergency Vehicle Preemption	A request to receive signal preemption from an Emergency Vehicle OBU shall be high priority	CVE-UN220-v02	Demonstration
CVE-FN3107-V01	V2I Mobility	Emergency Vehicle Preemption	An Emergency Vehicle OBU shall request to receive signal preemption for all possible movements for the leg of the intersection of which it is approaching.	CVE-UN220-v02	Demonstration
CVE-FN1479-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall request to receive signal priority at RSU-equipped intersections	CVE-UN310-v02 CVE-FN1484-V02	Demonstration
CVE-FN1480-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall broadcast an SRM when approaching an RSU-equipped intersection	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-UN310-v02 CVE-PR1105-V01	Demonstration
CVE-FN1481-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall broadcast an SRM when it is within a configurable distance of	CVE-UN310-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			the intersection it intends to request priority for		
CVE-FN1482-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall only request priority for movements is plans to make along a designated freight route (specific to the requesting HDV)	CVE-UN310-v02	Demonstration
CVE-FN1483-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall only request priority in an SRM	CVE-UN310-v02	Demonstration
CVE-FN1484-V02	V2I Mobility	Freight Signal Priority	An HDV OBU shall cease broadcasting SRMs for priority at a given intersection for a configurable amount of time after it has received an SSM from that intersection containing the RequestID of the SRM broadcasted the host HDV	CVE-FN1479-V01	Demonstration
CVE-FN1502-V01	V2I Mobility	Freight Signal Priority	A request to receive signal priority from an HDV Vehicle OBU shall be low priority	CVE-UN310-v02	Demonstration
CVE-FN1498-V01	V2I Mobility	General Priority/Preemption	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02 CVE-UN520-v02	Demonstration
CVE-FN1499-V01	V2I Mobility	General Priority/Preemption	The SRM shall contain information regarding the movement for which priority is being requested	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-FN1503-V01	V2I Mobility	General Priority/Preemption	High priority requests to receive signal priority shall be serviced before low priority requests to receive signal priority	CVE-PR1105-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-FN1463-V01 CVE-FN1480-V01 CVE-UN310-v02 CVE-PR1105-V01 CVE-UN510-v02 CVE-UN220-v02	
CVE-FN1504-V01	V2I Mobility	General Priority/Preemption	Multiple high priority requests shall be serviced in the order in which they are received	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-UN310-v02 CVE-PR1105-V01 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-FN1505-V01	V2I Mobility	General Priority/Preemption	Multiple low priority requests shall be serviced in the order in which they are received	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-UN310-v02 CVE-PR1105-V01 CVE-UN510-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-UN220-v02	
CVE-FN1508-V02	V2I Mobility	General Priority/Preemption	Roadside Equipment shall place a priority request or a preemption request to the traffic signal controller for the movement specified in the SRM if the following conditions are concurrently met: 1. The SRM "BasicVehicleRole" matches against the locally-stored list of BasicVehicleRoles are authorized to receive signal priority or preemption. 2. The request is made during the time period when priority or preemption will be granted for the vehicle with the given BasicVehicleRole. 3. The requested movement is allowed for the vehicle with the given BasicVehicleRole. 4. The intersection ID in the SRM matches the intersection ID	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-UN310-v02 CVE-PR1105-V01 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-FN1509-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall grant an early green for a phase for a movement that is requested in a priority SRM when the approach for that movement is red or yellow	CVE-UN310-v02 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1387-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01 CVE-UN510-v02	
CVE-FN1510-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall grant an extended green for a phase for a movement that is requested in a priority SRM when the approach for the requested movement is green	CVE-UN310-v02 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1387-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01 CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01 CVE-UN510-v02	
CVE-FN1511-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall not adjust the typical progression of phases to accommodate a priority request	CVE-CN1661-V01 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1387-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01 CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01	
CVE-FN1512-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller should minimize the length of preceding phases to accommodate a priority request	CVE-CN1661-V01 CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01	
CVE-FN1513-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller should immediately proceed to a pedestrian clearance interval (flashing red DON'T WALK) if an active pedestrian interval (solid white WALK) is ongoing when servicing a priority or preemption request	CVE-CN1661-V01 CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01	
CVE-FN1514-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall not reduce the duration of a pedestrian	CVE-CN1661-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			clearance interval (flashing red DON'T WALK) before progressing to the next phase when servicing a priority or preemption request	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01	

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01	
CVE-FN1515-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall next service a phase for a movement that is requested in a preemption SRM when the approach for the requested movement is red	CVE-UN220-v02 CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01	
CVE-FN1516-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall wait for the light to turn red and passage of the all-red interval before servicing a phase for a movement that is requested in a preemption SRM when the approach for the requested movement is yellow	CVE-CN1661-V01 CVE-DR1374-V02	Demonstration
CVE-FN1517-V01	V2I Mobility	General Priority/Preemption	The Traffic Signal Controller shall extend the current phase for a movement that is requested in a preemption SRM when the	CVE-CN1661-V01 CVE-DR1374-V02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			approach for the requested movement is green		
CVE-FN1518-V02	V2I Mobility	General Priority/Preemption	The Roadside Equipment shall receive output from the Traffic Signal Controller regarding the status of a priority request	CVE-UN310-v02 CVE-DR1374-V02 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-FN1519-V01	V2I Mobility	General Priority/Preemption	An RSU shall send an SSM to an HDV OBU containing the results of the requests made by one or more vehicles for a configurable period of time	CVE-UN310-v02 CVE-DR1374-V02 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-FN1520-V02	V2I Mobility	General Priority/Preemption	The Traffic CV Management System shall maintain a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request signal priority or preemption at each intersection.	CVE-UN310-v02 CVE-DR1420-V02 CVE-DR1421-V01 CVE-DR1422-V01 CVE-DR1423-V01 CVE-DR1424-V01 CVE-DR1425-V01 CVE-DR1426-V01 CVE-DR1427-V01 CVE-DR1428-V01 CVE-DR1429-V01 CVE-DR1430-V01 CVE-DR1431-V01 CVE-DR1432-V01 CVE-DR1433-V01 CVE-DR1434-V01 CVE-DR1435-V01 CVE-DR1436-V01 CVE-UN510-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-UN220-v02	
CVE-FN1524-V02	V2I Mobility	General Priority/Preemption	The Roadside Equipment shall have a method of determining if an SRM "BasicVehicleRole" is authorized to receive signal priority at the intersection	CVE-CN1662-V01 CVE-DR1292-V02 CVE-DR1293-V01 CVE-DR1295-V01	Demonstration
CVE-FN1525-V02	V2I Mobility	General Priority/Preemption	The Roadside Equipment shall have a method of determining if an SRM "BasicVehicleRole" is authorized to receive signal preemption at the intersection	CVE-CN1662-V01	Demonstration
CVE-FN3108-V02	V2I Mobility	General Priority/Preemption	The roadside equipment shall not place a priority request or a preemption request to the traffic signal controller if it determines that the vehicle OBU that is sending the SRM containing the request has already passes through the intersection.	CVE-CN1662-V01	Demonstration
CVE-FN1488-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall request to receive signal priority at RSU-equipped intersections	CVE-UN510-v02 CVE-UN520-v02	Demonstration
CVE-FN1489-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall send an SRM to an RSU when it is within a configurable distance of the intersection it intends to request priority for	CVE-UN510-v02 CVE-UN520-v02	Demonstration
CVE-FN1490-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority in an SRM	CVE-UN510-v02 CVE-UN520-v02	Demonstration
CVE-FN1491-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority for movements along the route being traversed by that transit vehicle	CVE-UN510-v02 CVE-UN520-v02	Demonstration
CVE-FN1492-V02	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall cease broadcasting SRMs for priority at a given intersection for a configurable amount of time after it has received an SSM from that	CVE-UN510-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			intersection containing the RequestID of the SRM broadcasted the host Transit Vehicle		
CVE-FN1501-V01	V2I Mobility	Transit Signal Priority	A request to receive signal priority from a Transit Vehicle OBU shall be low priority	CVE-UN510-v02 CVE-UN520-v02	Demonstration
CVE-FN1534-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall determine when to record a Transit Vehicle Interaction Event. Note: A Transit Vehicle Interaction Event contains the type of event along with a log of BSMs sent/received before and after the event.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1535-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall not issue alerts to the transit vehicle operator	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1536-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is emergency braking ahead by an OBU-equipped (remote) vehicle	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1537-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a forward collision is imminent with another OBU-equipped (remote) vehicle	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1538-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is an intersection collision detected with another OBU-equipped (remote) vehicle	CVE-UN530-v02 CVE-UN540-v02 CVE-DR1145-V01	Demonstration
CVE-FN1540-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a lane change collision is imminent with another OBU-equipped (remote) vehicle	CVE-UN530-v02 CVE-UN540-v02 CVE-DR1149-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1541-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall log a Transit Vehicle Interaction Event when the transit vehicle (host) runs a red light at an RSU-equipped intersection	CVE-UN530-v02 CVE-UN540-v02 CVE-IF1222-V01	Demonstration
CVE-FN1542-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle will enter an RSU-equipped school zone over the active school zone speed limit	CVE-UN530-v02 CVE-UN540-v02 CVE-IF1234-V01	Demonstration
CVE-FN1543-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle is inside of an RSU-equipped school zone over the active school zone speed limit	CVE-UN530-v02 CVE-UN540-v02 CVE-FN1554-V01	Demonstration
CVE-FN1544-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs received in local memory for a configurable amount of time.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1545-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SPaT messages received in local memory for a configurable amount of time.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1546-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any MAP messages received in local memory for a configurable amount of time (configuration should allow MAP messages to be stored for 7 days)	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1547-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs broadcast in local memory for a configurable amount of time.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1548-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SRMs broadcast in local memory for a configurable amount of time.	CVE-UN530-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1549-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SSMs received in local memory for a configurable amount of time.	CVE-UN530-v02	Demonstration
CVE-FN1550-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the type of event (emergency braking ahead, forward collision imminent, intersection movement, blind spot, lane change, red light violation, school zone speed limit, priority request)	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1551-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the transit vehicle OBU broadcasts an SRM	CVE-UN530-v02 CVE-DR1391-V01 CVE-DR1392-V01	Demonstration
CVE-FN1554-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove Transit Vehicle Interaction Event data with the oldest start times from memory until it is able to log a newly received interaction event	CVE-UN530-v02 CVE-UN540-v02 CVE-FN1543-V01	Demonstration
CVE-FN1555-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall upload all Transit Vehicle Interaction Event data to the Transit CV Management System when it connects to the vehicle's regular data upload service.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1556-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove all Transit Vehicle Interaction Event data from memory once uploaded to the Transit CV Management System.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1557-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the start time of the event (UTC)	CVE-UN530-v02 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1387-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01 CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01 CVE-FN1312-V01	
CVE-FN1558-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the end time of the event (UTC) (in the case where multiple events of the same warning are issued based on messages received from the same vehicle or intersection within a configurable amount of time)	CVE-UN530-v02 CVE-FN1312-V01	Demonstration
CVE-FN1559-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast	CVE-UN530-v02 CVE-DR1144-V01 CVE-DR1145-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			BSMs) from a configurable amount of time before the start time of the event	CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01	

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01	
CVE-FN1560-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast BSMs) from a configurable amount of time after the end time of the event	CVE-UN530-v02 CVE-DR1374-V02 CVE-FN1313-V01	Demonstration
CVE-FN3081-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3082-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if there is emergency braking ahead for each BSM it receives.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3083-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a forward collision is imminent for each BSM it receives	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3084-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if an intersection collision is imminent for each BSM it receives.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3085-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a lane change collision is imminent for each BSM it receives.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN3086-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also	CVE-UN530-v02 CVE-UN540-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			received a MAP message for the intersection that corresponds to the SPaT message.		
CVE-FN3087-V02	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.	CVE-UN530-v02 CVE-UN540-v02	Demonstration
CVE-FN1564-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Roadside Equipment shall send BSMs to the Traffic CV Management System as they are received from an OBU	CVE-UN410-v02	Demonstration
CVE-FN1566-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Roadside Equipment shall send SRMs to the Traffic CV Management System as they are received from an OBU	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-UN410-v02 CVE-PR1105-V01 CVE-IX1635-V01	Demonstration
CVE-FN1569-V02	V2I Mobility	Vehicle Data for Traffic Operations	The roadside equipment shall send SSMs to the Traffic CV Management System as they are generated by the roadside equipment.	CVE-UN410-v02 CVE-IX1635-V01	Demonstration
CVE-FN1572-V02	V2I Mobility	Vehicle Data for Traffic Operations	The roadside equipment shall send SPaT messages to the Traffic CV Management System as they are generated by the roadside equipment	CVE-UN410-v02 CVE-IX1635-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1580-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive BSMs sent by the roadside equipment	CVE-UN410-v02 CVE-IX1635-V01	Demonstration
CVE-FN1581-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SRMs sent by the roadside equipment	CVE-UN410-v02 CVE-DR1276-V01 CVE-IX1635-V01	Demonstration
CVE-FN1582-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SSMs sent by the roadside equipment	CVE-UN410-v02 CVE-DR1292-V02 CVE-DR1293-V01 CVE-DR1295-V01 CVE-IX1635-V01	Demonstration
CVE-FN1583-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SPaT Messages sent by the roadside equipment	CVE-UN410-v02	Demonstration
CVE-FN1585-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store BSMs sent by the roadside equipment	CVE-UN410-v02 CVE-UN440-v02	Demonstration
CVE-FN1586-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SRMs sent by the roadside equipment	CVE-UN410-v02 CVE-UN440-v02	Demonstration
CVE-FN1587-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SSMs sent by the roadside equipment	CVE-UN410-v02 CVE-UN440-v02	Demonstration
CVE-FN1588-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SPaT messages sent by the roadside equipment	CVE-UN410-v02 CVE-UN440-v02	Demonstration
CVE-FN1589-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SAE J2735 TIMs generated by Traffic Management Staff	CVE-UN410-v02 CVE-DR1402-V01 CVE-DR1403-V01 CVE-DR1404-V01	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1405-V01 CVE-DR1406-V01 CVE-DR1407-V01 CVE-DR1408-V01 CVE-DR1409-V01 CVE-DR1410-V01 CVE-DR1411-V01 CVE-DR1412-V01 CVE-DR1413-V01 CVE-DR1414-V01 CVE-DR1415-V01 CVE-DR1416-V01 CVE-DR1417-V01 CVE-DR1418-V01 CVE-DR1419-V01 CVE-UN440-v02	
CVE-FN1590-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store all MAP messages that are input by the Traffic Manager	CVE-UN410-v02 CVE-DR1402-V01 CVE-DR1403-V01 CVE-DR1404-V01 CVE-DR1405-V01 CVE-DR1406-V01 CVE-DR1407-V01 CVE-DR1408-V01 CVE-DR1409-V01 CVE-DR1410-V01 CVE-DR1411-V01 CVE-DR1412-V01 CVE-DR1413-V01	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1414-V01 CVE-DR1415-V01 CVE-DR1416-V01 CVE-DR1417-V01 CVE-DR1418-V01 CVE-DR1419-V01 CVE-UN440-v02	
CVE-FN1591-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall make all stored data available to the Traffic Manager	CVE-UN410-v02 CVE-DR1402-V01 CVE-DR1403-V01 CVE-DR1404-V01 CVE-DR1405-V01 CVE-DR1406-V01 CVE-DR1407-V01 CVE-DR1408-V01 CVE-DR1409-V01 CVE-DR1410-V01 CVE-DR1411-V01 CVE-DR1412-V01 CVE-DR1413-V01 CVE-DR1414-V01 CVE-DR1415-V01 CVE-DR1416-V01 CVE-DR1417-V01 CVE-DR1418-V01 CVE-DR1419-V01 CVE-UN440-v02	Inspection
CVE-FN3078-V01	V2I Safety	Red Light Violation Warning	The Red Light Violation Warning Application shall identify when a vehicle is	CVE-UN130-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			expected to cross the stop bar during a red signal by using the following data items: 1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. Normal deceleration rate 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of SPaT to the time the alert is issued) 6. SPaT data (received from the RSU) 7. MAP data (received from the RSU) 8. RTCM data (received from the RSU)		
CVE-FN1300-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIM to identify the school zone speed limit (J2735).	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN1301-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify when the school zone speed limit is active.	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN1302-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify the applicable regions of use geographical path (J2735).	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN3079-V02	V2I Safety	Reduced Speed School Zone	The Reduced Speed School Zone Application shall identify when a host vehicle is expected to enter the school zone but not below the school zone speed limit (given its current location, motion, and expected braking rate) during active school zone hours by using the following data items:	CVE-CN1660-V01 CVE-UN140-v02 CVE-UN610-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. TIM data (received from the RSU) 3. RTCM data (received from the RSU)		
CVE-FN3074-V01	V2V Safety	Blind Spot Warning	The Blind Spot Warning Application shall identify when a remote vehicle is within the blind spot (a configurable area to the rear right and rear left of a vehicle that moves with the vehicle) of a host vehicle, and is moving in the same direction of travel as the host vehicle by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued	CVE-CN1660-V01 CVE-UN120-v02	Demonstration
CVE-FN3075-V01	V2V Safety	Emergency Electronic Brake Light	The Emergency Electronic Brake Light Application shall identify when an emergency braking maneuver has been detected by a remote vehicle, the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items:	CVE-UN111-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Normal deceleration rate 4. Perception/reaction time 5. Expected DSRC Transmission Latency 6. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)		
CVE-FN3073-V01	V2V Safety	Forward Collision Warning	The Forward Collision Warning Application shall identify when the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle and the remote vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Normal deceleration rate 4. Perception/reaction time 5. Expected DSRC Transmission Latency 6. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)	CVE-UN112-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN3077-V01	V2V Safety	Intersection Movement Assist	The Intersection Movement Assist Application shall identify when the host vehicle has a trajectory (based on position, speed, acceleration) that may interfere with remote) vehicle trajectory in a side impact fashion, and the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle) by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)	CVE-UN113-v02 CVE-CN1660-V01	Demonstration
CVE-FN3076-V01	V2V Safety	Lane Change Warning	The Lane Change Warning Application shall identify when a host vehicle is changing lanes into a remote vehicle, and is moving in the same direction of travel as the host vehicle by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency	CVE-UN114-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued		
CVE-FN1215-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall not broadcast SRMs when its lights are off and siren is off	CVE-IX1609-V01	Demonstration
CVE-FN1216-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall only broadcast SRMs when its lights are on and siren is on.	CVE-IX1609-V01	Demonstration
CVE-FN1495-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall only request preemption in an SRM	CVE-UN220-v02	Demonstration
CVE-FN1496-V02	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall cease sending SRMs for preemption to an RSU at a given intersection for a configurable amount of time after it has received an SSM from the RSU at that intersection containing the RequestID of the SRM broadcasted the host Emergency Vehicle	CVE-UN220-v02	Demonstration
CVE-FN2957-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2958-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to an RSU	CVE-IX1632-V01	Demonstration
CVE-FN2961-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive position data from GNSS satellites	CVE-IX1621-V01	Demonstration
CVE-FN2964-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive security certificates from an SCMS via the RSU	CVE-IX1610-V01	Demonstration
CVE-FN2975-V02	Vehicle Onboard Equipment	Emergency Vehicle OBU	The RSU shall broadcast J2735 MAP messages received as an, RSU	CVE-IX1610-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU		
CVE-FN2977-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An RSU shall send an SSM to an Emergency Vehicle OBU containing the results of the requests made by one or more vehicles for a configurable period of time	CVE-IX1610-V01	Demonstration
CVE-FN2998-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	The Emergency Vehicle OBU shall be able to send the SRM at a configurable rate	CVE-IX1609-V01	Demonstration
CVE-FN1184-V01	Vehicle Onboard Equipment	General OBU	An OBU shall be capable of being reset and reconfigured so that it can be installed into another vehicle of the same type (e.g. LDV, HDV, etc.)	CVE-CN1663-V01	Demonstration
CVE-FN1185-V01	Vehicle Onboard Equipment	General OBU	An OBU host processor shall perform integrity checks on boot to ensure that it is in a known good software state.	CVE-CN1649-V01 CVE-CN1650-V01 CVE-CN1651-V01 CVE-CN1652-V01 CVE-CN1653-V01 CVE-CN1654-V01 CVE-CN1655-V01 CVE-CN1656-V01 CVE-CN1657-V01 CVE-CN1658-V01	Demonstration
CVE-FN1186-V01	Vehicle Onboard Equipment	General OBU	An OBU shall not continue to start up and will log an error if the host processor determines it is not in a known good software state on boot up.	CVE-SN870-v02	Demonstration
CVE-FN1198-V01	Vehicle Onboard Equipment	General OBU	The OBU should notify the vehicle operators of the power status of device (e.g., off, powering up and online).	CVE-IX1618-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1204-V02	Vehicle Onboard Equipment	General OBU	An OBU shall acquire time from the Location and Time Service (LTS) interface in accordance with J2945/1 section 6.2.4.	CVE-FN1192-V01 CVE-SN840-v02 CVE-FN1193-V01 CVE-IX1621-V01 CVE-IX1622-V01 CVE-IX1623-V01 CVE-IX1624-V01	Demonstration
CVE-FN1205-V01	Vehicle Onboard Equipment	General OBU	An OBU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.	CVE-SN830-v02 CVE-IX1621-V01 CVE-IX1622-V01 CVE-IX1623-V01 CVE-IX1624-V01	Demonstration
CVE-FN1207-V01	Vehicle Onboard Equipment	General OBU	The OBU may capture vehicle brake status over the OBU-OBD-II interface to the host vehicle	CVE-UN110-v02 CVE-UN111-v02 CVE-IX1617-V01 CVE-IX1608-V01 CVE-IX1641-V01 CVE-IX1612-V01	Demonstration
CVE-FN1209-V01	Vehicle Onboard Equipment	General OBU	An OBU device shall comply with IEEE 1609.2: Standard for WAVE Security Services for Applications and Management Messages	CVE-CN1648-V01	Demonstration
CVE-FN1212-V01	Vehicle Onboard Equipment	General OBU	The OBU shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted.	CVE-IX1609-V01 CVE-IX1615-V01 CVE-IX1619-V01 CVE-IX1632-V01	Demonstration
CVE-FN2959-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive position data from GNSS satellites	SMH-DR2328-V01 CVE-IX1622-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN2962-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive security certificates from an SCMS via the RSU	CVE-IX1616-V01	Demonstration
CVE-FN2968-V02	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2969-V02	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an RSU	CVE-IX1615-V01	Demonstration
CVE-FN2996-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	The HDV OBU shall be able to send the SRM at a configurable rate	CVE-IX1615-V01	Demonstration
CVE-FN3025-V01	Vehicle Onboard Equipment	Light-Duty Vehicle HMI	The LDV OBU shall not allow the driver to adjust settings while the vehicle is in motion.	CVE-IX1618-V01	Demonstration
CVE-FN1107-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is an OBU-equipped (remote) vehicle in the host vehicle's blind spot	CVE-UN120-v02	Demonstration
CVE-FN1108-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives	CVE-UN120-v02	Demonstration
CVE-FN1115-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is emergency braking ahead by an OBU-equipped (remote) vehicle	CVE-UN111-v02	Demonstration
CVE-FN1116-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if there is emergency braking ahead for each BSM it receives	CVE-UN111-v02	Demonstration
CVE-FN1122-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the LDV HMI when a forward collision is imminent with another OBU-equipped (remote) vehicle	CVE-UN112-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1123-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall present alerts to drivers (via the HMI) using an HMI device that drivers are familiar with and limits driver interaction.	CVE-IX1618-V01	Demonstration
CVE-FN1124-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a forward collision is imminent for each BSM it receives	CVE-UN112-v02	Demonstration
CVE-FN1131-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when an intersection collision is imminent with another OBU-equipped (remote) vehicle	CVE-UN113-v02	Demonstration
CVE-FN1132-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if an intersection collision is imminent for each BSM it receives	CVE-UN113-v02	Demonstration
CVE-FN1138-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when it is changing lanes into another OBU-equipped (remote) vehicle	CVE-UN114-v02	Demonstration
CVE-FN1139-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a lane change collision is imminent for each BSM it receives	CVE-UN114-v02	Demonstration
CVE-FN1187-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall communicate with an LDV Operator via an HMI	CVE-IX1618-V01	Demonstration
CVE-FN1188-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall have two levels of alert	CVE-PR1530-V01	Demonstration
CVE-FN1189-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall have a low-level alert	CVE-FN1195-V01	Demonstration
CVE-FN1190-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The low-level alert shall consist of a configurable audio/visual warning	CVE-FN1196-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1191-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall have a high-level alert	CVE-FN1195-V01	Demonstration
CVE-FN1192-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The high-level alert shall consist of a configurable audio/visual warning	CVE-FN1204-V02	Demonstration
CVE-FN1193-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The high-level alert shall be louder and more visible compared to the low-level alert	CVE-FN1196-V01 CVE-FN1204-V02	Demonstration
CVE-FN1194-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall not display more than one alert to the LDV Vehicle Operator at a time	CVE-PR1530-V01	Demonstration
CVE-FN1195-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall contain a configurable priority order for notifying with alerts	CVE-FN1189-V01 CVE-FN1191-V01	Demonstration
CVE-FN1196-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The order of alerts shall be configurable so that the order of alerts can be modified once priority has been established.	CVE-FN1190-V01 CVE-FN1193-V01	Demonstration
CVE-FN1197-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should provide system status information to LDV operators. Information included in the system status includes power status, system settings, status of applications availability, and pending update status	CVE-IX1618-V01	Demonstration
CVE-FN1202-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall provide messages that can be seen and/or heard by the LDV Operator via the HMI from the LDV Vehicle Operator's normal seating position	CVE-IX1618-V01	Demonstration
CVE-FN1203-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall provide only the highest priority alert to the LDV vehicle operator when more than one alert is currently active	CVE-IX1618-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN1210-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue an Emergency Electronic Brake Light alert	CVE-PR1530-V01	Demonstration
CVE-FN1213-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should provide a visual output (via the HMI) that is similar in look and feel (i.e. similar in size, consistent use of color in icons or graphics, similar styles of icons or graphics) from various applications, if presenting visual information to LDV Operators	CVE-IX1618-V01	Demonstration
CVE-FN1286-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when a red-light violation will occur at an RSU-equipped intersection	CVE-UN130-v02	Demonstration
CVE-FN1287-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also received a MAP message for the intersection that corresponds to the SPaT message.	CVE-UN130-v02	Demonstration
CVE-FN1298-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when the OBU-equipped (host) vehicle will enter an RSU-equipped school zone over the active school zone speed limit	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN1299-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert when the OBU-equipped (host) vehicle is inside of an RSU-equipped school zone over the active school zone speed limit	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN2952-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive BSMs from a Transit Vehicle OBU	CVE-IX1629-V01	Demonstration
CVE-FN2953-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive BSMs from an Emergency Vehicle OBU	CVE-IX1629-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN2970-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2971-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an RSU	CVE-IX1619-V01	Demonstration
CVE-FN3011-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Forward Collision Warning alert	CVE-UN112-v02 CVE-UN110-v02	Demonstration
CVE-FN3012-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue an Intersection Movement Assist alert	CVE-UN113-v02 CVE-UN110-v02	Demonstration
CVE-FN3013-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Lane Change Warning/Blind Spot Warning alert	CVE-UN120-v02 CVE-UN114-v02 CVE-UN110-v02	Demonstration
CVE-FN3014-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Red Light Violation Warning alert	CVE-UN130-v02	Demonstration
CVE-FN3015-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Reduced Speed School Zone alert	CVE-FN1304-V01 CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN3021-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall be customizable for the following options (via the HMI): Volume, Brightness (if screen is used), Text size (if screen is used), Display contrast (if screen is used), Mounting Eye Position (if screen is used)	CVE-IX1618-V01	Demonstration
CVE-FN3022-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should provide system status to drivers (via the HMI)	CVE-IX1618-V01	Inspection
CVE-FN3023-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should notify the LDV Operator of the power status of the OBU (via the HMI) (e.g. off, powering up, online, powering down)	CVE-IX1618-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN3024-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should allow the LDV Operator to adjust the system settings of the device (via the HMI) (e.g. version, brightness (if screen is used), volume, text size (if screen is used), contrast (if screen is used))	CVE-IX1618-V01	Demonstration
CVE-FN3026-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should notify the LDV Operator of application availability (via the HMI) (e.g. failed, operating, disabled).	CVE-IX1618-V01	Demonstration
CVE-FN3027-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU should notify the LDV Operator of pending updates for the LDV OBU (via the HMI) (e.g. applications, firmware, operating system).	CVE-IX1618-V01	Demonstration
CVE-FN3028-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall provide a visible and/or audible sound (via the HMI) when the vehicle is started up to indicate to the LDV Operator that they are in a CV-equipped vehicle.	CVE-IX1618-V01	Demonstration
CVE-FN3080-V02	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.	CVE-UN140-v02 CVE-UN610-v02	Demonstration
CVE-FN1206-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall transmit Transit Vehicle Interaction Events to the Transit CV Management System	CVE-IX1642-V01	Demonstration
CVE-FN1208-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall use Coordinated Universal Time (UTC) time for all logged data (e.g., events logs, probe vehicle data) based on the format defined in J2735 section 6.19 and epoch of January 1st, 1970.	CVE-CN1648-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-FN2954-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive BSMs from an HDV OBU	CVE-IX1630-V01	Demonstration
CVE-FN2955-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive BSMs from a Transit Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2956-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive BSMs from an Emergency Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2960-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive position data from GNSS satellites	CVE-IX1624-V01	Demonstration
CVE-FN2963-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive security certificates from an SCMS via the RSU	CVE-IX1631-V01	Demonstration
CVE-FN2966-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU	CVE-IX1630-V01	Demonstration
CVE-FN2967-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an RSU	CVE-IX1632-V01	Demonstration
CVE-FN2974-V02	Vehicle Onboard Equipment	Transit Vehicle OBU	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU	CVE-IX1631-V01	Demonstration
CVE-FN2976-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	An RSU shall send an SSM to a Transit Vehicle OBU containing the results of the requests made by one or more vehicles for a configurable period of time	CVE-IX1631-V01	Demonstration
CVE-FN2997-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	The Transit Vehicle OBU shall be able to send the SRM at a configurable rate	CVE-IX1632-V01	Demonstration
CVE-FN1494-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send an SRM to an RSU when it is less than a configurable amount of time away from	CVE-UN220-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
			arriving at the intersection it intends to request priority for		

Source: City of Columbus

3.2. PERFORMANCE REQUIREMENTS

This section provides the performance requirements (PR) for the system of interest (i.e. what the system will do). The requirements in **Table 10** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 10: Performance Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1105-V01	DSRC Messages	Basic Safety Message	The BSM shall be broadcast at a frequency of 10 Hz when congestion control algorithms (SAE J2945/1) do not prescribe a reduced rate	CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1506-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01	Test

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR3003-V01	DSRC Messages	Basic Safety Message	The BSM shall always include Part I data (SAE J2735, Section 6.8)	CVE-CN1648-V01	Demonstration
CVE-PR3009-V01	DSRC Messages	Basic Safety Message	The BSM shall be broadcast at the frequency specified by congestion control algorithms (SAE J2945/1) when congestion control algorithms (SAE J2945/1) prescribe a reduced frequency	CVE-CN1648-V01	Demonstration
CVE-PR1183-V01	DSRC Messages	MapData Message	The MAP message shall be expressed with an accuracy of 0.5 m or less.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Inspection
CVE-PR2993-V01	DSRC Messages	MapData Message	The MAP message shall be transmitted with a frequency of at least 1 Hz	CVE-IX1631-V01 CVE-IX1620-V02 CVE-IX1610-V01 CVE-IX1616-V01	Demonstration
CVE-PR1399-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT messages shall be generated and transmitted by the RSU with a minimum frequency of 10 Hz	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Test

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1400-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT MsgCount data field shall be incremented with every update that is made to the corresponding IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Test
CVE-PR1401-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT MovementStates shall be updated with at least the computation frequency of the traffic signal controller. If the controller is operating at 1 Hz, it is permissible to repeat the same MovementState information in 10 SPaT messages. However, if the controller is operating at 10 Hz or greater, the MovementStates needs to be updated for every message.	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Test
CVE-PR2995-V01	DSRC Messages	Signal Request Message	The SRM shall be broadcast at the configured frequency (functional reqs describe when to start/stop broadcasting)	CVE-IX1619-V01 CVE-IX1609-V01 CVE-IX1615-V01	Demonstration
CVE-PR2999-V01	DSRC Messages	Signal Status Message	The SSM shall be broadcast at the configured frequency (functional reqs describe when to start/stop broadcasting)	CVE-IX1620-V02 CVE-IX1610-V01 CVE-IX1616-V01	Demonstration
CVE-PR1365-V01	Roadside Equipment	Roadside Unit	The system clock of the RSU shall be accurate to within 10 ms of the UTC reference	CVE-IF1240-V02 CVE-IF1241-V02 CVE-IF1242-V01	Inspection
CVE-PR1366-V01	Roadside Equipment	Roadside Unit	All absolute times in any message shall be determined based on the RSU's system clock	CVE-IF1240-V02 CVE-IF1241-V02 CVE-IF1242-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1367-V01	Roadside Equipment	Roadside Unit	The time difference between minEndTime (in the UTC reference system) and the earliest possible physical phase change shall be no larger than 100 ms	CVE-IF1240-V02 CVE-IF1241-V02 CVE-IF1242-V01	Test
CVE-PR1368-V01	Roadside Equipment	Roadside Unit	The time difference between maxEndTime (in the UTC reference system) and the earliest possible physical phase change shall be no larger than 100 ms	CVE-IF1240-V02 CVE-IF1241-V02 CVE-IF1242-V01	Test
CVE-PR1369-V01	Roadside Equipment	Roadside Unit	The data elements MinuteOfTheYear and DSecond shall be present in each transmitted message and accurate within 100 ms of UTC time	CVE-CN1648-V01	Test
CVE-PR2994-V02	Roadside Equipment	Roadside Unit	School Zone RSUs shall broadcast the TIM at a frequency of 1 Hz	CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-PR1457-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall notify designated personnel within five minutes of limited connectivity. Note: Limited connectivity refers to a state when the Traffic CV Management System is not able to communicate with the RSU	CVE-UN430-v02	Test
CVE-PR1458-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall notify designated personnel within five minutes of a monitored function becoming unavailable	CVE-UN430-v02	Test
CVE-PR3029-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of archived CV data	CVE-UN410-v02 CVE-UN440-v02 CVE-CN1663-V01	Inspection
CVE-PR3031-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of backup archived CV data	CVE-UN440-v02 CVE-UN410-v02 CVE-CN1663-V01	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR3033-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the backup archived CV data once per day.	CVE-UN440-v02 CVE-UN410-v02 CVE-CN1663-V01	Demonstration
CVE-PR3035-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of archived Transit Vehicle Interaction Events	CVE-UN530-v02 CVE-UN540-v02	Inspection
CVE-PR3036-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of backup archived Transit Vehicle Interaction Events	CVE-UN530-v02 CVE-UN540-v02	Inspection
CVE-PR3037-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the backup archived Transit Vehicle Interaction Events once per day.	CVE-UN540-v02 CVE-UN530-v02	Demonstration
CVE-PR1531-V01	V2I Mobility	Emergency Vehicle Preemption	The EVP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN220-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR1527-V02	V2I Mobility	Freight Signal Priority	The FSP application should employ proven algorithms to enable freight signal priority	CVE-UN310-v02 CVE-CN1660-V01	Demonstration
CVE-PR1528-V01	V2I Mobility	Freight Signal Priority	The FSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN310-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR1529-V02	V2I Mobility	Transit Signal Priority	The TSP application should employ proven algorithms to enable transit signal priority	CVE-UN510-v02 CVE-UN520-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1530-V01	V2I Mobility	Transit Signal Priority	The TSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN510-v02 CVE-FN1188-V01 CVE-FN1194-V01 CVE-FN1210-V01 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR1290-V02	V2I Safety	Red Light Violation Warning	The RLVW application should employ proven algorithms to issue an RLVW	CVE-UN130-v02 CVE-CN1660-V01	Inspection
CVE-PR1291-V01	V2I Safety	Red Light Violation Warning	The RLVW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN130-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3118-V01	V2I Safety	Red Light Violation Warning	The RLVW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN130-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR1306-V02	V2I Safety	Reduced Speed School Zone	The RSSZ application should employ proven algorithms to issue an RSSZ warning	CVE-UN140-v02 CVE-UN610-v02 CVE-CN1660-V01	Inspection
CVE-PR1307-V01	V2I Safety	Reduced Speed School Zone	The RSSZ application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN140-v02 CVE-UN610-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3119-V01	V2I Safety	Reduced Speed School Zone	The RSSZ application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN140-v02 CVE-UN610-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1111-V02	V2V Safety	Blind Spot Warning	The BSW application should employ proven algorithms to issue an BSW alert	CVE-UN120-v02 CVE-CN1660-V01	Demonstration
CVE-PR1112-V01	V2V Safety	Blind Spot Warning	The BSW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN120-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3114-V01	V2V Safety	Emergency Electronic Brake Light	The EEBL application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN120-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR1119-V02	V2V Safety	Emergency Electronic Brake Light Warning	The EEBL application should employ proven algorithms to issue an EEBL alert.	CVE-UN111-v02 CVE-CN1660-V01	Demonstration
CVE-PR1120-V01	V2V Safety	Emergency Electronic Brake Light Warning	The EEBL application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN111-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR1127-V02	V2V Safety	Forward Collision Warning	The FCW application should employ proven algorithms to issue an FCW alert	CVE-UN112-v02 CVE-CN1660-V01	Demonstration
CVE-PR1128-V01	V2V Safety	Forward Collision Warning	The FCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN112-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3115-V01	V2V Safety	Forward Collision Warning	The FCW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN112-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR1135-V02	V2V Safety	Intersection Movement Assist	The IMA application should employ proven algorithms to issue an IMA alert	CVE-UN113-v02 CVE-CN1660-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR1136-V01	V2V Safety	Intersection Movement Assist	The IMA application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN113-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3116-V01	V2V Safety	Intersection Movement Assist	The IMA application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN113-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR1142-V02	V2V Safety	Lane Change Warning	The LCW application should employ proven algorithms to issue an LCW alert	CVE-UN114-v02 CVE-CN1660-V01	Demonstration
CVE-PR1143-V01	V2V Safety	Lane Change Warning	The LCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)	CVE-UN114-v02 CVE-CN1660-V01 CVE-CN1647-V01	Analyze
CVE-PR3117-V01	V2V Safety	Lane Change Warning	The LCW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN114-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR3113-V01	V2V Safety	Blind Spot Warning	The BSW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.	CVE-UN120-v02 CVE-CN1660-V01 CVE-CN1647-V01	Test
CVE-PR2907-V01	Vehicle Onboard Equipment	General OBU	The OBU shall have a minimum reserve (processor, dynamic storage, persistent storage) capacity of 50% upon deployment to have the capacity to install and run future firmware image updates	CVE-CN1663-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.	CVE-IX1618-V01 CVE-UN120-v02 CVE-UN113-v02 CVE-UN110-v02 CVE-UN111-v02 CVE-UN112-v02 CVE-UN114-v02 CVE-UN130-v02 CVE-UN140-v02	Demonstration
CVE-PR3020-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU Auditory signals (via the HMI) shall be loud enough to overcome masking sounds from road noise, the cab environment, and other equipment.	CVE-IX1618-V01	Demonstration
CVE-PR2913-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall be capable of holding 4 GB of interaction event data.	CVE-UN530-v02 CVE-UN540-v02	Inspection

Source: City of Columbus

3.3. INTERFACE REQUIREMENTS

The CVE interfaces allow dynamic and configurable functionality between internal components of the Smart Columbus SoS and external systems that provide data or some other stated functionality as per the user needs. The IF requirements in **Table 11** have been categorized into these two groups, which will help further clarify system boundaries.

Table 11: Interface Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1344-V01	Common	Common	An RSU shall receive security certificates from an SCMS	CVE-IX1634-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1341-V02	Roadside Equipment	Roadside Unit	An RSU shall receive TIMs as an, RSU Specification 4.1a, "Immediate Forward" message from a network host	CVE-IX1636-V02	Demonstration
CVE-IF1342-V02	Roadside Equipment	Roadside Unit	An RSU shall receive MAP messages as an, RSU Specification 4.1a, "Immediate Forward" message from a network host	CVE-IX1636-V02	Demonstration
CVE-IF1343-V01	Roadside Equipment	Roadside Unit	An RSU shall receive position data from the LTS	CVE-IX1625-V01	Demonstration
CVE-IF1345-V01	Roadside Equipment	Roadside Unit	An RSU shall receive SPaT messages from the Traffic Signal Controller	CVE-IX1638-V01	Demonstration
CVE-IF1346-V01	Roadside Equipment	Roadside Unit	An RSU should receive SSMs from a Traffic Signal Controller	CVE-IX1638-V01	Demonstration
CVE-IF1347-V01	Roadside Equipment	Roadside Unit	An RSU shall send information to request signal priority to the Traffic Signal Controller	CVE-UN220-v02 CVE-UN310-v02 CVE-UN510-v02 CVE-IX1637-V01	Demonstration
CVE-IF1348-V01	Roadside Equipment	Roadside Unit	An RSU shall be powered via power over Ethernet (cat6a)	CVE-CN1659-V01	Demonstration
CVE-IF1349-V01	Roadside Equipment	Roadside Unit	An RSU shall be grounded	CVE-CN1659-V01	Demonstration
CVE-IF1350-V01	Roadside Equipment	Roadside Unit	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be outfitted with an in-line grounding mechanism	CVE-IX1637-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1351-V01	Roadside Equipment	Roadside Unit	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be weatherproof (outdoor rated)	CVE-IX1637-V01	Demonstration
CVE-IF1352-V01	Roadside Equipment	Roadside Unit	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be double shielded	CVE-IX1637-V01	Demonstration
CVE-IF1353-V01	Roadside Equipment	Roadside Unit	The RSU-SCMS interface shall allow an RSU to request application certificates with different contents from the current ones during the lifetime of the current ones.	CVE-SN820-v02 CVE-IX1634-V01	Demonstration
CVE-IF1354-V01	Roadside Equipment	Roadside Unit	Communication between the RSU and an SCMS shall operate in an encrypted, end-to-end connection in accordance with the selected SCMS interface. (Note: An SCMS interface should not need any further security.)	CVE-SN820-v02 CVE-IX1633-V01 CVE-IX1634-V01	Demonstration
CVE-IF1356-V01	Roadside Equipment	Roadside Unit	An RSU shall send SPaT messages generated from traffic signal controller output to an LDV OBU	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-IF1357-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an LDV OBU	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-IF1358-V01	Roadside Equipment	Roadside Unit	An RSU shall send RTCM messages received from the CORS or another source to an LDV OBU	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1359-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1631-V01	Demonstration
CVE-IF1360-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 TIM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an LDV OBU	CVE-DR1292-V02 CVE-DR1293-V01 CVE-DR1295-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-IF1361-V01	Roadside Equipment	Roadside Unit	An RSU shall receive over the air messages via DSRC	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01 CVE-IX1609-V01 CVE-IX1615-V01 CVE-IX1619-V01 CVE-IX1632-V01	
CVE-IF1362-V01	Roadside Equipment	Roadside Unit	An RSU shall receive BSMs from an LDV OBU	CVE-IX1609-V01 CVE-IX1615-V01 CVE-IX1619-V01 CVE-IX1632-V01	Demonstration

CVE-IF1363-V01	Roadside Equipment	Roadside Unit	An RSU shall receive SRMs from an HDV OBU	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1180-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01 CVE-IX1609-V01 CVE-IX1615-V01	
CVE-IF2978-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 TIM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU	CVE-IX1631-V01	Demonstration
CVE-IF2985-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU	CVE-IX1631-V01	Demonstration
CVE-IF2986-V02	Roadside Equipment	Roadside Unit	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU	CVE-IX1610-V01	Demonstration
CVE-IF3044-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall use a UI to geographically display the location of each RSU and RSU information to Traffic Management Staff	CVE-UN430-v02 CVE-CN1663-V01 CVE-IX1611-V02	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1277-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall generate performance metrics (as configured by transit management staff and as defined in the Performance Measurement Plan)	CVE-IX1640-V01	Demonstration
CVE-IF1472-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall send Transit Vehicle Interaction Events to the Smart Columbus OS	CVE-IX1640-V01 CVE-SN810-v02	Demonstration
CVE-IF1473-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall make Transit Vehicle Interaction Events available to Transit Management Staff	CVE-UN530-v02 CVE-UN540-v02 CVE-IX1643-V01	Demonstration
CVE-IF1526-V01	V2I Mobility	Transit Signal Priority	The TSP Application shall receive data from the OBU's internal processing functions.	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-IF1561-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall receive data from the OBU's internal processing functions.	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02	Demonstration
CVE-IF1221-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU	CVE-IX1630-V01	Demonstration
CVE-IF1228-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive SPaT messages from an RSU	CVE-IX1610-V01	Demonstration
CVE-IF1232-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive MAP messages from an RSU	CVE-IX1610-V01	Demonstration
CVE-IF1236-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive RTCM messages from an RSU	CVE-IX1610-V01	Demonstration
CVE-IF1239-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive SSM messages from an RSU	CVE-IX1610-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1244-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive the flashing light status from the appropriate vehicle system	CVE-UN220-v02 CVE-IX1608-V01	Demonstration
CVE-IF1245-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive the siren status from the appropriate vehicle system	CVE-UN220-v02 CVE-IX1608-V01	Demonstration
CVE-IF1248-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall provide a means of ceasing the broadcast of DSRC messages	CVE-IX1644-V01	Demonstration
CVE-IF1251-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send SRMs to an RSU	CVE-IX1609-V01	Demonstration
CVE-IF1243-V01	Vehicle Onboard Equipment	General OBU	An LDV OBU shall receive security certificates from an SCMS via the RSU	CVE-IX1610-V01 CVE-IX1616-V01 CVE-IX1620-V02 CVE-IX1631-V01	Demonstration
CVE-IF1219-V02	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU	CVE-IX1629-V01 CVE-IX1630-V01 CVE-IX1615-V01	Demonstration
CVE-IF1226-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive SPaT messages from an RSU	CVE-IX1616-V01	Demonstration
CVE-IF1230-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive MAP messages from an RSU	CVE-IX1616-V01	Demonstration
CVE-IF1234-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive RTCM messages from an RSU	CVE-FN1542-V01 CVE-IX1616-V01	Demonstration
CVE-IF1237-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall receive SSM messages from an RSU	CVE-IX1616-V01	Demonstration
CVE-IF1249-V01	Vehicle Onboard Equipment	Heavy-Duty Vehicle OBU	An HDV OBU shall send SRMs to an RSU	CVE-IX1615-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1218-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU	CVE-IX1629-V01 CVE-IX1630-V01 CVE-IX1619-V01	Demonstration
CVE-IF1222-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall communicate alerts to an LDV Operator	CVE-IX1618-V01 CVE-FN1541-V01	Demonstration
CVE-IF1223-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive BSMs from an LDV OBU	CVE-IX1629-V01 CVE-IX1630-V01	Demonstration
CVE-IF1225-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive SPaT messages from an RSU	CVE-IX1620-V02	Demonstration
CVE-IF1229-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive MAP messages from an RSU	CVE-IX1620-V02	Demonstration
CVE-IF1233-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive RTCM messages from an RSU	CVE-IX1620-V02	Demonstration
CVE-IF1240-V02	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive TIM messages from an RSU	CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01 CVE-IX1620-V02	Demonstration
CVE-IF1242-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall receive position data from GNSS satellites	CVE-IX1623-V01 CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI	CVE-UN110-v02 CVE-UN111-v02 CVE-UN112-v02 CVE-UN113-v02 CVE-UN114-v02 CVE-UN120-v02 CVE-UN140-v02 CVE-UN140-v02 CVE-UN140-v02 CVE-UN610-v02 CVE-IX1618-V01	Demonstration
CVE-IF3019-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall include both a visual and/or auditory interface for sharing traveler information (via the HMI).	CVE-IX1618-V01	Demonstration
CVE-IF1220-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an LDV OBU	CVE-IX1629-V01 CVE-IX1630-V01 CVE-IX1632-V01	Demonstration
CVE-IF1224-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive BSMs from an LDV OBU	CVE-IX1629-V01 CVE-IX1630-V01	Demonstration
CVE-IF1227-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive SPaT messages from an RSU	CVE-IX1631-V01	Demonstration
CVE-IF1231-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive MAP messages from an RSU	CVE-IX1631-V01	Demonstration
CVE-IF1235-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive RTCM messages from an RSU	CVE-IX1631-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-IF1238-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive SSM messages from an RSU	CVE-DR1292-V02 CVE-DR1293-V01 CVE-DR1295-V01 CVE-IX1631-V01	Demonstration
CVE-IF1241-V02	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall receive TIM messages from an RSU	CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01 CVE-IX1631-V01	Demonstration
CVE-IF1250-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall send SRMs to an RSU	CVE-IX1632-V01	Demonstration

Source: City of Columbus

3.4. DATA REQUIREMENTS

The data requirements (DR) for the core system of interest defines the data collected, transformed, and stored from various sources as well as identifies new data that is expected to be generated. The requirements in **Table 12** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 12: Data Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR3005-V01	DSRC Messages	Basic Safety Message	The BSM Part I shall include all data elements contained in the (coreData) BSMcoreData data frame (SAE J2735, Section 6.8)	CVE-CN1648-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1144-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (msgIssueRevision) MsgCount data element (SAE J2735, Section 7.104)	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1145-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (intersections) IntersectionGeometryList data frame (a sequence of IntersectionGeometry; SAE J2735, Section 6.35)	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-FN1538-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1146-V01	DSRC Messages	MapData Message	The MAP Message shall contain the IntersectionGeometry data frame under the (intersections) IntersectionGeometryList data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1147-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the IntersectionGeometry data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1148-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (id) IntersectionID data element (SAE J2735, Section 7.56) under the (id) IntersectionReferenceID data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1149-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (revision) MsgCount data element (SAE J2735, Section 7.104) under the IntersectionGeometry data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-FN1540-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1150-V01	DSRC Messages	MapData Message	The MAP message shall contain the (refPoint) Position3D data frame (SAE J2735, Section 6.87) under the IntersectionGeometry data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1151-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (lat) Latitude data element (SAE J2735, Section 7.91) under the (refPoint) Position3D data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1152-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (long) Longitude data element (SAE J2735, Section 7.95) under the (refPoint) Position3D data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1153-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (laneWidth) LaneWidth data element (SAE J2735, Section 7.90) under the IntersectionGeometry data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1154-V01	DSRC Messages	MapData Message	The MAP Message shall contain the LaneList data frame (a sequence of GenericLane; SAE J2735, Section 6.47) under the IntersectionGeometry data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1155-V01	DSRC Messages	MapData Message	The MAP Message shall contain the GenericLane data frame (SAE J2735, Section 6.29) under the LaneList data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1156-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (laneID) LaneID data element (SAE J2735, Section 7.88) under the GenericLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1157-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (maneuvers) AllowedManeuvers data element (SAE J2735, Section 7.4) under the GenericLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1158-V01	DSRC Messages	MapData Message	The MAP Message shall contain the NodeListXY data frame (SAE J2735, Section 6.72) under the GenericLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1159-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (nodes) NodeSetXY data frame (a sequence of NodeXY; SAE J2735, Section 6.77) under the NodeListXY data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1160-V01	DSRC Messages	MapData Message	The MAP Message shall contain the NodeXY data frame (SAE J2735, Section 6.78) under the (nodes) NodeSetXY data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1161-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (delta) NodeOffsetPointXY data element (SAE J2735, Section 6.75) under the NodeXY data frame (Any representation Node-XY-20b through Node-XY-32b; SAE J2735, Section 6.61, 6.62, 6.63, 6.64, 6.65, 6.66)	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1162-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (connectsTo) ConnectsToList data frame (a sequence of Connection; SAE J2735, Section 6.16) under the GenericLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1163-V01	DSRC Messages	MapData Message	The MAP Message shall contain the Connection data frame (SAE J2735, Section 6.14) under the (connectsTo) ConnectsToList data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1164-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (connectingLane) ConnectingLane data frame (SAE J2735, Section 6.13) under the Connection data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1165-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the (connectingLane) ConnectingLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1166-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (maneuver) AllowedManeuvers data element (SAE J2735, Section 7.4) under the (connectingLane) ConnectingLane data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1167-V01	DSRC Messages	MapData Message	The MAP Message shall contain the (signalGroup) SignalGroupID data element (SAE J2735, Section 7.171) under the Connection data frame	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1168-V01	DSRC Messages	MapData Message	The MAP Message should describe all egress lanes. This makes it possible to connect each ingress lane to the corresponding egress lane and describe the allowed maneuvers on all ingress lanes.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1169-V01	DSRC Messages	MapData Message	The MAP Message egress lanes (if included) may optionally contain a maneuvers field or a connectsTo field	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1170-V01	DSRC Messages	MapData Message	The MAP Message egress lanes (if included) may optionally contain the nodes in the NodeSet sequenced such that the first node is the stop bar	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1171-V01	DSRC Messages	MapData Message	The MAP Message Node points shall correspond to the center of the lane	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1172-V01	DSRC Messages	MapData Message	The MAP Message Node points should extend to a recommended minimum of 300 m from the stop bar	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1173-V01	DSRC Messages	MapData Message	The MAP Message shall include a minimum of two node points to define the lane	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1174-V01	DSRC Messages	MapData Message	The MAP Message shall define node points such that the perpendicular distance between two node points and the center of the lane shall be less than 0.5 m	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1175-V01	DSRC Messages	MapData Message	The MAP Message nodes in NodeSet shall be sequenced, in the case of an ingress lane, such that the first node is the stop bar	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1176-V01	DSRC Messages	MapData Message	The MAP Message shall describe all ingress lanes	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1177-V01	DSRC Messages	MapData Message	The MAP Message shall contain a maneuvers field and a connectsTo field for each ingress lane. The connectsTo field describes one or more Connections to egress lanes.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1178-V01	DSRC Messages	MapData Message	The MAP Message Connection field shall contain the lane, maneuver, and signalGroup associated with the Connection. The signalGroup identifies which signal group in the SPaT controls the flow of traffic from the ingress lane to the egress lane.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1179-V01	DSRC Messages	MapData Message	The MAP message containing a single physical lane which has multiple different signals assigned (e.g., for straight and for right-turn movement), shall be represented by a single ingress lane and multiple connections that specify the relevant movements and the associated signal groups	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1181-V01	DSRC Messages	MapData Message	The MAP message IntersectionGeometry revision shall be changed only if the map information was updated.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1182-V01	DSRC Messages	MapData Message	The MAP message shall contain a laneList. Each lane in the laneList shall be identified as an ingress lane or an egress lane through the laneAttributes->directionalUse field.	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-DR1272-V01 CVE-FN1552-V01 CVE-IF1361-V01 CVE-IF1363-V01	Demonstration
CVE-DR1374-V02	DSRC Messages	Radio Technical Commission for Maritime Services Corrections Message	The RTCM message (SAE J2735, Section 7.163) shall include message type 1 GPS L1 observations at 1 Hz	CVE-FN1516-V01 CVE-FN1517-V01 CVE-FN1518-V02 CVE-FN1519-V01 CVE-FN1560-V01	Demonstration
CVE-DR1375-V02	DSRC Messages	Radio Technical Commission for Maritime Services Corrections Message	The RTCM message (SAE J2735, Section 7.163) shall include message type 2 Antenna Reference Point (ARP) coordinates at 1 Hz	CVE-CN1648-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR3295-V01	DSRC Messages	Radio Technical Commission for Maritime Services Corrections Message	The RTCM message (SAE J2735, Section 7.163) shall include message type 3 at 1 Hz	CVE-FN1516-V01 CVE-FN1517-V01 CVE-FN1518-V02 CVE-FN1519-V01 CVE-FN1560-V01	Demonstration
CVE-DR3296-V01	DSRC Messages	Radio Technical Commission for Maritime Services Corrections Message	The RTCM message (SAE J2735, Section 7.163) shall include message type 9 at 1 Hz	CVE-FN1516-V01 CVE-FN1517-V01 CVE-FN1518-V02 CVE-FN1519-V01 CVE-FN1560-V01	Demonstration
CVE-DR1292-V02	DSRC Messages	Traveler Information Message	The Traffic CV Management System shall generate a TIM consistent with SAE J2735	CVE-IF1238-V01 CVE-SR1271-V01 CVE-IF1360-V02 CVE-FN1475-V01 CVE-FN1523-V01 CVE-FN1524-V02 CVE-FN1582-V02	Demonstration
CVE-DR1294-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the speed limit for the reduced speed (school) zone	CVE-CN1648-V01	Demonstration
CVE-DR1296-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the reduced speed zone geometry	CVE-CN1648-V01	Demonstration
CVE-DR3089-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the event identification number	CVE-CN1648-V01	Demonstration
CVE-DR3090-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the event type	CVE-CN1648-V01	Demonstration
CVE-DR3091-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the event start time	CVE-CN1648-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR3092-V02	DSRC Messages	Traveler Information Message	The TIM shall contain the event duration	CVE-CN1648-V01	Demonstration
CVE-DR3093-V02	DSRC Messages	Traveler Information Message	The TIM shall contain all data elements in the Geographic Information data frame	CVE-CN1648-V01	Demonstration
CVE-DR1378-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (timeStamp) MinuteOfTheYear data element (SAE J2735, Section 7.100)	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1379-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (intersections) IntersectionStateList data frame (a sequence of IntersectionState; SAE J2735, Section 6.38)	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1380-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the IntersectionState data frame (SAE J2735, Section 6.37) under the IntersectionStateList data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1381-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1382-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (revision) MsgCount data element (SAE J2735, Section 7.104) under the IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1383-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (status) IntersectionStatusObject data element (SAE J2735, Section 7.57) under the IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1384-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (timeStamp) Dsecond data element (SAE J2735, Section 7.39) under the IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1385-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (states) MovementList data frame (a sequence of MovementState; SAE J2735, Section 6.52) under the IntersectionState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1386-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the MovementState data frame (SAE J2735, Section 6.53) under the MovementList data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1387-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (signalGroup) SignalGroupID data element (SAE J2735, Section 7.171) under the MovementState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01 CVE-IF1281-V01	
CVE-DR1388-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (state-time-speed) MovementEventList data frame (a sequence of MovementEvent; SAE J2735, Section 6.50) under the MovementState data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-DR1420-V02 CVE-DR1421-V01 CVE-DR1422-V01 CVE-DR1423-V01 CVE-DR1424-V01 CVE-DR1425-V01 CVE-DR1426-V01 CVE-DR1427-V01 CVE-DR1428-V01 CVE-DR1429-V01 CVE-DR1430-V01 CVE-DR1431-V01 CVE-DR1432-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
				CVE-DR1433-V01 CVE-DR1434-V01 CVE-DR1435-V01 CVE-DR1436-V01 CVE-IF1281-V01	
CVE-DR1389-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the MovementEvent data frame (SAE J2735, Section 6.51) under the MovementEventList data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1390-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (eventState) MovementPhaseState data element (SAE J2735, Section 7.103) under the MovementEvent data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1391-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (timing) TimeChangeDetails data frame (SAE J2735, Section 6.134) under the MovementEvent data frame	CVE-FN1551-V01 CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1392-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain the (minEndTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-FN1551-V01 CVE-IF1281-V01	Demonstration
CVE-DR1393-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message should contain the (maxEndTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1394-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message should contain the (likelyTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1395-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message shall contain a 'states' field, which is a list of one or more MovementStates. The number of MovementStates shall correspond to the number of movements defined in the MAP messages which should be based on controller traffic phases that are currently active at the intersection.	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1396-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message signalGroup shall be assigned number and is not necessarily based on the controller phase number	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1397-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message should provide maxEndTime or likelyTime	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1398-V01	DSRC Messages	Signal Phase and Timing Message	The SPaT Message should provide maxEndTime if the traffic signal controller is running fixed-time, and if transmitted shall be equal to minEndTime	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-IF1281-V01	Demonstration
CVE-DR1402-V01	DSRC Messages	Signal Request Message	The OBU shall generate an SRM consistent with SAE J2735	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1404-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (second) DSecond data element (SignalRequestMessage.second) (SAE J2735, Section 7.39)	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1405-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (requests) SignalRequestList data frame (sequence of SignalRequestPackage; SAE J2735, Section 6.118)	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1406-V01	DSRC Messages	Signal Request Message	The SRM shall contain the SignalRequestPackage data frame (SAE J2735, Section 6.119) under the SignalRequestList data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1407-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (request) SignalRequest data frame (SAE J2735, Section 6.120) under the SignalRequestPackage data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1408-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the SignalRequest data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1409-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (id) IntersectionID data element (SAE J2735, Section 7.56) under the intersectionReferenceID data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1410-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (requestID) RequestID data element (SAE J2735, Section 7.153) under the SignalRequest data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1411-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (requestType) PriorityRequestType data element (SAE J2735, Section 7.142) under the SignalRequest data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1412-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (inBoundLane) IntersectionAccessPoint data frame (SAE J2735, Section 6.33) under the SignalRequest data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1413-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the IntersectionAccessPoint data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1414-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (approach) ApproachID data element (SAE J2735, Section 7.11) under the IntersectionAccessPoint data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1415-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (connection) LaneConnectionID data element (SAE J2735, Section 7.86) under the IntersectionAccessPoint data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1416-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (requestor) RequestorDescription data frame (SAE J2735, Section 6.98)	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1417-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (id) VehicleID data frame (SAE J2735, Section 6.147) under the RequestorDescription data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1418-V01	DSRC Messages	Signal Request Message	The SRM shall contain the (entityID) TemporaryID (SAE J2735, Section 7.187) under the VehicleID data frame	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-FN1467-V01 CVE-MT1603-V01	Demonstration
CVE-DR1420-V02	DSRC Messages	Signal Status Message	The RSU shall broadcast SAE J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1422-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (second) DSecond data element (SignalStatusMessage.second) (SAE J2735, Section 7.39)	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1423-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (status) SignalStatusList data frame (sequence of SignalStatus; SAE J2735, Section 6.121)	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1424-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (sequenceNumber) MsgCount data element (SAE J2735, Section 7.104) under the SignalStatus data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1425-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the SignalStatus data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1426-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (sigStatus) SignalStatusPackageList data frame (sequence of SignalStatusPackage; SAE J2735, Section 6.122) under the SignalStatus data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1427-V01	DSRC Messages	Signal Status Message	The SSM shall contain the SignalStatusPackage data frame (SAE J2735, Section 6.123) under the SignalStatusPacakageList data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1428-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (requestor) SignalRequestorInfo data frame (SAE J2735, Section 6.117) under the SignalStatusPackage data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1429-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (id) VehicleID data frame (SAE J2735, Section 6.147) under the SignalRequestorInfo data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1430-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (request) RequestID (SAE J2735, Section 7.153) under the SignalRequestorInfo data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1431-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (sequenceNumber) MsgCount (SAE J2735, Section 7.104) under the SignalRequestorInfo data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1432-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (inboundOn) IntersectionAccessPoint data frame (SAE J2735, Section 6.33) under the SignalStatusPackage data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1433-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the IntesectionAccessPoint data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1434-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (approach) ApproachID data element (SAE J2735, Section 7.11) under the IntesectionAccessPoint data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1435-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (connection) LaneConnectionID data element (SAE J2735, Section 7.86) under the IntesectionAccessPoint data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1436-V01	DSRC Messages	Signal Status Message	The SSM shall contain the (status) PrioritizationResponseStatus data element (SAE J2735, Section 7.140) under the SignalStatusPackage data frame	CVE-FN1520-V02 CVE-FN1522-V01 CVE-FN1282-V01 CVE-DR1388-V01 CVE-FN1470-V01 CVE-MT1604-V01	Demonstration
CVE-DR1276-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall remove PII from data prior to sending it to the Smart Columbus OS where it is made publicly available.	CVE-FN1581-V02 CVE-CN3088-V01	Demonstration
CVE-DR1477-V01	V2I Mobility	General Priority/Preemption	The TSP Application shall require data from the SSM Message	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02 CVE-UN520-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DR1478-V01	V2I mobility	General Priority/Preemption	The TSP Application shall generate data for the SRM Message	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02 CVE-UN520-v02	Demonstration
CVE-DR1533-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle	CVE-UN310-v02 CVE-UN510-v02 CVE-UN220-v02 CVE-UN520-v02	Demonstration
CVE-DR1562-V02	V2I Mobility	Vehicle Data for Traffic Operations	The VDTO Application shall capture data from all messages transmitted or received by roadside equipment	CVE-UN410-v02	Demonstration

Source: City of Columbus

3.5. SECURITY REQUIREMENTS

The security requirements (SR) for the core system of interest specifies what is necessary to protect the integrity and operability of the system, its microservices, connections, and data. This includes physical security as well as cyber prevention, detection, identification, response and recovery requirements. The requirements in **Table 13** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 13: Security Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR1373-V01	Roadside Equipment	Roadside Unit	RSUs shall support role-based authentication to enable physical access.	CVE-SN820-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR3123-V01	Roadside Equipment	Roadside Unit	An RSU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.	CVE-IX1609-V01 CVE-IX1616-V01 CVE-IX1619-V01 CVE-IX1632-V01 CVE-CN1648-V01	Demonstration
CVE-SR3124-V01	Roadside Equipment	Roadside Unit	An RSU shall verify a DSRC message if a device identifies the message as containing a new DE_TemporaryID value.	CVE-SN820-v02	Demonstration
CVE-SR3125-V01	Roadside Equipment	Roadside Unit	An RSU shall support setting the certificate geographic region to be requested for application certificates.	CVE-CN1663-V01 CVE-SN820-v02	Demonstration
CVE-SR3126-V01	Roadside Equipment	Roadside Unit	An RSU shall support establishment of a standard TLS-based VPN with client authentication for communication to the Traffic CV Management System, with a long-term client cert and a single CA cert trusted to authorize connections from the Traffic CV Management System.	CVE-IX1635-V01	Demonstration
CVE-SR3127-V01	Roadside Equipment	Roadside Unit	An RSU 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.	CVE-SN820-v02 CVE-CN1648-V01	Demonstration
CVE-SR3128-V01	Roadside Equipment	Roadside Unit	An RSU shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).	CVE-UN430-v02	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR3129-V01	Roadside Equipment	Roadside Unit	An RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications.	CVE-UN710-v02 CVE-IX1626-V01 CVE-IX1628-V01 CVE-IX1633-V01 CVE-IX1637-V01	Demonstration
CVE-SR3130-V01	Roadside Equipment	Roadside Unit	An RSU shall comply with IEEE 1609.2: Standard for WAVE Security Services for Applications and Management Messages.	CVE-CN1648-V01	Demonstration
CVE-SR3131-V01	Roadside Equipment	Roadside Unit	An RSU shall delete old certificates if it has been moved to another intersection.	CVE-CN1663-V01 CVE-SN820-v02	Demonstration
CVE-SR1459-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall detect abnormal unauthorized activity on an IP connection.	CVE-UN430-v02	Demonstration
CVE-SR1460-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the DSRC communications performance.	CVE-UN430-v02	Demonstration
CVE-SR1461-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the data traffic usage to detect unapproved use of the IP connection.	CVE-UN430-v02	Demonstration
CVE-SR1254-V01	Vehicle Onboard Equipment	General OBU	The OBU shall cease transmission of BSMs if the OBU determines that it has been blacklisted. Note: Blacklists detail devices that should not be trusted in the system or network	CVE-SN870-v02	Demonstration
CVE-SR1255-V01	Vehicle Onboard Equipment	General OBU	The OBU shall prevent incoming messages with invalid conditions per criteria in the IEEE 1609.2 from being acted on.	CVE-SN870-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR1256-V01	Vehicle Onboard Equipment	General OBU	The OBU Vehicle Communications link shall have communications security to ensure the authenticity of all its messages in accordance to the standards prescribed by wireless messaging security standards.	CVE-SN870-v02 CVE-CN1648-V01	Demonstration
CVE-SR1257-V01	Vehicle Onboard Equipment	General OBU	The OBU shall carry out plausibility checking on the remote vehicle BSM data.	CVE-SN870-v02	Demonstration
CVE-SR1258-V01	Vehicle Onboard Equipment	General OBU	The OBU shall indicate successful receipt of the pseudonym certificates.	CVE-SN870-v02	Demonstration
CVE-SR1259-V01	Vehicle Onboard Equipment	General OBU	When the OBU has no valid BSM signing certificates, it shall store the log file entries as IEEE 1609.2 data of type unsecured.	CVE-SN870-v02	Demonstration
CVE-SR1261-V01	Vehicle Onboard Equipment	General OBU	The OBU shall obtain certificates via IPv6 connectivity through the RSU.	CVE-SN870-v02	Demonstration
CVE-SR1262-V01	Vehicle Onboard Equipment	General OBU	An OBU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.	CVE-SN870-v02	Demonstration
CVE-SR1263-V01	Vehicle Onboard Equipment	General OBU	An OBU shall support establishment of a standard TLS-based VPN with client authentication for communication to the Traffic CV Management System, with a long-term client cert and a single CA cert trusted to authorize connections from the Traffic CV Management System.	CVE-SN870-v02	Demonstration
CVE-SR1264-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.	CVE-SN870-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR1265-V01	Vehicle Onboard Equipment	General OBU	An OBU shall provide real-time tamper data which indicates that the device has been tampered with (e.g. opening of the case).	CVE-SN870-v02	Demonstration
CVE-SR1266-V01	Vehicle Onboard Equipment	General OBU	An OBU 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.	CVE-SN870-v02	Demonstration
CVE-SR1267-V01	Vehicle Onboard Equipment	General OBU	An OBU shall only transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it currently has valid certificates for that usage scenario	CVE-SN870-v02	Demonstration
CVE-SR1268-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when a device identifies the message as containing a new DE_TemporaryID value.	CVE-SN870-v02	Demonstration
CVE-SR1269-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when the message results in the issuance of an advisory, warning, or alert	CVE-SN870-v02	Demonstration
CVE-SR1270-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when 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	CVE-SN870-v02	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-SR1271-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when other potential threat situations such as red-light violations, and other safety applications are active	CVE-SN870-v02 CVE-DR1292-V02 CVE-DR1293-V01 CVE-DR1295-V01	Demonstration

Source: City of Columbus

3.6. NON-FUNCTIONAL REQUIREMENTS

The non-functional requirements (NF) for the core system of interest specifies the characteristics of the overall operation of the system such as availability, maintainability, reliability, safety, environmental, human factors, and ergonomics.

3.6.1. Physical Requirements

The physical requirements specify the construction, durability, adaptability and environmental characteristics of the system, such as installation location, device weight limits, dimension and volume limitations, temperature regulations, layout, access for maintenance, growth and expansion characteristics, etc. The requirements in **Table 14** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 14: Physical Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PY1370-V01	Roadside Equipment	Roadside Unit	RSU DSRC antennas shall be located to maximize the DSRC range along the corridors of interest.	CVE-CN1659-V01	Inspection
CVE-PY1371-V01	Roadside Equipment	Roadside Unit	RSU GPS antennas shall be located to maximize the GPS reception	CVE-CN1659-V01	Inspection
CVE-PY1372-V01	Roadside Equipment	Roadside Unit	Ethernet cable spans shall not exceed 100 meters (328 feet)	CVE-CN1648-V01	Inspection

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-PY2912-V01	Roadside Equipment	Roadside Unit	A traffic signal controller cabinet that contains Roadside Equipment shall be outfitted with tamper alert devices to prevent unauthorized physical access to networking components.	CVE-CN1663-V01	Demonstration
CVE-PY3120-V01	Roadside Equipment	Roadside Unit	RSUs shall be located on a network that is physically isolated from the existing CTSS network.	CVE-SN820-v02	Inspection
CVE-PY3034-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall store archived CV data and backup archived CV data on separate physical storage devices.	CVE-UN410-v02 CVE-UN440-v02 CVE-CN1663-V01	Inspection
CVE-PY3038-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall store archived Transit Vehicle Interaction Events and backup archived Transit Vehicle Interaction Events on separate physical storage devices.	CVE-UN530-v02 CVE-UN540-v02	Inspection
CVE-PY3016-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall be mounted or installed in a location where it does not obstruct the line of sight of the LDV Operator nor distract the LDV Operator from the primary task of driving.	CVE-IX1618-V01	Inspection
CVE-PY3018-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU shall be positioned in a location such that it can provide a visual output to the driver (via the HMI) that can be read from the driver's normal seated position, if visual alerts are used.	CVE-IX1618-V01	Inspection

Source: City of Columbus

3.6.2. Availability and Recoverability Requirements

The availability requirements define the times of day, days of year, and overall percentage the system can be used and when it will not be available for use. It also specifies the recovery time objective (RTO) of the system, which describes the time frame permitted for a system to become operational, the recovery point objective (RPO), which specifies up to what point in time shall the data be restored, as well as how the system is expected to restore services (e.g. failover, backups, etc.) in an event of a failure. The ability to recover quickly from a system failure or disaster depends on a blend of technologies and having a predefined plan for recovering the data on new hardware, when appropriate. The requirements in **Table 15** are organized by the functional groups and are related to the user needs identified in the project ConOps.

Table 15: Availability and Recovery Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-AR3121-V01	Roadside Equipment	Roadside Unit	An RSU shall be available 99% of the time when power is available to the network.	CVE-UN430-v02	Analyze
CVE-AR3122-V01	Roadside Equipment	Roadside Unit	RSU shall return to an operational state within 5 min of regaining power	CVE-UN430-v02	Demonstration

Source: City of Columbus

3.6.3. Maintainability Requirements

The maintainability requirements for the system specify the level of effort required to locate and correct an error during operation, establishing a quantitative requirement for planned and unplanned support (e.g. mean and maximum times to repair or resolve issues, number of people and skill levels required, support equipment necessary, maintenance staff hours, time and frequency of preventative maintenance, etc.). The requirements in **Table 16** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 16: Maintainability Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-MT1593-V01	Common	Common	DPS shall retain Support Staff to troubleshoot and diagnose RSU and OBU issues.	CVE-CN1645-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-MT1594-V01	Common	Common	A set of support, diagnostic and troubleshooting procedures shall be developed to guide the support staff.	CVE-CN1645-V01	Demonstration
CVE-MT1595-V01	Common	Common	DPS shall maintain a list of OBU equipment and contact information for vehicle owners that have OBUs installed	CVE-CN1645-V01	Demonstration
CVE-MT1596-V01	Common	Common	Support Staff Device installers shall be approved by DPS to install roadside equipment (including RSUs) in signal cabinets and along the roadside.	CVE-CN1645-V01	Demonstration
CVE-MT1597-V01	Common	Common	Support Staff Device installers shall be approved by DPS to install OBUs in participant vehicles.	CVE-CN1645-V01	Demonstration
CVE-MT1598-V01	Common	Common	Support Staff shall be trained by the RSU vendor to install RSU Devices	CVE-CN1645-V01	Demonstration
CVE-MT1599-V01	Common	Common	Support Staff shall be trained by the OBU vendor to install OBU Devices	CVE-CN1645-V01	Demonstration
CVE-MT1600-V01	Common	Common	Support Staff Device installers shall be approved by DPS to install OBU devices in private light-duty vehicles, city fleet vehicles, transit vehicles, Emergency Vehicles, and freight vehicles.	CVE-CN1645-V01	Demonstration
CVE-MT1602-V01	Common	Common	Department of Public Service shall maintain the RSUs installed along the roadside.	CVE-CN1645-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-MT1603-V01	Common	Common	Department of Public Service shall provide contact information for participants inquire about OBUs.	CVE-CN1645-V01 CVE-DR1402-V01 CVE-DR1403-V01 CVE-DR1404-V01 CVE-DR1405-V01 CVE-DR1406-V01 CVE-DR1407-V01 CVE-DR1408-V01 CVE-DR1409-V01 CVE-DR1410-V01 CVE-DR1411-V01 CVE-DR1412-V01 CVE-DR1413-V01 CVE-DR1414-V01 CVE-DR1415-V01 CVE-DR1416-V01 CVE-DR1417-V01 CVE-DR1418-V01 CVE-DR1419-V01	Demonstration

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-MT1604-V01	Common	Common	A participant shall be able to return the OBU to DPS for any reason (OBU malfunction, remove/uninstall OBU, etc.)	CVE-CN1645-V01 CVE-DR1420-V02 CVE-DR1421-V01 CVE-DR1422-V01 CVE-DR1423-V01 CVE-DR1424-V01 CVE-DR1425-V01 CVE-DR1426-V01 CVE-DR1427-V01 CVE-DR1428-V01 CVE-DR1429-V01 CVE-DR1430-V01 CVE-DR1431-V01 CVE-DR1432-V01 CVE-DR1433-V01 CVE-DR1434-V01 CVE-DR1435-V01 CVE-DR1436-V01	Demonstration
CVE-MT1364-V01	Roadside Equipment	Roadside Unit	RSUs shall support physical access to support maintenance activities.	CVE-CN1645-V01 CVE-CN1659-V01	Demonstration
CVE-MT1252-V01	Vehicle Onboard Equipment	General OBU	An OBU shall support physical access to support maintenance activities.	CVE-CN1663-V01	Demonstration
CVE-MT1253-V01	Vehicle Onboard Equipment	General OBU	An OBU shall support role-based authentication to enable physical access.	CVE-CN1663-V01	Demonstration

Source: City of Columbus

3.6.4. Storage and Transport Requirements

The storage and transport requirements (ST) specify the physical location and environment for the system including designated storage facility, installation site, repair facility and requirements for transporting equipment.

The OBU Procurement Document specified OBU storage and transport requirements.

3.6.5. Disposal Requirements

The disposal requirements (DR) specify the items related to the disposal of project/system components, due to either failure replacements, removal, end-of-life upgrade, or retirement. The requirements in **Table 17** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 17: Disposal Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-DP1465-V01	Common	Common	The CVE should remain operational after the completion of the deployment period	CVE-UN410-v02	Demonstration

Source: City of Columbus

3.7. ENABLING REQUIREMENTS

The enabling requirements specify details concerning the management of information as well as the production of the system and its lifecycle sustainment, including development, integration, verification, validation, and training.

3.7.1. Information Management Requirements

The information management (IM) requirements specify the acquisition, management, and ownership of information from one or more sources, the custodianship and the distribution of that information to those who need it, and its ultimate disposition through archiving or deletion.

<In the context of the CVE, the Operating System is the IM system. However, the CVE is not dependent on the Operating System for operational needs. The CVE does write data to the OS for archival and performance measures purpose as reflected in appropriate requirements.>

3.7.2. Life Cycle Sustainment Requirements

The life cycle sustainment (LC) requirements define what items the project or system will review, measure, and analyze as part of its commitment to quality during the life cycle of the system. The capacity to change or enhance the product and life cycle processes can be designed into the system architecture to enable the cost-effective sustainment of the system throughout its life cycle. This design attribute should be established early in the system's development to provide a basis for planning each incremental development effort.

<Life Cycle Sustainment Requirements have not been established for the CVE.>

3.8. POLICY AND REGULATION REQUIREMENTS

The policy and regulation requirements (RG) for the system of interest specifies relevant and applicable organizational policies and regulations that affect the development, operation or performance of the system (e.g. IT and labor policies, reports to regulatory agencies, health or safety criteria, etc.). This section also includes new policy and regulation imposed to realize the system. The requirements in **Table 18** are organized by the functional groups and are related to the user needs documented in the project ConOps.

Table 18: Policy and Regulation Requirements

ReqID	Functional Group	Sub-Component	Description	References	Verification Method
CVE-RG1605-V01	Common	Common	An RSU shall be licensed (subpart M of Part 90 of FCC Rules) by the FCC	CVE-CN1645-V01	Inspection
CVE-RG1606-V01	Common	Common	An RSU shall be registered (RSU sites, channels, and other relevant data) by site and segment with the FCC before operation	CVE-CN1645-V01	Demonstration
CVE-RG1607-V01	Common	Common	An OBU shall meet the license requirements as specified in subpart I of part 95 of FCC rules.	CVE-CN1645-V01	Inspection

Source: City of Columbus

Chapter 4. Engineering Principles

This section describes engineering principles that guide composition of the CVE project.

4.1. METHODS OF VERIFICATION

The software and hardware components that make up the CVE will be individually verified, then integrated to produce top-level assemblies and microservices. These assemblies will also be individually verified before being integrated with others to produce larger, evolving assemblies until the complete system has been integrated and verified. Throughout this process, the Smart Columbus program will utilize the Helix Requirements Management tool to capture, track and trace requirements starting with the user needs defined in the ConOps, through development, testing and deployment. This approach and software tool will be instrumental through the design and development phases of the project.

The requirements also maintain a verification method, which details the plan for verifying the requirement based on its stated definition. One of the verification methods listed in **Table 19** is assigned for each requirement. Using the requirements defined in the previous section.

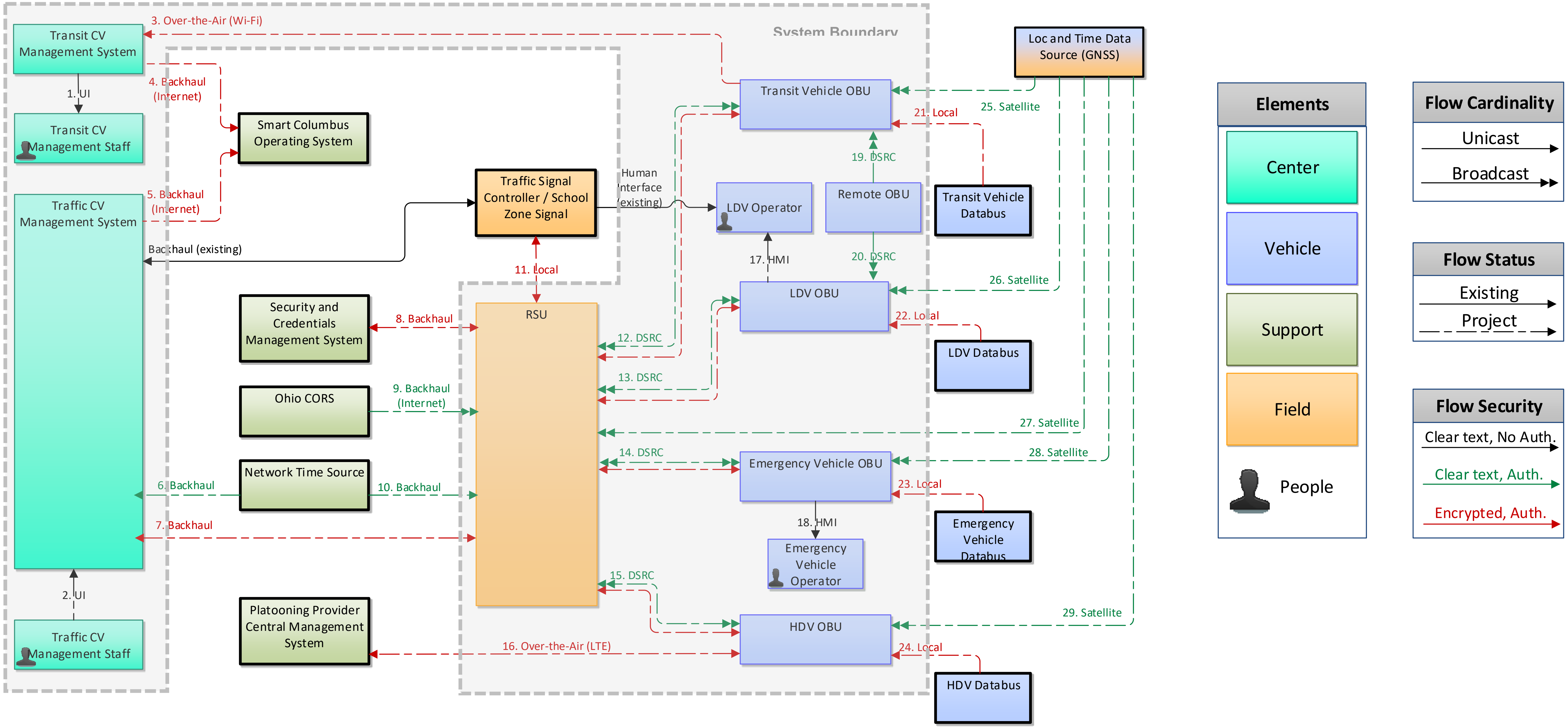
Table 19: Methods of Verification

Type	Description
Inspection	Verification through a visual, auditory, olfactory, or tactile comparison
Demonstration	Verification that exercises the system software or hardware as it is designed to be used, without external influence, to verify the results are specified by the requirement
Test	Verification using controlled and predefined inputs and other external elements (e.g. data, triggers, etc.) that influence or induce the system to produce the output specified by the requirement
Analyze	Verification through indirect and logical conclusion using mathematical analysis, models, calculations, testing equipment and derived outputs based on validated data sets

Source: City of Columbus

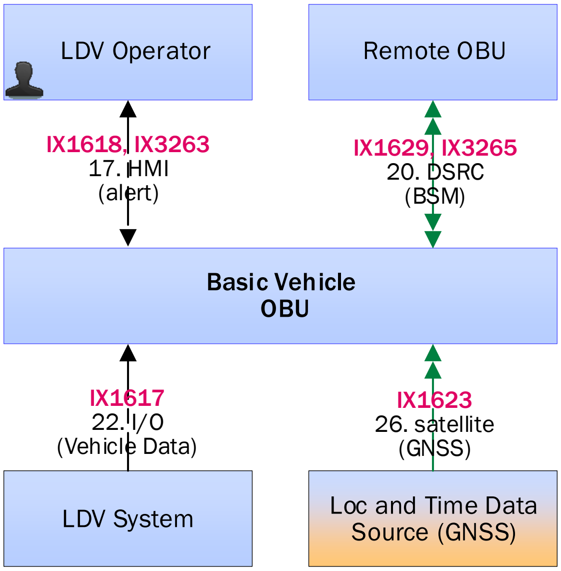
4.2. REFERENCE ARCHITECTURE

Originating with the National ITS Architecture, the connected vehicle industry has developed and supported the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), which has been used to define the message flows and elements of the CVE. **Figure 3** illustrates the reference architecture for the CVE. **Figure 4**, **Figure 5**, **Figure 6**, **Figure 7**, **Figure 8** and **Figure 9** show the decomposed (Level 2) representation of the CVE Applications.



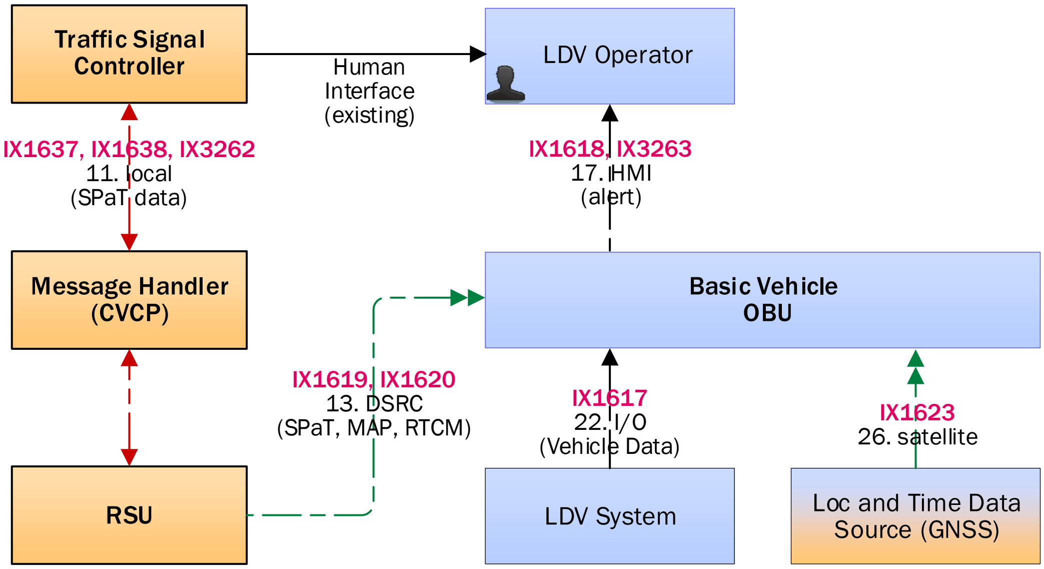
Source: City of Columbus

Figure 3: ARC-IT Representation of the Connected Vehicle Environment (Includes Support Systems)



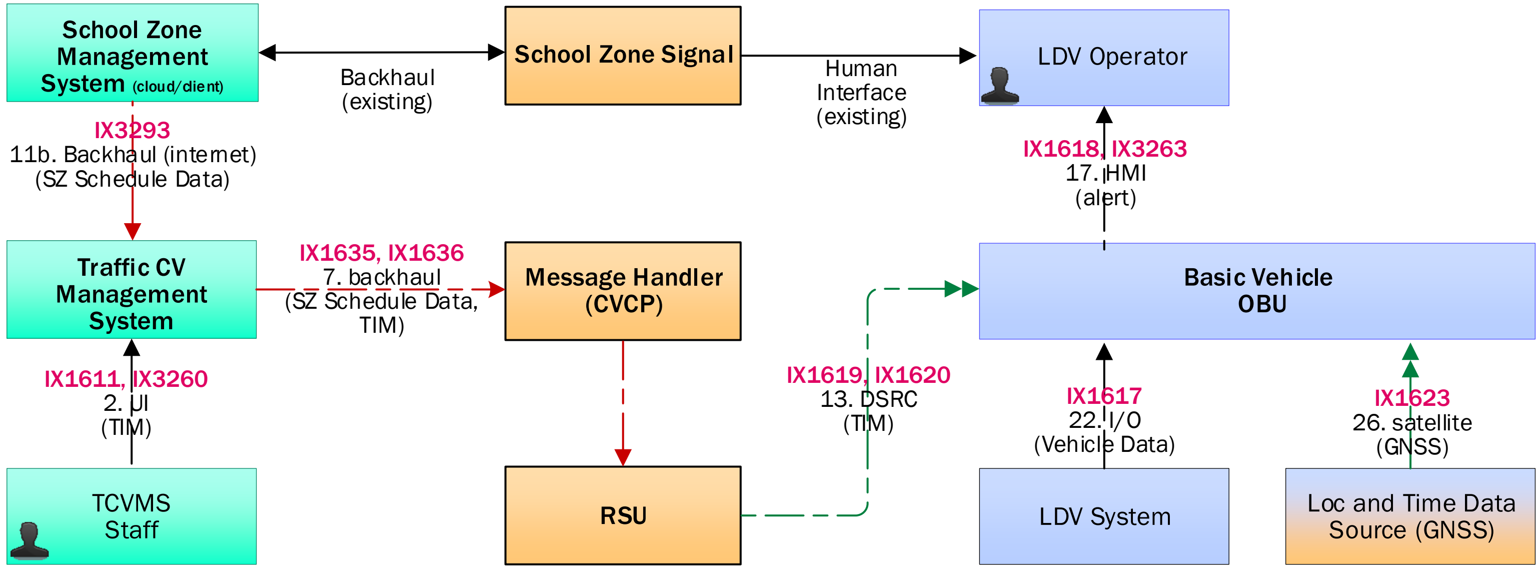
Source: City of Columbus

Figure 4: ARC-IT Representation of V2V Safety Applications (EEBL, FCW, BSW/LCW, IMA)



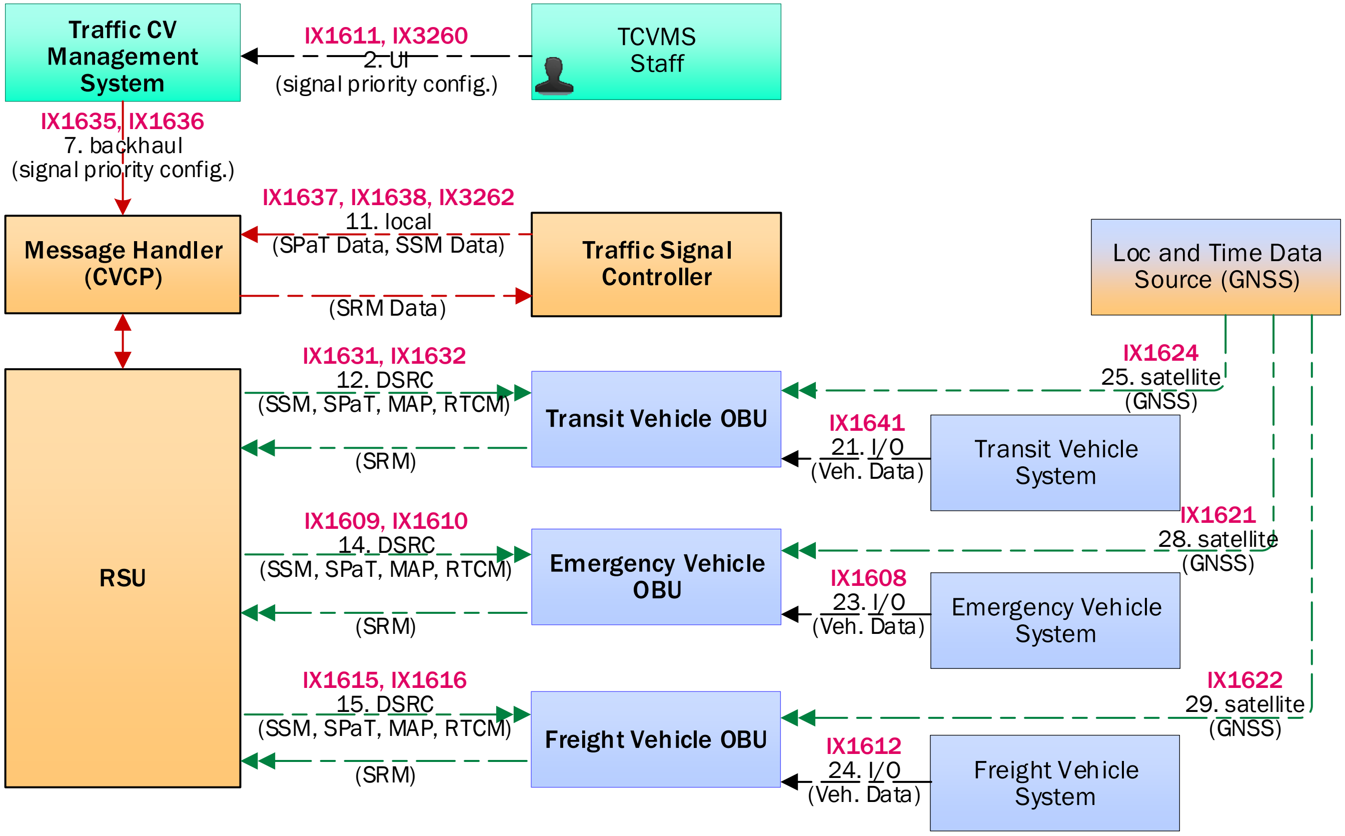
Source: City of Columbus

Figure 5: ARC-IT Representation of RLVW



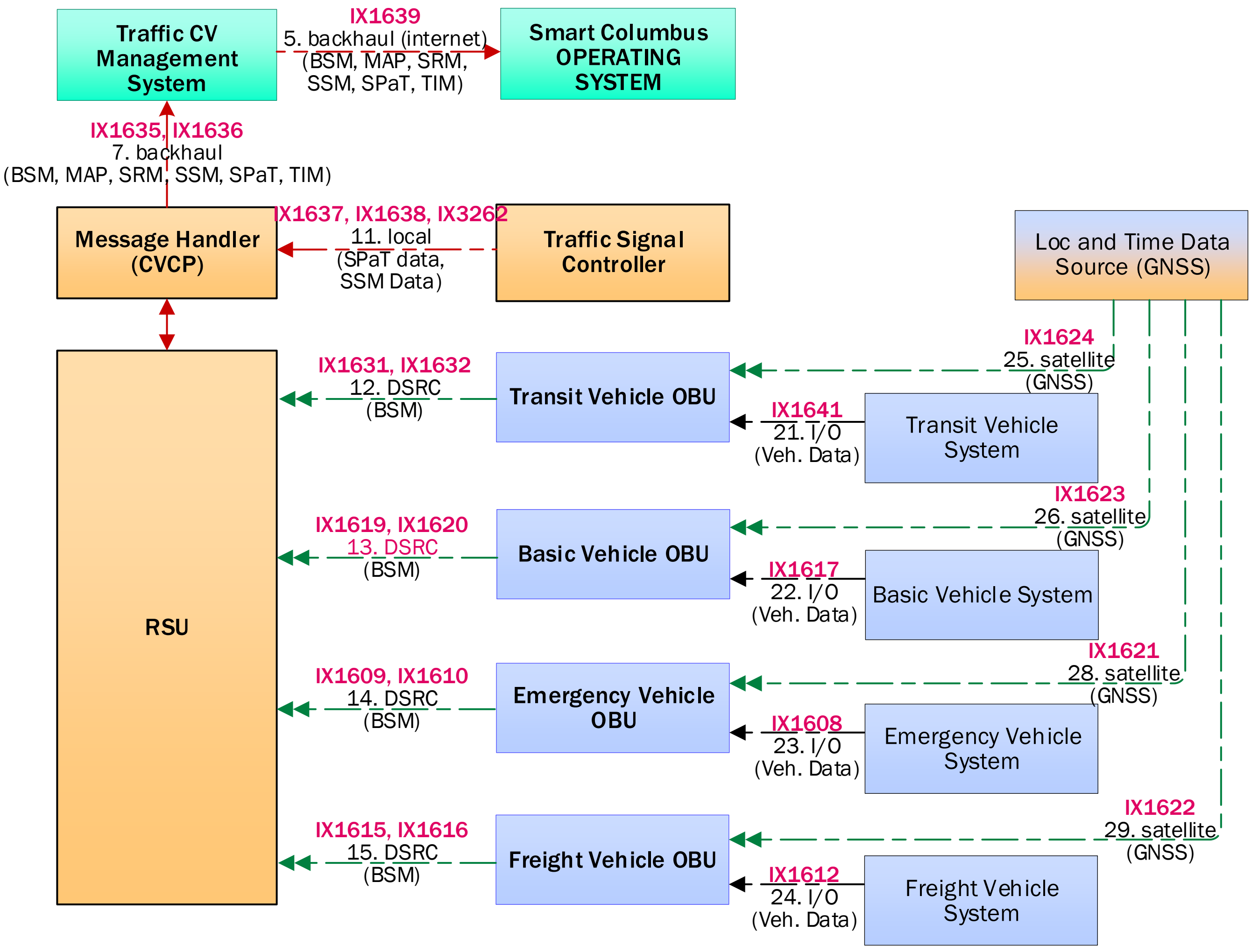
Source: City of Columbus

Figure 6: ARC-IT Representation of RSSZ



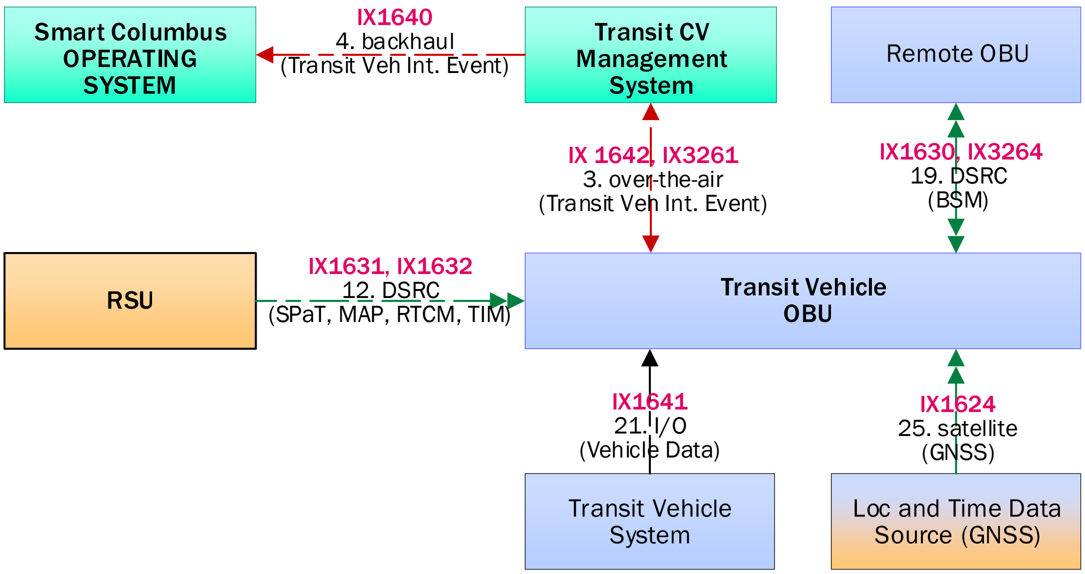
Source: City of Columbus

Figure 7: ARC-IT Representation of Signal Priority/Preemption Applications (TSP, FSP, EVP)



Source: City of Columbus

Figure 8: ARC-IT Representation of VDTO



Source: City of Columbus

Figure 9: ARC-IT Representation of TVIER

Appendix A. Document Terminology and Conventions

A.1 REFERENCE CONVENTIONS

The following conventions are used through this document:

- Titles of externally referenced documents or sources are underlined.
- Titles of internally referenced exhibits, sections, etc. are *italicized*.

A.1.1 Requirement Numbering Convention

Each requirement contains a unique ID for traceability and configuration management. Requirements for all projects in the Smart Columbus program will follow the same convention. This identifier contains three elements partitioned into five octets, each representing an identifiable attribute of the requirement. **Table 20** lists the naming convention of the requirements.

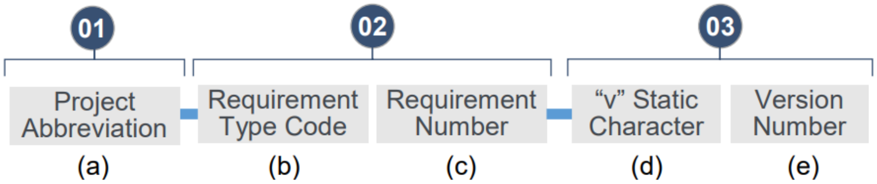


Table 20: Requirements Numbering Convention

	Description	Data Type, Casing	# of Characters and/or Digits
Project Abbreviation	The designated Smart Columbus project acronym (e.g. CVE, EPM, etc.)	String, upper case	Variable
Requirement Type Code	**Table 8: List of Requirement Types** • FN: Functional • PR: Performance • IF: Interface • DR: Data • SR: Security • RG: Policy and Regulation • PY: Physical • AR: Availability and Recovery • MT: Maintainability • ST: Storage and Transport • DP: Disposal • IM: Information Management • LC: Life Cycle Sustainability	String, upper case	2
Requirement Number	An integer incrementing by one, indicating the number of requirements established	Integer	3
"v" Static Character	Static letter "v" represents the requirement version	Character	1
Version Number	An integer incrementing by one, indicating the number of revisions made to the requirement	Integer	2

Source: City of Columbus

An example of a Functional Requirement for the Transit Pedestrian Indicator application under the Connected Vehicle Environment, would be "CVE-FN001-v01" in which the following applies:

- "CVE" is the Project Abbreviation
- "FN001" is the requirement type code coupled with the three-digit Requirement Number
- "v01" is the static "v" coupled with the two-digit version number

A.1.2 Requirements Table Headings

The columns in the requirements tables throughout this document have the following definitions:

- **ReqID:** a unique identifier providing a reference to a specific requirement.
- **Functional Group** and **Sub-Component:** These are intended to organize the requirements in a manner that allows similar requirements to be grouped together. The requirements in the tables in this section are grouped by functional group and sub-component.
- **Description:** Statement of the business function or conditions the system must meet.
- **Reference:** Additional requirement(s), User Needs, Constraints or Interfaces that serve as the source (reason) a requirement exists.
- **Verification Method:** As detailed in **Chapter 4**, the method expected to verify that a requirement has been met is assigned to each requirement.

A.1.3 Conformance

Requirements listed in this document use the following terminology:

- SHALL indicates the definition is an absolute requirement of the specification.
- SHALL NOT indicates the definition is an absolute prohibition of the specification.
- SHOULD (RECOMMENDED) indicates there may exist valid reasons or circumstances to omit a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT (NOT RECOMMENDED) indicates there may exist valid reasons or circumstances when a particular function of condition is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any function or condition described with this label.
- MAY (OPTIONAL) indicates an item is truly optional. Some vendors may choose to include or implement Optional Requirements to add value or enhance their overall product while other vendors may omit the same Optional Requirement to reduce cost, increase time to market, etc. An implementation which does not include an Optional Requirement SHALL be interoperable with implementations which does include the Optional Requirement, though perhaps with reduced functionality. In the same vein an implementation which does include an Optional Requirement SHALL be interoperable with an implementation which does not include the Optional Requirement (with the exception for the feature the option provides).

Appendix B. Requirements by System Functional Groups

Table 21 organizes requirements defined in **Chapter 3. System Requirements** into its functional groups. This organization is intended for ease of use and quick reference during system design.

Table 21: Requirements Organized by Functional Groups

Functional Group	ReqID	Description
Common	CVE-DP1465-V01	The CVE should remain operational after the completion of the deployment period
Common	CVE-IF1344-V01	An RSU shall receive security certificates from an SCMS
Common	CVE-MT1593-V01	DPS shall retain Support Staff to troubleshoot and diagnose RSU and OBU issues.
Common	CVE-MT1594-V01	A set of support, diagnostic and troubleshooting procedures shall be developed to guide the support staff.
Common	CVE-MT1595-V01	DPS shall maintain a list of OBU equipment and contact information for vehicle owners that have OBUs installed
Common	CVE-MT1596-V01	Support Staff Device installers shall be approved by DPS to install roadside equipment (including RSUs) in signal cabinets and along the roadside.
Common	CVE-MT1597-V01	Support Staff Device installers shall be approved by DPS to install OBUs in participant vehicles.
Common	CVE-MT1598-V01	Support Staff shall be trained by the RSU vendor to install RSU Devices
Common	CVE-MT1599-V01	Support Staff shall be trained by the OBU vendor to install OBU Devices
Common	CVE-MT1600-V01	Support Staff Device installers shall be approved by DPS to install OBU devices in private light-duty vehicles, city fleet vehicles, transit vehicles, Emergency Vehicles, freight vehicles, and CEAVs.
Common	CVE-MT1602-V01	Department of Public Service shall maintain the RSUs installed along the roadside.
Common	CVE-MT1603-V01	Department of Public Service shall provide contact information for participants inquire about OBUs.
Common	CVE-MT1604-V01	A participant shall be able to return the OBU to DPS for any reason (OBU malfunction, remove/uninstall OBU, etc.)
Common	CVE-RG1605-V01	An RSU shall be licensed (subpart M of Part 90 of FCC Rules) by the FCC
Common	CVE-RG1606-V01	An RSU shall be registered (RSU sites, channels, and other relevant data) by site and segment with the FCC before operation

Functional Group	ReqID	Description
Common	CVE-RG1607-V01	An OBU shall meet the license requirements as specified in subpart I of part 95 of FCC rules.
DSRC Messages	CVE-DR1144-V01	The MAP Message shall contain the (msgIssueRevision) MsgCount data element (SAE J2735, Section 7.104)
DSRC Messages	CVE-DR1145-V01	The MAP Message shall contain the (intersections) IntersectionGeometryList data frame (a sequence of IntersectionGeometry; SAE J2735, Section 6.35)
DSRC Messages	CVE-DR1146-V01	The MAP Message shall contain the IntersectionGeometry data frame under the (intersections) IntersectionGeometryList data frame
DSRC Messages	CVE-DR1147-V01	The MAP Message shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the IntersectionGeometry data frame
DSRC Messages	CVE-DR1148-V01	The MAP Message shall contain the (id) IntersectionID data element (SAE J2735, Section 7.56) under the (id) IntersectionReferenceID data frame
DSRC Messages	CVE-DR1149-V01	The MAP Message shall contain the (revision) MsgCount data element (SAE J2735, Section 7.104) under the IntersectionGeometry data frame
DSRC Messages	CVE-DR1150-V01	The MAP message shall contain the (refPoint) Position3D data frame (SAE J2735, Section 6.87) under the IntersectionGeometry data frame
DSRC Messages	CVE-DR1151-V01	The MAP Message shall contain the (lat) Latitude data element (SAE J2735, Section 7.91) under the (refPoint) Position3D data frame
DSRC Messages	CVE-DR1152-V01	The MAP Message shall contain the (long) Longitude data element (SAE J2735, Section 7.95) under the (refPoint) Position3D data frame
DSRC Messages	CVE-DR1153-V01	The MAP Message shall contain the (laneWidth) LaneWidth data element (SAE J2735, Section 7.90) under the IntersectionGeometry data frame
DSRC Messages	CVE-DR1154-V01	The MAP Message shall contain the LaneList data frame (a sequence of GenericLane; SAE J2735, Section 6.47) under the IntersectionGeometry data frame
DSRC Messages	CVE-DR1155-V01	The MAP Message shall contain the GenericLane data frame (SAE J2735, Section 6.29) under the LaneList data frame
DSRC Messages	CVE-DR1156-V01	The MAP Message shall contain the (laneID) LaneID data element (SAE J2735, Section 7.88) under the GenericLane data frame
DSRC Messages	CVE-DR1157-V01	The MAP Message shall contain the (maneuvers) AllowedManeuvers data element (SAE J2735, Section 7.4) under the GenericLane data frame

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1158-V01	The MAP Message shall contain the NodeListXY data frame (SAE J2735, Section 6.72) under the GenericLane data frame
DSRC Messages	CVE-DR1159-V01	The MAP Message shall contain the (nodes) NodeSetXY data frame (a sequence of NodeXY; SAE J2735, Section 6.77) under the NodeListXY data frame
DSRC Messages	CVE-DR1160-V01	The MAP Message shall contain the NodeXY data frame (SAE J2735, Section 6.78) under the (nodes) NodeSetXY data frame
DSRC Messages	CVE-DR1161-V01	The MAP Message shall contain the (delta) NodeOffsetPointXY data element (SAE J2735, Section 6.75) under the NodeXY data frame (Any representation Node-XY-20b through Node-XY-32b; SAE J2735, Section 6.61, 6.62, 6.63, 6.64, 6.65, 6.66)
DSRC Messages	CVE-DR1162-V01	The MAP Message shall contain the (connectsTo) ConnectsToList data frame (a sequence of Connection; SAE J2735, Section 6.16) under the GenericLane data frame
DSRC Messages	CVE-DR1163-V01	The MAP Message shall contain the Connection data frame (SAE J2735, Section 6.14) under the (connectsTo) ConnectsToList data frame
DSRC Messages	CVE-DR1164-V01	The MAP Message shall contain the (connectingLane) ConnectingLane data frame (SAE J2735, Section 6.13) under the Connection data frame
DSRC Messages	CVE-DR1165-V01	The MAP Message shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the (connectingLane) ConnectingLane data frame
DSRC Messages	CVE-DR1166-V01	The MAP Message shall contain the (maneuver) AllowedManeuvers data element (SAE J2735, Section 7.4) under the (connectingLane) ConnectingLane data frame
DSRC Messages	CVE-DR1167-V01	The MAP Message shall contain the (signalGroup) SignalGroupID data element (SAE J2735, Section 7.171) under the Connection data frame
DSRC Messages	CVE-DR1168-V01	The MAP Message should describe all egress lanes. This makes it possible to connect each ingress lane to the corresponding egress lane and describe the allowed maneuvers on all ingress lanes.
DSRC Messages	CVE-DR1169-V01	The MAP Message egress lanes (if included) may optionally contain a maneuvers field or a connectsTo field
DSRC Messages	CVE-DR1170-V01	The MAP Message egress lanes (if included) may optionally contain the nodes in the NodeSet sequenced such that the first node is the stop bar
DSRC Messages	CVE-DR1171-V01	The MAP Message Node points shall correspond to the center of the lane
DSRC Messages	CVE-DR1172-V01	The MAP Message Node points should extend to a recommended minimum of 300 m from the stop bar

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1173-V01	The MAP Message shall include a minimum of two node points to define the lane
DSRC Messages	CVE-DR1174-V01	The MAP Message shall define node points such that the perpendicular distance between two node points and the center of the lane shall be less than 0.5 m
DSRC Messages	CVE-DR1175-V01	The MAP Message nodes in NodeSet shall be sequenced, in the case of an ingress lane, such that the first node is the stop bar
DSRC Messages	CVE-DR1176-V01	The MAP Message shall describe all ingress lanes
DSRC Messages	CVE-DR1177-V01	The MAP Message shall contain a maneuvers field and a connectsTo field for each ingress lane. The connectsTo field describes one or more Connections to egress lanes.
DSRC Messages	CVE-DR1178-V01	The MAP Message Connection field shall contain the lane, maneuver, and signalGroup associated with the Connection. The signalGroup identifies which signal group in the SPaT controls the flow of traffic from the ingress lane to the egress lane.
DSRC Messages	CVE-DR1179-V01	The MAP message containing a single physical lane which has multiple different signals assigned (e.g., for straight and for right-turn movement), shall be represented by a single ingress lane and multiple connections that specify the relevant movements and the associated signal groups
DSRC Messages	CVE-DR1181-V01	The MAP message IntersectionGeometry revision shall be changed only if the map information was updated.
DSRC Messages	CVE-DR1182-V01	The MAP message shall contain a laneList. Each lane in the laneList shall be identified as an ingress lane or an egress lane through the laneAttributes->directionalUse field.
DSRC Messages	CVE-DR1292-V02	The Traffic CV Management System shall generate a TIM consistent with SAE J2735
DSRC Messages	CVE-DR1294-V02	The TIM shall contain the speed limit for the reduced speed (school) zone
DSRC Messages	CVE-DR1296-V02	The TIM shall contain the reduced speed zone geometry
DSRC Messages	CVE-DR1374-V02	The RTCM message (SAE J2735, Section 7.163) shall include message type 1 GPS L1 observations at 1 Hz
DSRC Messages	CVE-DR1375-V02	The RTCM message (SAE J2735, Section 7.163) shall include message type 1005 Antenna Reference Point (ARP) coordinates at 2 Hz
DSRC Messages	CVE-DR1378-V01	The SPaT Message shall contain the (timeStamp) MinuteOfTheYear data element (SAE J2735, Section 7.100)
DSRC Messages	CVE-DR1379-V01	The SPaT Message shall contain the (intersections) IntersectionStateList data frame (a sequence of IntersectionState; SAE J2735, Section 6.38)

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1380-V01	The SPaT Message shall contain the IntersectionState data frame (SAE J2735, Section 6.37) under the IntersectionStateList data frame
DSRC Messages	CVE-DR1381-V01	The SPaT Message shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the IntersectionState data frame
DSRC Messages	CVE-DR1382-V01	The SPaT Message shall contain the (revision) MsgCount data element (SAE J2735, Section 7.104) under the IntersectionState data frame
DSRC Messages	CVE-DR1383-V01	The SPaT Message shall contain the (status) IntersectionStatusObject data element (SAE J2735, Section 7.57) under the IntersectionState data frame
DSRC Messages	CVE-DR1384-V01	The SPaT Message shall contain the (timeStamp) Dsecond data element (SAE J2735, Section 7.39) under the IntersectionState data frame
DSRC Messages	CVE-DR1385-V01	The SPaT Message shall contain the (states) MovementList data frame (a sequence of MovementState; SAE J2735, Section 6.52) under the IntersectionState data frame
DSRC Messages	CVE-DR1386-V01	The SPaT Message shall contain the MovementState data frame (SAE J2735, Section 6.53) under the MovementList data frame
DSRC Messages	CVE-DR1387-V01	The SPaT Message shall contain the (signalGroup) SignalGroupID data element (SAE J2735, Section 7.171) under the MovementState data frame
DSRC Messages	CVE-DR1388-V01	The SPaT Message shall contain the (state-time-speed) MovementEventList data frame (a sequence of MovementEvent; SAE J2735, Section 6.50) under the MovementState data frame
DSRC Messages	CVE-DR1389-V01	The SPaT Message shall contain the MovementEvent data frame (SAE J2735, Section 6.51) under the MovementEventList data frame
DSRC Messages	CVE-DR1390-V01	The SPaT Message shall contain the (eventState) MovementPhaseState data element (SAE J2735, Section 7.103) under the MovementEvent data frame
DSRC Messages	CVE-DR1391-V01	The SPaT Message shall contain the (timing) TimeChangeDetails data frame (SAE J2735, Section 6.134) under the MovementEvent data frame
DSRC Messages	CVE-DR1392-V01	The SPaT Message shall contain the (minEndTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame
DSRC Messages	CVE-DR1393-V01	The SPaT Message should contain the (maxEndTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame
DSRC Messages	CVE-DR1394-V01	The SPaT Message should contain the (likelyTime) TimeMark data element (SAE J2735, Section 7.194) under the TimeChangeDetails data frame

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1395-V01	The SPaT Message shall contain a 'states' field, which is a list of one or more MovementStates. The number of MovementStates shall correspond to the number of movements defined in the MAP messages which should be based on controller traffic phases that are currently active at the intersection.
DSRC Messages	CVE-DR1396-V01	The SPaT Message signalGroup shall be assigned number and is not necessarily based on the controller phase number
DSRC Messages	CVE-DR1397-V01	The SPaT Message should provide maxEndTime or likelyTime
DSRC Messages	CVE-DR1398-V01	The SPaT Message should provide maxEndTime if the traffic signal controller is running fixed-time, and if transmitted shall be equal to minEndTime
DSRC Messages	CVE-DR1402-V01	The OBU shall generate an SRM consistent with SAE J2735
DSRC Messages	CVE-DR1404-V01	The SRM shall contain the (second) DSecond data element (SignalRequestMessage.second) (SAE J2735, Section 7.39)
DSRC Messages	CVE-DR1405-V01	The SRM shall contain the (requests) SignalRequestList data frame (sequence of SignalRequestPackage; SAE J2735, Section 6.118)
DSRC Messages	CVE-DR1406-V01	The SRM shall contain the SignalRequestPackage data frame (SAE J2735, Section 6.119) under the SignalRequestList data frame
DSRC Messages	CVE-DR1407-V01	The SRM shall contain the (request) SignalRequest data frame (SAE J2735, Section 6.120) under the SignalRequestPackage data frame
DSRC Messages	CVE-DR1408-V01	The SRM shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the SignalRequest data frame
DSRC Messages	CVE-DR1409-V01	The SRM shall contain the (id) IntersectionID data element (SAE J2735, Section 7.56) under the intersectionReferenceID data frame
DSRC Messages	CVE-DR1410-V01	The SRM shall contain the (requestID) RequestID data element (SAE J2735, Section 7.153) under the SignalRequest data frame
DSRC Messages	CVE-DR1411-V01	The SRM shall contain the (requestType) PriorityRequestType data element (SAE J2735, Section 7.142) under the SignalRequest data frame
DSRC Messages	CVE-DR1412-V01	The SRM shall contain the (inBoundLane) IntersectionAccessPoint data frame (SAE J2735, Section 6.33) under the SignalRequest data frame
DSRC Messages	CVE-DR1413-V01	The SRM shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the IntersectionAccessPoint data frame

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1414-V01	The SRM shall contain the (approach) ApproachID data element (SAE J2735, Section 7.11) under the IntersectionAccessPoint data frame
DSRC Messages	CVE-DR1415-V01	The SRM shall contain the (connection) LaneConnectionID data element (SAE J2735, Section 7.86) under the IntersectionAccessPoint data frame
DSRC Messages	CVE-DR1416-V01	The SRM shall contain the (requestor) RequestorDescription data frame (SAE J2735, Section 6.98)
DSRC Messages	CVE-DR1417-V01	The SRM shall contain the (id) VehicleID data frame (SAE J2735, Section 6.147) under the RequestorDescription data frame
DSRC Messages	CVE-DR1418-V01	The SRM shall contain the (entityID) TemporaryID (SAE J2735, Section 7.187) under the VehicleID data frame
DSRC Messages	CVE-DR1420-V02	The RSU shall broadcast SAE J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host
DSRC Messages	CVE-DR1422-V01	The SSM shall contain the (second) DSecond data element (SignalStatusMessage.second) (SAE J2735, Section 7.39)
DSRC Messages	CVE-DR1423-V01	The SSM shall contain the (status) SignalStatusList data frame (sequence of SignalStatus; SAE J2735, Section 6.121)
DSRC Messages	CVE-DR1424-V01	The SSM shall contain the (sequenceNumber) MsgCount data element (SAE J2735, Section 7.104) under the SignalStatus data frame
DSRC Messages	CVE-DR1425-V01	The SSM shall contain the (id) IntersectionReferenceID data frame (SAE J2735, Section 6.36) under the SignalStatus data frame
DSRC Messages	CVE-DR1426-V01	The SSM shall contain the (sigStatus) SignalStatusPackageList data frame (sequence of SignalStatusPackage; SAE J2735, Section 6.122) under the SignalStatus data frame
DSRC Messages	CVE-DR1427-V01	The SSM shall contain the SignalStatusPackage data frame (SAE J2735, Section 6.123) under the SignalStatusPacakageList data frame
DSRC Messages	CVE-DR1428-V01	The SSM shall contain the (requestor) SignalRequestorInfo data frame (SAE J2735, Section 6.117) under the SignalStatusPackage data frame
DSRC Messages	CVE-DR1429-V01	The SSM shall contain the (id) VehicleID data frame (SAE J2735, Section 6.147) under the SignalRequestorInfo data frame
DSRC Messages	CVE-DR1430-V01	The SSM shall contain the (request) RequestID (SAE J2735, Section 7.153) under the SignalRequestorInfo data frame
DSRC Messages	CVE-DR1431-V01	The SSM shall contain the (sequenceNumber) MsgCount (SAE J2735, Section 7.104) under the SignalRequestorInfo data frame
DSRC Messages	CVE-DR1432-V01	The SSM shall contain the (inboundOn) IntersectionAccessPoint data frame (SAE J2735, Section 6.33) under the SignalStatusPackage data frame

Functional Group	ReqID	Description
DSRC Messages	CVE-DR1433-V01	The SSM shall contain the (lane) LaneID data element (SAE J2735, Section 7.88) under the IntesectionAccessPoint data frame
DSRC Messages	CVE-DR1434-V01	The SSM shall contain the (approach) ApproachID data element (SAE J2735, Section 7.11) under the IntesectionAccessPoint data frame
DSRC Messages	CVE-DR1435-V01	The SSM shall contain the (connection) LaneConnectionID data element (SAE J2735, Section 7.86) under the IntesectionAccessPoint data frame
DSRC Messages	CVE-DR1436-V01	The SSM shall contain the (status) PrioritizationResponseStatus data element (SAE J2735, Section 7.140) under the SignalStatusPackage data frame
DSRC Messages	CVE-DR3005-V01	The BSM Part I shall include all data elements contained in the (coreData) BSMcoreData data frame (SAE J2735, Section 6.8)
DSRC Messages	CVE-DR3089-V02	The TIM shall contain the event identification number
DSRC Messages	CVE-DR3090-V02	The TIM shall contain the event type
DSRC Messages	CVE-DR3091-V02	The TIM shall contain the event start time
DSRC Messages	CVE-DR3092-V02	The TIM shall contain the event duration
DSRC Messages	CVE-DR3093-V02	The TIM shall contain all data elements in the Geographic Information data frame
DSRC Messages	CVE-PR1105-V01	The BSM shall be broadcast at a frequency of 10 Hz when congestion control algorithms (SAE J2945/1) do not prescribe a reduced rate
DSRC Messages	CVE-PR1183-V01	The MAP message shall be expressed with an accuracy of 0.5 m or less.
DSRC Messages	CVE-PR1399-V01	The SPaT messages shall be generated and transmitted by the RSU with a minimum frequency of 10 Hz
DSRC Messages	CVE-PR1400-V01	The SPaT MsgCount data field shall be incremented with every update that is made to the corresponding IntersectionState data frame
DSRC Messages	CVE-PR1401-V01	The SPaT MovementStates shall be updated with at least the computation frequency of the traffic signal controller. If the controller is operating at 1 Hz, it is permissible to repeat the same MovementState information in 10 SPaT messages. However, if the controller is operating at 10 Hz or greater, the MovementStates needs to be updated for every message.
DSRC Messages	CVE-PR2993-V01	The MAP message shall be transmitted with a frequency of at least 1 Hz
DSRC Messages	CVE-PR2995-V01	The SRM shall be broadcast at the configured frequency (functional reqs describe when to start/stop broadcasting)

Functional Group	ReqID	Description
DSRC Messages	CVE-PR2999-V01	The SSM shall be broadcast at the configured frequency (functional reqs describe when to start/stop broadcasting)
DSRC Messages	CVE-PR3003-V01	The BSM shall always include Part I data (SAE J2735, Section 6.8)
DSRC Messages	CVE-PR3009-V01	The BSM shall be broadcast at the frequency specified by congestion control algorithms (SAE J2945/1) when congestion control algorithms (SAE J2945/1) prescribe a reduced frequency
Roadside Equipment	CVE-AR3121-V01	An RSU shall be available 99% of the time when power is available to the network.
Roadside Equipment	CVE-AR3122-V01	RSU shall return to an operational state within 5 min of regaining power
Roadside Equipment	CVE-FN1113-V01	An RSU shall obtain position correction information from a Continuously Operating Reference Station (CORS) for packaging and broadcasting as the RTCM message.
Roadside Equipment	CVE-FN1308-V01	An RSU shall acquire time from the LTS interface in accordance with J2945/1 section 6.2.4.
Roadside Equipment	CVE-FN1309-V01	An RSU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.
Roadside Equipment	CVE-FN1310-V02	An RSU shall broadcast (school zone) TIMs to an LDV OBU when configured to perform this function.
Roadside Equipment	CVE-FN1311-V01	An RSU shall use Coordinated Universal Time (UTC) time for all logged data (e.g., events logs, probe vehicle data) based on the format defined in J2735 section 6.19 and epoch of January 1st, 1970.
Roadside Equipment	CVE-FN1312-V01	An RSU shall have access to a function that generates SPaT messages from SPaT data inputs
Roadside Equipment	CVE-FN1313-V01	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs
Roadside Equipment	CVE-FN1314-V01	An RSU shall have access to a function that generates SSM messages from SSM data inputs
Roadside Equipment	CVE-FN1316-V02	Select RSUs in/around designated school zones (Linden STEM Academy and Our Lady of Peace School) shall broadcast TIMs received from the Traffic CV Management System only when the school zone flashing signal is flashing.
Roadside Equipment	CVE-FN1317-V01	RSU functionality failure shall not affect the safe operation of the signal controller.
Roadside Equipment	CVE-FN1318-V01	All roadside equipment (including RSUs) shall support remote authenticated access.
Roadside Equipment	CVE-FN1319-V02	An RSU shall broadcast the WSA on channel 180
Roadside Equipment	CVE-FN1321-V01	An RSU shall support IPv6 tunneling over IPv4.

Functional Group	ReqID	Description
Roadside Equipment	CVE-FN1325-V01	It shall be possible for a system administrator with the appropriate permissions to configure the RSU to request application certificates with only designated geographic locations.
Roadside Equipment	CVE-FN1327-V01	The CVE shall provide an interface to allow the system administrator to request new certificates bound to the new location if it moves from one location to another. (Note: its interface will allow requesting a new RSU application certificate with a site.)
Roadside Equipment	CVE-FN1328-V01	An RSU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.
Roadside Equipment	CVE-FN1333-V01	An RSU shall not create or transmit messages if the 1609.2 certificates do now contain the permissions for the corresponding PSID.
Roadside Equipment	CVE-FN1335-V01	An RSU supplier shall provide the enrollment certificate for each RSU.
Roadside Equipment	CVE-FN2972-V02	An RSU shall broadcast (school zone) TIMs to a Transit Vehicle OBU when configured to perform this function.
Roadside Equipment	CVE-FN2973-V02	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU
Roadside Equipment	CVE-FN2979-V02	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU
Roadside Equipment	CVE-FN2980-V02	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU
Roadside Equipment	CVE-FN2981-V02	The RSU shall broadcast J2735 RTCM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU
Roadside Equipment	CVE-FN2982-V01	An RSU shall send SPaT messages generated from traffic signal controller output to an HDV OBU
Roadside Equipment	CVE-FN2983-V01	An RSU shall send SPaT messages generated from traffic signal controller output to a Transit Vehicle OBU
Roadside Equipment	CVE-FN2987-V01	An RSU shall receive BSMs from an HDV OBU
Roadside Equipment	CVE-FN2988-V01	An RSU shall receive BSMs from a Transit Vehicle OBU
Roadside Equipment	CVE-FN2989-V01	An RSU shall receive BSMs from an Emergency Vehicle OBU
Roadside Equipment	CVE-FN2990-V01	An RSU shall receive SRMs from a Transit Vehicle OBU
Roadside Equipment	CVE-FN2991-V01	An RSU shall receive SRMs from an Emergency Vehicle OBU

Functional Group	ReqID	Description
Roadside Equipment	CVE-FN3000-V01	The RSU shall be able to send the SSM at a configurable rate
Roadside Equipment	CVE-FN3109-V01	An RSU shall send SPaT messages generated from traffic signal controller output to an Emergency Vehicle OBU
Roadside Equipment	CVE-FN3228-V01	An RSU shall support over-the-air OBU firmware updates through IPv6
Roadside Equipment	CVE-FN3299-V01	An RSU shall support over-the-air OBU 1609.2 Certificate updates through IPv6
Roadside Equipment	CVE-FN3112-V01	The RSU shall support OBU operating system updates that need to occur over the range of more than one RSU.
Roadside Equipment	CVE-IF1341-V02	An RSU shall receive TIMs as an, RSU Specification 4.1a, "Immediate Forward" message from a network host
Roadside Equipment	CVE-IF1342-V02	An RSU shall receive MAP messages as an, RSU Specification 4.1a, "Immediate Forward" message from a network host
Roadside Equipment	CVE-IF1343-V01	An RSU shall receive position data from the LTS
Roadside Equipment	CVE-IF1345-V01	An RSU shall receive SPaT messages from the Traffic Signal Controller
Roadside Equipment	CVE-IF1346-V01	An RSU should receive SSMs from a Traffic Signal Controller
Roadside Equipment	CVE-IF1347-V01	An RSU shall send information to request signal priority to the Traffic Signal Controller
Roadside Equipment	CVE-IF1348-V01	An RSU shall be powered via power over Ethernet (cat6a)
Roadside Equipment	CVE-IF1349-V01	An RSU shall be grounded
Roadside Equipment	CVE-IF1350-V01	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be outfitted with an in-line grounding mechanism
Roadside Equipment	CVE-IF1351-V01	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be weatherproof (outdoor rated)
Roadside Equipment	CVE-IF1352-V01	Ethernet cable that connects to equipment located outside of the traffic signal controller cabinet shall be double shielded
Roadside Equipment	CVE-IF1353-V01	The RSU-SCMS interface shall allow an RSU to request application certificates with different contents from the current ones during the lifetime of the current ones.
Roadside Equipment	CVE-IF1354-V01	Communication between the RSU and an SCMS shall operate in an encrypted, end-to-end connection in accordance with the selected SCMS interface. (Note: An SCMS interface should not need any further security.)
Roadside Equipment	CVE-IF1356-V01	An RSU shall send SPaT messages generated from traffic signal controller output to an LDV OBU

Functional Group	ReqID	Description
Roadside Equipment	CVE-IF1357-V02	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an LDV OBU
Roadside Equipment	CVE-IF1358-V01	An RSU shall send RTCM messages received from the CORS or another source to an LDV OBU
Roadside Equipment	CVE-IF1359-V02	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an HDV OBU
Roadside Equipment	CVE-IF1360-V02	The RSU shall broadcast J2735 TIM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an LDV OBU
Roadside Equipment	CVE-IF1361-V01	An RSU shall receive over the air messages via DSRC
Roadside Equipment	CVE-IF1362-V01	An RSU shall receive BSMs from an LDV OBU
Roadside Equipment	CVE-IF1363-V01	An RSU shall receive SRMs from an HDV OBU
Roadside Equipment	CVE-IF2978-V02	The RSU shall broadcast J2735 TIM messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU
Roadside Equipment	CVE-IF2985-V02	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU
Roadside Equipment	CVE-IF2986-V02	The RSU shall broadcast J2735 SSMs received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU
Roadside Equipment	CVE-MT1364-V01	RSUs shall support physical access to support maintenance activities.
Roadside Equipment	CVE-PR1365-V01	The system clock of the RSU shall be accurate to within 10 ms of the UTC reference
Roadside Equipment	CVE-PR1366-V01	All absolute times in any message shall be determined based on the RSU's system clock
Roadside Equipment	CVE-PR1367-V01	The time difference between minEndTime (in the UTC reference system) and the earliest possible physical phase change shall be no larger than 100 ms
Roadside Equipment	CVE-PR1368-V01	The time difference between maxEndTime (in the UTC reference system) and the earliest possible physical phase change shall be no larger than 100 ms
Roadside Equipment	CVE-PR1369-V01	The data elements MinuteOfTheYear and DSecond shall be present in each transmitted message and accurate within 100 ms of UTC time
Roadside Equipment	CVE-PR2994-V02	School Zone RSUs shall broadcast the TIM at a frequency of 1 Hz

Functional Group	ReqID	Description
Roadside Equipment	CVE-PY1370-V01	RSU DSRC antennas shall be located to maximize the DSRC range along the corridors of interest.
Roadside Equipment	CVE-PY1371-V01	RSU GPS antennas shall be located to maximize the GPS reception
Roadside Equipment	CVE-PY1372-V01	Ethernet cable spans shall not exceed 100 meters (328 feet)
Roadside Equipment	CVE-PY2912-V01	A traffic signal controller cabinet that contains Roadside Equipment shall be outfitted with tamper alert devices to prevent unauthorized physical access to networking components.
Roadside Equipment	CVE-PY3120-V01	RSUs shall be located on a network that is physically isolated from the existing CTSS network.
Roadside Equipment	CVE-SR1373-V01	RSUs shall support role-based authentication to enable physical access.
Roadside Equipment	CVE-SR3123-V01	An RSU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.
Roadside Equipment	CVE-SR3124-V01	An RSU shall verify a DSRC message if a device identifies the message as containing a new DE_TemporaryID value.
Roadside Equipment	CVE-SR3125-V01	An RSU shall support setting the certificate geographic region to be requested for application certificates.
Roadside Equipment	CVE-SR3126-V01	An RSU shall support establishment of a standard TLS-based VPN with client authentication for communication to the Traffic CV Management System, with a long-term client cert and a single CA cert trusted to authorize connections from the Traffic CV Management System.
Roadside Equipment	CVE-SR3127-V01	An RSU 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.
Roadside Equipment	CVE-SR3128-V01	An RSU shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).
Roadside Equipment	CVE-SR3129-V01	An RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications.
Roadside Equipment	CVE-SR3130-V01	An RSU shall comply with IEEE 1609.2: Standard for WAVE Security Services for Applications and Management Messages.
Roadside Equipment	CVE-SR3131-V01	An RSU shall delete old certificates if it has been moved to another intersection.
Traffic Management Center	CVE-DR1276-V01	The Traffic CV Management System shall remove PII from data prior to sending it to the Smart Columbus OS where it is made publicly available.
Traffic Management Center	CVE-FN1437-V01	The Traffic CV Management System shall transmit performance metrics (as configured by traffic management staff and defined in the Performance Measurement Plan) to the Smart Columbus OS

Functional Group	ReqID	Description
Traffic Management Center	CVE-FN1438-V02	The Traffic CV Management System shall send TIMs to the Smart Columbus OS
Traffic Management Center	CVE-FN1439-V01	The Traffic CV Management System shall send MAP messages to the Smart Columbus OS
Traffic Management Center	CVE-FN1440-V02	The Traffic CV Management System shall enable loading of TIMs on roadside equipment
Traffic Management Center	CVE-FN1441-V02	The Traffic CV Management System shall enable loading of MAP messages on roadside equipment
Traffic Management Center	CVE-FN1442-V02	The Traffic CV Management System shall accept input for TIM messages from Traffic Management Staff
Traffic Management Center	CVE-FN1443-V01	The Traffic CV Management System shall accept input for MAP messages from Traffic Management Staff
Traffic Management Center	CVE-FN1444-V01	The Traffic CV Management System shall accept input for configurable parameters (for functions on the TCVMS and on roadside equipment) from Traffic Management Staff
Traffic Management Center	CVE-FN1445-V01	The Traffic CV Management System shall make the status of RSUs available to Traffic Management Staff
Traffic Management Center	CVE-FN1446-V01	The Traffic CV Management System shall provide the VISA' functions of Validation, Integration, Sanitization (De-identification), and Aggregation of CV Data as defined in the U.S DOT SEMI ODE requirements (Reference TBR)
Traffic Management Center	CVE-FN1447-V02	The Traffic CV Management System shall generate TIM messages
Traffic Management Center	CVE-FN1448-V01	The Traffic CV Management System shall generate MAP messages
Traffic Management Center	CVE-FN1449-V01	The Traffic CV Management System shall monitor the uptime status of RSUs
Traffic Management Center	CVE-FN1452-V01	The Traffic CV Management System shall make the status of all RSUs available to Traffic Management Staff
Traffic Management Center	CVE-FN1453-V01	The Traffic CV Management System should automate the generation of performance metrics as defined in the Performance Management Plan (TBD)

Functional Group	ReqID	Description
Traffic Management Center	CVE-FN1454-V01	The Traffic CV Management System should use CV data made available through the CVE to generate performance metrics as defined in the Performance Management Plan (TBD)
Traffic Management Center	CVE-FN1456-V01	The Traffic CV Management System shall receive BSMs from the RSU
Traffic Management Center	CVE-FN1463-V01	The Traffic CV Management System shall monitor tamper alert devices
Traffic Management Center	CVE-FN2909-V01	The Traffic CV Management System shall generate performance metrics (as configured by traffic management staff and as defined in the Performance Measurement Plan) from archived CV data
Traffic Management Center	CVE-FN2911-V01	The Traffic CV Management System shall remove PII from BSMs that are received before further processing
Traffic Management Center	CVE-FN3001-V02	The Traffic CV Management System shall accept inputs for all required elements of a TIM message via a user interface.
Traffic Management Center	CVE-FN3002-V01	The Traffic CV Management System shall accept inputs for all required elements of a MAP message via a user interface.
Traffic Management Center	CVE-FN3030-V01	The Traffic CV Management System shall provide a means of allowing Traffic Management Staff to download archived CV data.
Traffic Management Center	CVE-FN3032-V01	The Traffic CV Management System shall copy all archived CV data into the archived CV data backup storage
Traffic Management Center	CVE-FN3041-V01	The Traffic CV Management System shall allow traffic management staff to configure the generation of performance measures from archived CV data (e.g. a recurring database query).
Traffic Management Center	CVE-FN3045-V01	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of a traffic signal controller cabinet that has been tampered with (based on the status of the tamper alert device)
Traffic Management Center	CVE-FN3047-V01	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is not running normally (off, not responding, in safe mode, etc.)
Traffic Management Center	CVE-FN3049-V01	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is offline
Traffic Management Center	CVE-FN3052-V01	The Traffic CV Management System shall display different colored icons on the UI to indicate the real-time status of each RSU.

Functional Group	ReqID	Description
Traffic Management Center	CVE-FN3053-V01	The Traffic CV Management System shall allow Traffic Management Staff to select an RSU using the UI to reveal other RSU information (uptime percentage, tamper alert status, alert information, channel busy ratio, etc.)
Traffic Management Center	CVE-FN3054-V01	The Traffic CV Management System shall maintain a log of all alerts issued to traffic management staff
Traffic Management Center	CVE-FN3055-V01	The Traffic CV Management System shall display an alert icon next to a given RSU icon on the UI to indicate that an alert has been issued for that RSU.
Traffic Management Center	CVE-FN3110-V02	The Traffic CV Management System shall accept inputs from Traffic Management Staff for a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request Signal Priority or Preemption at each intersection.
Traffic Management Center	CVE-IF3044-V01	The Traffic CV Management System shall use a UI to geographically display the location of each RSU and RSU information to Traffic Management Staff
Traffic Management Center	CVE-PR1457-V01	The Traffic CV Management System shall notify designated personnel within five minutes of limited connectivity. Note: Limited connectivity refers to a state when the Traffic CV Management System is not able to communicate with the RSU
Traffic Management Center	CVE-PR1458-V01	The Traffic CV Management System shall notify designated personnel within five minutes of a monitored function becoming unavailable
Traffic Management Center	CVE-PR3029-V01	The Traffic CV Management System shall be able to store at a minimum of 10 TB of archived CV data
Traffic Management Center	CVE-PR3031-V01	The Traffic CV Management System shall be able to store at a minimum of 10 TB of backup archived CV data
Traffic Management Center	CVE-PR3033-V01	The Traffic CV Management System shall copy all archived CV data into the backup archived CV data once per day.
Traffic Management Center	CVE-PY3034-V01	The Traffic CV Management System shall store archived CV data and backup archived CV data on separate physical storage devices.
Traffic Management Center	CVE-SR1459-V01	The Traffic CV Management System shall detect abnormal unauthorized activity on an IP connection.
Traffic Management Center	CVE-SR1460-V02	The Traffic CV Management System shall monitor the DSRC communications performance.
Traffic Management Center	CVE-SR1461-V01	The Traffic CV Management System shall monitor the data traffic usage to detect unapproved use of the IP connection.

Functional Group	ReqID	Description
Traffic Management System	CVE-FN3051-V01	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU (network entry vector) where unauthorized use has been detected and information regarding the unauthorized device.
Transit Management Center	CVE-FN3039-V01	The Transit CV Management System shall provide a means of allowing Transit Management Staff to download archived Transit Vehicle Interaction Events.
Transit Management Center	CVE-FN3040-V01	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the archived CV data backup storage
Transit Management Center	CVE-FN3042-V01	The Transit CV Management System shall allow transit management staff to configure the generation of performance measures from archived CV data (e.g. a recurring database query).
Transit Management Center	CVE-FN3043-V01	The Transit CV Management System shall transmit performance metrics (as configured by transit management staff and defined in the Performance Measurement Plan) to the Smart Columbus OS
Transit Management Center	CVE-IF1277-V01	The Transit CV Management System shall generate performance metrics (as configured by transit management staff and as defined in the Performance Measurement Plan)
Transit Management Center	CVE-IF1472-V01	The Transit CV Management System shall send Transit Vehicle Interaction Events to the Smart Columbus OS
Transit Management Center	CVE-IF1473-V01	The Transit CV Management System shall make Transit Vehicle Interaction Events available to Transit Management Staff
Transit Management Center	CVE-PR3035-V01	The Transit CV Management System shall be able to store at a minimum of 5 TB of archived Transit Vehicle Interaction Events
Transit Management Center	CVE-PR3036-V01	The Transit CV Management System shall be able to store at a minimum of 5 TB of backup archived Transit Vehicle Interaction Events
Transit Management Center	CVE-PR3037-V01	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the backup archived Transit Vehicle Interaction Events once per day.
Transit Management Center	CVE-PY3038-V01	The Transit CV Management System shall store archived Transit Vehicle Interaction Events and backup archived Transit Vehicle Interaction Events on separate physical storage devices.
V2I Mobility	CVE-DR1477-V01	The TSP Application shall require data from the SSM Message
V2I mobility	CVE-DR1478-V01	The TSP Application shall generate data for the SRM Message
V2I Mobility	CVE-DR1533-V01	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle
V2I Mobility	CVE-DR1562-V02	The VDTO Application shall capture data from all messages transmitted or received by roadside equipment

Functional Group	ReqID	Description
V2I Mobility	CVE-FN1479-V01	An HDV OBU shall request to receive signal priority at RSU-equipped intersections
V2I Mobility	CVE-FN1480-V01	An HDV OBU shall broadcast an SRM when approaching an RSU-equipped intersection
V2I Mobility	CVE-FN1481-V01	An HDV OBU shall broadcast an SRM when it is within a configurable distance of the intersection it intends to request priority for
V2I Mobility	CVE-FN1482-V01	An HDV OBU shall only request priority for movements is plans to make along a designated freight route (specific to the requesting HDV)
V2I Mobility	CVE-FN1483-V01	An HDV OBU shall only request priority in an SRM
V2I Mobility	CVE-FN1484-V02	An HDV OBU shall cease broadcasting SRMs for priority at a given intersection for a configurable amount of time after it has received an SSM from that intersection containing the RequestID of the SRM broadcasted the host HDV
V2I Mobility	CVE-FN1488-V01	A Transit Vehicle OBU shall request to receive signal priority at RSU-equipped intersections
V2I Mobility	CVE-FN1489-V01	A Transit Vehicle OBU shall send an SRM to an RSU when it is within a configurable distance of the intersection it intends to request priority for
V2I Mobility	CVE-FN1490-V01	A Transit Vehicle OBU shall only request priority in an SRM
V2I Mobility	CVE-FN1491-V01	A Transit Vehicle OBU shall only request priority for movements along the route being traversed by that transit vehicle
V2I Mobility	CVE-FN1492-V02	A Transit Vehicle OBU shall cease broadcasting SRMs for priority at a given intersection for a configurable amount of time after it has received an SSM from that intersection containing the RequestID of the SRM broadcasted the host Transit Vehicle
V2I Mobility	CVE-FN1493-V01	An Emergency Vehicle OBU shall request to receive signal preemption at RSU-equipped intersections
V2I Mobility	CVE-FN1497-V02	The EVP application should employ proven algorithms to enable emergency vehicle preemption
V2I Mobility	CVE-FN1498-V01	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection
V2I Mobility	CVE-FN1499-V01	The SRM shall contain information regarding the movement for which priority is being requested
V2I Mobility	CVE-FN1500-V01	A request to receive signal preemption from an Emergency Vehicle OBU shall be high priority
V2I Mobility	CVE-FN1501-V01	A request to receive signal priority from a Transit Vehicle OBU shall be low priority
V2I Mobility	CVE-FN1502-V01	A request to receive signal priority from an HDV Vehicle OBU shall be low priority
V2I Mobility	CVE-FN1503-V01	High priority requests to receive signal priority shall be serviced before low priority requests to receive signal priority

Functional Group	ReqID	Description
V2I Mobility	CVE-FN1504-V01	Multiple high priority requests shall be serviced in the order in which they are received
V2I Mobility	CVE-FN1505-V01	Multiple low priority requests shall be serviced in the order in which they are received
V2I Mobility	CVE-FN1508-V02	Roadside Equipment shall place a priority request or a preemption request to the traffic signal controller for the movement specified in the SRM if the following conditions are concurrently met: 1. The SRM "BasicVehicleRole" matches against the locally-stored list of BasicVehicleRoles are authorized to receive signal priority or preemption. 2. The request is made during the time period when priority or preemption will be granted for the vehicle with the given BasicVehicleRole. 3. The requested movement is allowed for the vehicle with the given BasicVehicleRole. 4. The intersection ID in the SRM matches the intersection ID
V2I Mobility	CVE-FN1509-V01	The Traffic Signal Controller shall grant an early green for a phase for a movement that is requested in a priority SRM when the approach for that movement is red or yellow
V2I Mobility	CVE-FN1510-V01	The Traffic Signal Controller shall grant an extended green for a phase for a movement that is requested in a priority SRM when the approach for the requested movement is green
V2I Mobility	CVE-FN1511-V01	The Traffic Signal Controller shall not adjust the typical progression of phases to accommodate a priority request
V2I Mobility	CVE-FN1512-V01	The Traffic Signal Controller should minimize the length of preceding phases to accommodate a priority request
V2I Mobility	CVE-FN1513-V01	The Traffic Signal Controller should immediately proceed to a pedestrian clearance interval (flashing red DON'T WALK) if an active pedestrian interval (solid white WALK) is ongoing when servicing a priority or preemption request
V2I Mobility	CVE-FN1514-V01	The Traffic Signal Controller shall not reduce the duration of a pedestrian clearance interval (flashing red DON'T WALK) before progressing to the next phase when servicing a priority or preemption request
V2I Mobility	CVE-FN1515-V01	The Traffic Signal Controller shall next service a phase for a movement that is requested in a preemption SRM when the approach for the requested movement is red
V2I Mobility	CVE-FN1516-V01	The Traffic Signal Controller shall wait for the light to turn red and passage of the all-red interval before servicing a phase for a movement that is requested in a preemption SRM when the approach for the requested movement is yellow
V2I Mobility	CVE-FN1517-V01	The Traffic Signal Controller shall extend the current phase for a movement that is requested in a preemption SRM when the approach for the requested movement is green
V2I Mobility	CVE-FN1518-V02	The Roadside Equipment shall receive output from the Traffic Signal Controller regarding the status of a priority request

Functional Group	ReqID	Description
V2I Mobility	CVE-FN1519-V01	An RSU shall send an SSM to an HDV OBU containing the results of the requests made by one or more vehicles for a configurable period of time
V2I Mobility	CVE-FN1520-V02	The Traffic CV Management System shall maintain a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request signal priority or preemption at each intersection.
V2I Mobility	CVE-FN1524-V02	The Roadside Equipment shall have a method of determining if an SRM "BasicVehicleRole" is authorized to receive signal priority at the intersection
V2I Mobility	CVE-FN1525-V02	The Roadside Equipment shall have a method of determining if an SRM "BasicVehicleRole" is authorized to receive signal preemption at the intersection
V2I Mobility	CVE-FN1534-V01	A Transit Vehicle OBU shall determine when to record a Transit Vehicle Interaction Event. Note: A Transit Vehicle Interaction Event contains the type of event along with a log of BSMs sent/received before and after the event.
V2I Mobility	CVE-FN1535-V01	A Transit Vehicle OBU shall not issue alerts to the transit vehicle operator
V2I Mobility	CVE-FN1536-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is emergency braking ahead by an OBU-equipped (remote) vehicle
V2I Mobility	CVE-FN1537-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a forward collision is imminent with another OBU-equipped (remote) vehicle
V2I Mobility	CVE-FN1538-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is an intersection collision detected with another OBU-equipped (remote) vehicle
V2I Mobility	CVE-FN1540-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a lane change collision is imminent with another OBU-equipped (remote) vehicle
V2I Mobility	CVE-FN1541-V01	A Transit Vehicle OBU (host) shall log a Transit Vehicle Interaction Event when the transit vehicle (host) runs a red light at an RSU-equipped intersection
V2I Mobility	CVE-FN1542-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle will enter an RSU-equipped school zone over the active school zone speed limit
V2I Mobility	CVE-FN1543-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
V2I Mobility	CVE-FN1544-V01	A Transit Vehicle OBU shall store any BSMs received in local memory for a configurable amount of time.
V2I Mobility	CVE-FN1545-V01	A Transit Vehicle OBU shall store any SPaT messages received in local memory for a configurable amount of time.

Functional Group	ReqID	Description
V2I Mobility	CVE-FN1546-V01	A Transit Vehicle OBU shall store any MAP messages received in local memory for a configurable amount of time (configuration should allow MAP messages to be stored for 7 days)
V2I Mobility	CVE-FN1547-V01	A Transit Vehicle OBU shall store any BSMs broadcast in local memory for a configurable amount of time.
V2I Mobility	CVE-FN1548-V01	A Transit Vehicle OBU shall store any SRMs broadcast in local memory for a configurable amount of time.
V2I Mobility	CVE-FN1549-V01	A Transit Vehicle OBU shall store any SSMs received in local memory for a configurable amount of time.
V2I Mobility	CVE-FN1550-V01	A Transit Vehicle Interaction Event shall consist of the type of event (emergency braking ahead, forward collision imminent, intersection movement, blind spot, lane change, red light violation, school zone speed limit, priority request)
V2I Mobility	CVE-FN1551-V01	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the transit vehicle OBU broadcasts an SRM
V2I Mobility	CVE-FN1554-V01	A Transit Vehicle OBU shall remove Transit Vehicle Interaction Event data with the oldest start times from memory until it is able to log a newly received interaction event
V2I Mobility	CVE-FN1555-V01	A Transit Vehicle OBU shall upload all Transit Vehicle Interaction Event data to the Transit CV Management System when it connects to the vehicle's regular data upload service.
V2I Mobility	CVE-FN1556-V01	A Transit Vehicle OBU shall remove all Transit Vehicle Interaction Event data from memory once uploaded to the Transit CV Management System.
V2I Mobility	CVE-FN1557-V01	A Transit Vehicle Interaction Event shall consist of the start time of the event (UTC)
V2I Mobility	CVE-FN1558-V01	A Transit Vehicle Interaction Event shall consist of the end time of the event (UTC) (in the case where multiple events of the same warning are issued based on messages received from the same vehicle or intersection within a configurable amount of time)
V2I Mobility	CVE-FN1559-V01	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast BSMs) from a configurable amount of time before the start time of the event
V2I Mobility	CVE-FN1560-V01	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast BSMs) from a configurable amount of time after the end time of the event
V2I Mobility	CVE-FN1564-V02	The Roadside Equipment shall send BSMs to the Traffic CV Management System as they are received from an OBU
V2I Mobility	CVE-FN1566-V02	The Roadside Equipment shall send SRMs to the Traffic CV Management System as they are received from an OBU
V2I Mobility	CVE-FN1569-V02	The roadside equipment shall send SSMs to the Traffic CV Management System as they are generated by the roadside equipment.

Functional Group	ReqID	Description
V2I Mobility	CVE-FN1572-V02	The roadside equipment shall send SPaT messages to the Traffic CV Management System as they are generated by the roadside equipment
V2I Mobility	CVE-FN1580-V02	The Traffic CV Management System shall receive BSMs sent by the roadside equipment
V2I Mobility	CVE-FN1581-V02	The Traffic CV Management System shall receive SRMs sent by the roadside equipment
V2I Mobility	CVE-FN1582-V02	The Traffic CV Management System shall receive SSMs sent by the roadside equipment
V2I Mobility	CVE-FN1583-V02	The Traffic CV Management System shall receive SPaT Messages sent by the roadside equipment
V2I Mobility	CVE-FN1585-V02	The Traffic CV Management System shall store BSMs sent by the roadside equipment
V2I Mobility	CVE-FN1586-V02	The Traffic CV Management System shall store SRMs sent by the roadside equipment
V2I Mobility	CVE-FN1587-V02	The Traffic CV Management System shall store SSMs sent by the roadside equipment
V2I Mobility	CVE-FN1588-V02	The Traffic CV Management System shall store SPaT messages sent by the roadside equipment
V2I Mobility	CVE-FN1589-V02	The Traffic CV Management System shall store SAE J2735 TIMs generated by Traffic Management Staff
V2I Mobility	CVE-FN1590-V01	The Traffic CV Management System shall store all MAP messages that are input by the Traffic Manager
V2I Mobility	CVE-FN1591-V01	The Traffic CV Management System shall make all stored data available to the Traffic Manager
V2I Mobility	CVE-FN3081-V01	A Transit Vehicle OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives
V2I Mobility	CVE-FN3082-V01	A Transit Vehicle OBU (host) shall determine if there is emergency braking ahead for each BSM it receives.
V2I Mobility	CVE-FN3083-V01	A Transit Vehicle OBU (host) shall determine if a forward collision is imminent for each BSM it receives
V2I Mobility	CVE-FN3084-V01	A Transit Vehicle OBU (host) shall determine if an intersection collision is imminent for each BSM it receives.
V2I Mobility	CVE-FN3085-V01	A Transit Vehicle OBU (host) shall determine if a lane change collision is imminent for each BSM it receives.
V2I Mobility	CVE-FN3086-V01	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also received a MAP message for the intersection that corresponds to the SPaT message.
V2I Mobility	CVE-FN3087-V02	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.

Functional Group	ReqID	Description
V2I Mobility	CVE-FN3107-V01	An Emergency Vehicle OBU shall request to receive signal preemption for all possible movements for the leg of the intersection of which it is approaching.
V2I Mobility	CVE-FN3108-V02	The roadside equipment shall not place a priority request or a preemption request to the traffic signal controller if it determines that the vehicle OBU that is sending the SRM containing the request has already passes through the intersection.
V2I Mobility	CVE-IF1526-V01	The TSP Application shall receive data from the OBU's internal processing functions.
V2I Mobility	CVE-IF1561-V01	The TVIER Application shall receive data from the OBU's internal processing functions.
V2I Mobility	CVE-PR1527-V02	The FSP application should employ proven algorithms to enable freight signal priority
V2I Mobility	CVE-PR1528-V01	The FSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2I Mobility	CVE-PR1529-V02	The TSP application should employ proven algorithms to enable transit signal priority
V2I Mobility	CVE-PR1530-V01	The TSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2I Mobility	CVE-PR1531-V01	The EVP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2I Safety	CVE-FN1300-V02	The LDV OBU (host) shall parse received TIMs to identify the school zone speed limit (J2735).
V2I Safety	CVE-FN1301-V02	The LDV OBU (host) shall parse received TIMs to identify when the school zone speed limit is active.
V2I Safety	CVE-FN1302-V02	The LDV OBU (host) shall parse received TIMs to identify the applicable regions of use geographical path (J2735).
V2I Safety	CVE-FN3078-V01	The Red Light Violation Warning Application shall identify when a vehicle is expected to cross the stop bar during a red signal by using the following data items:
V2I Safety	CVE-FN3079-V02	The Reduced Speed School Zone Application shall identify when a host vehicle is expected to enter the school zone but not below the school zone speed limit (given its current location, motion, and expected braking rate) during active school zone hours by using the following data items: The Reduced Speed School Zone Application shall identify when a host vehicle is expected to enter the school zone but not below the school zone speed limit (given its current location, motion,

Functional Group	ReqID	Description
		and expected braking rate) during active school zone hours by using the following data items: 1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. TIM data (received from the RSU) 3. RTCM data (received from the RSU)
V2I Safety	CVE-PR1290-V02	The RLVW application should employ proven algorithms to issue an RLVW
V2I Safety	CVE-PR1291-V01	The RLVW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2I Safety	CVE-PR1306-V02	The RSSZ application should employ proven algorithms to issue an RSSZ warning
V2I Safety	CVE-PR1307-V01	The RSSZ application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2I Safety	CVE-PR3118-V01	The RLVW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
V2I Safety	CVE-PR3119-V01	The RSSZ application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
V2V Safety	CVE-FN3073-V01	The Forward Collision Warning Application shall identify when the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle and the remote vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items:
V2V Safety	CVE-FN3074-V01	The Blind Spot Warning Application shall identify when a remote vehicle is within the blind spot (a configurable area to the rear right and rear left of a vehicle that moves with the vehicle) of a host vehicle, and is moving in the same direction of travel as the host vehicle by using the following data items:
V2V Safety	CVE-FN3075-V01	The Emergency Electronic Brake Light Application shall identify when an emergency braking maneuver has been detected by a remote vehicle, the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items:
V2V Safety	CVE-FN3076-V01	The Lane Change Warning Application shall identify when a host vehicle is changing lanes into a remote vehicle, and is moving in the same direction of travel as the host vehicle by using the following data items:

Functional Group	ReqID	Description
V2V Safety	CVE-FN3077-V01	The Intersection Movement Assist Application shall identify when the host vehicle has a trajectory (based on position, speed, acceleration) that may interfere with remote) vehicle trajectory in a side impact fashion, and the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle) by using the following data items:
V2V Safety	CVE-PR1111-V02	The BSW application should employ proven algorithms to issue an BSW alert.
V2V Safety	CVE-PR1112-V01	The BSW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2V Safety	CVE-PR1119-V02	The EEBL application should employ proven algorithms to issue an EEBL alert.
V2V Safety	CVE-PR1120-V01	The EEBL application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2V Safety	CVE-PR1127-V02	The FCW application should employ proven algorithms to issue an FCW alert
V2V Safety	CVE-PR1128-V01	The FCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2V Safety	CVE-PR1135-V02	The IMA application should employ proven algorithms to issue an IMA alert
V2V Safety	CVE-PR1136-V01	The IMA application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2V Safety	CVE-PR1142-V02	The LCW application should employ proven algorithms to issue an LCW alert
V2V Safety	CVE-PR1143-V01	The LCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
V2V Safety	CVE-PR3114-V01	The EEBL application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
V2V Safety	CVE-PR3115-V01	The FCW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
V2V Safety	CVE-PR3116-V01	The IMA application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.

Functional Group	ReqID	Description
V2V Safety	CVE-PR3117-V01	The LCW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
V2V Safety Application	CVE-PR3113-V01	The BSW application shall issue alerts with a false discovery rate (number of false positive alerts divided by total number of alerts) no greater than 2%.
Vehicle Onboard Equipment	CVE-FN1107-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is an OBU-equipped (remote) vehicle in the host vehicle's blind spot
Vehicle Onboard Equipment	CVE-FN1108-V01	An LDV OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives
Vehicle Onboard Equipment	CVE-FN1115-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is emergency braking ahead by an OBU-equipped (remote) vehicle
Vehicle Onboard Equipment	CVE-FN1116-V01	An LDV OBU (host) shall determine if there is emergency braking ahead for each BSM it receives
Vehicle Onboard Equipment	CVE-FN1122-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the LDV HMI when a forward collision is imminent with another OBU-equipped (remote) vehicle
Vehicle Onboard Equipment	CVE-FN1123-V01	The LDV OBU shall present alerts to drivers (via the HMI) using an HMI device that drivers are familiar with and limits driver interaction.
Vehicle Onboard Equipment	CVE-FN1124-V01	An LDV OBU (host) shall determine if a forward collision is imminent for each BSM it receives
Vehicle Onboard Equipment	CVE-FN1131-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when an intersection collision is imminent with another OBU-equipped (remote) vehicle
Vehicle Onboard Equipment	CVE-FN1132-V01	An LDV OBU (host) shall determine if an intersection collision is imminent for each BSM it receives
Vehicle Onboard Equipment	CVE-FN1138-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when it is changing lanes into another OBU-equipped (remote) vehicle
Vehicle Onboard Equipment	CVE-FN1139-V01	An LDV OBU (host) shall determine if a lane change collision is imminent for each BSM it receives
Vehicle Onboard Equipment	CVE-FN1184-V01	An OBU shall be capable of being reset and reconfigured so that it can be installed into another vehicle of the same type (e.g. LDV, HDV, etc.)
Vehicle Onboard Equipment	CVE-FN1185-V01	An OBU host processor shall perform integrity checks on boot to ensure that it is in a known good software state.

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-FN1186-V01	An OBU shall not continue to start up and will log an error if the host processor determines it is not in a known good software state on boot up.
Vehicle Onboard Equipment	CVE-FN1187-V01	An LDV OBU shall communicate with an LDV Operator via an HMI
Vehicle Onboard Equipment	CVE-FN1188-V01	The LDV OBU shall have two levels of alert
Vehicle Onboard Equipment	CVE-FN1189-V01	The LDV OBU shall have a low-level alert
Vehicle Onboard Equipment	CVE-FN1190-V01	The low-level alert shall consist of a configurable audio/visual warning
Vehicle Onboard Equipment	CVE-FN1191-V01	The LDV OBU shall have a high-level alert
Vehicle Onboard Equipment	CVE-FN1192-V01	The high-level alert shall consist of a configurable audio/visual warning
Vehicle Onboard Equipment	CVE-FN1193-V01	The high-level alert shall be louder and more visible compared to the low-level alert
Vehicle Onboard Equipment	CVE-FN1194-V01	The LDV OBU shall not display more than one alert to the LDV Vehicle Operator at a time
Vehicle Onboard Equipment	CVE-FN1195-V01	The LDV OBU shall contain a configurable priority order for notifying with alerts
Vehicle Onboard Equipment	CVE-FN1196-V01	The order of alerts shall be configurable so that the order of alerts can be modified once priority has been established.
Vehicle Onboard Equipment	CVE-FN1197-V01	The LDV OBU should provide system status information to LDV operators. Information included in the system status includes power status, system settings, status of applications availability, and pending update status
Vehicle Onboard Equipment	CVE-FN1198-V01	The OBU should notify the vehicle operators of the power status of device (e.g., off, powering up and online).
Vehicle Onboard Equipment	CVE-FN1202-V01	The LDV OBU shall provide messages that can be seen and/or heard by the LDV Operator via the HMI from the LDV Vehicle Operator's normal seating position

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-FN1203-V01	The LDV OBU shall provide only the highest priority alert to the LDV vehicle operator when more than one alert is currently active
Vehicle Onboard Equipment	CVE-FN1204-V02	An OBU shall acquire time from the Location and Time Service (LTS) interface in accordance with J2945/1 section 6.2.4.
Vehicle Onboard Equipment	CVE-FN1205-V01	An OBU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.
Vehicle Onboard Equipment	CVE-FN1206-V01	A Transit Vehicle OBU shall transmit Transit Vehicle Interaction Events to the Transit CV Management System
Vehicle Onboard Equipment	CVE-FN1207-V01	The OBU may capture vehicle brake status over the OBU-OBD-II interface to the host vehicle
Vehicle Onboard Equipment	CVE-FN1208-V01	A Transit Vehicle OBU shall use Coordinated Universal Time (UTC) time for all logged data (e.g., events logs, probe vehicle data) based on the format defined in J2735 section 6.19 and epoch of January 1st, 1970.
Vehicle Onboard Equipment	CVE-FN1209-V01	An OBU device shall comply with IEEE 1609.2: Standard for WAVE Security Services for Applications and Management Messages
Vehicle Onboard Equipment	CVE-FN1210-V01	An LDV OBU shall determine when to issue an Emergency Electronic Brake Light alert
Vehicle Onboard Equipment	CVE-FN1212-V01	The OBU shall implement a download protocol that permits resumption of incomplete downloads instead of requiring an incomplete download to be restarted.
Vehicle Onboard Equipment	CVE-FN1213-V01	The LDV OBU should provide a visual output (via the HMI) that is similar in look and feel (i.e. similar in size, consistent use of color in icons or graphics, similar styles of icons or graphics) from various applications, if presenting visual information to LDV Operators
Vehicle Onboard Equipment	CVE-FN1215-V01	An Emergency Vehicle OBU shall not broadcast SRMs when its lights are off and siren is off
Vehicle Onboard Equipment	CVE-FN1216-V01	An Emergency Vehicle OBU shall only broadcast SRMs when its lights are on and siren is on.
Vehicle Onboard Equipment	CVE-FN1286-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when a red-light violation will occur at an RSU-equipped intersection
Vehicle Onboard Equipment	CVE-FN1287-V01	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives,

Functional Group	ReqID	Description
		provided it has also received a MAP message for the intersection that corresponds to the SPaT message.
Vehicle Onboard Equipment	CVE-FN1298-V01	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when the OBU-equipped (host) vehicle will enter an RSU-equipped school zone over the active school zone speed limit
Vehicle Onboard Equipment	CVE-FN1299-V01	An LDV OBU (host) shall issue an alert when the OBU-equipped (host) vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
Vehicle Onboard Equipment	CVE-FN1495-V01	An Emergency Vehicle OBU shall only request preemption in an SRM
Vehicle Onboard Equipment	CVE-FN1496-V02	An Emergency Vehicle OBU shall cease sending SRMs for preemption to an RSU at a given intersection for a configurable amount of time after it has received an SSM from the RSU at that intersection containing the RequestID of the SRM broadcasted the host Emergency Vehicle
Vehicle Onboard Equipment	CVE-FN2952-V01	An LDV OBU shall receive BSMs from a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2953-V01	An LDV OBU shall receive BSMs from an Emergency Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2954-V01	A Transit Vehicle OBU shall receive BSMs from an HDV OBU
Vehicle Onboard Equipment	CVE-FN2955-V01	A Transit Vehicle OBU shall receive BSMs from a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2956-V01	A Transit Vehicle OBU shall receive BSMs from an Emergency Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2957-V01	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2958-V01	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to an RSU
Vehicle Onboard Equipment	CVE-FN2959-V01	An HDV OBU shall receive position data from GNSS satellites
Vehicle Onboard Equipment	CVE-FN2960-V01	A Transit Vehicle OBU shall receive position data from GNSS satellites

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-FN2961-V01	An Emergency Vehicle OBU shall receive position data from GNSS satellites
Vehicle Onboard Equipment	CVE-FN2962-V01	An HDV OBU shall receive security certificates from an SCMS via the RSU
Vehicle Onboard Equipment	CVE-FN2963-V01	A Transit Vehicle OBU shall receive security certificates from an SCMS via the RSU
Vehicle Onboard Equipment	CVE-FN2964-V01	An Emergency Vehicle OBU shall receive security certificates from an SCMS via the RSU
Vehicle Onboard Equipment	CVE-FN2966-V01	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2967-V01	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an RSU
Vehicle Onboard Equipment	CVE-FN2968-V02	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2969-V02	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an RSU
Vehicle Onboard Equipment	CVE-FN2970-V01	An LDV OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2971-V01	An LDV OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an RSU
Vehicle Onboard Equipment	CVE-FN2974-V02	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to a Transit Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2975-V02	The RSU shall broadcast J2735 MAP messages received as an, RSU Specification 4.1a, "Immediate Forward" message from a network host, to an Emergency Vehicle OBU
Vehicle Onboard Equipment	CVE-FN2976-V01	An RSU shall send an SSM to a Transit Vehicle OBU containing the results of the requests made by one or more vehicles for a configurable period of time
Vehicle Onboard Equipment	CVE-FN2977-V01	An RSU shall send an SSM to an Emergency Vehicle OBU containing the results of the requests made by one or more vehicles for a configurable period of time
Vehicle Onboard Equipment	CVE-FN2996-V01	The HDV OBU shall be able to send the SRM at a configurable rate

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-FN2997-V01	The Transit Vehicle OBU shall be able to send the SRM at a configurable rate
Vehicle Onboard Equipment	CVE-FN2998-V01	The Emergency Vehicle OBU shall be able to send the SRM at a configurable rate
Vehicle Onboard Equipment	CVE-FN3011-V01	An LDV OBU shall determine when to issue a Forward Collision Warning alert
Vehicle Onboard Equipment	CVE-FN3012-V01	An LDV OBU shall determine when to issue an Intersection Movement Assist alert
Vehicle Onboard Equipment	CVE-FN3013-V01	An LDV OBU shall determine when to issue a Lane Change Warning/Blind Spot Warning alert
Vehicle Onboard Equipment	CVE-FN3014-V01	An LDV OBU shall determine when to issue a Red Light Violation Warning alert
Vehicle Onboard Equipment	CVE-FN3015-V01	An LDV OBU shall determine when to issue a Reduced Speed School Zone alert
Vehicle Onboard Equipment	CVE-FN3021-V01	The LDV OBU shall be customizable for the following options (via the HMI): Volume, Brightness (if screen is used), Text size (if screen is used), Display contrast (if screen is used), Mounting Eye Position (if screen is used)
Vehicle Onboard Equipment	CVE-FN3022-V01	The LDV OBU should provide system status to drivers (via the HMI)
Vehicle Onboard Equipment	CVE-FN3023-V01	The LDV OBU should notify the LDV Operator of the power status of the OBU (via the HMI) (e.g. off, powering up, online, powering down)
Vehicle Onboard Equipment	CVE-FN3024-V01	The LDV OBU should allow the LDV Operator to adjust the system settings of the device (via the HMI) (e.g. version, brightness (if screen is used), volume, text size (if screen is used), contrast (if screen is used))
Vehicle Onboard Equipment	CVE-FN3025-V01	The LDV OBU shall not allow the driver to adjust settings while the vehicle is in motion.
Vehicle Onboard Equipment	CVE-FN3026-V01	The LDV OBU should notify the LDV Operator of application availability (via the HMI) (e.g. failed, operating, disabled).
Vehicle Onboard Equipment	CVE-FN3027-V01	The LDV OBU should notify the LDV Operator of pending updates for the LDV OBU (via the HMI) (e.g. applications, firmware, operating system).

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-FN3028-V01	The LDV OBU shall provide a visible and/or audible sound (via the HMI) when the vehicle is started up to indicate to the LDV Operator that they are in a CV-equipped vehicle.
Vehicle Onboard Equipment	CVE-FN3080-V02	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.
Vehicle Onboard Equipment	CVE-IF1218-V01	An LDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU
Vehicle Onboard Equipment	CVE-IF1219-V02	An HDV OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU
Vehicle Onboard Equipment	CVE-IF1220-V01	A Transit Vehicle OBU shall broadcast BSMs (Part I) consistent with SAE J2735 to an LDV OBU
Vehicle Onboard Equipment	CVE-IF1221-V01	An Emergency Vehicle OBU shall send BSMs (Part I) consistent with SAE J2735 to an LDV OBU
Vehicle Onboard Equipment	CVE-IF1222-V01	An LDV OBU shall communicate alerts to an LDV Operator
Vehicle Onboard Equipment	CVE-IF1223-V01	An LDV OBU shall receive BSMs from an LDV OBU
Vehicle Onboard Equipment	CVE-IF1224-V01	A Transit Vehicle OBU shall receive BSMs from an LDV OBU
Vehicle Onboard Equipment	CVE-IF1225-V01	An LDV OBU shall receive SPaT messages from an RSU
Vehicle Onboard Equipment	CVE-IF1226-V01	An HDV OBU shall receive SPaT messages from an RSU
Vehicle Onboard Equipment	CVE-IF1227-V01	A Transit Vehicle OBU shall receive SPaT messages from an RSU
Vehicle Onboard Equipment	CVE-IF1228-V01	An Emergency Vehicle OBU shall receive SPaT messages from an RSU
Vehicle Onboard Equipment	CVE-IF1229-V01	An LDV OBU shall receive MAP messages from an RSU
Vehicle Onboard Equipment	CVE-IF1230-V01	An HDV OBU shall receive MAP messages from an RSU

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-IF1231-V01	A Transit Vehicle OBU shall receive MAP messages from an RSU
Vehicle Onboard Equipment	CVE-IF1232-V01	An Emergency Vehicle OBU shall receive MAP messages from an RSU
Vehicle Onboard Equipment	CVE-IF1233-V01	An LDV OBU shall receive RTCM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1234-V01	An HDV OBU shall receive RTCM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1235-V01	A Transit Vehicle OBU shall receive RTCM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1236-V01	An Emergency Vehicle OBU shall receive RTCM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1237-V01	An HDV OBU shall receive SSM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1238-V01	A Transit Vehicle OBU shall receive SSM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1239-V01	An Emergency Vehicle OBU shall receive SSM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1240-V02	An LDV OBU shall receive TIM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1241-V02	A Transit Vehicle OBU shall receive TIM messages from an RSU
Vehicle Onboard Equipment	CVE-IF1242-V01	An LDV OBU shall receive position data from GNSS satellites
Vehicle Onboard Equipment	CVE-IF1243-V01	An LDV OBU shall receive security certificates from an SCMS via the RSU
Vehicle Onboard Equipment	CVE-IF1244-V01	An Emergency Vehicle OBU shall receive the flashing light status from the appropriate vehicle system
Vehicle Onboard Equipment	CVE-IF1245-V01	An Emergency Vehicle OBU shall receive the siren status from the appropriate vehicle system

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-IF1246-V01	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Vehicle Onboard Equipment	CVE-IF1248-V01	An Emergency Vehicle OBU shall provide a means of ceasing the broadcast of DSRC messages
Vehicle Onboard Equipment	CVE-IF1249-V01	An HDV OBU shall send SRMs to an RSU
Vehicle Onboard Equipment	CVE-IF1250-V01	A Transit Vehicle OBU shall send SRMs to an RSU
Vehicle Onboard Equipment	CVE-IF1251-V01	An Emergency Vehicle OBU shall send SRMs to an RSU
Vehicle Onboard Equipment	CVE-IF3019-V01	The LDV OBU shall include both a visual and/or auditory interface for sharing traveler information (via the HMI).
Vehicle Onboard Equipment	CVE-MT1252-V01	An OBU shall support physical access to support maintenance activities.
Vehicle Onboard Equipment	CVE-MT1253-V01	An OBU shall support role-based authentication to enable physical access.
Vehicle Onboard Equipment	CVE-PR2907-V01	The OBU shall have a minimum reserve (processor, dynamic storage, persistent storage) capacity of 50% upon deployment to have the capacity to install and run future firmware image updates
Vehicle Onboard Equipment	CVE-PR2913-V01	A Transit Vehicle OBU shall be capable of holding 4 GB of interaction event data.
Vehicle Onboard Equipment	CVE-PR3017-V01	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
Vehicle Onboard Equipment	CVE-PR3020-V01	The LDV OBU Auditory signals (via the HMI) shall be loud enough to overcome masking sounds from road noise, the cab environment, and other equipment.
Vehicle Onboard Equipment	CVE-PY3016-V01	The LDV OBU HMI shall be mounted or installed in a location where it does not obstruct the line of sight of the LDV Operator nor distract the LDV Operator from the primary task of driving.
Vehicle Onboard Equipment	CVE-PY3018-V01	The LDV OBU shall be positioned in a location such that it can provide a visual output to the driver (via the HMI) that can be read from the driver's normal seated position, if visual alerts are used.

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-SR1254-V01	The OBU shall cease transmission of BSMs if the OBU determines that it has been blacklisted. Note: Blacklists detail devices that should not be trusted in the system or network
Vehicle Onboard Equipment	CVE-SR1255-V01	The OBU shall prevent incoming messages with invalid conditions per criteria in the IEEE 1609.2 from being acted on.
Vehicle Onboard Equipment	CVE-SR1256-V01	The OBU Vehicle Communications link shall have communications security to ensure the authenticity of all its messages in accordance to the standards prescribed by wireless messaging security standards.
Vehicle Onboard Equipment	CVE-SR1257-V01	The OBU shall carry out plausibility checking on the remote vehicle BSM data.
Vehicle Onboard Equipment	CVE-SR1258-V01	The OBU shall indicate successful receipt of the pseudonym certificates.
Vehicle Onboard Equipment	CVE-SR1259-V01	When the OBU has no valid BSM signing certificates, it shall store the log file entries as IEEE 1609.2 data of type unsecured.
Vehicle Onboard Equipment	CVE-SR1261-V01	The OBU shall obtain certificates via IPv6 connectivity through the RSU.
Vehicle Onboard Equipment	CVE-SR1262-V01	An OBU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.
Vehicle Onboard Equipment	CVE-SR1263-V01	An OBU shall support establishment of a standard TLS-based VPN with client authentication for communication to the Traffic CV Management System, with a long-term client cert and a single CA cert trusted to authorize connections from the Traffic CV Management System.
Vehicle Onboard Equipment	CVE-SR1264-V01	An OBU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.
Vehicle Onboard Equipment	CVE-SR1265-V01	An OBU shall provide real-time tamper data which indicates that the device has been tampered with (e.g. opening of the case).
Vehicle Onboard Equipment	CVE-SR1266-V01	An OBU 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.
Vehicle Onboard Equipment	CVE-SR1267-V01	An OBU shall only transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it currently has valid certificates for that usage scenario

Functional Group	ReqID	Description
Vehicle Onboard Equipment	CVE-SR1268-V01	An OBU shall verify a DSRC message when a device identifies the message as containing a new DE_TemporaryID value.
Vehicle Onboard Equipment	CVE-SR1269-V01	An OBU shall verify a DSRC message when the message results in the issuance of an advisory, warning, or alert
Vehicle Onboard Equipment	CVE-SR1270-V01	An OBU shall verify a DSRC message when 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
Vehicle Onboard Equipment	CVE-SR1271-V01	An OBU shall verify a DSRC message when other potential threat situations such as red-light violations, and other safety applications are active
Vehicle Onboard Equipment	CVE-FN1494-V01	An Emergency Vehicle OBU shall send an SRM to an RSU when it is less than a configurable amount of time away from arriving at the intersection it intends to request priority for

Source: City of Columbus

Appendix C. Data Matrix

Table 22 contains a preliminary list of project specific data elements identified as required for the proper functionality of the system.

Table 22: Data Matrix

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
MAP	(msgIssueRevision) MsgCount data element	RSU	ASN.1	CVE-MAP-DR1-v1
MAP	(intersections) IntersectionGeometryList data frame (a sequence of IntersectionGeometry)	RSU	ASN.1	CVE-MAP-DR2-v1
MAP	IntersectionGeometry data frame under the (intersections) IntersectionGeometryList data frame	RSU	ASN.1	CVE-MAP-DR3-v1
MAP	(id) IntersectionReferenceID data frame under the IntersectionGeometry data frame	RSU	ASN.1	CVE-MAP-DR4-v1
MAP	(id) IntersectionID data element under the (id) IntersectionReferenceID data frame	RSU	ASN.1	CVE-MAP-DR5-v1
MAP	(revision) MsgCount data element under the IntersectionGeometry data frame	RSU	ASN.1	CVE-MAP-DR6-v1
MAP	(refPoint) Position3D-2 data frame under the IntersectionGeometry data frame	RSU	ASN.1	CVE-MAP-DR7-v1
MAP	(lat) Latitude data element under the (refPoint) Position3D-2 data frame	RSU	ASN.1	CVE-MAP-DR8-v1
MAP	(long) Longitude data element under the (refPoint) Position3D-2 data frame	RSU	ASN.1	CVE-MAP-DR9-v1
MAP	(laneWidth) LaneWidth data element under the IntersectionGeometry data frame	RSU	ASN.1	CVE-MAP-DR10-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
MAP	LaneList data frame (a sequence of GenericLane) under the IntersectionGeometry data frame	RSU	ASN.1	CVE-MAP-DR11-v1
MAP	GenericLane data frame under the LaneList data frame	RSU	ASN.1	CVE-MAP-DR12-v1
MAP	(laneID) LaneID data element under the GenericLane data frame	RSU	ASN.1	CVE-MAP-DR13-v1
MAP	(maneuvers) AllowedManeuvers data element under the GenericLane data frame	RSU	ASN.1	CVE-MAP-DR14-v1
MAP	NodeList data frame under the GenericLane data frame	RSU	ASN.1	CVE-MAP-DR15-v1
MAP	(nodes) NodeSet data frame (a sequence of Node) under the NodeList data frame	RSU	ASN.1	CVE-MAP-DR16-v1
MAP	Node data frame under the (nodes) NodeSet data frame	RSU	ASN.1	CVE-MAP-DR17-v1
MAP	(delta) NodeOffsetPointXY data element under the Node data frame (Any representation Node-XY-20b through Node-XY-32b)	RSU	ASN.1	CVE-MAP-DR18-v1
MAP	(connectsTo) ConnectsToList data frame (a sequence of Connection) under the GenericLane data frame	RSU	ASN.1	CVE-MAP-DR19-v1
MAP	Connection data frame under the (connectsTo) ConnectsToList data frame	RSU	ASN.1	CVE-MAP-DR20-v1
MAP	(connectingLane) ConnectingLane data frame under the Connection data frame	RSU	ASN.1	CVE-MAP-DR21-v1
MAP	(lane) LaneID data element under the (connectingLane) ConnectingLane data frame	RSU	ASN.1	CVE-MAP-DR22-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
MAP	(maneuver) AllowedManeuvers data element under the (connectingLane) ConnectingLane data frame	RSU	ASN.1	CVE-MAP-DR23-v1
MAP	(signalGroup) SignalGroupID data element under the Connection data frame	RSU	ASN.1	CVE-MAP-DR24-v1
MAP	egress lanes (if included) may optionally contain a maneuvers field or a connectsTo field	RSU	ASN.1	CVE-MAP-DR26-v1
MAP	egress lanes (if included) may optionally contain the nodes in the NodeSet sequenced such that the first node is the stop bar	RSU	ASN.1	CVE-MAP-DR27-v1
MAP	Connection field shall contain the lane, maneuver, and signalGroup associated with the Connection. The signalGroup identifies which signal group in the SPaT controls the flow of traffic from the ingress lane to the egress lane.	RSU	ASN.1	CVE-MAP-DR35-v1
MAP	IntersectionGeometry revision shall be changed only if the map information was updated.	RSU	ASN.1	CVE-MAP-DR38-v1
MAP	laneList. Each lane in the laneList shall be identified as an ingress lane or an egress lane through the laneAttributes->directionalUse field.	RSU	ASN.1	CVE-MAP-DR39-v1
TIM	school zone speed limit (J2735) (specific data frames/elements TBD)	RSU	ASN.1	CVE-DR1294-V02
TIM	time periods when the school zone speed limit is active. (specific data frames/elements TBD)	RSU	ASN.1	CVE-DR3091-V02 and CVE-DR3092-V02
TIM	applicable regions of use geographical path (J2735). (specific data frames/elements TBD)	RSU	ASN.1	CVE-DR1296-V02

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
RTCM	message type 1 – GPS L1 observations at 1 Hz	RSU	ASN.1	CVE-DR1374-V02
RTCM	message type 2 – Antenna Reference Point (ARP) coordinates at 1 Hz	RSU	ASN.1	CVE-DR1375-V02
RTCM	message type 3-GPS Reference Station Parameters, at 1 Hz	RSU	ASN.1	CVE-DR3295-V01
RTCM	message type 9-GPS partial correction set, at 1 Hz	RSU	ASN.1	CVE-DR3296-V01
SPAT	(timeStamp) MinuteOfTheYear data element	RSU	ASN.1	CVE-SPAT-DR1-v1
SPAT	(intersections) IntersectionStateList data frame (a sequence of IntersectionState)	RSU	ASN.1	CVE-SPAT-DR2-v1
SPAT	IntersectionState data frame under the IntersectionStateList data frame	RSU	ASN.1	CVE-SPAT-DR3-v1
SPAT	(id) IntersectionReferenceID data element under the IntersectionState data frame	RSU	ASN.1	CVE-SPAT-DR4-v1
SPAT	(revision) MsgCount data element under the IntersectionState data frame	RSU	ASN.1	CVE-SPAT-DR5-v1
SPAT	(status) IntersectionStatusObject data element under the IntersectionState data frame	RSU	ASN.1	CVE-SPAT-DR6-v1
SPAT	(timeStamp) Dsecond data element under the IntersectionState data frame	RSU	ASN.1	CVE-SPAT-DR7-v1
SPAT	(states) MovementList data frame (a sequence of MovementState) under the IntersectionState data frame	RSU	ASN.1	CVE-SPAT-DR8-v1
SPAT	MovementState data frame under the MovementList data frame	RSU	ASN.1	CVE-SPAT-DR9-v1
SPAT	(signalGroup) SignalGroupID data element under the MovementState data frame	RSU	ASN.1	CVE-SPAT-DR10-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
SPAT	(state-time-speed) MovementEventList data frame (a sequence of MovementEvent) under the MovementState data frame	RSU	ASN.1	CVE-SPAT-DR11-v1
SPAT	MovementEvent data frame under the MovementEventList data frame	RSU	ASN.1	CVE-SPAT-DR12-v1
SPAT	(eventState) MovementPhaseState data element under the MovementEvent data frame	RSU	ASN.1	CVE-SPAT-DR13-v1
SPAT	(timing) TimeChangeDetails data frame under the MovementEvent data frame	RSU	ASN.1	CVE-SPAT-DR14-v1
SPAT	(minEndTime) TimeMark data element under the TimeChangeDetails data frame	RSU	ASN.1	CVE-SPAT-DR15-v1
SPAT	(maxEndTime) TimeMark data element under the TimeChangeDetails data frame	RSU	ASN.1	CVE-SPAT-DR16-v1
SPAT	(likelyTime) TimeMark data element under the TimeChangeDetails data frame	RSU	ASN.1	CVE-SPAT-DR17-v1
SPAT	“states” field, which is a list of one or more MovementStates. The number of MovementStates shall correspond to the number of controller traffic phases that are currently active at the intersection.	RSU	ASN.1	CVE-SPAT-DR18-v1
SPAT	signalGroup shall be assigned number and is not necessarily based on the controller phase number	RSU	ASN.1	CVE-SPAT-DR19-v1
SPAT	maxEndTime or likelyTime	RSU	ASN.1	CVE-SPAT-DR20-v2
SPAT	maxEndTime if the traffic signal controller is running fixed-time, and if transmitted shall be equal to minEndTime	RSU	ASN.1	CVE-SPAT-DR21-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
SRM	(second) DSecond data element	RSU	ASN.1	CVE-SRM-DR3-v1
SRM	(requests) SignalRequestList (sequence of SignalRequestPackage) data frame	RSU	ASN.1	CVE-SRM-DR4-v1
SRM	SignalRequestPackage data frame under the SignalRequestList data frame	RSU	ASN.1	CVE-SRM-DR5-v1
SRM	(request) SignalRequest data frame under the SignalRequestPackage data frame	RSU	ASN.1	CVE-SRM-DR6-v1
SRM	(id) IntersectionReferenceID data frame under the SignalRequest data frame	RSU	ASN.1	CVE-SRM-DR7-v1
SRM	(id) IntersectionID data element under the intersectionReferenceID data frame	RSU	ASN.1	CVE-SRM-DR8-v1
SRM	(requestID) RequestID data element under the SignalRequest data frame	RSU	ASN.1	CVE-SRM-DR9-v1
SRM	(requestType) PriorityRequestType data element under the SignalRequest data frame	RSU	ASN.1	CVE-SRM-DR10-v1
SRM	(inBoundLane) IntersectionAccessPoint data frame under the SignalRequest data frame	RSU	ASN.1	CVE-SRM-DR11-v1
SRM	(lane) LaneID data element under the IntersectionAccessPoint data frame	RSU	ASN.1	CVE-SRM-DR12-v1
SRM	(approach) ApproachID data element under the IntersectionAccessPoint data frame	RSU	ASN.1	CVE-SRM-DR13-v1
SRM	(connection) LaneConnectionID data element under the IntersectionAccessPoint data frame	RSU	ASN.1	CVE-SRM-DR14-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
SRM	(requestor) RequestorDescription data frame	RSU	ASN.1	CVE-SRM-DR15-v1
SRM	(id) VehicleID data frame under the RequestroDescription data frame	RSU	ASN.1	CVE-SRM-DR16-v1
SRM	(entityID) TemporaryID under the VehicleID data frame	RSU	ASN.1	CVE-SRM-DR17-v1
SRM	(stationID) StationID under the VehicleID data frame	RSU	ASN.1	CVE-SRM-DR18-v1
SSM	(second) DSecond data element	OBU	ASN.1	CVE-SSM-DR3-v1
SSM	(status) SignalStatus data frame	OBU	ASN.1	CVE-SSM-DR4-v1
SSM	(sequence) MsgCount data element under the SignalStatus data frame	OBU	ASN.1	CVE-SSM-DR5-v1
SSM	(id) IntersectionReferenceID data element under the SignalStatus data frame	OBU	ASN.1	CVE-SSM-DR6-v1
SSM	(sigStatus) SignalStatusPackageList data frame (sequence of SignalStatusPackage) under the SignalStatus data frame	OBU	ASN.1	CVE-SSM-DR7-v1
SSM	SignalStatusPackage data frame under the SignalStatusPacakageList data frame	OBU	ASN.1	CVE-SSM-DR8-v1
SSM	(requestor) SignalRequestorInfo data frame under the SignalStatusPackage data frame	OBU	ASN.1	CVE-SSM-DR9-v1
SSM	(id) VehicleID under the SignalRequestorInfor data frame	OBU	ASN.1	CVE-SSM-DR10-v1
SSM	(request) RequestID under the SignalRequestorInfor data frame	OBU	ASN.1	CVE-SSM-DR11-v1

Functional Group	Data Element	Source System(s)	Translation Rules	Derived From (ReqID)
SSM	(sequenceNumber) MsgCount under the SignalRequestorInfor data frame	OBU	ASN.1	CVE-SSM-DR12-v1
SSM	(inboundOn) IntersectionAccessPoint data frame under the SignalStatusPackage data frame	OBU	ASN.1	CVE-SSM-DR13-v1
SSM	(lane) LaneID data element under the IntesectionAccessPoint data frame	OBU	ASN.1	CVE-SSM-DR14-v1
SSM	(approach) ApproachID data element under the IntesectionAccessPoint data frame	OBU	ASN.1	CVE-SSM-DR15-v1
SSM	(connection) LaneConnectionID data element under the IntesectionAccessPoint data frame	OBU	ASN.1	CVE-SSM-DR16-v1
SSM	(status) PrioritizationResponseStatus data element under the SignalStatusPackage data frame	OBU	ASN.1	CVE-SSM-DR17-v1

Source: City of Columbus

Appendix D. Mapped User Needs

The list below provides a mapping of each user need established in the ConOps with the requirements that were created based off that user defined in **Table 23**. This organization is intended for ease of use and quick reference during system design.

Table 23: Mapped User Needs

USER NEED:	**CVE-UN120-v02**	USER: **Light-Duty Vehicle Operator**
Title:	Vehicle in Blind Spot	
Description:	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1111-V02	V2V Safety	Blind Spot Warning	The BSW application should employ proven algorithms to issue an BSW alert.
Performance	CVE-PR1112-V01	V2V Safety	Blind Spot Warning	The BSW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1107-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is an OBU-equipped (remote) vehicle in the host vehicle's blind spot
Functional	CVE-FN1108-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3074-V01	V2V Safety	Blind Spot Warning	The Blind Spot Warning Application shall identify when a remote vehicle is within the

				blind spot (a configurable area to the rear right and rear left of a vehicle that moves with the vehicle) of a host vehicle, and is moving in the same direction of travel as the host vehicle by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued
Functional	CVE-FN3013-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Lane Change Warning/Blind Spot Warning alert
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.

User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED: **CVE-UN130-v02** USER: **Light-Duty Vehicle Operator**

Title: Stop on Red Signal

Description: A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.

Priority: Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1290-V02	V2I Safety	Red Light Violation Warning	The RLVW application should employ proven algorithms to issue an RLVW
Performance	CVE-PR1291-V01	V2I Safety	Red Light Violation Warning	The RLVW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1286-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when a red-light violation will occur at an RSU-equipped intersection
Functional	CVE-FN1312-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SPaT messages from SPaT data inputs
Functional	CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM

				messages from RTCM data inputs
Functional	CVE-FN1287-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also received a MAP message for the intersection that corresponds to the SPaT message.
Functional	CVE-FN3078-V01	V2I Safety	Red Light Violation Warning	The Red Light Violation Warning Application shall identify when a vehicle is expected to cross the stop bar during a red signal by using the following data items: 1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. Normal deceleration rate 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of SPaT to the time the alert is issued) 6. SPaT data (received from the RSU) 7. MAP data (received from the RSU) 8. RTCM data (received from the RSU)
Functional	CVE-FN3014-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Red Light Violation Warning alert
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.

User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED:	**CVE-UN140-v02**	USER: **Light-Duty Vehicle Operator**
Title:	School Zone/ Decrease Speed	
Description:	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1306-V02	V2I Safety	Reduced Speed School Zone	The RSSZ application should employ proven algorithms to issue an RSSZ warning
Performance	CVE-PR1307-V01	V2I Safety	Reduced Speed School Zone	The RSSZ application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)

Functional	CVE-FN1298-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when the OBU-equipped (host) vehicle will enter an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1310-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast (school zone) TIMs to an LDV OBU when configured to perform this function.
Functional	CVE-FN1299-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert when the OBU-equipped (host) vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1300-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify the school zone speed limit (J2735).
Functional	CVE-FN1301-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify when the school zone speed limit is active.
Functional	CVE-FN1302-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify the applicable regions of use geographical path (J2735).
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3079-V02	V2I Safety	Reduced Speed School Zone	The Reduced Speed School Zone Application shall identify when a host vehicle is expected to enter the school zone but not below the school zone speed limit (given its current location, motion, and expected braking rate) during active school zone hours by using the following data items:

				1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. TIM data (received from the RSU) 3. RTCM data (received from the RSU)
Functional	CVE-FN3015-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Reduced Speed School Zone alert
Functional	CVE-FN3080-V02	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.

User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.

USER NEED:	CVE-UN220-v02	USER: Emergency Vehicle Operator
Title:	Emergency Vehicle Intersection Priority	
Description:	An emergency vehicle operator needs preemption service at CV-equipped signalized intersections.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1497-V02	V2I Mobility	Emergency Vehicle Preemption	The EVP application should employ proven algorithms to enable emergency vehicle preemption
Performance	CVE-PR1531-V01	V2I Mobility	Emergency Vehicle Preemption	The EVP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1314-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SSM messages from SSM data inputs
Interface	CVE-IF1347-V01	Roadside Equipment	Roadside Unit	An RSU shall send information to request signal priority to the Traffic Signal Controller
Interface	CVE-IF1244-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive the flashing light status from the appropriate vehicle system
Interface	CVE-IF1245-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall receive the siren status from the appropriate vehicle system
Functional	CVE-FN1493-V01	V2I Mobility	Emergency Vehicle Preemption	An Emergency Vehicle OBU shall request to receive signal preemption at RSU-equipped intersections

Functional	CVE-FN1494-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall send an SRM to an RSU when it is less than a configurable amount of time away from arriving at the intersection it intends to request priority for
Functional	CVE-FN1495-V01	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall only request preemption in an SRM
Functional	CVE-FN1496-V02	Vehicle Onboard Equipment	Emergency Vehicle OBU	An Emergency Vehicle OBU shall cease sending SRMs for preemption to an RSU at a given intersection for a configurable amount of time after it has received an SSM from the RSU at that intersection containing the RequestID of the SRM broadcasted the host Emergency Vehicle
Functional	CVE-FN1500-V01	V2I Mobility	Emergency Vehicle Preemption	A request to receive signal preemption from an Emergency Vehicle OBU shall be high priority
Functional	CVE-FN1515-V01	V2I Mobility	General Priority/ Preemption	The Traffic Signal Controller shall next service a phase for a movement that is requested in a preemption SRM when the approach for the requested movement is red
Functional	CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs
Data	CVE-DR1477-V01	V2I Mobility	General Priority/ Preemption	The TSP Application shall require data from the SSM Message
Data	CVE-DR1478-V01	V2I mobility	General Priority/ Preemption	The TSP Application shall generate data for the SRM Message
Data	CVE-DR1533-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle
Functional	CVE-FN1498-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection

Functional	CVE-FN1499-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain information regarding the movement for which priority is being requested
Functional	CVE-FN1503-V01	V2I Mobility	General Priority/ Preemption	High priority requests to receive signal priority shall be serviced before low priority requests to receive signal priority
Functional	CVE-FN1504-V01	V2I Mobility	General Priority/ Preemption	Multiple high priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1505-V01	V2I Mobility	General Priority/ Preemption	Multiple low priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1508-V02	V2I Mobility	General Priority/ Preemption	Roadside Equipment shall place a priority request or a preemption request to the traffic signal controller for the movement specified in the SRM if the following conditions are concurrently met: 1. The SRM "BasicVehicleRole" matches against the locally-stored list of BasicVehicleRoles are authorized to receive signal priority or preemption. 2. The request is made during the time period when priority or preemption will be granted for the vehicle with the given BasicVehicleRole. 3. The requested movement is allowed for the vehicle with the given BasicVehicleRole. 4. The intersection ID in the SRM matches the intersection ID
Functional	CVE-FN1518-V02	V2I Mobility	General Priority/ Preemption	The Roadside Equipment shall receive output from the Traffic Signal Controller regarding the status of a priority request
Functional	CVE-FN1519-V01	V2I Mobility	General Priority/ Preemption	An RSU shall send an SSM to an HDV OBU containing the results of the requests made by one or more vehicles for a configurable period of time
Functional	CVE-FN1520-V02	V2I Mobility	General Priority/ Preemption	The Traffic CV Management System shall maintain a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request signal

				priority or preemption at each intersection.
Interface	CVE-IF1526-V01	V2I Mobility	Transit Signal Priority	The TSP Application shall receive data from the OBU's internal processing functions.
Interface	CVE-IF1561-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall receive data from the OBU's internal processing functions.

USER NEED:	**CVE-UN310-v02**	USER: **Heavy-Duty Vehicle Operator**
Title:	Heavy-Duty Vehicle Intersection Priority	
Description:	A heavy-duty vehicle operator needs priority service at CV-equipped signalized intersections.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1527-V02	V2I Mobility	Freight Signal Priority	The FSP application should employ proven algorithms to enable freight signal priority
Performance	CVE-PR1528-V01	V2I Mobility	Freight Signal Priority	The FSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Data	CVE-DR1477-V01	V2I Mobility	General Priority/ Preemption	The TSP Application shall require data from the SSM Message
Data	CVE-DR1478-V01	V2I mobility	General Priority/ Preemption	The TSP Application shall generate data for the SRM Message
Data	CVE-DR1533-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle
Functional	CVE-FN1498-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection

Functional	CVE-FN1499-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain information regarding the movement for which priority is being requested
Functional	CVE-FN1503-V01	V2I Mobility	General Priority/ Preemption	High priority requests to receive signal priority shall be serviced before low priority requests to receive signal priority
Functional	CVE-FN1504-V01	V2I Mobility	General Priority/ Preemption	Multiple high priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1505-V01	V2I Mobility	General Priority/ Preemption	Multiple low priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1508-V02	V2I Mobility	General Priority/ Preemption	Roadside Equipment shall place a priority request or a preemption request to the traffic signal controller for the movement specified in the SRM if the following conditions are concurrently met: 1. The SRM "BasicVehicleRole" matches against the locally-stored list of BasicVehicleRoles are authorized to receive signal priority or preemption. 2. The request is made during the time period when priority or preemption will be granted for the vehicle with the given BasicVehicleRole. 3. The requested movement is allowed for the vehicle with the given BasicVehicleRole. 4. The intersection ID in the SRM matches the intersection ID
Functional	CVE-FN1518-V02	V2I Mobility	General Priority/ Preemption	The Roadside Equipment shall receive output from the Traffic Signal Controller regarding the status of a priority request
Functional	CVE-FN1519-V01	V2I Mobility	General Priority/ Preemption	An RSU shall send an SSM to an HDV OBU containing the results of the requests made by one or more vehicles for a configurable period of time
Functional	CVE-FN1520-V02	V2I Mobility	General Priority/ Preemption	The Traffic CV Management System shall maintain a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request signal

				priority or preemption at each intersection.
Interface	CVE-IF1526-V01	V2I Mobility	Transit Signal Priority	The TSP Application shall receive data from the OBU's internal processing functions.
Interface	CVE-IF1561-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall receive data from the OBU's internal processing functions.
Functional	CVE-FN1502-V01	V2I Mobility	Freight Signal Priority	A request to receive signal priority from an HDV Vehicle OBU shall be low priority
Functional	CVE-FN1509-V01	V2I Mobility	General Priority/ Preemption	The Traffic Signal Controller shall grant an early green for a phase for a movement that is requested in a priority SRM when the approach for that movement is red or yellow
Functional	CVE-FN1510-V01	V2I Mobility	General Priority/ Preemption	The Traffic Signal Controller shall grant an extended green for a phase for a movement that is requested in a priority SRM when the approach for the requested movement is green
Functional	CVE-FN1479-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall request to receive signal priority at RSU-equipped intersections
Functional	CVE-FN1480-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall broadcast an SRM when approaching an RSU-equipped intersection
Functional	CVE-FN1481-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall broadcast an SRM when it is within a configurable distance of the intersection it intends to request priority for
Functional	CVE-FN1482-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall only request priority for movements is plans to make along a designated freight route (specific to the requesting HDV)
Functional	CVE-FN1483-V01	V2I Mobility	Freight Signal Priority	An HDV OBU shall only request priority in an SRM
Functional	CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs

Functional	CVE-FN1314-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SSM messages from SSM data inputs
Interface	CVE-IF1347-V01	Roadside Equipment	Roadside Unit	An RSU shall send information to request signal priority to the Traffic Signal Controller

USER NEED:	**CVE-UN410-v02**	USER: **Traffic Manager**
Title:	Monitor Performance	
Description:	A traffic manager needs the ability to monitor the status of traffic by obtaining data from the CVE.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1566-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Roadside Equipment shall send SRMs to the Traffic CV Management System as they are received from an OBU
Functional	CVE-FN1569-V02	V2I Mobility	Vehicle Data for Traffic Operations	The roadside equipment shall send SSMs to the Traffic CV Management System as they are generated by the roadside equipment.
Functional	CVE-FN1572-V02	V2I Mobility	Vehicle Data for Traffic Operations	The roadside equipment shall send SPaT messages to the Traffic CV Management System as they are generated by the roadside equipment
Functional	CVE-FN1580-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive BSMs sent by the roadside equipment
Functional	CVE-FN1581-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SRMs sent by the roadside equipment
Functional	CVE-FN1582-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SSMs sent by the roadside equipment
Functional	CVE-FN1437-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall transmit performance metrics (as configured by traffic management staff and defined in the Performance

				Measurement Plan) to the Smart Columbus OS
Functional	CVE-FN1438-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send TIMs to the Smart Columbus OS
Functional	CVE-FN1439-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send MAP messages to the Smart Columbus OS
Disposal	CVE-DP1465-V01	Common	Common	The CVE should remain operational after the completion of the deployment period
Data	CVE-DR1562-V02	V2I Mobility	Vehicle Data for Traffic Operations	The VDTO Application shall capture data from all messages transmitted or received by roadside equipment
Functional	CVE-FN1446-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide the VISA' functions of Validation, Integration, Sanitization (De-identification), and Aggregation of CV Data as defined in the U.S DOT SEMI ODE requirements (Reference TBR)
Functional	CVE-FN1453-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System should automate the generation of performance metrics as defined in the Performance Management Plan (TBD)
Functional	CVE-FN1454-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System should use CV data made available through the CVE to generate performance metrics as defined in the Performance Management Plan (TBD)
Functional	CVE-FN1564-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Roadside Equipment shall send BSMs to the Traffic CV Management System as they are received from an OBU
Functional	CVE-FN1583-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall receive SPaT Messages sent by the roadside equipment
Functional	CVE-FN1585-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store BSMs sent by the roadside equipment

Functional	CVE-FN1586-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SRMs sent by the roadside equipment
Functional	CVE-FN1587-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SSMs sent by the roadside equipment
Functional	CVE-FN1588-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SPaT messages sent by the roadside equipment
Functional	CVE-FN1589-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SAE J2735 TIMs generated by Traffic Management Staff
Functional	CVE-FN1590-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store all MAP messages that are input by the Traffic Manager
Functional	CVE-FN1591-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall make all stored data available to the Traffic Manager
Functional	CVE-FN2909-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate performance metrics (as configured by traffic management staff and as defined in the Performance Measurement Plan) from archived CV data
Performance	CVE-PR3029-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of archived CV data
Functional	CVE-FN3030-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide a means of allowing Traffic Management Staff to download archived CV data.
Performance	CVE-PR3031-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of backup archived CV data
Functional	CVE-FN3032-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the archived CV data backup storage

Performance	CVE-PR3033-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the backup archived CV data once per day.
Physical	CVE-PY3034-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall store archived CV data and backup archived CV data on separate physical storage devices.

USER NEED:	**CVE-UN420-v02**	USER: **Traffic Manager**
Title:	Update Static Messages	
Description:	A traffic manager needs the ability to update static messages within the CVE.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1442-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for TIM messages from Traffic Management Staff
Functional	CVE-FN1443-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for MAP messages from Traffic Management Staff
Functional	CVE-FN1444-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for configurable parameters (for functions on the TCVMS and on roadside equipment) from Traffic Management Staff
Functional	CVE-FN1447-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate TIM messages
Functional	CVE-FN1448-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate MAP messages
Functional	CVE-FN3002-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept inputs for all required elements of a MAP message via a user interface.
Functional	CVE-FN3001-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept inputs for all required elements of a TIM message via a user interface.

USER NEED:	CVE-UN430-v02	USER: **Traffic Manager**

Title:	Configure and Monitor Roadside Devices
Description:	A traffic manager needs to configure and monitor the status of roadside devices for operation within the CVE.
Priority:	Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1441-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall enable loading of MAP messages on roadside equipment
Functional	CVE-FN1442-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for TIM messages from Traffic Management Staff
Functional	CVE-FN1443-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for MAP messages from Traffic Management Staff
Functional	CVE-FN1444-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall accept input for configurable parameters (for functions on the TCVMS and on roadside equipment) from Traffic Management Staff
Functional	CVE-FN1445-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall make the status of RSUs available to Traffic Management Staff
Functional	CVE-FN1440-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall enable loading of TIMs on roadside equipment
Functional	CVE-FN1447-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate TIM messages
Functional	CVE-FN1448-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall generate MAP messages
Functional	CVE-FN1449-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the uptime status of RSUs

Functional	CVE-FN1452-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall make the status of all RSUs available to Traffic Management Staff
Functional	CVE-FN1463-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor tamper alert devices
Performance	CVE-PR1457-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall notify designated personnel within five minutes of limited connectivity. Note: Limited connectivity refers to a state when the Traffic CV Management System is not able to communicate with the RSU
Performance	CVE-PR1458-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall notify designated personnel within five minutes of a monitored function becoming unavailable
Security	CVE-SR1459-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall detect abnormal unauthorized activity on an IP connection.
Security	CVE-SR1460-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the DSRC communications performance.
Security	CVE-SR1461-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall monitor the data traffic usage to detect unapproved use of the IP connection.
Interface	CVE-IF3044-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall use a UI to geographically display the location of each RSU and RSU information to Traffic Management Staff
Functional	CVE-FN3045-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of a traffic signal controller cabinet that has been tampered with (based on the status of the tamper alert device)

Functional	CVE-FN3047-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is not running normally (off, not responding, in safe mode, etc.)
Functional	CVE-FN3049-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU that is offline
Functional	CVE-FN3051-V01	Traffic Management System	Traffic CV Management System	The Traffic CV Management System shall provide an alert to Traffic Management Staff via the UI to the location of an RSU (network entry vector) where unauthorized use has been detected and information regarding the unauthorized device.
Functional	CVE-FN3052-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall display different colored icons on the UI to indicate the real-time status of each RSU.
Functional	CVE-FN3053-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall allow Traffic Management Staff to select an RSU using the UI to reveal other RSU information (uptime percentage, tamper alert status, alert information, channel busy ratio, etc.)
Functional	CVE-FN3054-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall maintain a log of all alerts issued to traffic management staff
Functional	CVE-FN3055-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall display an alert icon next to a given RSU icon on the UI to indicate that an alert has been issued for that RSU.
Security	CVE-SR3128-V01	Roadside Equipment	Roadside Unit	An RSU shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).

USER NEED: **CVE-UN440-v02** USER: **Traffic Manager**

Title:	Data Archive Configuration
Description:	A traffic manager needs to configure the mechanism that is used to archive data.
Priority:	Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1585-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store BSMs sent by the roadside equipment
Functional	CVE-FN1586-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SRMs sent by the roadside equipment
Functional	CVE-FN1587-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SSMs sent by the roadside equipment
Functional	CVE-FN1588-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SPaT messages sent by the roadside equipment
Functional	CVE-FN1589-V02	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store SAE J2735 TIMs generated by Traffic Management Staff
Functional	CVE-FN1590-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall store all MAP messages that are input by the Traffic Manager
Functional	CVE-FN1591-V01	V2I Mobility	Vehicle Data for Traffic Operations	The Traffic CV Management System shall make all stored data available to the Traffic Manager
Performance	CVE-PR3029-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of archived CV data
Functional	CVE-FN3030-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall provide a means of allowing Traffic Management Staff to download archived CV data.
Performance	CVE-PR3031-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall be able to store at a minimum of 10 TB of backup archived CV data

Functional	CVE-FN3032-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the archived CV data backup storage
Performance	CVE-PR3033-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall copy all archived CV data into the backup archived CV data once per day.
Physical	CVE-PY3034-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall store archived CV data and backup archived CV data on separate physical storage devices.
Functional	CVE-FN3041-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall allow traffic management staff to configure the generation of performance measures from archived CV data (e.g. a recurring database query).

USER NEED:	**CVE-UN510-v02**	USER: **Transit Manager**
Title:	Service Management	
Description:	A transit manager needs to keep buses on schedule by reducing delays experienced at signalized intersections.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1530-V01	V2I Mobility	Transit Signal Priority	The TSP application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Performance	CVE-PR1529-V02	V2I Mobility	Transit Signal Priority	The TSP application should employ proven algorithms to enable transit signal priority
Functional	CVE-FN1488-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall request to receive signal priority at RSU-equipped intersections
Functional	CVE-FN1489-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall send an SRM to an RSU when it is within a configurable

				distance of the intersection it intends to request priority for
Functional	CVE-FN1490-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority in an SRM
Functional	CVE-FN1491-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority for movements along the route being traversed by that transit vehicle
Functional	CVE-FN1501-V01	V2I Mobility	Transit Signal Priority	A request to receive signal priority from a Transit Vehicle OBU shall be low priority
Functional	CVE-FN1492-V02	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall cease broadcasting SRMs for priority at a given intersection for a configurable amount of time after it has received an SSM from that intersection containing the RequestID of the SRM broadcasted the host Transit Vehicle
Functional	CVE-FN1509-V01	V2I Mobility	General Priority/ Preemption	The Traffic Signal Controller shall grant an early green for a phase for a movement that is requested in a priority SRM when the approach for that movement is red or yellow
Functional	CVE-FN1510-V01	V2I Mobility	General Priority/ Preemption	The Traffic Signal Controller shall grant an extended green for a phase for a movement that is requested in a priority SRM when the approach for the requested movement is green
Functional	CVE-FN1314-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates SSM messages from SSM data inputs
Interface	CVE-IF1347-V01	Roadside Equipment	Roadside Unit	An RSU shall send information to request signal priority to the Traffic Signal Controller
Functional	CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs
Data	CVE-DR1477-V01	V2I Mobility	General Priority/ Preemption	The TSP Application shall require data from the SSM Message

Data	CVE-DR1478-V01	V2I mobility	General Priority/ Preemption	The TSP Application shall generate data for the SRM Message
Data	CVE-DR1533-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle
Functional	CVE-FN1498-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection
Functional	CVE-FN1499-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain information regarding the movement for which priority is being requested
Functional	CVE-FN1503-V01	V2I Mobility	General Priority/ Preemption	High priority requests to receive signal priority shall be serviced before low priority requests to receive signal priority
Functional	CVE-FN1504-V01	V2I Mobility	General Priority/ Preemption	Multiple high priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1505-V01	V2I Mobility	General Priority/ Preemption	Multiple low priority requests shall be serviced in the order in which they are received
Functional	CVE-FN1508-V02	V2I Mobility	General Priority/ Preemption	Roadside Equipment shall place a priority request or a preemption request to the traffic signal controller for the movement specified in the SRM if the following conditions are concurrently met: 1. The SRM "BasicVehicleRole" matches against the locally-stored list of BasicVehicleRoles are authorized to receive signal priority or preemption. 2. The request is made during the time period when priority or preemption will be granted for the vehicle with the given BasicVehicleRole. 3. The requested movement is allowed for the vehicle with the given BasicVehicleRole. 4. The intersection ID in the SRM matches the intersection ID

Functional	CVE-FN1518-V02	V2I Mobility	General Priority/ Preemption	The Roadside Equipment shall receive output from the Traffic Signal Controller regarding the status of a priority request
Functional	CVE-FN1519-V01	V2I Mobility	General Priority/ Preemption	An RSU shall send an SSM to an HDV OBU containing the results of the requests made by one or more vehicles for a configurable period of time
Functional	CVE-FN1520-V02	V2I Mobility	General Priority/ Preemption	The Traffic CV Management System shall maintain a modifiable list of SAE J2735 SRM "BasicVehicleRole" as authorized to request signal priority or preemption at each intersection.
Interface	CVE-IF1526-V01	V2I Mobility	Transit Signal Priority	The TSP Application shall receive data from the OBU's internal processing functions.
Interface	CVE-IF1561-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall receive data from the OBU's internal processing functions.

USER NEED:	**CVE-UN520-v02**	USER: **Transit Manager**
Title:	On Schedule Status	
Description:	A transit manager needs to know if any of its fleet in operation is behind schedule resulting from heavy traffic or increased passenger loads.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1488-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall request to receive signal priority at RSU-equipped intersections
Functional	CVE-FN1489-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall send an SRM to an RSU when it is within a configurable distance of the intersection it intends to request priority for
Functional	CVE-FN1490-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority in an SRM
Functional	CVE-FN1491-V01	V2I Mobility	Transit Signal Priority	A Transit Vehicle OBU shall only request priority for

				movements along the route being traversed by that transit vehicle
Functional	CVE-FN1501-V01	V2I Mobility	Transit Signal Priority	A request to receive signal priority from a Transit Vehicle OBU shall be low priority
Performance	CVE-PR1529-V02	V2I Mobility	Transit Signal Priority	The TSP application should employ proven algorithms to enable transit signal priority
Functional	CVE-FN1498-V01	V2I Mobility	General Priority/ Preemption	The SRM shall contain the intersection ID that is provided in the MAP message for the priority requested intersection
Data	CVE-DR1478-V01	V2I mobility	General Priority/ Preemption	The TSP Application shall generate data for the SRM Message
Data	CVE-DR1477-V01	V2I Mobility	General Priority/ Preemption	The TSP Application shall require data from the SSM Message
Data	CVE-DR1533-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	The TVIER Application shall capture data from V2V Safety and V2I Safety applications deployed on the Transit Vehicle

USER NEED:	**CVE-UN530-v02**	USER: **Transit Manager**
Title:	Monitor Transit Vehicle Interactions	
Description:	A transit manager needs to assess interactions between transit vehicles and other CV-equipped vehicles on the roadway.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1551-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the transit vehicle OBU broadcasts an SRM
Functional	CVE-FN1557-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the start time of the event (UTC)
Functional	CVE-FN1558-V01	V2I Mobility	Transit Vehicle Interaction	A Transit Vehicle Interaction Event shall consist of the end time of the event (UTC) (in the

			Event Recording	case where multiple events of the same warning are issued based on messages received from the same vehicle or intersection within a configurable amount of time)
Functional	CVE-FN1559-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast BSMs) from a configurable amount of time before the start time of the event
Functional	CVE-FN1560-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of all locally stored messages (SPaT, MAP, received BSMs, broadcast BSMs) from a configurable amount of time after the end time of the event
Functional	CVE-FN1536-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is emergency braking ahead by an OBU-equipped (remote) vehicle
Functional	CVE-FN1537-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a forward collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1538-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is an intersection collision detected with another OBU-equipped (remote) vehicle
Functional	CVE-FN1540-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a lane change collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1541-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall log a Transit Vehicle Interaction Event when the transit vehicle (host) runs a red light at an RSU-equipped intersection
Functional	CVE-FN1542-V01	V2I Mobility	Transit Vehicle Interaction	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle will

			Event Recording	enter an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1543-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
Interface	CVE-IF1473-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall make Transit Vehicle Interaction Events available to Transit Management Staff
Functional	CVE-FN1534-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall determine when to record a Transit Vehicle Interaction Event. Note: A Transit Vehicle Interaction Event contains the type of event along with a log of BSMs sent/received before and after the event.
Functional	CVE-FN1535-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall not issue alerts to the transit vehicle operator
Functional	CVE-FN1544-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs received in local memory for a configurable amount of time.
Functional	CVE-FN1545-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SPaT messages received in local memory for a configurable amount of time.
Functional	CVE-FN1546-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any MAP messages received in local memory for a configurable amount of time (configuration should allow MAP messages to be stored for 7 days)
Functional	CVE-FN1547-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs broadcast in local memory for a configurable amount of time.

Functional	CVE-FN1550-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the type of event (emergency braking ahead, forward collision imminent, intersection movement, blind spot, lane change, red light violation, school zone speed limit, priority request)
Functional	CVE-FN1554-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove Transit Vehicle Interaction Event data with the oldest start times from memory until it is able to log a newly received interaction event
Functional	CVE-FN1555-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall upload all Transit Vehicle Interaction Event data to the Transit CV Management System when it connects to the vehicle's regular data upload service.
Functional	CVE-FN1556-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove all Transit Vehicle Interaction Event data from memory once uploaded to the Transit CV Management System.
Functional	CVE-FN1548-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SRMs broadcast in local memory for a configurable amount of time.
Functional	CVE-FN1549-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SSMs received in local memory for a configurable amount of time.
Performance	CVE-PR3035-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of archived Transit Vehicle Interaction Events
Performance	CVE-PR3036-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of backup archived Transit Vehicle Interaction Events

Performance	CVE-PR3037-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the backup archived Transit Vehicle Interaction Events once per day.
Physical	CVE-PY3038-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall store archived Transit Vehicle Interaction Events and backup archived Transit Vehicle Interaction Events on separate physical storage devices.
Functional	CVE-FN3039-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall provide a means of allowing Transit Management Staff to download archived Transit Vehicle Interaction Events.
Functional	CVE-FN3040-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the archived CV data backup storage
Functional	CVE-FN3081-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives
Functional	CVE-FN3082-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if there is emergency braking ahead for each BSM it receives.
Functional	CVE-FN3083-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a forward collision is imminent for each BSM it receives
Functional	CVE-FN3084-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if an intersection collision is imminent for each BSM it receives.
Functional	CVE-FN3085-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a lane change collision is imminent for each BSM it receives.

Functional	CVE-FN3086-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also received a MAP message for the intersection that corresponds to the SPaT message.
Functional	CVE-FN3087-V02	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.
Performance	CVE-PR2913-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall be capable of holding 4 GB of interaction event data.

USER NEED:	CVE-UN540-v02	USER: Transit Manager
Title:	Transit Vehicle Operator CVE Output	
Description:	A Transit Manager needs to understand the number of alert and warnings that will be issued to Transit Vehicle Operators.	
Priority:	Desirable	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1534-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall determine when to record a Transit Vehicle Interaction Event. Note: A Transit Vehicle Interaction Event contains the type of event along with a log of BSMs sent/received before and after the event.
Functional	CVE-FN1535-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall not issue alerts to the transit vehicle operator
Functional	CVE-FN1536-V01	V2I Mobility	Transit Vehicle Interaction	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is emergency

			Event Recording	braking ahead by an OBU-equipped (remote) vehicle
Functional	CVE-FN1537-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a forward collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1538-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when there is an intersection collision detected with another OBU-equipped (remote) vehicle
Functional	CVE-FN1540-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when a lane change collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1541-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall log a Transit Vehicle Interaction Event when the transit vehicle (host) runs a red light at an RSU-equipped intersection
Functional	CVE-FN1542-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle will enter an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1543-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall log a Transit Vehicle Interaction Event when the vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1544-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs received in local memory for a configurable amount of time.
Functional	CVE-FN1545-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any SPaT messages received in local memory for a configurable amount of time.

Functional	CVE-FN1546-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any MAP messages received in local memory for a configurable amount of time (configuration should allow MAP messages to be stored for 7 days)
Functional	CVE-FN1547-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall store any BSMs broadcast in local memory for a configurable amount of time.
Functional	CVE-FN1550-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle Interaction Event shall consist of the type of event (emergency braking ahead, forward collision imminent, intersection movement, blind spot, lane change, red light violation, school zone speed limit, priority request)
Functional	CVE-FN1554-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove Transit Vehicle Interaction Event data with the oldest start times from memory until it is able to log a newly received interaction event
Functional	CVE-FN1555-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall upload all Transit Vehicle Interaction Event data to the Transit CV Management System when it connects to the vehicle's regular data upload service.
Functional	CVE-FN1556-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU shall remove all Transit Vehicle Interaction Event data from memory once uploaded to the Transit CV Management System.
Interface	CVE-IF1473-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall make Transit Vehicle Interaction Events available to Transit Management Staff
Performance	CVE-PR3035-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of archived Transit Vehicle Interaction Events

Performance	CVE-PR3036-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall be able to store at a minimum of 5 TB of backup archived Transit Vehicle Interaction Events
Performance	CVE-PR3037-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the backup archived Transit Vehicle Interaction Events once per day.
Physical	CVE-PY3038-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall store archived Transit Vehicle Interaction Events and backup archived Transit Vehicle Interaction Events on separate physical storage devices.
Functional	CVE-FN3039-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall provide a means of allowing Transit Management Staff to download archived Transit Vehicle Interaction Events.
Functional	CVE-FN3040-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall copy all archived Transit Vehicle Interaction Events into the archived CV data backup storage
Functional	CVE-FN3081-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a vehicle is in its blind spot for each BSM it receives
Functional	CVE-FN3082-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if there is emergency braking ahead for each BSM it receives.
Functional	CVE-FN3083-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a forward collision is imminent for each BSM it receives
Functional	CVE-FN3084-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if an intersection collision is imminent for each BSM it receives.

Functional	CVE-FN3085-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if a lane change collision is imminent for each BSM it receives.
Functional	CVE-FN3086-V01	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will run a red light for each SPaT message it receives, provided it has also received a MAP message for the intersection that corresponds to the SPaT message.
Functional	CVE-FN3087-V02	V2I Mobility	Transit Vehicle Interaction Event Recording	A Transit Vehicle OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.
Performance	CVE-PR2913-V01	Vehicle Onboard Equipment	Transit Vehicle OBU	A Transit Vehicle OBU shall be capable of holding 4 GB of interaction event data.

USER NEED:	**CVE-UN610-v02**	USER: **Pedestrian**
Title:	School Zone Pedestrian Safety	
Description:	A pedestrian in a school zone needs vehicles to travel at or below the school zone speed limit during active school zone hours.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1316-V02	Roadside Equipment	Roadside Unit	Select RSUs in/around designated school zones (Linden STEM Academy and Our Lady of Peace School) shall broadcast TIMs only when the school zone flashing signal is flashing.
Functional	CVE-FN1298-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when the OBU-equipped (host) vehicle will enter an RSU-equipped school zone over the active school zone speed limit

Functional	CVE-FN1299-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert when the OBU-equipped (host) vehicle is inside of an RSU-equipped school zone over the active school zone speed limit
Functional	CVE-FN1300-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify the school zone speed limit (J2735).
Functional	CVE-FN1301-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify when the school zone speed limit is active.
Functional	CVE-FN1302-V02	V2I Safety	Reduced Speed School Zone	The LDV OBU (host) shall parse received TIMs to identify the applicable regions of use geographical path (J2735).
Performance	CVE-PR1306-V02	V2I Safety	Reduced Speed School Zone	The RSSZ application should employ proven algorithms to issue an RSSZ warning
Performance	CVE-PR1307-V01	V2I Safety	Reduced Speed School Zone	The RSSZ application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1310-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast (school zone) TIMs to an LDV OBU when configured to perform this function.
Functional	CVE-FN1313-V01	Roadside Equipment	Roadside Unit	An RSU shall have access to a function that generates RTCM messages from RTCM data inputs
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3079-V02	V2I Safety	Reduced Speed School Zone	The Reduced Speed School Zone Application shall identify when a host vehicle is expected to enter the school zone but not below the school zone speed limit (given its current location, motion, and expected braking rate) during active school zone hours by using the following data items:

				1. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 2. TIM data (received from the RSU) 3. RTCM data (received from the RSU)
Functional	CVE-FN3015-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Reduced Speed School Zone alert
Functional	CVE-FN3080-V02	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if the OBU-equipped (host) vehicle will be speeding in a school zone once per second, provided it is receiving a school zone TIM.

USER NEED:	CVE-UN710-v02	USER: **Network Manager**
Title:	Maintain Connectivity	
Description:	A Network Manager needs to maintain connectivity between CVE devices that communicate via backhaul.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1321-V01	Roadside Equipment	Roadside Unit	An RSU shall support IPv6 tunneling over IPv4.
Security	CVE-SR3129-V01	Roadside Equipment	Roadside Unit	An RSU shall implement a firewall blocking all IP access from devices to any IP address other than those approved for specific applications.

USER NEED:	CVE-SN810-v02	USER: **General System**
Title:	Operating System Connectivity	
Description:	A roadside device needs to be connected to the Operating System.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description

Functional	CVE-FN1437-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall transmit performance metrics (as configured by traffic management staff and defined in the Performance Measurement Plan) to the Smart Columbus OS
Functional	CVE-FN1438-V02	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send TIMs to the Smart Columbus OS
Functional	CVE-FN1439-V01	Traffic Management Center	Traffic CV Management System	The Traffic CV Management System shall send MAP messages to the Smart Columbus OS
Interface	CVE-IF1472-V01	Transit Management Center	Transit CV Management System	The Transit CV Management System shall send Transit Vehicle Interaction Events to the Smart Columbus OS

USER NEED:	**CVE-SN820-v02**	USER: **General System**
Title:	Roadside Device Wireless Communications Security	
Description:	A roadside device needs to be connected to the SCMS.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1325-V01	Roadside Equipment	Roadside Unit	It shall be possible for a system administrator with the appropriate permissions to configure the RSU to request application certificates with only designated geographic locations.
Functional	CVE-FN1333-V01	Roadside Equipment	Roadside Unit	An RSU shall not create or transmit messages if the 1609.2 certificates do now contain the permissions for the corresponding PSID.
Interface	CVE-IF1353-V01	Roadside Equipment	Roadside Unit	The RSU-SCMS interface shall allow an RSU to request application certificates with different contents from the current ones during the lifetime of the current ones.

Interface	CVE-IF1354-V01	Roadside Equipment	Roadside Unit	Communication between the RSU and an SCMS shall operate in an encrypted, end-to-end connection in accordance with the selected SCMS interface. (Note: An SCMS interface should not need any further security.)
Security	CVE-SR1373-V01	Roadside Equipment	Roadside Unit	RSUs shall support role-based authentication to enable physical access.
Security	CVE-SR3131-V01	Roadside Equipment	Roadside Unit	An RSU shall delete old certificates if it has been moved to another intersection.
Security	CVE-SR3127-V01	Roadside Equipment	Roadside Unit	An RSU 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.
Security	CVE-SR3125-V01	Roadside Equipment	Roadside Unit	An RSU shall support setting the certificate geographic region to be requested for application certificates.
Security	CVE-SR3124-V01	Roadside Equipment	Roadside Unit	An RSU shall verify a DSRC message if a device identifies the message as containing a new DE_TemporaryID value.

USER NEED:	**CVE-SN830-v02**	USER: **General System**
Title:	In-Vehicle Positioning	
Description:	An in-vehicle device needs to have available position information.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1205-V01	Vehicle Onboard Equipment	General OBU	An OBU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.

USER NEED:	**CVE-SN840-v02**	USER: **General System**
Title:	In-Vehicle Time Synchronization	

Description:	An in-vehicle device needs to be synchronized with a common time source.
Priority:	Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1204-V02	Vehicle Onboard Equipment	General OBU	An OBU shall acquire time from the Location and Time Service (LTS) interface in accordance with J2945/1 section 6.2.4.

USER NEED:	CVE-SN850-v02	USER: General System
Title:	Roadside Time Synchronization	
Description:	A roadside device needs to be synchronized with a common time source.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1308-V01	Roadside Equipment	Roadside Unit	An RSU shall acquire time from the LTS interface in accordance with J2945/1 section 6.2.4.

USER NEED:	CVE-SN860-v02	USER: General System
Title:	Position Correction	
Description:	A roadside device needs to have access to position correction information.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1309-V01	Roadside Equipment	Roadside Unit	An RSU shall acquire location from the LTS interface in accordance with J2945/1 section 6.2.1.
Functional	CVE-FN1113-V01	Roadside Equipment	Roadside Unit	An RSU shall obtain position correction information from a Continuously Operating Reference Station (CORS) for

				packaging and broadcasting as the RTCM message.

USER NEED:	CVE-SN870-v02	USER: General System
Title:	In-Vehicle Device Wireless Communications Security	
Description:	An in-vehicle device needs to be able to maintain access control lists and obtain new certificates when necessary.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Functional	CVE-FN1319-V02	Roadside Equipment	Roadside Unit	An RSU shall broadcast the WSA on channel 180
Functional	CVE-FN1186-V01	Vehicle Onboard Equipment	General OBU	An OBU shall not continue to start up and will log an error if the host processor determines it is not in a known good software state on boot up.
Security	CVE-SR1254-V01	Vehicle Onboard Equipment	General OBU	The OBU shall cease transmission of BSMs if the OBU determines that it has been blacklisted. Note: Blacklists detail devices that should not be trusted in the system or network
Security	CVE-SR1255-V01	Vehicle Onboard Equipment	General OBU	The OBU shall prevent incoming messages with invalid conditions per criteria in the IEEE 1609.2 from being acted on.
Security	CVE-SR1256-V01	Vehicle Onboard Equipment	General OBU	The OBU Vehicle Communications link shall have communications security to ensure the authenticity of all its messages in accordance to the standards prescribed by wireless messaging security standards.
Security	CVE-SR1257-V01	Vehicle Onboard Equipment	General OBU	The OBU shall carry out plausibility checking on the remote vehicle BSM data.
Security	CVE-SR1258-V01	Vehicle Onboard Equipment	General OBU	The OBU shall indicate successful receipt of the pseudonym certificates.

Security	CVE-SR1259-V01	Vehicle Onboard Equipment	General OBU	When the OBU has no valid BSM signing certificates, it shall store the log file entries as IEEE 1609.2 data of type unsecured.
Security	CVE-SR1261-V01	Vehicle Onboard Equipment	General OBU	The OBU shall obtain certificates via IPv6 connectivity through the RSU.
Security	CVE-SR1262-V01	Vehicle Onboard Equipment	General OBU	An OBU shall communicate using SNMPv3 with SNMP messages protected by being sent over TLS.
Security	CVE-SR1263-V01	Vehicle Onboard Equipment	General OBU	An OBU shall support establishment of a standard TLS-based VPN with client authentication for communication to the Traffic CV Management System, with a long-term client cert and a single CA cert trusted to authorize connections from the Traffic CV Management System.
Security	CVE-SR1264-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify received messages per IEEE 1609.2 and per the relevant security profiles before using them for operations in any application.
Security	CVE-SR1265-V01	Vehicle Onboard Equipment	General OBU	An OBU shall provide real-time tamper data which indicates that the device has been tampered with (e.g. opening of the case).
Security	CVE-SR1266-V01	Vehicle Onboard Equipment	General OBU	An OBU 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.
Security	CVE-SR1267-V01	Vehicle Onboard Equipment	General OBU	An OBU shall only transmit messages for any usage scenario if the usage scenario requires it to use 1609.2 certificates and it currently has valid certificates for that usage scenario
Security	CVE-SR1268-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when a device identifies the message as

				containing a new DE_TemporaryID value.
Security	CVE-SR1269-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when the message results in the issuance of an advisory, warning, or alert
Security	CVE-SR1270-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when 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
Security	CVE-SR1271-V01	Vehicle Onboard Equipment	General OBU	An OBU shall verify a DSRC message when other potential threat situations such as red-light violations, and other safety applications are active

USER NEED:	**CVE-UN110-v02**	USER: **Light-Duty Vehicle Operator**
Title:	Vehicle Collision Avoidance	
Description:	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN1207-V01	Vehicle Onboard Equipment	General OBU	The OBU may capture vehicle brake status over the OBU-OBD-II interface to the host vehicle
Functional	CVE-FN3013-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Lane Change Warning/Blind Spot Warning alert
Functional	CVE-FN3012-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue an Intersection Movement Assist alert
Functional	CVE-FN3011-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Forward Collision Warning alert

Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED:	**CVE-UN111-v02**	USER: **Light-Duty Vehicle Operator**
Title:	Emergency Braking Ahead	
Description:	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1119-V02	V2V Safety	Emergency Electronic Brake Light Warning	The EEBL application should employ proven algorithms to issue an EEBL alert.
Performance	CVE-PR1120-V01	V2V Safety	Emergency Electronic Brake Light Warning	The EEBL application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1115-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when there is emergency braking ahead by an OBU-equipped (remote) vehicle
Functional	CVE-FN1116-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if there is emergency braking ahead for each BSM it receives
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN1207-V01	Vehicle Onboard Equipment	General OBU	The OBU may capture vehicle brake status over the OBU-OBD-II interface to the host vehicle
Functional	CVE-FN3075-V01	V2V Safety	Emergency Electronic Brake Light	The Emergency Electronic Brake Light Application shall identify when an emergency braking maneuver has been detected by a remote vehicle, the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS,

				OBU Onboard sensors, and/or the host vehicle CANBus) 3. Normal deceleration rate 4. Perception/reaction time 5. Expected DSRC Transmission Latency 6. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED: **CVE-UN112-v02** USER: **Light-Duty Vehicle Operator**

Title:	Safe Following Distance
Description:	A light-duty vehicle operator needs to be informed if their following distance is too close.
Priority:	Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1127-V02	V2V Safety	Forward Collision Warning	The FCW application should employ proven algorithms to issue an FCW alert
Performance	CVE-PR1128-V01	V2V Safety	Forward Collision Warning	The FCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1122-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the LDV HMI when a forward collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1124-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a forward collision is imminent for each BSM it receives
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3073-V01	V2V Safety	Forward Collision Warning	The Forward Collision Warning Application shall identify when the host vehicle is within a calculated distance threshold (a function of the speed of the host vehicle and the remote vehicle) and is directly ahead in the same lane (not necessarily moving in the same direction of travel) by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU)

				2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Normal deceleration rate 4. Perception/reaction time 5. Expected DSRC Transmission Latency 6. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)
Functional	CVE-FN3011-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Forward Collision Warning alert
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.

User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED:	**CVE-UN113-v02**	USER: **Light-Duty Vehicle Operator**
Title:	Monitor Vehicle Trajectories at Intersection	
Description:	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.	
Priority:	Essential	

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1135-V02	V2V Safety	Intersection Movement Assist	The IMA application should employ proven algorithms to issue an IMA alert
Performance	CVE-PR1136-V01	V2V Safety	Intersection Movement Assist	The IMA application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1131-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when an intersection collision is imminent with another OBU-equipped (remote) vehicle
Functional	CVE-FN1132-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if an intersection collision is imminent for each BSM it receives
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3077-V01	V2V Safety	Intersection Movement Assist	The Intersection Movement Assist Application shall identify when the host vehicle has a trajectory (based on position, speed, acceleration) that may interfere with remote) vehicle trajectory in a side impact fashion, and the host vehicle is within a calculated distance threshold

				(a function of the speed of the host vehicle) by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued)
Functional	CVE-FN3012-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue an Intersection Movement Assist alert
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.
User Need	CVE-UN114-v02		Lane Change Collision Warning	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be

				red when the vehicle is expected to enter a CV-equipped intersection.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

USER NEED:	**CVE-UN114-v02**	USER: **Light-Duty Vehicle Operator**

Title:	Lane Change Collision Warning
Description:	A light-duty vehicle operator needs to be warned if they are changing lanes into the path of another CV-equipped vehicle.
Priority:	Essential

Related Requirements, Constraints, and System Interfaces

Type	Identifier	Functional Group	Sub-Component	Description
Performance	CVE-PR1142-V02	V2V Safety	Lane Change Warning	The LCW application should employ proven algorithms to issue an LCW alert
Performance	CVE-PR1143-V01	V2V Safety	Lane Change Warning	The LCW application shall meet TRL 6 criteria (has been tested in a realistic environment outside of a laboratory and satisfies operational requirements when confronted with realistic problems)
Functional	CVE-FN1138-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall issue an alert to the LDV Operator via the HMI when it is changing lanes into another OBU-equipped (remote) vehicle
Functional	CVE-FN1139-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU (host) shall determine if a lane change collision is imminent for each BSM it receives
Interface	CVE-IF1246-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall issue alerts to the LDV Operator via an HMI
Functional	CVE-FN3076-V01	V2V Safety	Lane Change Warning	The Lane Change Warning Application shall identify when a host vehicle is changing lanes into a remote vehicle, and is moving in the same direction of travel as the host

				vehicle by using the following data items: 1. Location and motion data for the remote vehicle (BSM data received from the remote OBU) 2. Location and motion data for the host vehicle (from GPS, OBU Onboard sensors, and/or the host vehicle CANBus) 3. Perception/reaction time 4. Expected DSRC Transmission Latency 5. Expected processing time (time from receipt of BSM from remote OBU to the time the alert is issued
Functional	CVE-FN3013-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	An LDV OBU shall determine when to issue a Lane Change Warning/Blind Spot Warning alert
Performance	CVE-PR3017-V01	Vehicle Onboard Equipment	Light-Duty Vehicle OBU	The LDV OBU HMI shall present an alert to the LDV Operator in a succinct manner while the LDV Operator is engaged in the driving task to minimize the 'eyes off the road' time.
User Need	CVE-UN120-v02		Vehicle in Blind Spot	A light-duty vehicle operator needs to be notified if another CV-equipped vehicle is in their blind spot.
User Need	CVE-UN113-v02		Monitor Vehicle Trajectories at Intersection	A light-duty vehicle operator approaching an intersection needs to be aware of CV-equipped vehicles on intersecting trajectories.
User Need	CVE-UN110-v02		Vehicle Collision Avoidance	A light-duty vehicle operator needs to know of an event that may lead to a crash with a CV-equipped vehicle.
User Need	CVE-UN111-v02		Emergency Braking Ahead	A light-duty vehicle operator needs to know when a CV-equipped vehicle in its path of travel is braking in an emergency fashion.
User Need	CVE-UN112-v02		Safe Following Distance	A light-duty vehicle operator needs to be informed if their following distance is too close.

User Need	CVE-UN130-v02		Stop on Red Signal	A light-duty vehicle operator needs to know if a signal will be red when the vehicle is expected to enter a CV-equipped intersection.
User Need	CVE-UN140-v02		School Zone/ Decrease Speed	A light-duty vehicle operator needs to know when they are exceeding the school zone speed limit in an active school zone that is CV equipped.

Source: City of Columbus

Appendix E. Other Mapped Relations

The list below provides a mapping of all the relations established for system constraints, system interfaces along with a mapping of requirements related to other requirements. These relations were created based off the user needs defined in the project ConOps. This organization is intended for ease of use and quick reference during system design.

Table 24: Constraint Relations

Constraint ID	Reference	Requirement ID	
CVE-CN1645-V01	Constraint 1	CVE-MT1364-V01 CVE-FN1335-V01 CVE-MT1593-V01 CVE-MT1594-V01 CVE-MT1595-V01 CVE-MT1596-V01 CVE-MT1597-V01 CVE-MT1598-V01 CVE-MT1599-V01	CVE-MT1600-V01 CVE-MT1602-V01 CVE-MT1603-V01 CVE-MT1604-V01 CVE-RG1605-V01 CVE-RG1606-V01 CVE-RG1607-V01 CVE-CN1663-V01
CVE-CN1647-V01	Constraint 3	CVE-PR1112-V01 CVE-PR1120-V01 CVE-PR1128-V01 CVE-PR1136-V01 CVE-PR1143-V01	CVE-PR1291-V01 CVE-PR1307-V01 CVE-PR1528-V01 CVE-PR1530-V01 CVE-PR1531-V01
CVE-CN1648-V01	Constraint 4	CVE-DR1375-V02 CVE-FN1208-V01 CVE-FN1209-V01 CVE-FN1311-V01 CVE-PR1369-V01 CVE-PY1372-V01 CVE-FN1333-V01 CVE-FN1308-V01 CVE-FN1309-V01 CVE-PR3009-V01 CVE-DR3005-V01 CVE-PR3003-V01	CVE-SR1256-V01 CVE-DR1294-V02 CVE-DR1296-V02 CVE-DR3089-V02 CVE-DR3090-V02 CVE-DR3091-V02 CVE-DR3093-V02 CVE-DR3092-V02 CVE-SR3130-V01 CVE-SR3127-V01 CVE-SR3123-V01
CVE-CN1649-V01	Constraint 5	CVE-FN1185-V01	
CVE-CN1650-V01	Constraint 6	CVE-FN1185-V01	
CVE-CN1651-V01	Constraint 7	CVE-FN1185-V01	
CVE-CN1652-V01	Constraint 8	CVE-FN1185-V01	
CVE-CN1653-V01	Constraint 9	CVE-FN1185-V01	
CVE-CN1654-V01	Constraint 10	CVE-FN1185-V01	
CVE-CN1655-V01	Constraint 11	CVE-FN1185-V01	
CVE-CN1656-V01	Constraint 12	CVE-FN1185-V01	
CVE-CN1657-V01	Constraint 13	CVE-FN1185-V01	
CVE-CN1658-V01	Constraint 14	CVE-FN1185-V01	

Constraint ID	Reference	Requirement ID	
CVE-CN1659-V01	Constraint 15	CVE-FN1317-V01	CVE-PY1370-V01
		CVE-IF1348-V01	CVE-PY1371-V01
		CVE-IF1349-V01	CVE-MT1364-V01
CVE-CN1660-V01	Constraint 16	CVE-PR1119-V02	CVE-PR1527-V02
		CVE-PR1120-V01	CVE-PR1530-V01
		CVE-PR1127-V02	CVE-PR1528-V01
		CVE-PR1128-V01	CVE-PR1306-V02
		CVE-PR1135-V02	CVE-PR1307-V01
		CVE-PR1136-V01	CVE-PR1529-V02
		CVE-PR1142-V02	CVE-FN3073-V01
		CVE-PR1143-V01	CVE-FN3074-V01
		CVE-PR1111-V02	CVE-FN3075-V01
		CVE-PR1112-V01	CVE-FN3077-V01
		CVE-PR1290-V02	CVE-FN3076-V01
		CVE-PR1291-V01	CVE-FN3078-V01
		CVE-FN1497-V02	CVE-FN3079-V02
		CVE-PR1531-V01	
CVE-CN1661-V01	Constraint 17	CVE-FN1511-V01	CVE-FN1514-V01
		CVE-FN1512-V01	CVE-FN1516-V01
		CVE-FN1513-V01	CVE-FN1517-V01
CVE-CN1662-V01	Constraint 18	CVE-FN1524-V02	CVE-FN1525-V02
CVE-CN1663-V01	Constraint 19	CVE-FN1184-V01	CVE-FN3030-V01
		CVE-MT1252-V01	CVE-PR3029-V01
		CVE-MT1253-V01	CVE-FN3047-V01
		CVE-FN1325-V01	CVE-FN3049-V01
		CVE-FN3001-V02	CVE-FN3051-V01
		CVE-FN3002-V01	CVE-FN3052-V01
		CVE-FN3045-V01	CVE-FN3053-V01
		CVE-IF3044-V01	CVE-FN3055-V01
		CVE-FN3041-V01	CVE-PY2912-V01
		CVE-PY3034-V01	CVE-CN1645-V01
		CVE-PR3033-V01	CVE-PR2907-V01
		CVE-FN3032-V01	CVE-SR3131-V01
		CVE-PR3031-V01	CVE-SR3125-V01
CVE-CN1664-V01	Constraint 20	CVE-FN3042-V01	
CVE-CN3106-V01	Constraint 23		
CVE-CN3088-V01	Constraint 22	CVE-FN2911-V01	CVE-FN1438-V02
		CVE-DR1276-V01	

Source: City of Columbus

Table 25: System Interface Relations

Interface ID	Reference	Requirement ID	
CVE-IX1608-V01	Interface 23	CVE-IF1244-V01	CVE-FN1207-V01
		CVE-IF1245-V01	
CVE-IX1609-V01	Interface 14.1	CVE-IF1251-V01	CVE-IX1619-V01
		CVE-IF1362-V01	CVE-IX1615-V01
		CVE-IF1361-V01	CVE-FN1215-V01
		CVE-IF1363-V01	CVE-FN1216-V01
		CVE-FN1212-V01	CVE-SR3123-V01
		CVE-FN2989-V01	CVE-IX1616-V01
		CVE-FN2991-V01	CVE-IX1619-V01
		CVE-FN2998-V01	CVE-IX1632-V01
		CVE-PR2995-V01	
CVE-IX1610-V01	Interface 14.2	CVE-IF1228-V01	CVE-IF2986-V02
		CVE-IF1232-V01	CVE-FN3000-V01
		CVE-IF1236-V01	CVE-FN2964-V01
		CVE-IF1239-V01	CVE-FN2975-V02
		CVE-IF1243-V01	CVE-FN2977-V01
		CVE-IF1356-V01	CVE-PR2993-V01
		CVE-IF1357-V02	CVE-IX1631-V01
		CVE-IF1358-V01	CVE-IX1620-V02
		CVE-IF1359-V02	CVE-IX1616-V01
		CVE-FN1319-V02	CVE-PR2999-V01
		CVE-FN2981-V02	
CVE-IX1611-V02	Interface 2	CVE-FN1442-V02	CVE-FN3045-V01
		CVE-FN1443-V01	CVE-FN3047-V01
		CVE-FN1444-V01	CVE-FN3049-V01
		CVE-FN1445-V01	CVE-FN3051-V01
		CVE-FN3001-V02	CVE-FN3052-V01
		CVE-FN3002-V01	CVE-FN3053-V01
		CVE-FN3041-V01	CVE-FN3055-V01
		CVE-IF3044-V01	
CVE-IX1612-V01	Interface 24	CVE-FN1207-V01	
CVE-IX1613-V01	Interface 16.1		CVE-IX1614-V01
CVE-IX1614-V01	Interface 16.2		CVE-IX1613-V01
CVE-IX1615-V01	Interface 15.1	CVE-IF1249-V01	CVE-FN2987-V01
		CVE-IF1219-V02	CVE-FN2969-V02
		CVE-FN1212-V01	CVE-FN2996-V01
		CVE-IF1361-V01	CVE-PR2995-V01
		CVE-IF1362-V01	CVE-IX1619-V01
		CVE-IF1363-V01	CVE-IX1609-V01
CVE-IX1616-V01	Interface 15.2	CVE-IF1226-V01	CVE-FN3000-V01
		CVE-IF1230-V01	CVE-FN2962-V01
		CVE-IF1234-V01	CVE-PR2993-V01
		CVE-IF1237-V01	CVE-IX1631-V01
		CVE-IF1243-V01	CVE-IX1620-V02
		CVE-IF1356-V01	CVE-IX1610-V01
		CVE-IF1357-V02	CVE-PR2999-V01
		CVE-IF1358-V01	CVE-IX1610-V01
		CVE-IF1359-V02	CVE-SR3123-V01
		CVE-FN2973-V02	CVE-IX1609-V01
		CVE-FN2979-V02	CVE-IX1619-V01
		CVE-FN2982-V01	CVE-IX1632-V01

Interface ID	Reference	Requirement ID	
CVE-IX1617-V01	Interface 22	CVE-FN1207-V01	
CVE-IX1618-V01	Interface 17	CVE-FN1187-V01 CVE-FN1197-V01 CVE-FN1198-V01 CVE-FN1202-V01 CVE-FN1213-V01 CVE-IF1222-V01 CVE-IF1246-V01 CVE-FN1123-V01 CVE-FN1203-V01 CVE-PY3016-V01 CVE-PR3017-V01	CVE-PY3018-V01 CVE-IF3019-V01 CVE-PR3020-V01 CVE-FN3021-V01 CVE-FN3022-V01 CVE-FN3024-V01 CVE-FN3025-V01 CVE-FN3026-V01 CVE-FN3023-V01 CVE-FN3027-V01 CVE-FN3028-V01
CVE-IX1619-V01	Interface 13.1	CVE-IF1218-V01 CVE-FN1212-V01 CVE-IF1361-V01 CVE-IF1362-V01 CVE-FN2971-V01 CVE-PR2995-V01	CVE-IX1609-V01 CVE-IX1615-V01 CVE-SR3123-V01 CVE-IX1609-V01 CVE-IX1616-V01 CVE-IX1632-V01
CVE-IX1620-V02	Interface 13.2	CVE-IF1225-V01 CVE-IF1229-V01 CVE-IF1233-V01 CVE-IF1240-V02 CVE-IF1360-V02 CVE-FN1310-V02 CVE-IF1243-V01 CVE-IF1356-V01 CVE-IF1357-V02 CVE-IF1358-V01	CVE-FN1310-V02 CVE-FN1319-V02 CVE-PR2994-V02 CVE-PR2993-V01 CVE-IX1631-V01 CVE-IX1610-V01 CVE-IX1616-V01 CVE-PR2999-V01 CVE-IX1610-V01 CVE-IX1616-V01
CVE-IX1621-V01	Interface 28	CVE-FN1205-V01 CVE-FN1204-V02	CVE-FN2961-V01
CVE-IX1622-V01	Interface 29	CVE-FN1204-V02 CVE-FN1205-V01	CVE-FN2959-V01 SMH-DR2328-V01
CVE-IX1623-V01	Interface 26	CVE-IF1242-V01 CVE-FN1204-V02	CVE-FN1205-V01
CVE-IX1624-V01	Interface 25	CVE-FN1204-V02 CVE-FN1205-V01	CVE-FN2960-V01
CVE-IX1625-V01	Interface 27	CVE-IF1343-V01 CVE-FN1308-V01	CVE-FN1309-V01
CVE-IX1626-V01	Interface 10	CVE-FN1321-V01 CVE-FN1308-V01 CVE-SR3129-V01	CVE-IX1628-V01 CVE-IX1633-V01 CVE-IX1637-V01
CVE-IX1627-V01	Interface 6		
CVE-IX1628-V01	Interface 9	CVE-FN1113-V01 CVE-FN1321-V01 CVE-SR3129-V01	CVE-IX1626-V01 CVE-IX1633-V01 CVE-IX1637-V01
CVE-IX1629-V01	Interface 20	CVE-IF1223-V01 CVE-IF1224-V01 CVE-IF1218-V01 CVE-IF1219-V02	CVE-IF1220-V01 CVE-FN2952-V01 CVE-FN2953-V01

Interface ID	Reference	Requirement ID	
CVE-IX1630-V01	Interface 19	CVE-IF1223-V01 CVE-IF1224-V01 CVE-IF1218-V01 CVE-IF1219-V02 CVE-IF1220-V01 CVE-IF1221-V01 CVE-FN2954-V01	CVE-FN2955-V01 CVE-FN2956-V01 CVE-FN2957-V01 CVE-FN2966-V01 CVE-FN2968-V02 CVE-FN2970-V01
CVE-IX1631-V01	Interface 12.1	CVE-IF1227-V01 CVE-IF1231-V01 CVE-IF1235-V01 CVE-IF1238-V01 CVE-IF1241-V02 CVE-IF1360-V02 CVE-IF1359-V02 CVE-FN1310-V02 CVE-IF1243-V01 CVE-IF1356-V01 CVE-IF1357-V02 CVE-IF1358-V01 CVE-FN1319-V02 CVE-FN2972-V02	CVE-IF2978-V02 CVE-FN2980-V02 CVE-FN2983-V01 CVE-IF2985-V02 CVE-PR2994-V02 CVE-FN3000-V01 CVE-FN2963-V01 CVE-FN2974-V02 CVE-FN2976-V01 CVE-PR2993-V01 CVE-IX1620-V02 CVE-IX1610-V01 CVE-IX1616-V01
CVE-IX1632-V01	Interface 12.2	CVE-IF1250-V01 CVE-IF1220-V01 CVE-FN1212-V01 CVE-IF1361-V01 CVE-IF1362-V01 CVE-FN2988-V01 CVE-FN2990-V01	CVE-FN2958-V01 CVE-FN2967-V01 CVE-FN2997-V01 CVE-SR3123-V01 CVE-IX1609-V01 CVE-IX1616-V01 CVE-IX1619-V01
CVE-IX1633-V01	Interface 8.1	CVE-IF1354-V01 CVE-FN1321-V01 CVE-SR3129-V01	CVE-IX1626-V01 CVE-IX1628-V01 CVE-IX1637-V01
CVE-IX1634-V01	Interface 8.2	CVE-FN1327-V01 CVE-IF1344-V01	CVE-IF1354-V01 CVE-IF1353-V01
CVE-IX1635-V01	Interface 7.1	CVE-FN1318-V01 CVE-FN1328-V01 CVE-FN1456-V01 CVE-FN1566-V02 CVE-FN1569-V02	CVE-FN1572-V02 CVE-FN1580-V02 CVE-FN1581-V02 CVE-FN1582-V02 CVE-SR3126-V01
CVE-IX1636-V02	Interface 7.2	CVE-IF1341-V02 CVE-IF1342-V02	CVE-FN1441-V02
CVE-IX1637-V01	Interface 11.1	CVE-IF1350-V01 CVE-IF1351-V01 CVE-IF1352-V01 CVE-IF1347-V01 CVE-FN1321-V01	CVE-SR3129-V01 CVE-IX1626-V01 CVE-IX1628-V01 CVE-IX1633-V01
CVE-IX1638-V01	Interface 11.2	CVE-IF1345-V01	CVE-IF1346-V01
CVE-IX1639-V01	Interface 5	CVE-FN1437-V01 CVE-FN1438-V02	CVE-FN1439-V01
CVE-IX1640-V01	Interface 2	CVE-IF1472-V01	CVE-IF1277-V01
CVE-IX1641-V01	Interface 21	CVE-FN1207-V01	
CVE-IX1642-V01	Interface 3	CVE-FN1206-V01	
CVE-IX1643-V01	Interface 1	CVE-IF1473-V01	CVE-FN3043-V01

Interface ID	Reference	Requirement ID
CVE-IX1644-V01	Interface 18	CVE-IF1248-V01

Source: City of Columbus

Table 26: Requirements Mapped to Requirements

Requirement ID	Related Requirements
CVE-PR1105-V01	CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01 CVE-FN1508-V02 CVE-FN1566-V02 CVE-FN1463-V01 CVE-FN1480-V01
CVE-DR1144-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1145-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-FN1538-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1146-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1147-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1148-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1149-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-FN1540-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1150-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1151-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1152-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1153-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01

Requirement ID	Related Requirements
CVE-DR1154-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1155-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1156-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1157-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1158-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1159-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1160-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1161-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1162-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1163-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1164-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1165-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1166-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01

Requirement ID	Related Requirements
CVE-DR1167-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1168-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1169-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1170-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1171-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1172-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1173-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1174-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1175-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1176-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1177-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1178-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1179-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01

Requirement ID	Related Requirements
CVE-DR1181-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-DR1182-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-PR1183-V01	CVE-FN1512-V01 CVE-FN1513-V01 CVE-FN1514-V01 CVE-FN1515-V01 CVE-FN1559-V01 CVE-IF1361-V01 CVE-IF1363-V01
CVE-FN1188-V01	CVE-PR1530-V01
CVE-FN1189-V01	CVE-FN1195-V01
CVE-FN1190-V01	CVE-FN1196-V01
CVE-FN1191-V01	CVE-FN1195-V01
CVE-FN1192-V01	CVE-FN1204-V02
CVE-FN1193-V01	CVE-FN1196-V01 CVE-FN1204-V02
CVE-FN1194-V01	CVE-PR1530-V01
CVE-FN1195-V01	CVE-FN1189-V01 CVE-FN1191-V01
CVE-FN1196-V01	CVE-FN1190-V01 CVE-FN1193-V01
CVE-FN1204-V02	CVE-FN1192-V01 CVE-FN1193-V01
CVE-FN1210-V01	CVE-PR1530-V01
CVE-IF1222-V01	CVE-FN1541-V01
CVE-IF1234-V01	CVE-FN1542-V01
CVE-IF1238-V01	CVE-DR1292-V02
CVE-IF1240-V02	CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01
CVE-IF1241-V02	CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01
CVE-IF1242-V01	CVE-PR1365-V01 CVE-PR1366-V01 CVE-PR1367-V01 CVE-PR1368-V01
CVE-SR1271-V01	CVE-DR1292-V02
CVE-DR1276-V01	CVE-FN1581-V02
CVE-DR1292-V02	CVE-IF1238-V01 CVE-SR1271-V01 CVE-IF1360-V02 CVE-FN1524-V02 CVE-FN1582-V02
CVE-FN1312-V01	CVE-FN1557-V01
CVE-FN1313-V01	CVE-FN1560-V01
CVE-FN1314-V01	
CVE-IF1360-V02	CVE-DR1292-V02

Requirement ID	Related Requirements	
CVE-IF1361-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01	CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-IF1363-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01	CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-PR1365-V01	CVE-IF1240-V02 CVE-IF1241-V02	CVE-IF1242-V01
CVE-PR1366-V01	CVE-IF1240-V02 CVE-IF1241-V02	CVE-IF1242-V01
CVE-PR1367-V01	CVE-IF1240-V02 CVE-IF1241-V02	CVE-IF1242-V01
CVE-PR1368-V01	CVE-IF1240-V02 CVE-IF1241-V02	CVE-IF1242-V01
CVE-DR1374-V02	CVE-FN1516-V01 CVE-FN1517-V01 CVE-FN1518-V02	CVE-FN1519-V01 CVE-FN1560-V01
CVE-DR1378-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01

Requirement ID	Related Requirements	
CVE-DR1379-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1380-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1381-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1382-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1383-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1384-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1385-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1386-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1387-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1388-V01	CVE-DR1389-V01 CVE-DR1390-V01 CVE-DR1391-V01 CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01
CVE-DR1388-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-DR1420-V02 CVE-DR1422-V01 CVE-DR1423-V01 CVE-DR1424-V01 CVE-DR1425-V01 CVE-DR1426-V01	CVE-DR1427-V01 CVE-DR1428-V01 CVE-DR1429-V01 CVE-DR1430-V01 CVE-DR1431-V01 CVE-DR1432-V01 CVE-DR1433-V01 CVE-DR1434-V01 CVE-DR1435-V01 CVE-DR1436-V01
CVE-DR1389-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01	CVE-FN1557-V01 CVE-DR1387-V01

Requirement ID	Related Requirements
CVE-DR1390-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1391-V01	CVE-FN1551-V01 CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1392-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01 CVE-FN1551-V01
CVE-DR1393-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1394-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1395-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1396-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1397-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1398-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-PR1399-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-PR1400-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-PR1401-V01	CVE-FN1509-V01 CVE-FN1510-V01 CVE-FN1511-V01 CVE-FN1557-V01 CVE-DR1387-V01
CVE-DR1402-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01
CVE-DR1404-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01
CVE-DR1405-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01
CVE-DR1406-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01
CVE-DR1407-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01
CVE-DR1408-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01 CVE-MT1603-V01

Requirement ID	Related Requirements	
CVE-DR1409-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1410-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1411-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1412-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1413-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1414-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1415-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1416-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1417-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1418-V01	CVE-FN1589-V02 CVE-FN1590-V01 CVE-FN1591-V01	CVE-MT1603-V01
CVE-DR1420-V02	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1422-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1423-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1424-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1425-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1426-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1427-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01
CVE-DR1428-V01	CVE-FN1520-V02	CVE-DR1388-V01 CVE-MT1604-V01

Requirement ID	Related Requirements	
CVE-DR1429-V01	CVE-FN1520-V02	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1430-V01	CVE-FN1520-V02	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1431-V01	CVE-FN1520-V02	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1432-V01	CVE-FN1520-V02	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1433-V01	CVE-FN1520-V02	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1434-V01	CVE-FN1520-V021	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1435-V01	CVE-FN1520-V021	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-DR1436-V01	CVE-FN1520-V021	CVE-DR1388-V01
		CVE-MT1604-V01
CVE-FN1463-V01	CVE-PR1105-V01	CVE-FN1508-V02
	CVE-FN1503-V01	CVE-FN1566-V02
	CVE-FN1504-V01	CVE-FN1480-V01
	CVE-FN1505-V01	CVE-PR1105-V01
CVE-FN1479-V01	CVE-FN1484-V02	
CVE-FN1480-V01	CVE-PR1105-V01	CVE-FN1508-V02
	CVE-FN1503-V01	CVE-FN1566-V02
	CVE-FN1504-V01	CVE-FN1463-V01
	CVE-FN1505-V01	CVE-PR1105-V01
CVE-FN1484-V02	CVE-FN1479-V01	
CVE-FN1503-V01	CVE-PR1105-V01	CVE-FN1566-V02
	CVE-FN1504-V01	CVE-FN1463-V01
	CVE-FN1505-V01	CVE-FN1480-V01
	CVE-FN1508-V02	CVE-PR1105-V01
CVE-FN1504-V01	CVE-PR1105-V01	CVE-FN1566-V02
	CVE-FN1503-V01	CVE-FN1463-V01
	CVE-FN1505-V01	CVE-FN1480-V01
	CVE-FN1508-V02	CVE-PR1105-V01
CVE-FN1505-V01	CVE-PR1105-V01	CVE-FN1566-V02
	CVE-FN1503-V01	CVE-FN1463-V01
	CVE-FN1504-V01	CVE-FN1480-V01
	CVE-FN1508-V02	CVE-PR1105-V01
CVE-FN1508-V02	CVE-PR1105-V01	CVE-FN1566-V02
	CVE-FN1503-V01	CVE-FN1463-V01
	CVE-FN1504-V01	CVE-FN1480-V01
	CVE-FN1505-V01	CVE-PR1105-V01

Requirement ID	Related Requirements	
CVE-FN1509-V01	CVE-DR1378-V01	CVE-DR1390-V01
	CVE-DR1379-V01	CVE-DR1391-V01
	CVE-DR1380-V01	CVE-DR1392-V01
	CVE-DR1381-V01	CVE-DR1393-V01
	CVE-DR1382-V01	CVE-DR1394-V01
	CVE-DR1383-V01	CVE-DR1395-V01
	CVE-DR1384-V01	CVE-DR1396-V01
	CVE-DR1385-V01	CVE-DR1397-V01
	CVE-DR1386-V01	CVE-DR1398-V01
	CVE-DR1387-V01	CVE-PR1399-V01
	CVE-DR1388-V01	CVE-PR1400-V01
	CVE-DR1389-V01	CVE-PR1401-V01
CVE-FN1510-V01	CVE-DR1378-V01	CVE-DR1390-V01
	CVE-DR1379-V01	CVE-DR1391-V01
	CVE-DR1380-V01	CVE-DR1392-V01
	CVE-DR1381-V01	CVE-DR1393-V01
	CVE-DR1382-V01	CVE-DR1394-V01
	CVE-DR1383-V01	CVE-DR1395-V01
	CVE-DR1384-V01	CVE-DR1396-V01
	CVE-DR1385-V01	CVE-DR1397-V01
	CVE-DR1386-V01	CVE-DR1398-V01
	CVE-DR1387-V01	CVE-PR1399-V01
	CVE-DR1388-V01	CVE-PR1400-V01
	CVE-DR1389-V01	CVE-PR1401-V01
CVE-FN1511-V01	CVE-DR1378-V01	CVE-DR1390-V01
	CVE-DR1379-V01	CVE-DR1391-V01
	CVE-DR1380-V01	CVE-DR1392-V01
	CVE-DR1381-V01	CVE-DR1393-V01
	CVE-DR1382-V01	CVE-DR1394-V01
	CVE-DR1383-V01	CVE-DR1395-V01
	CVE-DR1384-V01	CVE-DR1396-V01
	CVE-DR1385-V01	CVE-DR1397-V01
	CVE-DR1386-V01	CVE-DR1398-V01
	CVE-DR1387-V01	CVE-PR1399-V01
	CVE-DR1388-V01	CVE-PR1400-V01
	CVE-DR1389-V01	CVE-PR1401-V01

Requirement ID	Related Requirements
CVE-FN1512-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-FN1513-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01

Requirement ID	Related Requirements
CVE-FN1514-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-FN1515-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01 CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-FN1516-V01	CVE-DR1374-V02
CVE-FN1517-V01	CVE-DR1374-V02
CVE-FN1518-V02	CVE-DR1374-V02
CVE-FN1519-V01	CVE-DR1374-V02
CVE-FN1520-V02	CVE-DR1420-V02 CVE-DR1422-V01 CVE-DR1423-V01 CVE-DR1424-V01 CVE-DR1425-V01 CVE-DR1426-V01 CVE-DR1427-V01 CVE-DR1428-V01 CVE-DR1429-V01 CVE-DR1430-V01 CVE-DR1431-V01 CVE-DR1432-V01 CVE-DR1433-V01 CVE-DR1434-V01 CVE-DR1435-V01 CVE-DR1436-V01
CVE-FN1524-V02	CVE-DR1292-V02

Requirement ID	Related Requirements	
CVE-PR1530-V01	CVE-FN1188-V01 CVE-FN1194-V01	CVE-FN1210-V01
CVE-FN1538-V01	CVE-DR1145-V01	
CVE-FN1540-V01	CVE-DR1149-V01	
CVE-FN1541-V01	CVE-IF1222-V01	
CVE-FN1542-V01	CVE-IF1234-V01	
CVE-FN1551-V01	CVE-DR1391-V01	CVE-DR1392-V01
CVE-FN1557-V01	CVE-DR1378-V01 CVE-DR1379-V01 CVE-DR1380-V01 CVE-DR1381-V01 CVE-DR1382-V01 CVE-DR1383-V01 CVE-DR1384-V01 CVE-DR1385-V01 CVE-DR1386-V01 CVE-DR1387-V01 CVE-DR1388-V01 CVE-DR1389-V01 CVE-DR1390-V01	CVE-DR1391-V01 CVE-DR1392-V01 CVE-DR1393-V01 CVE-DR1394-V01 CVE-DR1395-V01 CVE-DR1396-V01 CVE-DR1397-V01 CVE-DR1398-V01 CVE-PR1399-V01 CVE-PR1400-V01 CVE-PR1401-V01 CVE-FN1312-V01
CVE-FN1559-V01	CVE-DR1144-V01 CVE-DR1145-V01 CVE-DR1146-V01 CVE-DR1147-V01 CVE-DR1148-V01 CVE-DR1149-V01 CVE-DR1150-V01 CVE-DR1151-V01 CVE-DR1152-V01 CVE-DR1153-V01 CVE-DR1154-V01 CVE-DR1155-V01 CVE-DR1156-V01 CVE-DR1157-V01 CVE-DR1158-V01 CVE-DR1159-V01 CVE-DR1160-V01 CVE-DR1161-V01 CVE-DR1162-V01 CVE-DR1163-V01	CVE-DR1164-V01 CVE-DR1165-V01 CVE-DR1166-V01 CVE-DR1167-V01 CVE-DR1168-V01 CVE-DR1169-V01 CVE-DR1170-V01 CVE-DR1171-V01 CVE-DR1172-V01 CVE-DR1173-V01 CVE-DR1174-V01 CVE-DR1175-V01 CVE-DR1176-V01 CVE-DR1177-V01 CVE-DR1178-V01 CVE-DR1179-V01 CVE-DR1181-V01 CVE-DR1182-V01 CVE-PR1183-V01
CVE-FN1560-V01	CVE-DR1374-V02	CVE-FN1313-V01
CVE-FN1566-V02	CVE-PR1105-V01 CVE-FN1503-V01 CVE-FN1504-V01 CVE-FN1505-V01	CVE-FN1508-V02 CVE-FN1463-V01 CVE-FN1480-V01 CVE-PR1105-V01
CVE-FN1581-V02	CVE-DR1276-V01	
CVE-FN1582-V02	CVE-DR1292-V02	

Requirement ID	Related Requirements	
CVE-FN1589-V02	CVE-DR1402-V01	CVE-DR1411-V01
	CVE-DR1404-V01	CVE-DR1412-V01
	CVE-DR1405-V01	CVE-DR1413-V01
	CVE-DR1406-V01	CVE-DR1414-V01
	CVE-DR1407-V01	CVE-DR1415-V01
	CVE-DR1408-V01	CVE-DR1416-V01
	CVE-DR1409-V01	CVE-DR1417-V01
	CVE-DR1410-V01	CVE-DR1418-V01
CVE-FN1590-V01	CVE-DR1402-V01	CVE-DR1411-V01
	CVE-DR1404-V01	CVE-DR1412-V01
	CVE-DR1405-V01	CVE-DR1413-V01
	CVE-DR1406-V01	CVE-DR1414-V01
	CVE-DR1407-V01	CVE-DR1415-V01
	CVE-DR1408-V01	CVE-DR1416-V01
	CVE-DR1409-V01	CVE-DR1417-V01
	CVE-DR1410-V01	CVE-DR1418-V01
CVE-FN1591-V01	CVE-DR1402-V01	CVE-DR1411-V01
	CVE-DR1404-V01	CVE-DR1412-V01
	CVE-DR1405-V01	CVE-DR1413-V01
	CVE-DR1406-V01	CVE-DR1414-V01
	CVE-DR1407-V01	CVE-DR1415-V01
	CVE-DR1408-V01	CVE-DR1416-V01
	CVE-DR1409-V01	CVE-DR1417-V01
	CVE-DR1410-V01	CVE-DR1418-V01
CVE-MT1603-V01	CVE-DR1402-V01	CVE-DR1411-V01
	CVE-DR1404-V01	CVE-DR1412-V01
	CVE-DR1405-V01	CVE-DR1413-V01
	CVE-DR1406-V01	CVE-DR1414-V01
	CVE-DR1407-V01	CVE-DR1415-V01
	CVE-DR1408-V01	CVE-DR1416-V01
	CVE-DR1409-V01	CVE-DR1417-V01
	CVE-DR1410-V01	CVE-DR1418-V01
CVE-MT1604-V01	CVE-DR1420-V02	CVE-DR1429-V01
	CVE-DR1422-V01	CVE-DR1430-V01
	CVE-DR1423-V01	CVE-DR1431-V01
	CVE-DR1424-V01	CVE-DR1432-V01
	CVE-DR1425-V01	CVE-DR1433-V01
	CVE-DR1426-V01	CVE-DR1434-V01
	CVE-DR1427-V01	CVE-DR1435-V01
	CVE-DR1428-V01	CVE-DR1436-V01

Source: City of Columbus

Appendix F. Acronyms and Definitions

Table 27 contains project specific acronyms used throughout this document.

Table 27: Acronym List

Acronym/Abbreviation	Definition
AV	Autonomous Vehicle
BRT	Bus Rapid Transit
BSM	Basic Safety Message
BSW	Blind Spot Warning
CEAV	Connected Electric Automated Vehicle (Smart Columbus Project #8)
CFR	Code of Federal Regulations
CMAX	Brand for COTA Cleveland Avenue Bus Rapid Transit
COTA	Central Ohio Transit Authority
ConOps	Concept of Operations
CTSS	Columbus Traffic Signal System
CV	Connected Vehicle
CVE	Connected Vehicle Environment
CVRIA	Connected Vehicle Reference Implementation Architecture
DoT	City of Columbus Department of Technology
DMS	Dynamic Message Sign
DPS	City of Columbus Department of Public Service
DSRC	Dedicated Short Range Communications
EEBL	Emergency Electronic Brake Light
EMS	Emergency Medical Service
EVP	Emergency Vehicle Preempt
FCW	Forward Collision Warning
FHWA	Federal Highway Administration
FSP	Freight Signal Priority
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers

Acronym/Abbreviation	Definition
IMA	Intersection Movement Assist
IT	Information Technology
ITS	Intelligent Transportation Systems
LCW	Lane Change Warning
LDV	Light-duty Vehicle
MAP	Map Message
MMITSS	Multi-Modal Intelligent Traffic Signal System
MORPC	Mid-Ohio Regional Planning Commission
NB	Northbound
NHTSA	National Highway Traffic Safety Administration
O&M	Operations and Maintenance
OBU	Onboard Unit (one onboard device)
ODOT	Ohio Department of Transportation
OEM	Original Equipment Manufacturer
OSADP	Open-Source Application Data Portal
OSU	Ohio State University
PII	Personally Identifiable Information
RFQ	Request for Quote
RLVW	Red Light Violation Warning
RSSZ	Reduced Speed School Zone
RSU	(DSRC) Roadside Unit
RTCM	Radio Technical Commission for Maritime
SAE	Society of Automotive Engineers
SB	Southbound
SCMS	Security and Credentials Management System
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Process
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSM	Signal Status Message
STEM	Science Technology Engineering and Math
TIM	Traveler Information Message

Acronym/Abbreviation	Definition
TRB	Transportation Research Board
TRL	Technology Readiness Level
TSC	Traffic Signal Controller
TSP	Transit Signal Priority
TWLTL	Two-Way Left-Turn Lanes
UI	User Interface
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VDTO	Vehicle Data for Traffic Operations
VRU	Vulnerable Road User

Source: City of Columbus

Appendix G. Glossary

Table 28 contains project specific terms used throughout this document.

Table 28: Glossary

Term	Definition
Alert	Indication to vehicle operator of potential situation for which they should take action. Less critical than a warning.
App	Software application
Automated vehicle	A vehicle that can sense its environment and navigate without human input
Connected Vehicle	A vehicle capable of communicating with other vehicles, infrastructure, and smartphones
CV Technology	Technology that lays the foundation for a fully interoperable, open, wireless environment for enhancing safety and mobility for vehicles and pedestrians in school zones
CV Message Suppression	Application that allows the vehicle operator to cease the broadcasting of CV messages from their vehicle
Dynamic Message Sign (DMS)	An ITS device used to convey information to drivers about travel time, roadway conditions and other information for which they should be aware.
Data privacy	The reasonable expectation that data of a sensitive nature will be kept confidential, sanitized and/or encrypted, and respectfully and responsibly maintained by all users, managers, and collectors of the data
Data retention	The continued storage of data for compliance or business reasons
Data security	The tools, policies, practices, and procedures used to protect data from being accessed, manipulated, or destroyed or being leveraged by those with a malicious intent or without authorization, as well as the corrective actions taken when data breaches are suspected or have been identified.
Data sharing policies	Adopted plan around the practice of making data available to others
Dedicated Short Range Communications (DSRC)	A two-way short- to medium-range wireless communications capability that permits very high data transmission critical in communications-based active safety applications
Dependency	When one project, agency, or entity requires data or functionality provided by another project, agency, or entity to meet its objectives
Diminished operations	When pre-determined signal timing plans are not implemented at the proper time, or when traffic detection does not function properly
Emergency Electronic Break Light Warning (EEBL)	Application that enables a vehicle to broadcast a self-generated emergency break event to surrounding vehicles

Term	Definition
Enabling Technologies	An innovation that alone or paired with an existing solution produces a better end user solution at a rapid rate
Experience Columbus	An organization whose mission is to market and promote Columbus services, attractions, and facilities to visitors, meeting planners, convention delegates, and residents
Failure operations	When a complete failure of the intersection occurs, primarily due to loss of power or other malfunctions
Forward Collision Warning (FCW)	Application that is intended to warn the vehicle operator of the vehicle in case of an impending rear-end collision with another vehicle ahead in traffic in the same and direction of travel
Global Navigation Satellite System	Standard generic term for satellite navigation systems that provide autonomous geo-spatial positioning with global coverage. GPS, GLONASS, Galileo and Beidou are examples.
Global Positioning System	US Standard implementation of GNSS
Host vehicle	The vehicle that issues the alert or warning to the vehicle operator in a safety-critical situation
Intersection Movement Assist (IMA) (V2V Safety)	Application that warns the vehicle operator of a vehicle when it is not safe to enter an intersection due to high collision probability with other vehicles at stop sign-controlled and uncontrolled intersections
Lane Change Warning/Blind Spot Warning (V2V Safety)	Application that is intended to warn the vehicle operator of the vehicle during a lane change attempt of the blind spot zone into which the vehicle intends to switch is, or will soon be, occupied by another vehicle traveling in the same direction
Normal operations	When a signalized intersection is cycling through its pre-planned phases correctly, servicing all approaches, including pedestrian phases
Notification	General term used for message, alert or warning issued to vehicle operator.
Onboard equipment	All equipment that is located in the vehicle, including any or all of the following items: GNSS receiver, vehicle data bus, a DSRC radio, a processing unit, and a display
Open-data	Information that is freely available for anyone to use and republish as they wish
Open-source concepts	The notion of open collaboration and voluntary contribution for software development by writing and exchanging programming code
Performance metric	A measurement used to determine how a project is performing
Personally Identifiable Information (PII)	Information used in security and privacy laws that can be used to identify an individual, such as vehicle, driver, and payment information
Procurement	The act of obtaining or acquiring goods, services or works, from a competitive bidding process
Real-time data	Information that is delivered immediately after collection

Term	Definition
Red Light Violation Warning (RLVW)	Application that enables a connected vehicle approaching an instrumented signalized intersection to receive information from the infrastructure about the signal timing and geometry of the intersection
Reduced Speed School Zone (RSSZ)	Application that provides connected vehicles that are approaching a school zone with information on the zone's posted speed limit
Roadside equipment	All equipment located on the roadside, including any or all of the following items: traffic signal controllers, GNSS receiver, a DSRC radio, and a processing unit
Operating System user	Administrators interested in gathering performance and usage information from the Common Payment System
Signal preemption	An interruption of the current intersection state to provide service to a specified phase, typically used for emergency first responders
Signal priority	The ability to provide either an early green or extended green for a specific phase
Operating System	A dynamic governed platform that integrates data and data services for the Smart Columbus program
Smart sensors	A device that takes input from the physical environment and uses built-in technology to perform functions upon detection of specific input and then process data before passing it on
System analytics or data analytics	The analysis of data, procedures, or business practices to locate information that can be used to create more efficient solutions
System integration user	A firm that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together
Systems Engineering (waterfall) approach	A linear and sequential product or software development model that includes Conception, Initiation, Analysis, Design, Construction, Testing, Production/Implementation, and Maintenance phases
Third-party	Organizations not affiliated with the Smart Columbus program
Traffic Signal Priority/Preemption (V2I Mobility)	Application that provides improved mobility for emergency vehicle operators, heavy-duty vehicle operators, and transit vehicle operators
Two-Way Left-Turn Lanes	A roadway design comprised of a shared, center 'turn' lane to be used by vehicles from either direction.
User Interface	Visual, audible, or haptic interface between a human and a machine, likely a computer of some form. Used to both convey and collect information.
Vehicle Data for Traffic Operations (VDTO)	Application that uses probe data obtained from vehicles in the network to support traffic operations, including incident detection and the implementation of localized operational strategies
Vulnerable road users	Pedestrian, cyclist, or motorist who has a higher risk in traffic

Term	Definition
Warning	Indication to vehicle operator of imminent situation for which they should take immediate action. Highest level of criticality.

Source: City of Columbus

Appendix H. Version History

Table 29: Version History

Version Number	Date	Author(s), Agency	Summary of Changes
0.1	08/22/2018	WSP	Initial Version for CoC Review
1.0	09/05/2018	City of Columbus	Draft USDOT Submittal
1.1	10/30/2018	City of Columbus	Revised Draft, distributed for System Requirements webinar
2.0	11/13/2018	WSP	Revised Draft for CoC review
3.0	11/30/2018	WSP	Final USDOT Submittal
4.0	04/25/2019	City of Columbus	Transfer to new template
5.0	04/30/2021	WSP	Post-Deployment Updated
6.0	05/12/2021	City of Columbus	Comments to revision 5
7.0	05/20/2021	WSP	Final Post-Deployment Update

Source: City of Columbus

SMRT
COLUMBUS

THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR