Connected Vehicle Environment (CVE) Test Report
for the Smart Columbus Demonstration Program

FINAL REPORT | May 5, 2021
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.

Acknowledgment 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.
Acknowledgments

The Smart Columbus Program would like to thank the Connected Vehicle Environment (CVE) project team, which includes representatives from various agencies and stakeholders, for their support and valuable input.

- Central Ohio Transit Authority (COTA)
- Ohio Department of Transportation (ODOT) / DriveOhio
- Kapsch
- Danlaw
- Siemens
- Wistron NeWeb Corp (WNC)
- BrandMotion
- Columbus Division of Police
- Columbus Division of Fire
- Department of Public Safety
- Franklin County Engineer’s Office
- WSP USA
- HNTB
Abstract

The purpose of this Test Report is to document the results of CVE system testing that was conducted prior to launch of the system for private resident participation. The primary goal of the Test Report is to document how well the system conforms to the allocated test procedures and required functionalities. This determination includes a blend of analysis, demonstration, inspection, and testing of various devices, subsystems, and data in order to provide final acceptance of the system and move forward to the next phase in the project, operations.

The Test Report contains a summary of test activities, identifies any issues and notable findings that occurred during testing, and documents the acceptance of functionalities.
Table of Contents

Chapter 1. Introduction........................................................................................................... 1
  1.1. Project Background........................................................................................................ 1

Chapter 2. CVE Overview...................................................................................................... 3
  2.1. System Components...................................................................................................... 3
  2.2. Applications.................................................................................................................. 4
  2.3. DSRC Messages............................................................................................................ 5
  2.4. CVE Monitoring .......................................................................................................... 9

Chapter 3. Testing Overview.................................................................................................. 11
  3.1. Test Roles..................................................................................................................... 11
  3.2. CVE Components ....................................................................................................... 12
  3.3. Functions Tested........................................................................................................... 14
  3.4. Test Tools .................................................................................................................... 16
  3.5. System Interfaces ........................................................................................................ 18
  3.6. Testing Locations ........................................................................................................ 18
  3.7. Variances .................................................................................................................... 22
  3.8. References .................................................................................................................. 25

Chapter 4. Test Results......................................................................................................... 27
  4.1. Test results.................................................................................................................... 27
  4.2. Defect Management Tool ........................................................................................... 104
  4.3. Channel 180 Tests ...................................................................................................... 112

Chapter 5. Summary of Results ............................................................................................ 115
  5.1. Test Metrics ................................................................................................................ 115
  5.2. Outstanding Issues ...................................................................................................... 117
  5.3. Change Request Log ................................................................................................... 120
  5.4. Exit Criteria ................................................................................................................ 124
List of Tables

Table 1: Connected Vehicle Environment Project Scope ......................................................... 2
Table 2: CV Application Component Matrix ...................................................................... 6
Table 3: CV Application Message Matrix ........................................................................... 8
Table 4: Organizational Support .......................................................................................... 11
Table 5: Test Roles .................................................................................................................. 12
Table 6: CVE Component functionality .............................................................................. 12
Table 7: Back-Office and Support System functionality ..................................................... 13
Table 8: References ................................................................................................................ 25
Table 9: OBU Test Results .................................................................................................... 28
Table 10: OBU Application Test Results ........................................................................... 28
Table 11: Kapsch RSU Test Results .................................................................................... 56
Table 12: Danlaw RSU Test Results .................................................................................... 64
Table 13: Siemens RSU Test Results .................................................................................... 72
Table 14: Message Handler Test Results ............................................................................ 80
Table 15: Econolite Traffic Signal Controller Test Results .............................................. 90
Table 16: Siemens Traffic Signal Controller Test Results ............................................... 93
Table 17: TCVMS Test Results ........................................................................................... 96
Table 18: TrCVMS Test Results ........................................................................................ 103
Table 19: Defect Tracker ...................................................................................................... 105
Table 20: Channel 180 Test Scenarios .............................................................................. 112
Table 21: Test Cases Passed vs Failed ............................................................................. 115
Table 22: Test Cases by Test Status .................................................................................. 115
Table 23: Defect by Status Type ......................................................................................... 116
Table 24: Change Request Status ...................................................................................... 116
Table 25: Open Issues ......................................................................................................... 117
Table 26: Change Request Log ........................................................................................... 120
Table 27: Test Exist Criteria ............................................................................................... 124
Table 28: Acceptance Test Signoff .................................................................................... 125
Table 29: Numbering Convention Definitions .................................................................. 128
Table 30: Acronyms List .................................................................................................... 129
Table 31: Glossary ............................................................................................................... 133
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RSU Deployment Map</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>CMCC System Map</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Roadside Equipment Details</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>CVTT Components</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>CVE System Interface Diagram</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Lab Setup RSU and Test Tool</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>Lab Setup Signal Controllers</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>Lab Setup Conference Table</td>
<td>19</td>
</tr>
<tr>
<td>9</td>
<td>Demonstration Area Signalized Intersections</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>Demonstration Area School Zones</td>
<td>20</td>
</tr>
<tr>
<td>11</td>
<td>Demonstration Area: Test Tool Setup</td>
<td>21</td>
</tr>
<tr>
<td>12</td>
<td>Field: Intersections</td>
<td>22</td>
</tr>
<tr>
<td>13</td>
<td>Numbering Convention</td>
<td>127</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction

A Test Plan, complete with detailed Test Procedures, was developed by a multidisciplinary team comprised of project stakeholders to detail the methods to formally test the functionality of the Smart Columbus Connected Vehicle Environment (CVE). This Test Report documents the results of the testing activities, used to validate the functionalities of the CVE. The Test Report contains a summary of the functionality tested, an overview of the CVE, as tested, a summary of the test activities, as well as identifies issues that occurred during testing.

Due to the unique characteristics of this project, multiple phases and iterations of testing were conducted to ensure a holistic and successful outcome. Test Phases included Local Device Assembly Test (LDAT), Subsystem Test (SST), Final System Test (FST), and Final Acceptance. These individual phases each built upon information and data from prior phases. Constraints and functionality demonstrated during each phase were dependent on the results of each preceding phase. Testing was conducted in three (3) locations: A Laboratory, serving as a controlled indoor environment; a Demonstration Area, comprised of a controlled outdoor environment; and in the Field, at 6 pre-defined, First Article, locations. This Test Report summarizes the full results of the comprehensive testing process based on the completion of all Test Phases.

1.1. PROJECT BACKGROUND

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 these awards, 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 everyday challenges faced by city residents

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 Connected Vehicle Environment (CVE) project 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 of other technologies delivered through the other seven projects. The CVE project will integrate smart traveler applications and connected vehicles (CVs) into its transportation network by focusing on deploying CV infrastructure and CV applications as follows:

- 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 units (OBUs), front and backhaul communications, equipment interfaces). The CVE will generate the needed transportation-related data the applications use.
The CVE is expected to enhance safety awareness 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.

CV infrastructure deployment will occur along four major corridors/areas. The deployment of in-vehicle devices will target populations that are located near, or that frequently use, the corridors where infrastructure is deployed. Table 1 lists the improvements associated with the CVE.

### Table 1: Connected Vehicle Environment Project Scope

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications and Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>85+ RSUs</strong></td>
<td></td>
</tr>
<tr>
<td>The project will install RSUs and necessary communications equipment at 85 signalized intersections in the project areas. One intersection will have multiple RSUs.</td>
<td>CV Applications The project will deploy V2V safety, V2I safety, and V2I mobility applications.</td>
</tr>
<tr>
<td><strong>1000+ OBUs</strong></td>
<td></td>
</tr>
<tr>
<td>The project will install on-board units on participating private, fleet, emergency, transit, and freight vehicles.</td>
<td>Data Capture The project will capture, relate, store, and respond to data the infrastructure generates and for use in traffic management applications.</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*

The intent of the CVE project is to improve safety awareness 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 improvement in freight operations, another of the City’s goals.

CV is just one component, but if it proves to be effective, other projects can also benefit from the positive outcomes. The goal of the CVE project was not to develop applications to a high level of maturity, but to leverage what has already been developed. Therefore, it is important to understand that the ability of the CVE to address the user needs captured in the CVE Concept of Operations (ConOps) depends on the availability of hardware and software solutions that have been previously deployed (and subsequently improved upon). To this end, throughout the CVE systems engineering process, several applications were considered. Each application was scrutinized in detail to ensure that only applications that were ready for deployment were included in the deployment of the CVE. Performance requirements detailed in the System Requirements document (see V2V Safety, V2I Safety, and V2I Mobility functional groups) outline expectations for each application that was deployed. The implementation of software is expected to demonstrate the efficacy of the deployed infrastructure.

The applications and technology deployed as part of the CVE project are the same as (or very similar to) applications and technology employed in other connected vehicle projects. As similar applications were developed and employed as part of the USDOT’s CV pilot projects, their maturity continues to increase. Selected vendors continue to improve applications, based on experience in testing and implementation. The design and implementation of the CVE benefited from these improvements.
Chapter 2. CVE Overview

The 85+ DSRC Roadside Units, supplied by Kapsch, Danlaw, and Siemens, were installed along Cleveland Avenue between E 2nd Avenue and Morse Rd, Morse Rd between High Street and Stygler Rd, High Street between E 5th Avenue and Morse Rd, and Alum Creek between SR-317 and I-270 Westbound Off-Ramp. Figure 1 is a map of the RSU deployment.

Figure 1: RSU Deployment Map
Source: City of Columbus

2.1. SYSTEM COMPONENTS

The CVE is composed of several roadside components, on-board units (OBU) for multiple vehicle types, and external back-office and support systems. A detailed list of components and functionality tested are provide in Chapter 3, however, a brief list of components is provided here:
• **Roadside Equipment**
  - Roadside Unit (RSU)
  - Message Handler (MH)
  - Traffic Signal Controller (TSC)

• **OBU Types**
  - Aftermarket Safety Device (ASD)
  - Vehicle Awareness Device (VAD)
  - VAD with Transit Signal Priority
  - VAD with Freight Signal Priority
  - VAD with Emergency Signal Preemption

All OBUs were provided by Siemens. ASDs are installed in approximately 600 Light-duty vehicles, VADs with logging capabilities are installed in approximately 325 Transit vehicles, of which 15 are transit signal priority enabled, VADs with freight signal priority are installed in approximately 14 Heavy Duty Freight vehicles, and VADs with emergency signal preemption are installed in approximately 110 Police and Fire vehicles.

NOTE: Aftermarket Safety Devices are the only OBUs with a Human Machine Interface (HMI) and therefore the only device type in which alerts/warning are issued to the vehicle operator.

• **Back Office/Support Systems:**
  - Traffic Connected Vehicle Management System (TCVMS), composed of the following three subsystems:
    - Traffic Management Center (TMC)
      - Columbus utilizes Centracs Advanced Traffic Management System (ATMS) for traffic signal control
    - Smart Columbus Operating System (OS)
    - Connected Mobility Control Center (CMCC)
  - Transit Connected Vehicle Management System (TrCVMS)
  - Position Correction System
  - Security Credential Management System (SCMS)
    - SCMS services are provided by Integrity Security Services (ISS) through a contract with DriveOhio, part of the Ohio Department of Transportation (ODOT)
  - OBU Firmware Service
  - School Zone System

### 2.2. APPLICATIONS

The CVE supports the following Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) applications:

- V2V Emergency Electronic Brake Light (EEBL)
- V2V Forward Collision Warning (FCW)
- V2V Lane Change/Blind Spot Warning (LCW/BSW)
- V2V Intersection Movement Assist (IMA)
- V2I Transit Signal Priority
- V2I Freight Signal Priority
- V2I Emergency Vehicle Signal Preemption
- V2I Red Light Violation Warning (RLVW)
- V2I Reduce Speed in School Zone Warning (RSSZ)

The CVE also supports OBUs requesting and downloading security credentials, from ISS, and firmware updates provided by Siemens, to modify configuration parameters as well as address operational issues discovered during testing and general operation.
2.3. DSRC MESSAGES

The following Society of Automotive Engineers (SAE) J2735-032016 messages are broadcast by RSUs and OBUs to support the applications:

- OBU Basic Safety Message (BSM)
- OBU Signal Request Message (SRM)
- RSU Signal Status Message (SSM)
- RSU Signal Phase and Timing (SPaT)
- RSU MAP
- RSU Traveler Information Messages (TIM)
- RSU Radio Technical Commission for Maritime Services (RTCM)

RSUs also broadcast Institute of Electrical and Electronic Engineers (IEEE) 1609.3-2016 Wireless Access in Vehicular Environment (WAVE) Service Advertisements (WSA) to announce IPv6 services, for certificate top off and firmware updates, Signal Priority/Preemption (SRM/SSM), and Position Correction Services (RTCM).

Table 2 lists the infrastructure components, vehicle types, and external systems that support each CVE application. Applications are categorized as Vehicle-to-Vehicle (V2) Safety, Vehicle-to-Infrastructure (V2I) Mobility, and V2I Safety.
### Table 2: CV Application Component Matrix

<table>
<thead>
<tr>
<th>Applications</th>
<th>Infrastructure</th>
<th>OBU Type</th>
<th>External Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RSU</td>
<td>Message Handler</td>
<td>Traffic Signal Controller</td>
</tr>
<tr>
<td>V2V Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Electronic Brake Light</td>
<td></td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>Forward Collision Warning</td>
<td></td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>Intersection Movement Assist</td>
<td></td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>Lane Change Warning/Blind Spot Warning</td>
<td></td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V2I Mobility</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Transit Signal Priority</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Freight Signal Priority</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Emergency Vehicle Signal Preemption</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Applications</td>
<td>Infrastructure</td>
<td>OBU Type</td>
<td>External Systems</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td>RSU</td>
<td>Message Handler</td>
<td>Traffic Signal Controller</td>
</tr>
<tr>
<td>Vehicle Data for Traffic Operations</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Transit Vehicle Interaction Event Recording</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Red Light Violation Warning</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Reduced Speed School Zone</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Device updates</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over-the-Air Certificate Top Off</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over-the-Air OBU Firmware updates</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*log only

Source: City of Columbus
Table 3 lists the SAE J2735-032016 messages required to support each application.

**Table 3: CV Application Message Matrix**

<table>
<thead>
<tr>
<th>Applications</th>
<th>Signal Phase and Timing</th>
<th>MAP</th>
<th>Traveler Information</th>
<th>WSA</th>
<th>RTCM</th>
<th>Signal Status Message</th>
<th>Signal Request Message</th>
<th>Basic Safety Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V2V Safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Electronic Brake Light</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward Collision Warning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intersection Movement Assist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lane Change Warning/ Blind Spot Warning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>V2I Mobility</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transit Signal Priority</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Freight Signal Priority</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Emergency Vehicle Preemption</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Vehicle Data for Traffic Operations</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Transit Vehicle Interaction Event Recording (TVIER)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>V2I Safety</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Light Violation Warning</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced Speed School Zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
2.4. CVE MONITORING

RSUs are monitored and managed through the CMCC interface provided by Kapsch. The CMCC enables the operator to monitor the overall system through a map view and individual devices at each intersection through an equipment details view. Figure 2 depicts the CMCC map view and Figure 3 depicts the intersection equipment details view.

Figure 2: CMCC System Map
Source: City of Columbus

Figure 3: Roadside Equipment Details
Source: City of Columbus
The CMCC provides alerts to Centracs when RSU malfunctions are detected. Centracs, in turn, provides RSU alerts, as well as alerts for controller errors, traffic cabinet intrusion, network intrusion and others to the operator as they are detected. Operators monitor Centracs on a routine bases and only utilize the CMCC when RSU alerts are indicated.
Chapter 3. Testing Overview

Testing focused on three primary functions; 1) the exchange of data between RSUs and OBUs in order to demonstrate V2V and V2I applications; culminating in an alert issued to the ASD vehicle operator, 2) OBUs downloading new security credentials (certificate top off), and 3) OBUs downloading and applying firmware updates.

This Section provides an overview of the testing process, including the organizations and personnel involved, the components and functionality tested, and the tools utilized.

3.1. TEST ROLES

Several teams participated in CVE testing, including, the OBU System Integrator, composed of Siemens, Brandmotion, and Wistron NeWeb Corporation (WNC), the RSU integrator, composed of Kapsch, Danlaw, Econolite and Pathmaster. WSP provided testing oversight and the Smart City Program Office provided overall testing management. Table 4 identifies each organization, and their role in testing, and Table 5 lists the individuals and their role during testing.

Table 4: Organizational Support

<table>
<thead>
<tr>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart City Program Office</td>
<td>CVE Project Manager</td>
</tr>
<tr>
<td>WSP</td>
<td>Test Manager</td>
</tr>
<tr>
<td>Kapsch</td>
<td>Kapsch and Danlaw RSU and CMCC Test Conductor and device operator</td>
</tr>
<tr>
<td>Siemens</td>
<td>Siemens RSU, OBU, and TrCVMS Test Conductor and device operator</td>
</tr>
<tr>
<td>WNC</td>
<td>OBU Test Conductor and device operator</td>
</tr>
<tr>
<td>BrandMotion</td>
<td>OBU Installer</td>
</tr>
<tr>
<td>Central Ohio Transit Authority (COTA)</td>
<td>Transit vehicle and operator provider and Transit vehicle Data Consumer</td>
</tr>
</tbody>
</table>

Source: City of Columbus
Table 5: Test Roles

<table>
<thead>
<tr>
<th>Test Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE Project Manager</td>
<td>Ryan Bollo (Smart City Program Office)</td>
</tr>
<tr>
<td>Test Manager</td>
<td>Frank Perry (WSP)</td>
</tr>
<tr>
<td>Traffic Data Consumer</td>
<td>Rob Baily (Kapsch)</td>
</tr>
<tr>
<td></td>
<td>Sara Khosravi (Kapsch)</td>
</tr>
<tr>
<td>Transit Data Consumer</td>
<td>Iouri Nemirovski (Siemens)</td>
</tr>
<tr>
<td></td>
<td>Wolfgang Buckel (Siemens)</td>
</tr>
<tr>
<td>OBU Test Conductor</td>
<td>Amadou Kane (WNC)</td>
</tr>
<tr>
<td></td>
<td>Maulikbhai Patel (Siemens)</td>
</tr>
<tr>
<td>RSU Test Conductor</td>
<td>Rob Baily (Kapsch)</td>
</tr>
<tr>
<td></td>
<td>Paul Hill (Kapsch)</td>
</tr>
<tr>
<td></td>
<td>Paul Hill (Kapsch)</td>
</tr>
<tr>
<td></td>
<td>Maulikbhai Patel (Siemens)</td>
</tr>
<tr>
<td></td>
<td>Wolfgang Buckel (Siemens)</td>
</tr>
<tr>
<td>Data Recorder</td>
<td>Frank Perry (WSP)</td>
</tr>
<tr>
<td></td>
<td>Tom Timcho (WSP)</td>
</tr>
<tr>
<td>Vehicle Drivers</td>
<td>Venkateshwar Jadhav (Siemens)</td>
</tr>
<tr>
<td></td>
<td>Iouri Nemirovski (Siemens)</td>
</tr>
<tr>
<td></td>
<td>Maulikbhai Patel (Siemens)</td>
</tr>
<tr>
<td></td>
<td>Tom Timcho (WSP)</td>
</tr>
<tr>
<td></td>
<td>Ryan Bollo (City of Columbus)</td>
</tr>
<tr>
<td></td>
<td>Sonja Summer (City of Columbus)</td>
</tr>
<tr>
<td>Test Observers</td>
<td>Andy Wolpert (City of Columbus)</td>
</tr>
<tr>
<td></td>
<td>Jeff Kupko (Michael Baker Inc.)</td>
</tr>
</tbody>
</table>

Source: City of Columbus

3.2. CVE COMPONENTS

This section lists the components, back-office systems, and supporting systems that compose the CVE, along the general functionality provided by each. Table 6 contains the list of CVE components and Table 7 contains the list of back-office and support systems.

Table 6: CVE Component functionality

<table>
<thead>
<tr>
<th>Device</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kapsch RSU</td>
<td>Broadcast infrastructure-based V2I messages and forward Vehicle-based V2V and V2I messages to back office systems for processing</td>
</tr>
<tr>
<td>Danlaw RSU</td>
<td>Broadcast infrastructure-based V2I messages and forward Vehicle-based V2V and V2I messages to back office systems for processing</td>
</tr>
<tr>
<td>Siemens RSU</td>
<td>Broadcast infrastructure-based V2I messages and forward Vehicle-based V2V and V2I messages to back office systems for processing</td>
</tr>
</tbody>
</table>
## Chapter 3. Testing Overview

### Connected Vehicle Environment

<table>
<thead>
<tr>
<th>Device</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Handler (Econolite Connected Vehicle Co-Processor (CVC))</td>
<td>Generate infrastructure-based V2I messages and process vehicle-based V2V and V2I messages</td>
</tr>
<tr>
<td>Siemens Aftermarket Safety Device OBU</td>
<td>Generate and broadcast BSMs, alert drivers of V2V and V2I events and request and download security credential and firmware updates</td>
</tr>
<tr>
<td>Siemens VAD</td>
<td>Generate and broadcast BSMs and request and download security credential and firmware updates</td>
</tr>
<tr>
<td>Siemens VAD with Transit Signal Priority</td>
<td>Generate and broadcast BSMs and transit signal priority SRMs, log V2V and V2I events, and request and download security credential and firmware updates</td>
</tr>
<tr>
<td>Siemens VAD with Freight Signal Priority</td>
<td>Generate and broadcast BSMs and freight signal priority SRMs, and request and download security credential and firmware updates</td>
</tr>
<tr>
<td>Siemens VAD with Emergency Signal Preemption</td>
<td>Generate and broadcast BSM emergency signal preemption SRMs, and request and download security credential and firmware updates</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*

### Table 7: Back-Office and Support System functionality

<table>
<thead>
<tr>
<th>Supporting System</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>City CVE IT Network</td>
<td>Enable communication between roadside equipment and back-office systems and services</td>
</tr>
<tr>
<td>TCVMS: TMC Centracs</td>
<td>Monitor CVE infrastructure devices as well as cabinet and network intrusion</td>
</tr>
<tr>
<td>TCVMS: OS</td>
<td>Archive CVE data</td>
</tr>
<tr>
<td>TCVMS: CMCC</td>
<td>Manage RSUs and Message Handlers</td>
</tr>
<tr>
<td>TrCVMS</td>
<td>Process data from Transit Vehicle OBUs</td>
</tr>
<tr>
<td>Position Correction System</td>
<td>Provide position correction data to Message Handlers for generating Radio Technical Commission for Maritime (RTCM) messages</td>
</tr>
<tr>
<td>SCMS</td>
<td>Generate and distribute IEEE 1609.2-2016 Certificates to RSUs and OBUs upon request</td>
</tr>
<tr>
<td>OBU Firmware Service</td>
<td>Provide firmware updates for OBUs upon request</td>
</tr>
<tr>
<td>School Zone System</td>
<td>Provide School Zone active date and time data to Message Handlers for generating Reduced Speed School Zone TIM</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
3.3. FUNCTIONS TESTED

This section describes the functionality tested for each CVE component type and back-office system.

3.3.1. Roadside Equipment

3.3.1.1. Roadside Units

The following RSU functionality was tested:

- Broadcast Institute of Electrical and Electronic Engineers (IEEE) 1609.3-2016 Wireless Access in Vehicular Environments (WAVE) Service Advertisements (WSAs) once per second on Channel 180. WSAs advertise Signal Phasing and Timing (SPaT), MAP, Radio Technical Commission for Maritime Services (RTCM), Signal Request Messages (SRM), and Internet Protocol (IP) services and provide IPv6 network information through the WAVE Routing Advertisements (WRA).
- Broadcast Society of Automotive Engineers (SAE) J2735-032016 SPaT messages 10 times per second on Channel 180
- Broadcast J2735-032016 MAP messages once per second on Channel 180
- Broadcast J2735-032016 RTCM messages once every 2 seconds on Channel 180
- Broadcast J2735-032016 Signal Status Messages (SSM) once per second on Channel 180, while a signal priority or preemption request is active
- Request and receive IEEE 1609.2-2016 certificates from the Ohio Department of Transportation (ODOT) SCMS
- Broadcast J2735-032016 TIMs once per second on Channel 180 to support RSSZ
- Forward OBU generated J2735-032016 Basic Safety Messages (BSM) to the Message Handler
- Forward OBU generated J2735-032016 Signal Request Messages (SRM) to the Message Handler

3.3.1.2. Message Handler

The following Message Handler functionality was tested:

- Generate and send SAE J2735-032016 Signal Phase and Timing (SPaT), System Status Messages (SSM), and Radio Technical Commission for Maritime Services (RTCM) messages to the RSU, as Immediate Forward messages, for broadcast
- Store and send SAE J2735-032016 MAP and TIMs to the RSU, as Immediate Forward messages for broadcast
- Update the startTime and duration values in the TIM based on data from the School Zone System
- Send signal priority and signal preemption requests to the Traffic Signal Controller
- Forward SAE J2735-032016 SPaT, SSMs, RTCMs, BSMs, and SRMs to the TCVMS

3.3.1.3. Traffic Signal Controller

The following Traffic Signal Controller functionality was tested:

- Send signal phase and timing data to the Message Handler
- Process signal priority and signal preemption requests received from the Message Handler
- Send signal priority/preemption status data to the Message Handler

3.3.2. Vehicle On-Board Units

3.3.2.1. Aftermarket Safety Device

The following ASD OBU functionality was tested:

- Generate and broadcast J2735-032016 Part I BSMs 10 times per second on Channel 172
- Receive and process RTCMs on Channel 180
• Provide EEBL, FCW, LCW.BSW, IMA, RLVW, and RSSZ warnings to drivers, when appropriate
• Request and receive IEEE 1609.2-2016 certificates from ISS through an RSU over IPv6 on Channel 180
• Request and receive firmware updates from Siemens through an RSU over IPv6 on Channel 180

3.3.2.2. Vehicle Awareness Device with Transit Signal Priority

The following VAD with Transit Signal Priority functionality was tested:
• Generate and broadcast J2735-032016 Part I BSMs 10 times per second on Channel 172
• Receive and process RTCMs on Channel 180
• Generate, broadcast, and log J2735-032016 SRMs, with a vehicle role of “Transit”, requesting Transit Signal Priority, on Channel 180
• Receive and log SSMs
• Log BSM, EEBL, FCW, LCW/BSW, IMA, RLVW, and RSSZ events, when appropriate
• Send log files to the TrCVMS
• Request and receive IEEE 1609.2-2016 certificates from ISS through an RSU over IPv6 on Channel 180
• Request and receive firmware updates from Siemens through an RSU over IPv6 on Channel 180

3.3.2.3. Vehicle Awareness Device with Freight Signal Priority

The following VAD with Freight Signal Priority functionality was tested:
• Generate and broadcast J2735-032016 Part I BSMs 10 times per second on Channel 172
• Receive and process RTCMs on Channel 180
• Generate and broadcast J2735-032016 SRMs, with a vehicle role of “truck”, requesting Freight Signal Priority, on Channel 180
• Receive J2735-032016 SSMs from Channel 180
• Request and receive IEEE 1609.2-2016 certificates from ISS through an RSU over IPv6 on Channel 180
• Request and receive firmware updates from Siemens through an RSU over IPv6 on Channel 180

3.3.2.4. Vehicle Awareness Device with Emergency Signal Preemption

The following VAD with Emergency Signal Preemption functionality was tested:
• Generate and broadcast J2735-032016 Part I BSMs 10 times per second on Channel 172
• Receive and process RTCMs on Channel 180
• Generate and broadcast J2735-032016 SRMs, with a vehicle role of “police”, “fire”, or “ambulance”, requesting Freight Signal Priority, on Channel 180
• Request and receive IEEE 1609.2-2016 certificates from ISS through an RSU over IPv6 on Channel 180
• Request and receive firmware updates from Siemens through an RSU over IPv6 on Channel 180
3.3.3. Back-Office Systems

3.3.3.1. Traffic CV Management System

The following TCVMS functionality was tested:
- (CMCC) Send MAP and TIM (RSSZ) messages to the Message Handler at each applicable roadside location
- (CMCC) Send SPaT, MAP, SRM, SSM, TIM, BSM, and RTCMs to the OS
- (OS) Archive SPaT, MAP, SRM, SSM, TIM, BSM, and RTCMs
- (TMC) Roadside Cabinet and Network intrusion detection and reporting
- (TMC) RSU degraded operation/failure Reporting
- (CMCC) RSU degraded operation/failure detection and general management

3.3.3.2. Transit CV Management System

The following TrCVMS functionality was tested:
- Receive and archive log files from Transit vehicle OBUs
- Send Transit Vehicle data to the Smart Columbus Operating System

3.4. TEST TOOLS

3.4.1. Connected Vehicle Test Tool

A Connected Vehicle Test Tool (CVTT), a specialized Kapsch DSRC OBU, was utilized to visualize SPaT and MAP messages as well as verify the content of WSAs, TIM, BSMs, SRM, SSM, and RTCM messages. The CVTT generates tool specific log files as well as captures received packets in a pcap file format for post processing. The CVTT also streams received packets to a laptop for real-time analysis. Pcap files were analyzed to verify the proper operation of each RSU and OBU. The Kapsch Connected Vehicle Validation website was not utilized for data/message analysis. The CVTT was calibrated by the manufacture prior to delivery. The CVTT components are shown in Figure 4.
3.4.2. Wireshark

A special version of Wireshark designed to decode J2735-032016 Messages, running on a Windows Laptop, was utilized to capture and view DSRC packets in real-time, as received from the CVTT, as well as for post processing pcap files generated by the CVTT.

3.4.3. CMCC

The CMCC was utilized to send MAP messages and TIM to the appropriate Message Handlers as well as monitoring the general health and status of RSUs under test.
Chapter 3. Testing Overview

3.5. SYSTEM INTERFACES

Figure 5 depicts the various interfaces between the CVE components, as well as how the CVTT monitored communications between RSUs and OBUs.

![Diagram of CVE System Interfaces](image)

**Figure 5: CVE System Interface Diagram**

*Source: City of Columbus*

3.6. TESTING LOCATIONS

As defined in the Test Plan, testing was conducted in 4 Phases: Local Device Assembly Test (LDAT), Subsystem Test (SST), Final System Test (FST), and Final Acceptance. Testing was conducted at three (3) locations: Lab, Demonstration Area, and Field. This section describes the three Test locations and the testing performed at each.
3.6.1. Lab

LDAT and Roadside Equipment SST were performed in a conference room set up as a Lab/Bench environment in the City of Columbus Traffic Management Center (TMC). LDAT, which exercised the functionality and operation of each standalone device tool place in November 2019. SST, which served as initial integration testing, exercising the functionality and operation of each subsystem (i.e. RSU, Message Handler, and Traffic Signal Controller), took place in December 2019, January of 2020, and February 2020. Figure 6 through Figure 8 show the Lab Test environment.

Note: these pictures were taken during our February 2020 integration session, before COVID-19 protocols were put in place.
3.6.2. Demonstration Area

The Demonstration Area was setup in the TCM parking lot; consisting of mock-ups for 3 signalized intersections (Figure 9) and 3 school zones (Figure 10) for controlled application testing. SST was performed on both the Roadside Equipment and OBUs to verify V2I and V2V application operation.

Figure 9: Demonstration Area Signalized Intersections

Source: City of Columbus

Figure 10: Demonstration Area School Zones

Source: City of Columbus
Figure 11 depicts the CVTT with a Wireshark Laptop setup in a test vehicle to log and verify DSRC messages.

![CVTT with Wireshark Laptop setup in a test vehicle](image)

**Figure 11: Demonstration Area: Test Tool Setup**

*Source: City of Columbus*

It's important to note that this vehicle was stationary during testing.

### 3.6.3. Field Testing

After SST was successfully completed in the Lab and Demonstration Area, Roadside Equipment were installed at 6 field project intersections. SST was performed at each of the 6 locations to ensure configuration or other issues were not overlooked during Demonstration Area testing. **Figure 11** shows the CVTT with Wireshark Laptop setup and **Figure 12** shows the location of the First Article intersections, from the CMCC.
During Field SST, the test vehicle was either stationary or a data recorder, following COVID protocols, was in the vehicle during testing.

After the completion of Field Testing SST, 30-Day Burn-In testing was conducted on these same 6 intersections, to ensure the reliable and sustained operation of the Roadside Equipment.

### 3.6.4. Final Acceptance Testing

Final Acceptance test was performed, in the Demonstration Area, in October of 2020 sufficient for system “Go-Live” sign-off. Go-Live Acceptance Testing consisted of verifying the Roadside Units were broadcasting messages with the correct content, ASDs were providing appropriate driver alerts, and VADs were requesting and granted transit signal priority, freight signal priority, and emergency vehicle preemption. A final SST test session was performed in December 2020 to address outstanding issues from October, not related to Go-Live criteria.

### 3.7. VARIANCES

This section documents several variances observed and accounted for during CVE Testing, ranging from the COVID-19 Pandemic, FCC’s announced intention to reallocate the 5.9 GHz band, and differences and limitations in equipment operation.

#### 3.7.1. Schedule impact of COVID-19

Travel restrictions due to COVID-19 were put in place in March 2020, shortly after the completion of SST Lab testing. The team was able to conduct limited virtual testing during the lock-down, between March and June 2020. Local WSP staff and City of Columbus Staff drove test vehicles in the Demonstration Area with WNC and Kapsch staff remotely logged into the OBU’s and RSU’s, respectively. In-person testing, following COVID-19 protocols, resumed in July 2020. An additional testing session was performed in the
Demonstration Area in August 2020, again following COVID-19 protocols. Go-Live Final Acceptance Testing was competed in October 2020, with a follow up session completed in December 2020, following COVID-19 protocols.

### 3.7.2. DSRC Channel Plan

Due to the re-allocation of the 5.9 GHz band proposed by the Federal Communications Commission (FCC) in its Notice of Proposed Rulemaking (NPRM) released on November 12, 2019, and the limitation that the FCC would only grant RSU licenses for the existing DSRC 10 MHz Channel 180, Smart Columbus decided to modify its DSRC Service Channel plan to only broadcast V2I messages on Channel 180. The WSA, normally broadcast on the Control Channel, 178, was also moved to broadcast on Service Channel 180. Since DSRC OBUs do not require an FCC license, vehicle-to-vehicle communications remain on the Safety Channel, 172.

### 3.7.3. Channel 180 Congestion Tests

The Test Plan called for testing Channel 180 congestion in a build-up format; starting with 1 OBU with 1 RSU and adding OBUs until either an application(s) failed due to not receiving expected messages (channel congestion) or when 5 OBUs were operating simultaneously.

Congestion Testing began with verifying 1 VAD w/Transit Signal Priority could request, and be granted, Signal Priority while performing a firmware request and download from a single RSU. This test encompassed SPaT, MAP, SRM, SSM, and IPv6 services on Channel 180.

In order to streamline testing, after the successfully completion of the 1 VAD with Transit Signal Priority test, the team moved straight to the 5 OBU Test; 4 ASDs running the RLVW application while downloading firmware updates and 1 VAD w/Transit Signal Priority requesting Signal Priority while downloading a firmware update from the same RSU. The thought was that if the 5 OBU test was successfully, the same test with fewer OBUs would be successful as well. This test encompassed the RLVW application, SPaT, MAP, SRM, SSM, TIM, and IPv6 from 1 RSU.

If the 5 OBU test would have failed, the team would have decreased the number of OBUs until the Test passed; ultimately identifying the system breaking point.

### 3.7.4. WSA

According to FHWA RSU Specification 4.1, Provider Service Identifiers (PSID) for messages sent to the RSU as Immediate Forward for broadcast on a Service Channel, shall be advertised in the WSA. This is to inform OBUs as to the services that are available from the RSU. However, in traditional Connected Vehicle deployments, SPaT and MAP are broadcast on the Safety Channel, 172, but not advertised in the WSA. The rational is that when an OBU is broadcasting BSMs on Channel 172 in the vicinity of an RSU broadcasting SPaT and MAP on Channel 172, the OBU will naturally receive SPaT and MAP.

The Message Handler sends SPaT and MAP (and TIM) messages to the RSU as Immediate Forward messages. Kapsch and Danlaw RSUs follow the OBU will receive SPaT and MAP when broadcasting BSMs philosophy and do not advertise SPaT and MAP in the WSA, however, Siemens RSUs follow the RSU Specification 4.1 requirement that Provider Service Identifiers (PSID) for messages sent to the RSU as Immediate Forward for broadcast on a Service Channel, shall be advertised in the WSA.

Additional development would have been required for the WSAs from all three RSUs to contain the same content; either Kapsch and Danlaw RSUs advertise SPaT and MAP or the Siemens RSUs do not advertise SPaT and MAP. The team decided to accept two versions of the WSA; 1 in which SPaT and MAP are not advertised (Kapsch and Danlaw) and 1 in which SPaT and MAP are advertised (Siemens).
As discussed in Section 3.7.2 DSRC Channel Plan, V2I messages, including SPaT, MAP, TIM, SSM, and WSA's are broadcast on Service Channel 180. As OBUs, monitor channel 180 for WSA's they will receive SPaT, MAP, TIMs, and SSMs as applicable.

### 3.7.5. Signal Preemption/Priority

The CVE Design calls for OBUs to include the appropriate Vehicle Role (transit, truck, fire, police) in the SRM and sign the SRM with an IEEE 1609.2-2016 certificate containing Service Specific Permissions (SSP) for the applicable Vehicle Role. The RSU would verify the SRM signature and, if valid, forward the message and certificate to the Message Handler for further processing. The Message Handler would compare the SRM Vehicle Role with the SSP contained in the certificate. If they matched, the Message Handler would send a Priority or Preemption request to the Traffic Signal Controller, based on the SRM Vehicle Role. If the SRM Vehicle Role was “Transit” or “Truck”, Signal Priority was requested. Transit Signal Priority is only enabled on Cleveland Ave and Freight Signal Priority is only enabled on the Alum Creek corridor and a portion of Morse Rd to the east of I-270. If the SRM Vehicle Role was “Fire” or “Police”, Signal Preemption was requested. Signal Preemption is only enabled on the Morse, Cleveland, and High St corridors.

RSUs verify SRM signatures but do not include the 1609.2-2016 certificate when forwarding SRMs to the Message Handler. Without the certificate the Message Handler cannot compare the SRM Vehicle Role to the SSP, therefore this second verification cannot be performed.

The fact that RSUs verify message signatures before forwarding, limits forwarding to only messages signed with certificates generated by the same SCMS that provides Smart Columbus certificates.

There is not a specific CVE requirement for RSUs to include the 1609.2 certificate when forwarding messages. The City did consult with the RSU manufacturers about adding this functionality. The outcome of these discussions was that additional development, compensation, and a delay in schedule, would be required for the RSUs to include the 1609.2 certificate when forwarding SRMs to the Message Handler.

Given the RSUs verify SRM certificates, Signal Priority and Preemption are limited to specific corridors and the overall number of OBUs, in general, in the Columbus area is low, the team felt the risk of a non-Smart Columbus OBU requesting and being granted Signal Priority/Preemption was low and determined to move forward without comparing the SRM Vehicle Role to the certificate SSP.

### 3.7.6. RTCM

During Demonstration Area SST, several application tests were conducted with the OBUs configured to utilize RTCM for position correction. Utilizing RTCM position correction made OBU position accuracy worse, not better. WNC worked extensively with their GPS chip provider, however, the GPS chip provider was not able to resolve the issue.

Even if the OBU could utilize RTCM effectively, the OBU would need to constantly receive RTCM corrections in order to maintain position accuracy. This would not have been possible, as RSUs are only deployed on specific corridors. Given that OBUs could not effectively utilize RTCM corrections and even if they could it required constant updates, the Smart Columbus Team decided to not utilize RTCM position corrections for the OBUs. RSUs broadcast RTCM, but OBUs do not utilize them.
3.8. REFERENCES

Table 8 below contains the Smart Columbus documents which provide additional background on the CVE project and should be referred for details on user needs, requirements, and contractual agreements that guided the development of this Test Report.

Table 8: References

<table>
<thead>
<tr>
<th>Title</th>
<th>Pub. Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>City of Columbus Solicitation Number: RFQ011270, Connected Vehicle Environment On-Board Unit Integrator Request for Proposal, Smart Columbus, Capital Improvements Project No: 530163 – 100030</td>
<td>January 29, 2019</td>
</tr>
<tr>
<td>City of Columbus Solicitation Number: RFQ011273, Connected Vehicle Environment Road-Side Unit Integrator Request for Proposal, Smart Columbus, Capital Improvements Project No: 530163 – 100031</td>
<td>January 29, 2019</td>
</tr>
<tr>
<td>Connected Vehicle Environment (CVE) Concept of Operation for the Smart Columbus Demonstration Program</td>
<td>August 07, 2018</td>
</tr>
<tr>
<td>Connected Vehicle Environment (CVE) System Requirements for the Smart Columbus Demonstration Program</td>
<td>November 30, 2018</td>
</tr>
<tr>
<td>Connected Vehicle Environment (CVE) Interface Control Document for the Smart Columbus Demonstration Program</td>
<td>May 4, 2021</td>
</tr>
<tr>
<td>Connected Vehicle Environment (CVE) System Design Document for the Smart Columbus Demonstration Program</td>
<td>March 10, 2021</td>
</tr>
<tr>
<td>Connected Vehicle Environment (CVE) Test Plan for the Smart Columbus Demonstration Program</td>
<td>April 17, 2020</td>
</tr>
</tbody>
</table>

Source: City of Columbus

This Test Report was adopted from the IEEE 829-2008 Standard for Software and System Test Documentation.
Chapter 4. Test Results

This section presents the results of testing for each of the tests performed. It also includes a defect management log with outstanding issues, design changes, and high-level metrics of the testing process.

4.1. TEST RESULTS

As mentioned in Section 3.6 Testing Locations testing took place between November 2019 through December 2020, with suspensions between March 2020 and June of 2020 due to the COVID-19 Pandemic.

Throughout testing, issues, comments and solutions were recorded through a series of web-based, shared documents. This format allowed issues to be communicated and addressed on an ongoing basis by all personnel, including the Smart Columbus team, the OBU integration team, and the RSU integration team.

As in the Test Plan, tests focused on functionality of individual components as well as subsystems. Results are reported in this Subsection by component/subsystem.

Test data including pcap files, CVTT log files, screenshots, data recorder logs, and other files are available on the Smart Columbus SharePoint Site (https://smartcolumbusprogram.sharepoint.com/Task%20B%20CVE%20Deliverables/Forms/ContentType.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence) for USDOT. The Test Status field in the following tables provide a simplified view of the result of each Test Case. Test Status has one have the following values:

- **PASS** – indicates the component or subsystem test resulted in the expect outcome of the Test Case
- **Implicit Pass** – indicates a test was not explicitly conducted for the subject Test Case, however, component or subsystem tests for one or more similar Test Cases resulted in the expect outcome of the subject Test Case
- **Failed** – indicates the component or subsystem test did not result in the expect outcome of the Test Case. Further action is required.
- **In Progress** – indicates the data required to evaluate the functionality of the component or subsystem has been collected, but has not been analyzed to determine if the test passed or failed
- **Deprecated** – indicates the requirement or function associated with the Test Case was removed, therefore the test was not conducted.
- **Deferred** – indicates development is required or the subject component or subsystem requires a software or firmware update before it can perform the function(s) associated with the Test Case.
### 4.1.1. OBU Tests

Table 9 contains the OBU Test Results.

Table 9: OBU Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU001-v01 | Verify OBUs broadcast BSMs as defined in SAE J2945/1 (10 BSMs/sec) | 1. Power on the OBU under test  
2. Power on the connected vehicle test tool (CVTT)  
3. Capture 5 minutes of BSMs with the CVTT  
4. Review pcap file to confirm OBU broadcast 10 BSMs/sec | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 10/12/2020 - 10/14/2020 | 10/12/2020: HDV, Police, Fire, and Transit  
10/14/2020: LDV |
| CVE-OBU002-v02 | Verify a transit vehicle FCW interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) is stopped in the roadway  
2. Vehicle with OBU2 (V2) (transit) approaches V1 from behind  
3. Based on BSMs from OBU1, OBU2 determines a threat exists  
4. Since V2 (transit) does not contain an HMI, OBU2 only records the FCW event  
5. Review V2 (transit) OBU2 log files to confirm FCW was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 12/17/2020 | Reviewed COTA TVIER Logs |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU003-v02  | Verify a transit vehicle EEBL interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) leads vehicle with OBU2 (V2) (transit) on the roadway  
2. V1 performs a hard-braking maneuver such that an EEBL event flag is set in its BSMs  
3. Based on BSMs from OBU1, OBU2 determines a threat exists  
4. Since V2 (transit) does not contain a HMI, OBU2 only records the EEBL event  
5. Review V2 (transit) OBU2 log files to confirm EEBL was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 01/13/2021 | Reviewed TVIER Logs |
| CVE-OBU004-v02  | Verify a transit vehicle IMA interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) approaches vehicle with OBU2 (V2) (transit) in roadway segment in a lane to the left of V2  
2. V2 begins to turn left in front of V1  
3. Based on BSMs from OBU1, OBU2 determines a threat exists  
4. Since V2 (transit) does not contain a HMI, OBU2 only records the IMA event  
5. Review V2 (transit) OBU2 log files to confirm IMA was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 01/13/2021 | Reviewed TVIER Logs |
| CVE-OBU005-v02  | Verify a transit vehicle LCW interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) drives on the left side of the vehicle with OBU2 (V2) (transit)  
2. V2 attempts to change lanes to the left  
3. Based on BSMs from OBU1, OBU2 determines a threat exists  
4. Since V2 (transit) does not contain a HMI, OBU2 only records the LCW event  
5. Review V2 (transit) OBU2 log files to confirm LCW was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 12/17/2020 | Reviewed TVIER Logs |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU006-v02    | Verify a transit vehicle RLVW interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) (transit) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
2. V1 maintains constant speed and heading  
3. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists  
4. Since V1 (transit) does not contain and HMI, OBU1 only records the RLVW event  
5. Review V2 (transit) OBU1 log files to confirm RLVW was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 12/17/2020  | Reviewed TVIER Logs                                           |
| CVE-OBU007-v02    | Verify a transit vehicle RSSZ interaction event log consists of all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) (transit) approaches the school zone segment above the school zone speed limit  
2. Based on the RSSZ from the RSU, OBU1 determines a threat exists  
3. Since V1 (transit) does not contain and HMI, OBU1 only records the RSSZ event  
4. Review V2 (transit) OBU1 log files to confirm RSSZ was recorded | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 01/13/2021  | Reviewed TVIER Logs                                           |
| CVE-OBU008-v02    | Verify a transit vehicle TSP interaction event log consists of an SRM and all received messages for a predetermined period before and after the warning generating the event was issued | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal priority  
3. OBU1 records the SRM event | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 02/08/2021  | Reviewed CMAX OBU logs                                      |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU009-v01 | Verify a Transit vehicle OBU logs messages (SPaT, MAP, SRM, SSM, TIM) that it receives for a pre-determined period | 1. Vehicle with OBU1 (V1) approaches the intersection  
2. OBU1 records SPaT, MAP, TIM, and WSA | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 12/17/2020 | Reviewed TVIER Logs |
| CVE-OBU011-v01 | Verify a transit vehicle OBU uploads transit vehicle interaction event data to the TrCVMS when arriving to the COTA garage, and deletes local transit vehicle interaction events after uploading | 1. OBU1 approaches RSU and begins offloading its log files to the TrCVMS  
2. OBU1 deletes its log files, once off loaded  
3. Verify log files are archived in the TrCVMS  
4. Verify OBU1 deleted its log files | • Test Conductor  
• Transit Data Consumer  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 12/17/2020 | Reviewed TVIER Logs |
| CVE-OBU012-v01 | Verify the EV OBU broadcasts SRMs only when lights and sirens are active, and it is approaching an equipped intersection | 1. EV approaches the demonstration area intersection with its lights and sirens off (not requesting preemption)  
2. EV approaches the demonstration area intersection with its lights and sirens on at a speed in which OBU1 broadcasts SRMs (to request preemption) | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | Police and Fire OBUs (OBU version 14) |
## Chapter 4. Test Results

### CVE-OBU013-v01

**Verify the EV OBU receives an SSM**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>EV approaches the demonstration area intersection with its lights and sirens on at a speed in which OBU broadcasts SRMs (to request preemption)</td>
</tr>
<tr>
<td>2.</td>
<td>RSU forwards SRMs to Message Handler</td>
</tr>
<tr>
<td>3.</td>
<td>Message Handler sends a preemption call to the Signal Controller</td>
</tr>
<tr>
<td>4.</td>
<td>Signal controller sends signal status data to the Message Handler</td>
</tr>
<tr>
<td>5.</td>
<td>Message Handler sends SSMs to the RSU</td>
</tr>
<tr>
<td>6.</td>
<td>RSU broadcast SSMs</td>
</tr>
<tr>
<td>7.</td>
<td>OBU receives and logs SSMs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test Conductor</th>
<th>OBU Data Producer</th>
<th>Vehicle Drivers</th>
<th>Data Recorder</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Results:**

- **Pass:** 10/14/2020 (OBU version 14)
- **Police OBU:** Kapsch RSU, Econolite Controller
- **Fire OBU:** Siemens RSU, Econolite Controller
- **Other:**
  - Police OBU: Danlaw RSU, Econolite Controller
  - Fire OBU: Siemens RSU, Econolite Controller

---

**Test Conductor:**

- Test Conductor
- OBU Data Producer
- Vehicle Drivers
- Data Recorder

---

**Note:**

- The report includes a detailed list of test conductors and their respective roles, such as OBU data producer and vehicle drivers. The results are marked as Pass on 10/14/2020, indicating successful completion of the test scenario.
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU014-v02  | Verify the transit vehicle OBU broadcasts SRMs only when approaching an equipped intersection | 1. OBU drives around the demonstration area, avoiding the intersection (not requesting priority)  
2. OBU approaches the demonstration area intersection at a speed in which OBU1 broadcasts SRMs (to request priority) | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | (OBU version 14) |
| CVE-OBU015-v01  | Verify the transit vehicle OBU receives an SSM                             | 1. A location is set up as an intersection in the demonstration area  
2. RSU is broadcasting SPaT and MAP for the intersection in the demonstration area and WSAs advertising SRM on Channel 180  
3. CVTT is configured to capture packets on Channel 180  
4. OBU1 approaches the demonstration area intersection at a speed in which OBU1 broadcasts SRMs (to request priority)  
5. RSU forwards SRMs to Message Handler  
6. Message Handler sends a priority call to the Signal Controller  
7. Signal controller sends signal status data to the Message Handler  
8. Message Handler sends SSMs to the RSU  
9. RSU broadcast SSMs  
10.OBU1 receives and logs SSMs | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | (OBU version 14) |

| Transit Vehicle OBU  
Kapsch RSU  
Econolite Controller | Transit Vehicle OBU  
Danlaw RSU  
Econolite Controller | Transit Vehicle OBU  
Siemens RSU  
Econolite Controller |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU016-v01 | Verify the HDV OBU broadcasts SRMs only when approaching an equipped intersection | 1. A location is set up as an intersection in the demonstration area  
2. RSU is broadcasting SPaT and MAP for the intersection in the demonstration area and WSAs advertising SRM on Channel 180  
3. CVTT is configured to capture packets on Channel 180  
4. OBU1 drives around the demonstration area, avoiding the intersection (not requesting priority)  
5. OBU1 approaches the demonstration area intersection at a speed in which OBU1 broadcasts SRMs (to request priority) | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 10/14/2020 | (OBU version 14)  
HD Vehicle OBU  
Kapsch RSU  
Econolite Controller |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-OBU017-v01</td>
<td>Verify the HDV OBU receives an SSM</td>
<td>1. A location is set up as an intersection in the demonstration area</td>
<td>• Test Conductor</td>
<td>PASS</td>
<td>10/14/2020</td>
<td>(OBU version 14)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. RSU is broadcasting SPaT and MAP for the intersection in the demonstration area and WSAs advertising SRM on Channel 180</td>
<td>• OBU Data Producer</td>
<td></td>
<td></td>
<td>HD Vehicle OBU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. CVTT is configured to capture packets on Channel 180</td>
<td>• Vehicle Drivers</td>
<td></td>
<td></td>
<td>Kapsch RSU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection</td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td>Econolite Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. OBU1 broadcast SRMs on Channel 180</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. RSU forwards SRMs to Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Message Handler sends a priority call to the Signal Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Signal controller sends signal status data to the Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Message Handler sends SSMs to the RSU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. RSU broadcast SSMs on Channel 180</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>11. OBU1 receives and logs SSMs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU018-v01 | Verify a host transit vehicle OBU broadcasts SRMs, receives SSMs, and logs the TSP event with congestion on Channel 180. | 1. A location is set up as an intersection in the demonstration area  
2. RSU is broadcasting SPaT and MAP for an intersection in the demonstration area and WSAs advertising SRM on Channel 180  
3. CVTT is configured to capture packets on Channel 180  
4. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
5. OBU1 broadcast SRMs on Channel 180  
6. RSU forwards SRMs to Message Handler  
7. Message Handler sends a priority call to the Signal Controller  
8. Signal controller sends signal status data to the Message Handler  
9. Message Handler sends SSMs to the RSU  
10. RSU broadcast SSMs on Channel 180  
11. OBU1 logs received messages and TSP Event | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS          | 10/14/2020   | (OBU version 14)  
Transit Vehicle OBU  
Kapsch RSU  
Econolite Controller |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU019-v01    | Verify a host transit vehicle OBU broadcasts SRMs, receives SSMs, logs the TSP event, and downloads a firmware update with congestion on Channel 180. 1-Transit OBU (SRM, OTA) 1 RSU (SPaT, MAP, SSM, and WSA) | 1. A location is set up as an intersection in the demonstration area  
2. RSU is broadcasting SPaT and MAP for the intersection in the demonstration area and WSAs advertising SRM and IP Services on Channel 180  
3. CVTT is configured to capture packets on Channel 180  
4. Vehicle with OBU1 (V1) drives into communication range of the RSU  
5. OBU1 begins downloading a firmware update on Channel 180  
6. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
7. OBU1 broadcast SRMs  
8. RSU forwards SRMs to Message Handler  
9. Message Handler sends a priority call to the Signal Controller  
10. Signal controller sends signal status data to the Message Handler  
11. Message Handler sends SSMs to the RSU  
12. RSU broadcast SSMs on Channel 180  
13. OBU1 logs received messages and TSP Event  
14. OBU1 completes firmware download | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS          | 10/15/2020        | (OBU version 14)  
Transit Vehicle OBU  
Kapsch RSU  
Econolite Controller |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU020-v01  | Verify an LDV OBU can request, download, and apply a new firmware update     | 1. Vehicle with OBU1 (V1) drives into communication range of the RSU  
2. Vehicle with OBU1 (V1) begins downloading a firmware update on Channel 180  
3. Once firmware is downloaded, the OBU is powered down  
4. Upon power down, OBU1 (V1) updates its firmware  
5. After 5 minutes, OBU1 (V1) is powered on  
6. OBU1 (V1) displays new firmware version during boot up | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020  | (OBU version 14) Siemens RSU |
| CVE-OBU021-v01  | Verify a transit OBU can request, download, and apply a new firmware update | 1. Vehicle with OBU1 (V1) drives into communication range of the RSU  
2. Vehicle with OBU1 (V1) begins downloading a firmware update on Channel 180  
3. Once firmware is downloaded, the OBU is powered down  
4. Upon power down, OBU1 (V1) updates its firmware  
5. After 5 minutes, OBU1 (V1) is powered on  
6. OBU1 (V1) displays new firmware version during boot up | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020  | (OBU version 14) Kapsch RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-OBU022-v01</td>
<td>Verify an EV-Police OBU can request, download, and apply a new firmware update through each RSU Manufacturer</td>
<td>1. Vehicle with OBU1 (V1) drives into communication range of the RSU 2. Vehicle with OBU1 (V1) begins downloading a firmware update on Channel 180 3. Once firmware is downloaded, the OBU is powered down 4. Upon power down, OBU1 (V1) updates its firmware 5. After 5 minutes, OBU1 (V1) is powered on 6. OBU1 (V1) displays new firmware version during boot up</td>
<td>• Test Conductor  • OBU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>PASS</td>
<td>10/12/2020</td>
<td>(OBU version 14) Kapsch RSU</td>
</tr>
<tr>
<td>CVE-OBU022-v01</td>
<td>Verify an EV-Fire OBU can request, download, and apply a new firmware update through each RSU Manufacturer</td>
<td>1. Vehicle with OBU1 (V1) drives into communication range of the RSU 2. Vehicle with OBU1 (V1) begins downloading a firmware update on Channel 180 3. Once firmware is downloaded, the OBU is powered down 4. Upon power down, OBU1 (V1) updates its firmware 5. After 5 minutes, OBU1 (V1) is powered on 6. OBU1 (V1) displays new firmware version during boot up</td>
<td>• Test Conductor  • OBU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>PASS</td>
<td>10/12/2020</td>
<td>(OBU version 14) Danlaw RSU</td>
</tr>
</tbody>
</table>
### Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU023-v01 | Verify an HDV OBU can request, download, and apply a new firmware update through each RSU Manufacturer | 1. Vehicle with OBU1 (V1) drives into communication range of the RSU  
2. Vehicle with OBU1 (V1) begins downloading a firmware update on Channel 180  
3. Once firmware is downloaded, the OBU is powered down  
4. Upon power down, OBU1 (V1) updates its firmware  
5. After 5 minutes, OBU1 (V1) is powered on  
6. OBU1 (V1) displays new firmware version during boot up | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020 | (OBU version 14)  
Danlaw RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU024-v01    | Verify an LDV OBU can request, download, and apply new 1609.2-2016 Certificates through each RSU Manufacturer                                                                                           | 1. Data Producer, removes the last 2 batches of certificates stored on the OBU  
2. Data Recorder observes that the last 2 batches of certificates have been removed from the OBU  
3. Vehicle with OBU1 (V1) drives into communication range of the RSU  
4. Vehicle with OBU1 (V1) sends a request to download the last 2 batches of certificates to the SCMS on Channel 180  
5. Vehicle with OBUs (V1) drives out of RSU communication range  
6. Vehicle with OBU1 (V1) drives back into communication range of the RSU  
7. Vehicle with OBU1 (V1) sends a request to download the certificates requested in step 4  
8. OBU1 downloads certificates on Channel 180  
9. Data recorder observes additional certificates stored on the OBU | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder                                                                 | PASS           | 10/15/2020              | (OBU version 14) Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU025-v01    | Verify a transit OBU can request, download, and apply new 1609.2-2016      | 1. Data Producer, removes the last 2 batches of certificates stored on the OBU  
2. Data Recorder observes that the last 2 batches of certificates have been removed from the OBU  
3. Vehicle with OBU1 (V1) drives into communication range of the RSU  
4. Vehicle with OBU1 (V1) sends a request to download the last 2 batches of certificates to the SCMS on Channel 180  
5. Vehicle with OBUs (V1) drives out of RSU communication range  
6. Vehicle with OBU1 (V1) drives back into communication range of the RSU  
7. Vehicle with OBU1 (V1) sends a request to download the certificates requested in step 4  
8. OBU1 downloads certificates on Channel 180  
9. Data recorder observes additional certificates stored on the OBU | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS                    | 10/15/2020                      | (OBU version 14)  
Kapsch RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU026-v01 | Verify an EV-Police OBU can request, download, and apply new 1609.2-2016 Certificates through each RSU Manufacturer | 1. Data Producer, removes the last 2 batches of certificates stored on the OBU  
2. Data Recorder observes that the last 2 batches of certificates have been removed from the OBU  
3. Vehicle with OBU1 (V1) drives into communication range of the RSU  
4. Vehicle with OBU1 (V1) sends a request to download the last 2 batches of certificates to the SCMS on Channel 180  
5. Vehicle with OBUs (V1) drives out of RSU communication range  
6. Vehicle with OBU1 (V1) drives back into communication range of the RSU  
7. Vehicle with OBU1 (V1) sends a request to download the certificates requested in step 4  
8. OBU1 downloads certificates on Channel 180  
9. Data recorder observes additional certificates stored on the OBU | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 10/15/2020 | (OBU version 14)  
Kapsch RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU026-v01   | Verify an EV-Fire OBU can request, download, and apply new 1609.2-2016 Certificates through each RSU Manufacturer | 1. Data Producer, removes the last 2 batches of certificates stored on the OBU  
2. Data Recorder observes that the last 2 batches of certificates have been removed from the OBU  
3. Vehicle with OBU1 (V1) drives into communication range of the RSU  
4. Vehicle with OBU1 (V1) sends a request to download the last 2 batches of certificates to the SCMS on Channel 180  
5. Vehicle with OBUs (V1) drives out of RSU communication range  
6. Vehicle with OBU1 (V1) drives back into communication range of the RSU  
7. Vehicle with OBU1 (V1) sends a request to download the certificates requested in step 4  
8. OBU1 downloads certificates on Channel 180  
9. Data recorder observes additional certificates stored on the OBU | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/15/2020 | (OBU version 14)  
Danlaw RSU |
### Test Case ID: CVE-OBU027-v01

**Objective:** Verify an HDV OBU can request, download, and apply new 1609.2-2016 Certificates through an RSU.

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-OBU027-v01 | Verify an HDV OBU can request, download, and apply new 1609.2-2016 Certificates through an RSU | 1. Data Producer, removes the last 2 batches of certificates stored on the OBU  
2. Data Recorder observes that the last 2 batches of certificates have been removed from the OBU  
3. Vehicle with OBU1 (V1) drives into communication range of the RSU  
4. Vehicle with OBU1 (V1) sends a request to download the last 2 batches of certificates to the SCMS on Channel 180  
5. Vehicle with OBUs (V1) drives out of RSU communication range  
6. Vehicle with OBU1 (V1) drives back into communication range of the RSU  
7. Vehicle with OBU1 (V1) sends a request to download the certificates requested in step 4  
8. OBU1 downloads certificates on Channel 180  
9. Data recorder observes additional certificates stored on the OBU | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 10/15/2020 (OBU version 14) | Danlaw RSU |

*Source: City of Columbus*
### 4.1.2. OBU Applications

Table 10 contains the OBU Application Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App001-v01| Verify a host LDV OBU issues an EEBL warning when it receives a BSM from a remote OBU (under conditions in which an EEBL warning should be issued) | 1. Vehicle with OBU1 (V1) leads vehicle with OBU2 (V2) on the road segment  
2. V1 performs a hard-braking maneuver such that an EEBL event flag is set in OBU1’s BSM.  
3. Based on BSMs from OBU1, OBU2 determines a threat exists, and issues an EEBL alert to the driver  
4. Data recorder logs an EEBL alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020 (OBU version 14)        |                                           |
| CVE-App002-v01| Verify a host LDV OBU issues an FCW warning when it receives a BSM from a remote OBU (under conditions in which an FCW warning should be issued) | 1. Vehicle with OBU1 (V1) is stopped on the roadway segment  
2. Vehicle with OBU2 (V2) approaches V1 from behind  
3. Based on BSMs from OBU1, OBU2 determines a threat exists and issues an FCW alert  
4. Data recorder logs an FCW alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020 (OBU version 14)        |                                           |
| CVE-App003-v01| Verify a host LDV OBU issues an LCW warning when it receives a BSM from a remote OBU (under conditions in which an LCW warning should be issued) | 1. Vehicle with OBU1 (V1) drives next to the vehicle with OBU2 (V2), on the left side  
2. V2 attempts to change lanes to the left  
3. Based on BSMs from OBU1, OBU2 determines a threat exists and issues an LCW alert  
4. Data recorder logs an LCW alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/13/2020 (OBU version 14)        |                                           |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App004-v01 | Verify a host LDV OBU issues an IMA warning when it receives a BSM from a remote OBU (under conditions in which an IMA warning should be issued) | 1. Vehicle with OBU1 (V1) approaches vehicle with OBU2 (V2) in the lane to the left of V2  
2. V2 begins to turn left in front of V1  
3. Based on BSMs from OBU1, OBU2 issues an IMA alert  
4. Data recorder logs an IMA alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS        | 10/13/2020  | (OBU version 14) |
| CVE-App005-v01 | Verify a host LDV OBU issues an RLVW warning when it receives SPA-T and MAP from an RSU (under conditions in which an RLVW warning should be issued) | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
2. V1 maintains constant speed and heading  
3. Based on SPA-T and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert  
4. Data recorder logs an RLVW alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS        | 10/14/2020  | (OBU version 14)  
Kapsch RSU/Econolite Signal Controller  
Danlaw RSU/Econolite Signal Controller  
Siemens RSU/Econolite Signal Controller |
| CVE-App006-v01 | Verify a host LDV OBU issues an RSSZ warning when it receives a TIM from an RSU (under conditions in which an RSSZ warning should be issued) | 1. Vehicle with OBU1 (V1) approaches the school zone segment above the school zone speed limit  
2. Based on the TIM from the RSU, OBU1 determines a threat exists and issues RSSZ alert  
3. Data recorder logs an RSSZ alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS        | 10/14/2020  | (OBU version 14)  
Kapsch RSU/Econolite Signal Controller  
Danlaw RSU/Econolite Signal Controller  
Siemens RSU/Econolite Signal Controller |
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App008-v01 | Verify a high-priority warning takes precedence over a low priority warning when both warning types are present | 1. Vehicle with OBU1 (V1) leads vehicle with OBU2 (V2) in the school zone driving above the school zone speed limit  
2. Both V1 and V2 drivers receive RSSZ alerts  
3. While in the school zone, V1 performs a hard-braking maneuver such that an EEBL event is contained in its BSM.  
4. Verify the HMI in V2 only shows an EEBL warning | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | (OBU version 14) |
| CVE-App009-v01 | Verify a host LDV OBU issues an RLVW warning (under conditions in which an RLVW warning should be issued) when SPaT, MAP, TIM, and WSAs are broadcast on Channel 180 from the same RSU | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
2. V1 maintains constant speed and heading  
3. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert  
4. Data recorder observes a RLVW alert on OBU1’s HMI and logs the alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | (OBU version 14)  
Kapsch RSU  
Danlaw RSU  
Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-App010-v01</td>
<td>Verify a host LDV OBU issues an RLVW warning (under conditions in which an RLVW warning should be issued) when a firmware update is in process and SPaT, MAP, TIM, and WSAs are broadcast on Channel 180 from the same RSU 1-LDV OBU (RLVW, OTA) 1 RSU (SPaT, MAP, TIM, WSA)</td>
<td>1. Vehicle with OBU1 (V1) drives into communication range of the RSU 2. Vehicle with OBU1 (V1) begins downloading a firmware update 3. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection 4. V1 maintains constant speed and heading 5. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert 6. Data recorder observes a RLVW alert on OBU1’s HMI and logs the alert in the test log</td>
<td>• Test Conductor  • OBU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>Implicit PASS</td>
<td>10/16/2020</td>
<td>Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 1 OBU will pass</td>
</tr>
</tbody>
</table>
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-App00011_v01</td>
<td>Verify a host LDV OBU issues an RLVW warning (under conditions in which an RLVV warning should be issued) when a Transit vehicle OBU is broadcasting SRMs and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU</td>
<td>1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection 2. V1 maintains constant speed and heading 3. Vehicle with OBU2 (V2) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection 4. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert 5. Based on the SPaT, MAP, and WSA from the RSU, OBU2 broadcasts an SRM, requesting signal priority 6. Data recorder observes a RLVW alert on OBU1’s HMI and logs the alert in the test log</td>
<td>• Test Conductor  • OBU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>Implicit PASS</td>
<td>10/16/2020</td>
<td>Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 2 OBU will pass</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>CVE-App012-v01</td>
<td>Verify a host LDV OBU issues an RLVW warning (under conditions in which an RLVV warning should be issued) when a Transit vehicle OBU is broadcasting SRMs, a firmware update is in process, and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU</td>
<td>1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection 2. V1 maintains constant speed and heading 3. Vehicle with OBU2 (V2) drives into communication range of the RSU 4. Vehicle with OBU2 (V2) begins downloading a firmware update 5. Vehicle with OBU2 (V2) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection 6. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVV alert 7. Based on the SPaT, MAP, and WSA from the RSU, OBU2 broadcasts an SRM, requesting signal priority 8. Data recorder observes a RLVV alert on OBU1’s HMI and logs the alert in the test log</td>
<td>• Test Conductor  • OBU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>Implicit PASS</td>
<td>10/16/2020</td>
<td>Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 2 OBU will pass</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CVE-App013-v01| Verify a host LDV OBU issues an RLVW warning (under conditions in which an RLVW warning should be issued) when a Transit vehicle OBU is broadcasting SRMs, 2 OBUs have a firmware update is in process, and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU | 1. Vehicle with OBU1 (V1) drives into communication range of the RSU  
2. Vehicle with OBU1 (V1) begins downloading a firmware update  
3. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
4. V1 maintains constant speed and heading  
5. Vehicle with OBU2 (V2) drives into communication range of the RSU  
6. Vehicle with OBU2 (V2) begins downloading a firmware update  
7. Vehicle with OBU2 (V2) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
8. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert  
9. Based on the SPaT, MAP, and WSA from the RSU, OBU2 broadcasts an SRM, requesting signal priority  
10. Data recorder observes a RLVW alert on OBU1’s HMI and logs the alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder  

| Implicit PASS | 10/16/2020 | Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 2 OBU will pass |
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App014-v01 | Verify 2 host LDV OBUs issue an RLVW warning (under conditions in which an RLVW warning should be issued) when a Transit vehicle OBU is broadcasting SRMs, 3 OBUs have a firmware update is in process, and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU | 1. Vehicle with OBU1 (V1) and OBU2 (V2) drives into communication range of the RSU  
2. OBU1 and OBU2 begin downloading a firmware update  
3. V1 and V2 approach the intersection at a speed in which the light will be Red when they arrive  
4. V1 and V2 maintain constant speed and heading  
5. Vehicle with OBU3 (V3) drives into communication range of the RSU  
6. OBU3 begins downloading a firmware update  
7. V3 approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
8. Based on SPaT and MAP from the RSU, OBU1 and OBU2 determine a threat exists and issues a RLVW alert  
9. Based on the SPaT, MAP, and WSA from the RSU, OBU3 broadcasts an SRM, requesting signal priority  
10. Data recorder1 observes a RLVW alert on OBU1 HMI and logs the alert in the test log  
11. Data recorder2 observes a RLVW alert on OBU2 HMI and logs the alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | Implicit PASS | 10/16/2020 | Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 3 OBU will pass |
## Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App015-v01 | Verify 3 host LDV OBUs issue an RLVW warning (under conditions in which an RLVW warning should be issued) when a Transit vehicle OBU is broadcasting SRMs, 4 OBUs have a firmware update in process, and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU | 1. Vehicle with OBU1 (V1), OBU2 (V2), and OBU3 (V3) drive into communication range of the RSU  
2. OBU1, OBU2, and OBU3 begin downloading a firmware update  
3. V1, V2, and V3 approach the intersection at a speed in which the light will be Red when they arrive  
4. V1, V2, and V3 maintain constant speed and heading  
5. Vehicle with OBU4 (V4) drives into communication range of the RSU  
6. OBU4 begins downloading a firmware update  
7. V4 approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
8. Based on SPaT and MAP from the RSU, OBU1, OBU2, and OBU3 determine a threat exists and issues a RLVW alert  
9. Based on the SPaT, MAP, and WSA from the RSU, OBU4 broadcasts an SRM, requesting signal priority  
10. Data recorder1 observes a RLVW alert on OBU1 HMI and logs the alert in the test log  
11. Data recorder2 observes a RLVW alert on OBU2 HMI and logs the alert in the test log  
12. Data recorder3 observes a RLVW alert on OBU3 HMI and logs the alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | Implicit PASS | 10/16/2020 | Since CVE-App016-v01 (using 5 OBUs) Passed, it is implied that a test with 4 OBU will pass |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-App016-v01 | Verify 4 host LDV OBUs issue an RLVW warning (under conditions in which an RLVW warning should be issued) when a Transit vehicle OBU is broadcasting SRMs, 5 OBUs have a firmware update is in process, and SPaT, MAP, TIM, SSMs, and WSAs are broadcast on Channel 180 from the same RSU | 1. Vehicle with OBU1 (V1), OBU2 (V2), OBU3 (V3), and OBU4 (V4) drive into communication range of the RSU  
2. OBU1, OBU2, OBU3, and OBU4 begin downloading a firmware update  
3. V1, V2, V3, and V4 approach the intersection at a speed in which the light will be Red when they arrive  
4. V1, V2, V3, and V4 maintain constant speed and heading  
5. Vehicle with OBU5 (V5) drives into communication range of the RSU  
6. OBU5 begins downloading a firmware update  
7. V5 approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
8. Based on SPaT and MAP from the RSU, OBU1, OBU2, OBU3, and OBU4 determine a threat exists and issues a RLVW alert  
9. Based on the SPaT, MAP, and WSA from the RSU, OBU5 broadcasts an SRM, requesting signal priority  
10. Data recorder1 observes a RLVW alert on OBU1 HMI and logs the alert in the test log  
11. Data recorder2 observes a RLVW alert on OBU2 HMI and logs the alert in the test log  
12. Data recorder3 observes a RLVW alert on OBU3 HMI and logs the alert in the test log  
13. Data recorder4 observes a RLVW alert on OBU4 HMI and logs the alert in the test log | • Test Conductor  
• OBU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS | 10/16/2020 | (OBU version 14) |

Source: City of Columbus
### 4.1.3. RSU-Kapsch

Table 11 contains the Kapsch RSU Test Results.

**Table 11: Kapsch RSU Test Results**

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU001-v02 | Verify RSU forwards BSMs, received from passing vehicles, to Message Handler | 1. OBU, broadcasting BSMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving BSMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 | |
| CVE-RSU002-v01 | Verify RSU forwards SRMs, received from approaching vehicles, to the Message Handler | 1. OBU, broadcasting SRMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving SRMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/14/2020 | |
| CVE-RSU003-v01 | Verify RSUs broadcast SPaT messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting SPaT from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SPaT based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 | |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU004-v01    | Verify SPaT broadcast by RSUs match the signal head status                | 1. Begin broadcasting SPaT from the Message Handler  
2. Begin broadcasting MAP from the Message Handler  
3. RSU broadcasts SPaT and MAP  
4. Using the CVTT SPaT/MAP visualization functionality, monitor the CVTT to verify SPaT status matches the signal head status for all lanes within the intersection | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 12/16/2020 | Compared Signal Controller Phase changes at the Lab with CVMS web-based SPaT Status |
| CVE-RSU006-v02    | Verify RSUs broadcast MAP messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 10/12/2020 |                                                                         |
| CVE-RSU007-v02    | Verify MAP message matches intersection geometry                          | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler  
3. Using the CVTT MAP display functionality verify the MAP message matches/aligns with the RSU installation intersection geometry | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 10/12/2020 |                                                                         |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU008-v01 | Verify RSUs broadcast RTCM messages received from the Message Handler over DSRC on Channel 180 once every 2 seconds | 1. Begin broadcasting RTCMs from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting RTCMs based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS        | 10/16/2020 |          |
| CVE-RSU009-v01 | Verify RSUs broadcast SSMs received from the Message Handler over DSRC on Channel 180 at 1 Hz | 1. Begin broadcasting SSMs from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SSM based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS        | 10/14/2020 |          |
| CVE-RSU010-v01 | Verify RSUs broadcast TIMs on Channel 180 at 1 Hz | 1. Begin broadcasting the TIM message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the TIM message provided by the Message Handler based on the message stored on the device  
3. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting TIMs based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS        | 10/14/2020 |          |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU011-v01| Verify RSUs report Channel Busy Ratio to TCVMS, when above a predetermined threshold | 1. RSU (2) is configured for a Channel Busy Ratio threshold of 5% (which should trigger a Channel Busy Report with minimal DSRC activity)  
2. Using the CVTT message capture functionality capture WSA, MAP, and TIMs from RSU (1)  
3. Begin broadcasting WSA, MAP, and TIM from RSU (1)  
4. Monitor RSU (2) to verify it detects a Channel Busy Ratio above 5% and sends a Channel Busy Report to the TCVMS | Deprecated                        | 10/14/2020 | RSU does not support this functionality |
| CVE-RSU012-v01| Verify RSU broadcast WSA with correct parameters (including WRA)            | 1. Begin broadcasting WSAs from the RSU  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting WSAs containing the correct parameters, including the WRA | Test Conductor  
OBU Data Producer  
RSU Data Producer  
Vehicle Driver  
Data Recorder | PASS       | 10/14/2020 |                                           |
| CVE-RSU013-v01| Verify IPv6 connectivity to SCMS                                           | 1. Remove certificates from the RSU  
2. From the RSU, initiate a certificate request to the SCMS  
3. Monitor the certificate directory on the RSU to verify the RSU has received and stored new certificates | Test Conductor  
OBU Data Producer  
RSU Data Producer  
Data Recorder | PASS       | 10/14/2020 |                                           |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU014-v01 | Document RSU Communication Range for RLVW on Channel 180                | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
2. V1 maintains constant speed and heading  
3. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert  
4. Data recorder logs an RLVW alert in the test log  
5. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT and Map message.  
6. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT and Map message  
7. Data recorder records the distance between the RSU and the first received SPaT and Map messages as the RSU RLVW Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 04/06/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for SPaT and MAP messages, required for RLVW, is between 500m and 600m |
### Test Case ID: CVE-RSU015-v01

**Objective:** Document RSU Communication Range for Signal Priority on Channel 180

**Procedure:**
1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal priority
3. OBU1 records the SRM event
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message.
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message.
6. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Priority Request Range in the test log

**Tester Role:**
- Test Conductor
- OBU Data Producer
- RSU Data Producer
- Vehicle Driver
- Data Recorder

**Test Status:** PASS

**Date Run:** 04/06/2021

**Comments:**
Due to COVID-19 contact tracing, data could not be collected when originally scheduled. Data collected 02/05/2021

Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Priority, is between 500m and 600m.
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU016-v01      | Document RSU Communication Range for Signal Preemption on Channel 180    | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal preemption  
3. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message  
4. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message  
5. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Preemption Request Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 04/06/2021  | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Preemption, is between 500m and 600m |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU017-v01 | Document RSU Communication Range for RSSZ on Channel 180 | 1. Vehicle with OBU1 (V1) approaches the school zone segment above the school zone speed limit  
2. Based on the TIM from the RSU, OBU1 determines a threat exists and issues and RSSZ alert  
3. Data recorder logs an RSSZ alert in the test log  
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received TIM.  
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received TIM.  
6. Data recorder records the distance between the RSU and the first received TIM as the RSSZ Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 04/06/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for TIM, required for RSSZ, is between 500m and 600m |
### 4.1.4. RSU-Danlaw

Table 12 contains the Danlaw RSU Test Results.

**Table 12: Danlaw RSU Test Results**

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU001-v02 | Verify RSU forwards BSMs, received from passing vehicles, to Message Handler | 1. OBU, broadcasting BSMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving BSMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 |           |
| CVE-RSU002-v01 | Verify RSU forwards SRMs, received from approaching vehicles, to the Message Handler | 1. OBU, broadcasting SRMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving SRMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/14/2020 |           |
| CVE-RSU003-v01 | Verify RSUs broadcast SPaT messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting SPaT from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SPaT based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 |           |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU004-v01 | Verify SPaT broadcast by RSUs match the signal head status | 1. Begin broadcasting SPaT from the Message Handler  
2. Begin broadcasting MAP from the Message Handler  
3. RSU broadcasts SPaT and MAP  
4. Using the CVTT SPaT/MAP visualization functionality, monitor the CVTT to verify SPaT status matches the signal head status for all lanes within the intersection | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 12/17/2020 | Compared Signal Controller Phase changes at High St and Weber with CVMS web-based SPaT Status |
| CVE-RSU006-v02 | Verify RSUs broadcast MAP messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 | |
| CVE-RSU007-v02 | Verify MAP message matches intersection geometry | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler  
3. Using the CVTT MAP display functionality verify the MAP message matches/aligns with the RSU installation intersection geometry | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 | |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-RSU008-v01</td>
<td>Verify RSUs broadcast RTCM messages received from the Message Handler over DSRC on Channel 180 once every 2 seconds</td>
<td>1. Begin broadcasting RTCMs from the Message Handler 2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting RTCMs based on the messages provided by the Message Handler</td>
<td>• Test Conductor  • OBU Data Producer  • RSU Data Producer  • Vehicle Driver  • Data Recorder</td>
<td>PASS</td>
<td>10/16/2020</td>
<td></td>
</tr>
<tr>
<td>CVE-RSU009-v01</td>
<td>Verify RSUs broadcast SSMs received from the Message Handler over DSRC on Channel 180 at 1 Hz</td>
<td>1. Begin broadcasting SSMs from the Message Handler 2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SSM based on the messages provided by the Message Handler</td>
<td>• Test Conductor  • OBU Data Producer  • RSU Data Producer  • Vehicle Driver  • Data Recorder</td>
<td>PASS</td>
<td>10/14/2020</td>
<td></td>
</tr>
<tr>
<td>CVE-RSU010-v01</td>
<td>Verify RSUs broadcast TIMs on Channel 180 at 1 Hz</td>
<td>1. Begin broadcasting the TIM message from the Message Handler 2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the TIM message provided by the Message Handler based on the message stored on the device 3. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting TIMs based on the messages provided by the Message Handler</td>
<td>• Test Conductor  • OBU Data Producer  • RSU Data Producer  • Vehicle Driver  • Data Recorder</td>
<td>PASS</td>
<td>10/12/2020</td>
<td></td>
</tr>
</tbody>
</table>
### Table: Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU011-v01| Verify RSUs report Channel Busy Ratio to TCVMS, when above a predetermined threshold | 1. RSU (2) is configured for a Channel Busy Ratio threshold of 5% (which should trigger a Channel Busy Report with minimal DSRC activity)  
2. Using the CVTT message capture functionality capture WSA, MAP, and TIMs from RSU (1)  
3. Begin broadcasting WSA, MAP, and TIM from RSU (1)  
4. Monitor RSU (2) to verify it detects a Channel Busy Ratio above 5% and sends a Channel Busy Report to the TCVMS | Test Conductor, OBU Data Producer, RSU Data Producer, Vehicle Driver, Data Recorder | Deprecated |           | RSU does not support this functionality |
| CVE-RSU012-v01| Verify RSU broadcast WSA with correct parameters (including WRA)           | 1. Begin broadcasting WSAs from the RSU  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting WSAs containing the correct parameters, including the WRA | Test Conductor, OBU Data Producer, RSU Data Producer, Vehicle Driver, Data Recorder | PASS          | 10/14/2020 |                                                  |
| CVE-RSU013-v01| Verify IPv6 connectivity to SCMS                                           | 1. Remove certificates from the RSU  
2. From the RSU, initiate a certificate request to the SCMS  
3. Monitor the certificate directory on the RSU to verify the RSU has received and stored new certificates | Test Conductor, OBU Data Producer, RSU Data Producer, Data Recorder | PASS          | 10/14/2020 |                                                  |
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU014-v01 | Document RSU Communication Range for RLVW on Channel 180 | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection  
2. V1 maintains constant speed and heading  
3. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert  
4. Data recorder logs an RLVW alert in the test log  
5. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT and Map message.  
6. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT and Map message  
7. Data recorder records the distance between the RSU and the first received SPaT and Map messages as the RSU RLVW Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 04/07/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled. | 02/05/2021 | Data Analysis indicates the average communication range for SPaT and MAP messages, required for RLVW, is between 500m and 600m |
### Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU015-v01| Document RSU Communication Range for Signal Priority on Channel 180       | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal priority  
3. OBU1 records the SRM event  
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message  
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message  
6. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Priority Request Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 04/07/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Priority, is between 500m and 600m |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU016-v01       | Document RSU Communication Range for Signal Preemption on Channel 180    | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal preemption  
3. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message  
4. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message  
5. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Preemption Request Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 04/07/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Preemption, is between 500m and 600m |
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU017-v01     | Document RSU Communication Range for RSSZ on Channel 180                 | 1. Vehicle with OBU1 (V1) approaches the school zone segment above the school zone speed limit  
2. Based on the TIM from the RSU, OBU1 determines a threat exists and issues and RSSZ alert  
3. Data recorder logs an RSSZ alert in the test log  
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received TIM.  
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received TIM.  
6. Data recorder records the distance between the RSU and the first received TIM as the RSU RSSZ Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 04/07/2021   | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for TIM, required for RSSZ, is between 500m and 600m |

*Source: City of Columbus*
### 4.1.5. RSU-Siemens

Table 13 contains the Siemens RSU Test Results.

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU001-v02 | Verify RSU forwards BSMs, received from passing vehicles, to Message Handler | 1. OBU, broadcasting BSMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving BSMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 10/14/2020 |          |
| CVE-RSU002-v01 | Verify RSU forwards SRMs, received from approaching vehicles, to the Message Handler | 1. OBU, broadcasting SRMs, is brought into communication range of the RSU Under Test  
2. The Message Handler is monitored to verify it is receiving SRMs | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 10/16/2020 |          |
| CVE-RSU003-v01 | Verify RSUs broadcast SPaT messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting SPaT from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SPaT based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 10/14/2020 |          |
## Test Results

### Connected Vehicle Environment

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU004-v01 | Verify SPaT broadcast by RSUs match the signal head status | 1. Begin broadcasting SPaT from the Message Handler  
2. Begin broadcasting MAP from the Message Handler  
3. RSU broadcasts SPaT and MAP  
4. Using the CVTT SPaT/MAP visualization functionality, monitor the CVTT to verify SPaT status matches the signal head status for all lanes within the intersection | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 12/17/2020 | Compared Signal Controller Phase changes at Morse Rd. and I-270 SB Ramp with CVMS web-based SPaT Status |
| CVE-RSU006-v02 | Verify RSUs broadcast MAP messages received from the Message Handler over DSRC on Channel 180 at 10 Hz | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/14/2020 | |
| CVE-RSU007-v02 | Verify MAP message matches intersection geometry | 1. Begin broadcasting the MAP message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the MAP message provided by the Message Handler  
3. Using the CVTT MAP display functionality verify the MAP message matches/aligns with the RSU installation intersection geometry | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/14/2020 | |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU008-v01 | Verify RSUs broadcast RTCM messages received from the Message Handler over DSRC on Channel 180 once every 2 seconds | 1. Begin broadcasting RTCMs from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting RTCMs based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/16/2020 | |
| CVE-RSU009-v01 | Verify RSUs broadcast SSMs received from the Message Handler over DSRC on Channel 180 at 1 Hz | 1. Begin broadcasting SSMs from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting SSM based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/16/2020 | |
| CVE-RSU010-v01 | Verify RSUs broadcast TIMs on Channel 180 at 1 Hz | 1. Begin broadcasting the TIM message from the Message Handler  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting the TIM message provided by the Message Handler based on the message stored on the device  
3. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting TIMs based on the messages provided by the Message Handler | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/14/2020 | |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU011-v01 | Verify RSUs report Channel Busy Ratio to TCVMS, when above a predetermined threshold | 1. RSU (2) is configured for a Channel Busy Ratio threshold of 5% (which should trigger a Channel Busy Report with minimal DSRC activity)  
2. Using the CVTT message capture functionality capture WSA, MAP, and TIMs from RSU (1)  
3. Begin broadcasting WSA, MAP, and TIM from RSU (1)  
4. Monitor RSU (2) to verify it detects a Channel Busy Ratio above 5% and sends a Channel Busy Report to the TCVMS | Deprecated | RSU does not support this functionality |
| CVE-RSU012-v01 | Verify RSU broadcast WSA with correct parameters (including WRA)            | 1. Begin broadcasting WSAs from the RSU  
2. Using the CVTT message capture functionality, monitor the RSU to verify it is broadcasting WSAs containing the correct parameters, including the WRA | Test Conductor, OBU Data Producer, RSU Data Producer, Vehicle Driver, Data Recorder | PASS | 10/14/2020 |                                |
| CVE-RSU013-v01 | Verify IPv6 connectivity to SCMS                                            | 1. Remove certificates from the RSU  
2. From the RSU, initiate a certificate request to the SCMS  
3. Monitor the certificate directory on the RSU to verify the RSU has received and stored new certificates | Test Conductor, OBU Data Producer, RSU Data Producer, Data Recorder | PASS | 10/15/2020 |                                |
### Test Results

**Test Case ID** | **Objective** | **Procedure** | **Tester Role** | **Test Status** | **Date Run** | **Comments**
--- | --- | --- | --- | --- | --- | ---
CVE-RSU014-v01 | Document RSU Communication Range for RLVW on Channel 180 | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when V1 arrives at the intersection
2. V1 maintains constant speed and heading
3. Based on SPaT and MAP from the RSU, OBU1 determines a threat exists and issues a RLVW alert
4. Data recorder logs an RLVW alert in the test log
5. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT and Map message.
6. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT and Map message
7. Data recorder records the distance between the RSU and the first received SPaT and Map messages as the RSU RLVW Range in the test log | • Test Conductor
• OBU Data Producer
• RSU Data Producer
• Vehicle Driver
• Data Recorder | PASS | 04/08/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.
Data collected 02/05/2021
Data Analysis indicates the average communication range for SPaT and MAP messages, required for RLVW, is between 500m and 600m
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU015-v01 | Document RSU Communication Range for Signal Priority on Channel 180 | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal priority  
3. OBU1 records the SRM event  
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message.  
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message  
6. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Priority Request Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 04/08/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled. |

Data collected 02/05/2021  
Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Priority, is between 500m and 600m
## Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU016-v01   | Document RSU Communication Range for Signal Preemption on Channel 180    | 1. Vehicle with OBU1 (V1) approaches the intersection at a speed in which the light will be Red when vehicle arrives at the intersection  
2. Based on the SPaT, MAP, and WSA from the RSU, OBU1 broadcasts an SRM, requesting signal preemption  
3. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received SPaT, Map, and WSA message  
4. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received SPaT, Map, and WSA message  
5. Data recorder records the distance between the RSU and the first received SPaT, Map, and WSA messages as the RSU Signal Preemption Request Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS         | 04/08/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for WSA, SRM, and SSM, required for Signal Preemption is between 500m and 600m |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-RSU017-v01 | Document RSU Communication Range for RSSZ on Channel 180 | 1. Vehicle with OBU1 (V1) approaches the school zone segment above the school zone speed limit  
2. Based on the TIM from the RSU, OBU1 determines a threat exists and issues and RSSZ alert  
3. Data recorder logs an RSSZ alert in the test log  
4. (Post-Process) Data recorder plots the RSU Latitude and Longitude and the Latitude, Longitude, and Receive Signal Strength of each received TIM.  
5. Data recorder compares the Latitude and Longitude of the RSU to the Latitude and Longitude of the first received TIM.  
6. Data recorder records the distance between the RSU and the first received TIM as the RSU RSSZ Range in the test log | • Test Conductor  
• OBU Data Producer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 04/08/2021 | Due to COVID-19 contact tracing, data could not be collected when originally scheduled.  
Data collected 02/05/2021  
Data Analysis indicates the average communication range for TIM, required for RSSZ, is between 500m and 600m |
### 4.1.6. Message Handler

Table 14 contains the Message Handler Test Results.

**Table 14: Message Handler Test Results**

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-MH001-v01 | Econolite TSC: Verify the Message Handler generates and forwards SAE J2735-032016-2016 SPaT messages, based on SPaT data received from the local Signal Controller, to the local RSU | 1. Connect Laptop (L1) running Wireshark to the RSU port on the Signal Controller\Message Handler  
2. Power on the Signal Controller  
3. The Message Handler powers on with the Signal Controller  
4. Signal Controller sends signal phase and timing data to Message Handler  
5. Message Handler generates and sends J2735 SPaT messages to L1  
6. Capture data flowing from the Message Handler using Wireshark on L1  
7. Inspect messages coming from the Message Handler on L1 to verify they conform to J2735 SPaT messages | • Test Conductor  
• RSU Data Producer  
• Data Recorder | PASS | 10/12/2020  
10/14/2020 | 10/12/2020: Kapsch RSU  
10/12/2020: Danlaw RSU  
10/14/2020: Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-MH001-v01</td>
<td>Siemens TSC: Verify the Message Handler generates and forwards SAE J2735-032016-2016 SPaT messages, based on SPaT data received from the local Signal Controller, to the local RSU</td>
<td>1. Connect Laptop (L1) running Wireshark to the RSU port on the Signal Controller; Message Handler 2. Power on the Signal Controller 3. The Message Handler powers on with the Signal Controller 4. Signal Controller sends signal phase and timing data to Message Handler 5. Message Handler generates and sends J2735 SPaT messages to L1 6. Capture data flowing from the Message Handler using Wireshark on L1 7. Inspect messages coming from the Message Handler on L1 to verify they conform to J2735 SPaT messages</td>
<td>Test Conductor, RSU Data Producer, Data Recorder</td>
<td>PASS</td>
<td>12/17/2020</td>
<td>Kapsch RSU</td>
</tr>
<tr>
<td>CVE-MH002-v01</td>
<td>Verify the Message Handler properly determines if OBU requesting priority is authorized to receive priority</td>
<td>1. Power on RSU and Message Handler (Message Handler requires the Signal Controller to be powered on as well) 2. Power on OBU1 3. OBU1 broadcasts SRMs with a BasicVehicleRole of “basicVehicle”; not authorized for signal priority 4. RSU forwards SRMs from OBU1 to the Message Handler 5. Verify Message Handler does not send a priority request to the Signal Controller</td>
<td>Test Conductor, Traffic Data Consumer, RSU Data Producer, Vehicle Drivers, Data Recorder</td>
<td>PASS</td>
<td>12/16/2020</td>
<td>Message Handler verifies Vehicle Role is permitted to request Priority or Preemption</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CVE-MH004-v01     | Econolite TSC: Verify the Message Handler places a priority call to the local Signal Controller based on an authorized SRM. | 1. Power on RSU and Message Handler (Message Handler required the Signal Controller to be powered on as well)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of "Transit"; authorized for signal priority  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Verify Message Handler sends priority requests to the Signal Controller | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | Kapsch RSU  
Danlaw RSU  
Siemens RSU |
| CVE-MH004-v01     | Siemens TSC: Verify the Message Handler places a priority call to the local Signal Controller based on an authorized SRM | 1. Power on RSU and Message Handler (Message Handler required the Signal Controller to be powered on as well)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of "Transit"; authorized for signal priority  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Verify Message Handler sends priority requests to the Signal Controller | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Drivers  
• Data Recorder | FAIL         | 04/21/2021 | Signal Priority is not implemented in the Siemens TSC as of 04/21/2021.  
City is still expecting a FW update from Siemens for NTCIP 1211 |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-MH005-v01 | Verify the Message Handler places a preemption call to the local Signal Controller based on an authorized SRM | 1. Power on RSU and Message Handler (Message Handler required the Signal Controller to be powered on as well)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of “Police”; authorized for signal preemption  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Verify Message Handler sends preemption requests to the Signal Controller | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Drivers  
• Data Recorder | PASS         | 10/14/2020 | Kapsch RSU  
Danlaw RSU  
Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-MH006-v01</td>
<td>Econolite TSC: Verify the Message Handler generates and forwards SAE J2735-032016-2016 SSMs, based on status data received from the local Signal Controller, to the local RSU</td>
<td>1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller) 2. Power on OBU1 3. OBU1 broadcasts SRMs with a BasicVehicleRole of &quot;Transit&quot;; authorized for signal priority 4. RSU forwards SRMs from OBU1 to the Message Handler 5. Message Handler sends priority requests to the Signal Controller 6. Signal Controller sends signal status data to the Message Handler 7. Message Handler generates and send SSMs to the RSU 8. Inspect messages coming from the Message Handler to verify they conform to J2735 SSMs</td>
<td>• Test Conductor  • Traffic Data Consumer  • RSU Data Producer  • Vehicle Drivers  • Data Recorder</td>
<td>PASS</td>
<td>10/14/2020</td>
<td>Kapsch RSU Danlaw RSU Siemens RSU</td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CVE-MH006-v01   | Siemens TSC: Verify the Message Handler generates and forwards SAE J2735-032016-2016 SSMs, based on status data received from the local Signal Controller, to the local RSU | 1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of “Transit”; authorized for signal priority  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Message Handler sends priority requests to the Signal Controller  
6. Signal Controller sends signal status data to the Message Handler  
7. Message Handler generates and send SSMs to the RSU  
8. Inspect messages coming from the Message Handler to verify they conform to J2735 SSMs | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Drivers  
• Data Recorder | FAIL           | 04/21/2021 | Signal Priority is not implemented in the Siemens TSC as of 04/21/2021.  
City is still expecting a FW update from Siemens for NTCIP 1211 |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-MH007-v01</td>
<td>Verify the Message Handler reports a cabinet tamper events to TCVMS</td>
<td>1. Connect a toggle switch (S1) to the cabinet tamper detection input/output (IO) port of the Message Handler</td>
<td></td>
<td>Deprecated</td>
<td>10/14/2020</td>
<td>This is a Controller Cabinet/TMC functionality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Set S1 to “inactive” (no event detected)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Connect a laptop (L1) running Wireshark to the TCVMS port on the Message Handler (L1 acts as the TCVMS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Log received packets on L1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Power on the Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. In Wireshark on L1, inspect packets coming from the Message Handler in Wireshark to verify the Message Handler is NOT sending event messages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Set S1 to “active” (event detected)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. In Wireshark on L1, inspect packets coming from the Message Handler to verify the Message Handler is sending event messages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Message Handler logs events based on S1 set to “active”</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
</tbody>
</table>
| CVE-MH008-v01     | Verify the Message Handler generates and forwards SAE J2735-032016-2016 RTCM messages, based on data received from the Position Correction System to the local RSU | 1. Connect Laptop (L1) running Wireshark to the RSU port on the Signal Controller; Message Handler  
2. Power on the Signal Controller  
3. The Message Handler powers on with the Signal Controller  
4. RTCM data source sends RTCM data to Message Handler  
5. Message Handler generates and sends J2735 RTCM messages to L1  
6. Capture data flowing from the Message Handler using Wireshark on L1  
7. Inspect message coming from the Message Handler on L1 to verify they conform to J2735 RTCM messages | Test Conductor; RSU Data Producer; Vehicle Drivers; Data Recorder | PASS         | 10/14/2020  
10/16/2020      | 10/14/2020: Kapsch RSU  
10/16/2020: Danlaw RSU  
10/16/2020: Siemens RSU |
| CVE-MHTP009-v01   | Verify Message Handler stores MAP files received from the TCVMS            | 1. From TCVMS, send the MAP file to the Message Handler  
2. Inspect Message Handler to verify the MAP file is loaded in the appropriate location (directory) | Test Conductor; RSU Data Producer; Data Recorder | PASS         | 10/12/2020  
10/14/2020      | 10/12/2020: Kapsch RSU  
10/12/2020: Danlaw RSU  
10/14/2020: Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-MHTP010- v01 | Verify Message Handler sends MAP messages to the local RSU as Immediate Forward messages | 1. Connect a laptop (L1) running Wireshark to the RSU port on the Message Handler (L1 acts as the RSU)  
2. Configure Wireshark on L1 to capture packets from the Message Handler  
3. Begin sending MAP messages from the Message Handler to L1 (acting as an RSU)  
4. Log received packets on L1  
5. Inspect packets coming from the Message Handler on L1 to verify the Message Handler is sending J2735-032016 MAP messages | • Test Conductor  
• RSU Data Producer  
• Data Recorder | PASS | 10/12/2020  
10/14/2020 | 10/12/2020: Kapsch RSU  
10/12/2020: Danlaw RSU  
10/14/2020: Siemens RSU |
| CVE-MHTP011- v01 | Verify Message Handler sends TIM messages to the local RSU as Immediate Forward messages | 1. Connect a laptop (L1) running Wireshark to the RSU port on the Message Handler (L1 acts as the RSU)  
2. Configure Wireshark on L1 to capture packets from the Message Handler  
3. Begin sending TIMs from the Message Handler to L1 (acting as an RSU)  
4. Log received packets on L1  
5. Inspect packets coming from the Message Handler on L1 to verify the Message Handler is sending J2735-032016 TIM messages | • Test Conductor  
• RSU Data Producer  
• Data Recorder | PASS | 10/12/2020  
10/14/2020 | 10/12/2020: Kapsch RSU  
10/12/2020: Danlaw RSU  
10/14/2020: Siemens RSU |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-MHTP012-v01 | Verify Message Handler updates the *Start Time* and *Duration* of a stored TIM when the school zone is active | 1. Connect a laptop (L1) running Wireshark to the RSU port on the Message Handler (L1 acts as the RSU)  
2. Configure Wireshark on L1 to capture packets from the Message Handler  
3. Begin sending TIMs from the Message Handler to L1  
4. Log received packets on L1 both before and after the School Zone Speed Limit becomes active  
5. Inspect packets coming from the Message Handler on L1 to verify the TIM contains the Start Time and Duration of the active School Zone Speed Limit | • Test Conductor  
• RSU Data Producer  
• Data Recorder | PASS         | 09/18/2020 | Confirmed at High St School Zone |

*Source: City of Columbus*
4.1.7. **TSC-Econolite**

Table 15 contains the Econolite Traffic Signal Controller Test Results.

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TSC001-v01 | Verify Traffic Signal Controller sends SPaT data to the Message Handler | 1. Connect a laptop (L1) running Wireshark to the Signal Controller  
2. Power on the Signal Controller  
3. Log received packets on L1  
4. Inspect packets coming from the Signal Controller on L1 to verify the Signal Controller is send SPaT data | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS | 10/12/2020 |
| CVE-TSC002-v01 | Verify Traffic Signal Controller processes a signal priority call from the Message Handler | 1. Power on RSU, Message Handler, OBU1, and Signal Controller  
2. OBU1 broadcasts SRMs signed with a signal priority certificate  
3. RSU forwards SRM to the Message Handler  
4. Message Handler sends a signal priority call to the Signal Controller  
5. Signal controller changes timing based on the priority call  
6. Data recorder log the time change in the test log | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-TSC003-v01</td>
<td>Verify Traffic Signal Controller processes a signal preemption call from the Message Handler</td>
<td>1. Power on RSU, Signal Controller, Message Handler, and OBU1 (Message Handler powers on with the Signal Controller) 2. OBU1 broadcasts SRMs signed with a signal preemption certificate 3. RSU forwards SRM to the Message Handler 4. Message Handler sends a signal preemption call to the Signal Controller 5. Signal controller changes timing based on the preemption call 6. Data recorder logs the time change in the test log</td>
<td>• Test Conductor  • Traffic Data Consumer  • RSU Data Producer  • Vehicle Driver  • Data Recorder</td>
<td>PASS</td>
<td>10/12/2020</td>
<td></td>
</tr>
<tr>
<td>CVE-TSC004-v01</td>
<td>Verify Traffic Signal Controller sends priority status to the Message Handler</td>
<td>1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller) 2. Power on OBU1 3. OBU1 broadcasts SRMs with a BasicVehicleRole of “Transit”; authorized for signal priority 4. RSU forwards SRMs from OBU1 to the Message Handler 5. Message Handler sends priority requests to the Signal Controller 6. Signal Controller sends signal status data to the Message Handler 7. Inspect data from the Signal Controller to verify it is sending priority signal status data to the Message Handler</td>
<td>• Test Conductor  • Traffic Data Consumer  • RSU Data Producer  • Vehicle Driver  • Data Recorder</td>
<td>PASS</td>
<td>10/12/2020</td>
<td></td>
</tr>
</tbody>
</table>
## Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TSC005-v01 | Verify Traffic Signal Controller sends preemption status to the Message Handler | 1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of "Police"; authorized for signal preemption  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Message Handler sends preemption requests to the Signal Controller  
6. Signal Controller sends signal status data to the Message Handler  
7. Inspect data from the Signal Controller to verify it is sending preemption signal status data to the Message Handler | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | PASS | 10/12/2020 | Source: City of Columbus |
### 4.1.8. TSC-Siemens

**Table 16** contains the Siemens Traffic Signal Controller Test Results.

**Table 16: Siemens Traffic Signal Controller Test Results**

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-TSC001-v01</td>
<td>Verify Traffic Signal Controller sends SPaT data to the Message Handler</td>
<td>1. Connect a laptop (L1) running Wireshark to the Signal Controller</td>
<td>• Test Conductor</td>
<td>PASS</td>
<td>12/17/2020</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Power on the Signal Controller</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Log received packets on L1</td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Inspect packets coming from the Signal Controller on L1 to verify the</td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signal Controller is send SPaT data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. OBU1 broadcasts SRMs signed with a signal priority certificate</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td>City is still expecting a FW update from Siemens for NTCIP 1211.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. RSU forwards SRM to the Message Handler</td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Message Handler sends a signal priority call to the Signal Controller</td>
<td>• Vehicle Driver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Signal controller changes timing based on the priority call</td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Data recorder log the time change in the test log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>-------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CVE-TSC003-v01| Verify Traffic Signal Controller processes a signal preemption call from the Message Handler | 1. Power on RSU, Signal Controller/Message Handler, and OBU1 (Message Handler powers on with the Signal Controller)  
2. OBU1 broadcasts SRMs signed with a signal preemption certificate  
3. RSU forwards SRM to the Message Handler  
4. Message Handler sends a signal preemption call to the Signal Controller  
5. Signal controller changes timing based on the preemption call  
6. Data recorder logs the time change in the test log | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | Deprecated |  | Siemens Controllers will only support Priority with this project |
| CVE-TSC004-v01| Verify Traffic Signal Controller sends priority status to the Message Handler | 1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of “Transit”; authorized for signal priority  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Message Handler sends priority requests to the Signal Controller  
6. Signal Controller sends signal status data to the Message Handler  
7. Inspect data from the Signal Controller to verify it is sending priority signal status data to the Message Handler | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | FAIL | 12/17/2020 | Signal Priority is not implemented in the Siemens TSC as of 04/21/2021.  
City is still expecting a FW update from Siemens for NTCIP 1211
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TSC005-v01 | Verify Traffic Signal Controller sends preemption status to the Message Handler | 1. Power on RSU, signal controller, and Message Handler (Message Handler powers on with the Signal Controller)  
2. Power on OBU1  
3. OBU1 broadcasts SRMs with a BasicVehicleRole of "Police"; authorized for signal preemption  
4. RSU forwards SRMs from OBU1 to the Message Handler  
5. Message Handler sends preemption requests to the Signal Controller  
6. Signal Controller sends signal status data to the Message Handler  
7. Inspect data from the Signal Controller to verify it is sending preemption signal status data to the Message Handler | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Vehicle Driver  
• Data Recorder | Deprecated |          | Siemens Controllers will only support Priority |

Source: City of Columbus
4.1.9. **TCVMS**

Table 17 contains the Traffic Connected Vehicle Management System Test Results. Note the TCVMS is composed of the City of Columbus Traffic Management System, Centracs, the Smart Columbus Operating System, and the CMCC provided by Kapsch. The Objective contains the subsystem the test applies to.

**Table 17: TCVMS Test Results**

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-TCVMS001-</td>
<td>CMCC: Verify traffic CV management staff can input a MAP message payload to</td>
<td>1. Login to the TCVMS and configure MAP message for specific RSU</td>
<td>Test Conductor</td>
<td>PASS</td>
<td>10/12/2020</td>
<td></td>
</tr>
<tr>
<td>v01</td>
<td>the TCVMS and specify which RSU it should be broadcast from</td>
<td>2. Execute TCVMS process for sending MAP messages to designated RSUs</td>
<td>RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Confirm MAP message payload matches the message sent from the TCVMS</td>
<td>Data Recorder</td>
<td></td>
<td></td>
<td>Kapsch RSU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Danlaw RSU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Siemens RSU</td>
</tr>
<tr>
<td>CVE-TCVMS002-</td>
<td>CMCC: Verify traffic CV management staff can input a TIM payload to the</td>
<td>1. Login to the TCVMS and configure TIM for specific RSU</td>
<td>Test Conductor</td>
<td>PASS</td>
<td>10/14/2020</td>
<td></td>
</tr>
<tr>
<td>v01</td>
<td>TCVMS and specify which RSU it should be broadcast from</td>
<td>2. Execute TCVMS process for sending TIM messages to designated RSUs</td>
<td>RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Confirm TIM message payload matches the message sent from the TCVMS</td>
<td>Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-TCVMS003-</td>
<td>CMCC: The TCVMS archives the MAP message locally and forwards it to the</td>
<td>1. Login to the TCVMS and confirm MAP messages for RSU are stored locally in the designated</td>
<td>Test Conductor</td>
<td>PASS</td>
<td>12/16/2020</td>
<td>OS Inspection</td>
</tr>
<tr>
<td>v01</td>
<td>Operating System</td>
<td>folder</td>
<td>Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute TCVMS process for sending MAP messages to the Operating System</td>
<td>RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Confirm MAP message is archived in the Operating System</td>
<td>Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| CVE-TCVMS004-| CMCC: Verify the TCVMS archives the TIM locally and forwards it to the Smart Columbus Operating System (Operating System)                      | 1. Login to the TCVMS and generate a TIM for a specific RSU  
2. Monitor TCVMS to confirm the TIM is sent to the Operating System  
3. Confirm the TIM generated in Step 1 is archived in the Operating System                                                                 | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder                                                                 | PASS         | 12/16/2020 | OS Inspection |
| v01           |                                                                                                                                           |                                                                                                                                                                                                         |                                                                               |             |            |                 |
| CVE-TCVMS005-| CMCC: Verify the TCVMS archives the TIM locally and forwards it to the Smart Columbus Operating System (Operating System)                      | 1. Login to the TCVMS and confirm TIMs are stored locally in the designated folder  
2. Execute TCVMS process for sending TIMs to the Operating System  
3. Confirm TIMs are archived in the Operating System                                                                 | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder                                                                 | PASS         | 12/16/2020 | OS Inspection |
| v01           |                                                                                                                                           |                                                                                                                                                                                                         |                                                                               |             |            |                 |
| CVE-TCVMS006-| CMCC: Verify the TCVMS archives the TIM locally and forwards it to the Smart Columbus Operating System (Operating System)                      | 1. Login to the TCVMS and confirm SPaT messages are stored locally in the designated folder  
2. Execute TCVMS process for sending SPaT messages to the Operating System  
3. Confirm SPaT messages are archived in the Operating System                                                                 | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder                                                                 | PASS         | 12/16/2020 | OS Inspection |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TCVMS007- v01 | CMCC: Verify the TCVMS archives the SRM locally and forwards it to the Operating System | 1. Login to the TCVMS and confirm SRM messages are stored locally in the designated folder  
2. Execute TCVMS process for sending SRM messages to the Operating System  
3. Confirm SRM messages are archived in the Operating System | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS        | 12/16/2020 | OS Inspection |
| CVE-TCVMS008- v01 | CMCC: Verify the TCVMS archives the SSM locally and forwards it to the Operating System | 1. Login to the TCVMS and confirm SSM messages are stored locally in the designated folder  
2. Execute TCVMS process for sending SSM messages to the Operating System  
3. Confirm SSM messages are archived in the Operating System | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS        | 12/16/2020 | OS Inspection |
| CVE-TCVMS009- v01 | CMCC: Verify the TCVMS archives the RTCM locally and forwards it to the Operating System | 1. Login to the TCVMS and confirm RTCM messages are stored locally in the designated folder  
2. Execute TCVMS process for sending RTCM messages to the Operating System  
3. Confirm RTCM messages are archived in the Operating System | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | Deprecated  | 12/16/2020 | OS Inspection: No Records Found  
OBUs do not use RTCM, so the RTCM requirement is deprecated |
| CVE-TCVMS010- v01 | OS: Verify traffic CV management staff can specify a performance metric to the TCVMS (and specify how it is calculated) | 1. Login to the TCVMS  
2. Configure performance metric(s) to be generated in TCVMS  
3. Execute TCVMC command to generate performance metric(s)  
4. Confirm TCVMS returns request performance metric(s) | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS        | 04/02/2021 | All CVE performance measure data can be accessed through the OS |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TCVMS011-v01 | OS: Verify generated performance metrics are uploaded to the Operating System | 1. Login to the TCVMS and confirm performance metrics are stored locally in the designated folder  
2. Execute TCVMS process for sending performance metrics to the Operating System  
3. Confirm TCVMS performance metrics are archived in the Operating System | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS | 04/02/2021 | A set of queries are run monthly against collected CVE data to generate performance measures |
| CVE-TCVMS012-v01 | TCVMS: Verify PII is removed prior to sending data to Operating System | 1. OBU, broadcasting BSMs, is brought into communication range of the RSU  
2. RSU forwards BSMs to TCVMS  
3. TCVMS receives BSMs  
4. TCVMS logs "raw" (with PII) BSMs (log1) (for testing)  
5. TCVMS removes PII and logs (log2) BSMs in "normal" operation  
6. Confirm BSMs logged in log2 do not contain PII | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS | 12/16/2020 | Inspected OS |
| CVE-TCVMS013-v01 | CMCC: Verify traffic CV management staff can specify a source for each RSU to receive RTCM data | 1. Login to the TCVMS and confirm RTCM source parameters  
2. Execute TCVMS process for sending configuration parameters to RSUs  
3. Confirm RSU is configured with the correct RTCM source parameters | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS | 10/12/2020 | A single source provides RTCM to all RSUs |
<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-TCVMS014-v01</td>
<td>TMC: Verify TCVMS can detect unauthorized network activity</td>
<td>1. Attempt to log into the TCVMS four times using a wrong password</td>
<td>• Test Conductor</td>
<td>Deprecated</td>
<td></td>
<td>This is part of the Columbus Department of Technology Network Intrusion Detection System, not part of the CVE TCVMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. After the fourth attempt, confirm an email was sent to operations staff</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-TCVMS015-v01</td>
<td>TMC: Verify TCVMS can detect traffic signal cabinet tampering and issue the proper notifications to Traffic CV management staff</td>
<td>1. Select a controller cabinet in the field that is easy and safe to access without disrupting vehicle traffic</td>
<td>• Test Conductor</td>
<td>PASS</td>
<td>12/16/2020</td>
<td>See TMC Door Alarm Config.jpg and TMC Door Alarm Enable.jpg Test Result data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Confirm the TCVMS dashboard is not indicating a cabinet door alert for the selected cabinet</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Open cabinet door (event detected)</td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Confirm icon appears on the TCVMS dashboard indicating a cabinet door alert for the selected cabinet</td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-TCVMS016-v01</td>
<td>CMCC: Verify traffic CV management staff can modify configurable setting of an RSU using the TCVMS</td>
<td>1. Login to the TCVMS and confirm RSU configuration parameters</td>
<td>• Test Conductor</td>
<td>PASS</td>
<td>10/12/2020</td>
<td>Kapsch RSU Danlaw RSU Siemens RSU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute TCVMS process for sending configuration parameters to RSUs</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Confirm RSU is configured with the parameters provided by the TCVMS</td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Case ID</td>
<td>Objective</td>
<td>Procedure</td>
<td>Tester Role</td>
<td>Test Status</td>
<td>Date Run</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CVE-TCVMS017-v01| CMCC: Verify Traffic CV management staff have access to the following RSU data via the TCVMS: uptime status, connectivity, RSU graphical display, etc. | 1. Login to the TCVMS  
2. Execute TCVMS process for retrieving status elements from RSUs  
3. Confirm TCVMS receives status elements from RSUs | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | PASS         | 10/12/2020  
10/14/2020 | 10/12/2020: Kapsch RSU  
10/12/2020: Danlaw RSU  
10/14/2020: Siemens RSU |
| CVE-TCVMS018-v01| TMC: Verify alert is issued for unauthorized network activity using dashboard icon and an email is sent to traffic CV management staff | 1. Login to the TCVMS and monitor the dashboard and administrator email  
2. From a separate console/computer, attempt to log into the TCVMS with the wrong credentials 3 times  
3. Monitor TCVMS dashboard for icon indicating a failed log in attempt | • Test Conductor  
• Traffic Data Consumer  
• RSU Data Producer  
• Data Recorder | Deprecated | | This is part of the Columbus Department of Technology Network Intrusion Detection System, not part of the CVE TCVMS |
## Chapter 4. Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TCVMS019-v01 | TMC: Verify alert is issued when RSU is not operating as intended (degraded/failure conditions, or limited network connectivity) using dashboard icon and an email is to traffic CV management staff | 1. Login to the TCVMS and monitor the dashboard and administrator email  
2. From a separate console/computer, reboot an RSU  
3. Monitor TCVMS dashboard for icon indicating a loss of connection to an RSU | **Test Conductor**  
**Traffic Data Consumer**  
**RSU Data Producer**  
**Data Recorder** | PASS        | 04/07/2021 | "e-mail" requirement removed  
See TMC RSU Alert Notification.jpg, TMC RSU Alert List.jpg, and TMC RSU Alert Detail.jpg Test Result data |
| CVE-TCVMS020-v01 | TMC: Verify TCVMS logs all alerts/emails to traffic CV management staff                                                                 | 1. Login to the TCVMS and confirm Alerts and email notifications are stored locally in the designated folder | **Test Conductor**  
**Traffic Data Consumer**  
**RSU Data Producer**  
**Data Recorder** | PASS        | 12/16/2020 | "e-mail" requirement removed  
See TMC Door Alarm log.jpg Test Result data |
| CVE-TCVMS021-v01 | OS: Verify traffic CV management staff can query archived data on the TCVMS                                                                 | 1. Login to the TCVMS and run a query for data, for a given date and time range  
2. Confirm data matching the query criteria is returned | **Test Conductor**  
**Traffic Data Consumer**  
**RSU Data Producer**  
**Data Recorder** | PASS        | 12/16/2020 | OS Inspection                                                             |

Source: City of Columbus
### 4.1.10. TrCVMS

Table 18 contains the Transit Connected Vehicle Management System Test Results maintained by COTA.

#### Table 18: TrCVMS Test Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-TrCVMS001-v01</td>
<td>Verify transit CV management staff can specify a performance metric to the TrCVMS</td>
<td>1. Login to the TrCVMS 2. Configure performance metric(s) to be generated in TrCVMS 3. Execute TrCVMS command to generate performance metric(s) 4. Confirm TrCVMS returns request performance metric(s)</td>
<td>• Test Conductor  • Transit Data Consumer  • Data Recorder</td>
<td>PASS</td>
<td>01/08/2021</td>
<td>Reviewed TVIER Logs</td>
</tr>
<tr>
<td>CVE-TrCVMS002-v01</td>
<td>Verify generated performance metrics are uploaded to the Operating System</td>
<td>1. Login to the TrCVMS and confirm performance metrics are stored locally in the designated folder 2. Execute TrCVMS process for sending performance metrics to the Operating System 3. Confirm TrCVMS performance metrics are archived in the Operating System</td>
<td>• Test Conductor  • Transit Data Consumer  • Data Recorder</td>
<td>PASS</td>
<td>02/08/2021</td>
<td>OS Inspection</td>
</tr>
<tr>
<td>CVE-TrCVMS003-v01</td>
<td>Verify transit CV management staff can query archived data on the TrCVMS</td>
<td>1. Login to the TrCVMS and run a query for data, for a given date and time range 2. Confirm data matching the query criteria is returned</td>
<td>• Test Conductor  • Transit Data Consumer  • Data Recorder</td>
<td>PASS</td>
<td>12/17/2020</td>
<td>Reviewed TVIER Logs</td>
</tr>
</tbody>
</table>
Chapter 4. Test Results

### Test Results Table

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-TrCVMS004-v01 | Verify the TrCVMS archives the transit vehicle interaction events and forwards them to the Operating System | 1. Login to the TrCVMS and confirm transit vehicle event logs are stored locally in the designated folder  
2. Execute TrCVMS process for sending transit vehicle event logs to the Operating System  
3. Confirm transit vehicle event logs are archived in the Operating System | • Test Conductor  
• Transit Data Consumer  
• Data Recorder | PASS | 01/08/2021 | Reviewed TVIER Logs |

Source: City of Columbus

### 4.2. DEFECT MANAGEMENT TOOL

The defect tool was used during testing to capture, track, monitor, and address anomalies observed during the testing period. For each entry, the test team worked to understand and reproduce (where possible) the defect, identify the root cause, summarize a response, and log the activities taken to resolve the issue. This process helps with prioritizing defects based on severity level (critical to low) and maintains traceability to the test ID as well as status. The status field provides a simplified view of the various states a defect passes through as it moves toward resolution and closure. A defect can have the following status values:

- **Opened** – indicates the defect has been logged and reported for correction.
- **Re-Opened** – indicates a defect was once closed and then reopened for modification.
- **Closed** – indicates a defect was received, reviewed, and determined was not a defect (i.e., duplicate entry or a request for enhancement). In these cases, no corrective action is taken, and an explanation is provided by the development team while closing-out the defect ticket.
- **Canceled** – indicates a scenario or test case where the defect derived was canceled and therefore, the defect is canceled by default.
- **Resolved** – indicates a defect has been successfully reviewed, verified, and a resolution was implemented to solve the problem along with the resolution date when a defect was corrected.
- **Returned** – indicates the defect was returned to the tester for additional information.
- **Deferred** – indicates the defect has been designated for correction for a later date or a change in requirement.
In cases when a conflict arose between a design element that tied to a requirement and the software product, the test manager coordinated with the test lead to determine if a change to the system design and/or requirement was appropriate. The City of Columbus project manager carefully reviewed all requests to make a change that impacts the system design and requirements. All change requests have been captured within the change logger tool. **Table 19** provides an overview of the resulting defects captured, closed, canceled, or resolved during testing.

**Table 19: Defect Tracker**

<table>
<thead>
<tr>
<th>DATE OPENED</th>
<th>DEFECT NO.</th>
<th>DEFECT DESCRIPTION</th>
<th>SEVERITY</th>
<th>DEFECT STATUS</th>
<th>ASSIGNED TO</th>
<th>RESOLUTION DESCRIPTION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/16/2019</td>
<td>CVE-OBU-DEFECT0-01-v01</td>
<td>OTA through Danlaw RSU Not completed. Danlaw and WNC will meet in Detroit offline to finish testing</td>
<td>High</td>
<td>Resolved</td>
<td>DanLaw</td>
<td>Danlaw resolved with FW update</td>
<td>verified/resolved on 10/12/2020</td>
</tr>
<tr>
<td>07/08/2020</td>
<td>CVE-OBU-DEFECT0-02-v01</td>
<td>SRM missing (TransitStatus) Data Frame, containing “Loading” and “DoorOpen” indication.</td>
<td>Medium</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v11</td>
<td></td>
</tr>
<tr>
<td>07/10/2020</td>
<td>CVE-OBU-DEFECT0-03-v01</td>
<td>OBU gives an RSSZ Alert even if the Start Time is up to 2 hours in the future</td>
<td>Low</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v11</td>
<td></td>
</tr>
<tr>
<td>07/10/2020</td>
<td>CVE-OBU-DEFECT0-04-v01</td>
<td>OBU did not give an RLVW alert</td>
<td>High</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v11</td>
<td></td>
</tr>
<tr>
<td>08/20/2020</td>
<td>CVE-OBU-DEFECT0-05-v01</td>
<td>Multiple OBUs with the same IP Address and (BSM) TempID</td>
<td>Critical</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v14</td>
<td>verified/resolved on 10/12/2020</td>
</tr>
<tr>
<td>08/20/2020</td>
<td>CVE-OBU-DEFECT0-06-v01</td>
<td>Transit Signal Request Messages (SRM) “Loading” and “Door Open” bits in TransitVehicleStatus Data Frame, do not toggle as expected; “Loading” bit is never active and “Door Open” bit is always active</td>
<td>Medium</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v14</td>
<td>verified/resolved on 10/14/2020</td>
</tr>
</tbody>
</table>
## Chapter 4. Test Results

<table>
<thead>
<tr>
<th>DATE OPENED</th>
<th>DEFECT NO.</th>
<th>DEFECT DESCRIPTION</th>
<th>SEVERITY</th>
<th>DEFECT STATUS</th>
<th>ASSIGNED TO</th>
<th>RESOLUTION DESCRIPTION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/20/2020</td>
<td>CVE-OBU-DEFECT0-07-v01</td>
<td>LDV (BasicVehicle OBU configuration) requests Signal Priority</td>
<td>Critical</td>
<td>Resolved</td>
<td>Siemens</td>
<td>Siemens vendor (WNC) resolved with OBU firmware version v14</td>
<td>verified/resolved on 10/14/2020</td>
</tr>
<tr>
<td>08/20/2020</td>
<td>CVE-OBU-DEFECT0-08-v01</td>
<td>Position Accuracy is worse with RTCM, than without</td>
<td>Critical</td>
<td>Canceled</td>
<td>Siemens</td>
<td>Smart Columbus and Siemens agreed to use the OBU internal GNSS and NOT use RTCM until the GNSS chip provider provides a resolution</td>
<td>Canceled on 10/12/2020</td>
</tr>
<tr>
<td>08/20/2020</td>
<td>CVE-OBU-DEFECT0-09-v01</td>
<td>Not able to configure the Siemens RSU using SNMP (via the CVCP)</td>
<td>Medium</td>
<td>Resolved</td>
<td>Siemens/Kapsch</td>
<td>Kapsch confirmed resolved on 11/18/2020</td>
<td></td>
</tr>
<tr>
<td>10/12/2020</td>
<td>CVE-OBU-DEFECT0-10-v01</td>
<td>Fire/Police/Transit/HDV OBUs downloaded 3 yrs. worth of certs; should only download and maintain 2 weeks’ worth, due to Preemption/Priority</td>
<td>Critical</td>
<td>Resolved</td>
<td>Siemens (WNC)</td>
<td>12/17/2020: Siemens demonstrated the issue has been resolved 10/12/2020: This is an ISS issue, Siemens to confirm when resolved</td>
<td>Resolved on 12/17/2020</td>
</tr>
<tr>
<td>10/15/2020</td>
<td>CVE-OBU-DEFECT011-v01</td>
<td>CVCP does not verify SRM; assumes RSU verifies certificate and only forwards valid/authorized SRMs</td>
<td>Critical</td>
<td>Canceled</td>
<td>Kapsch</td>
<td>RSUs verify SRM certificate, forwards SRM payload to CVCP. CVCP sends Signal Priority/Preemption request to the TSC based on SRM vehicle role; SSP is not evaluated</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSU only forwards SRM payload to CVCP, not 1609.2-2016 certificate containing the SSP</td>
<td></td>
<td></td>
<td></td>
<td>Development (cost and schedule impacts) required for all 3 RSU manufacturers to include 1609.2-2016 certificate with SRM Payload</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Development (cost and schedule impacts) required for CVCP to evaluate SSP if 1609.2-2016 certificate included with SRM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Given the RSUs verify SRM signatures, Signal Priority and Preemption are limited to specific corridors and the overall number of OBU requests is low, the team felt the risk of a non-Smart Columbus OBU requesting and getting the SRM message would be low.</td>
<td></td>
</tr>
</tbody>
</table>
| | | | | | | There is not a specific CVE requirement for RSUs to include the 1609.2 certificate when forwarding messages. The City consulted with the RSU manufacturers about adding this functionality. The outcome of these discussions was that additional development, compensation, and a delay in schedule, would be required for the RSUs to include the 1609.2 certificate when forwarding SRMs to the Message Handler.
<table>
<thead>
<tr>
<th>DATE OPENED</th>
<th>DEFECT NO.</th>
<th>DEFECT DESCRIPTION</th>
<th>SEVERITY</th>
<th>DEFECT STATUS</th>
<th>ASSIGNED TO</th>
<th>RESOLUTION DESCRIPTION</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>

being granted Signal Priority/Preemption was low and determined to move forward without comparing the SRM Vehicle Role to the certificate SSP.
<table>
<thead>
<tr>
<th>DATE OPENED</th>
<th>DEFECT NO.</th>
<th>DEFECT DESCRIPTION</th>
<th>SEVERITY</th>
<th>DEFECT STATUS</th>
<th>ASSIGNED TO</th>
<th>RESOLUTION DESCRIPTION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/17/2020</td>
<td>CVE-RSU-DEFECT012-v01</td>
<td>Kapsch RSU is not capable of reporting &quot;Channel Busy Ratio&quot;</td>
<td>Low</td>
<td>Canceled</td>
<td>Kapsch</td>
<td>Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>Development would be required to fully resolve this issue. After consulting with the RSU manufacturers, the team determined that not collecting &quot;Channel Busy Ratio&quot; provided a low risk to the overall CVE Performance measures and accepted RSU functionality without reporting &quot;Channel Busy Ratio&quot;</td>
</tr>
<tr>
<td>12/17/2020</td>
<td>CVE-RSU-DEFECT013-v02</td>
<td>Danlaw RSU is not capable of reporting &quot;Channel Busy Ratio&quot;</td>
<td>Low</td>
<td>Canceled</td>
<td>Kapsch</td>
<td>Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>Development would be required to fully resolve this issue. After consulting with the RSU manufacturers, the team determined that not collecting &quot;Channel Busy Ratio&quot; provided a low risk to the overall CVE Performance measures and accepted RSU functionality without reporting &quot;Channel Busy Ratio&quot;</td>
</tr>
<tr>
<td>DATE OPENED</td>
<td>DEFECT NO.</td>
<td>DEFECT DESCRIPTION</td>
<td>SEVERITY</td>
<td>DEFECT STATUS</td>
<td>ASSIGNED TO</td>
<td>RESOLUTION DESCRIPTION</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>--------------------</td>
<td>----------</td>
<td>---------------</td>
<td>-------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>12/17/2020</td>
<td>CVE-RSU-DEFECT014-v03</td>
<td>Siemens RSU is not capable of reporting &quot;Channel Busy Ratio&quot;</td>
<td>Low</td>
<td>Canceled</td>
<td>Siemens</td>
<td>Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>Development would be required to fully resolve this issue. After consulting with the RSU manufacturers, the team determined that not collecting &quot;Channel Busy Ratio&quot; provided a low risk to the overall CVE Performance measures and accepted RSU functionality without reporting &quot;Channel Busy Ratio&quot;</td>
</tr>
<tr>
<td>12/17/2020</td>
<td>CVE-MH-DEFECT015-v03</td>
<td>Message Handler does not report Cabinet Door Tamper Event</td>
<td>Low</td>
<td>Canceled</td>
<td>Kapsch</td>
<td>The Controller Cabinet reports when the cabinet door is open</td>
<td>No need for duplicate functionality. This function is not required from the Message Handler</td>
</tr>
<tr>
<td>12/17/2020</td>
<td>CVE-TSC-DEFECT016-v03</td>
<td>Siemens Traffic Signal Controller only supports Signal Priority; it does not support Signal Preemption</td>
<td>Medium</td>
<td>Canceled</td>
<td>Siemens</td>
<td>The City will deploy Econolite at intersections that require Signal Preemption</td>
<td>The City does not plan to request Siemens develop Signal Preemption functionality for the Controller</td>
</tr>
<tr>
<td>12/17/2020</td>
<td>CVE-TCVMS-DEFECT017-v03</td>
<td>TMC Operators do not receive e-mail alerts when RSU issues are detected</td>
<td>Medium</td>
<td>Canceled</td>
<td>Kapsch</td>
<td>TMC Operators are alerted to RSU issues through a Dashboard indication</td>
<td>City and TMC Staff agree that the Dashboard indication of an RSU issue is sufficient</td>
</tr>
</tbody>
</table>
### Chapter 4. Test Results

<table>
<thead>
<tr>
<th>DATE OPENED</th>
<th>DEFECT NO.</th>
<th>DEFECT DESCRIPTION</th>
<th>SEVERITY</th>
<th>DEFECT STATUS</th>
<th>ASSIGNED TO</th>
<th>RESOLUTION DESCRIPTION</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/21/2021</td>
<td>CVE-MH-Defect018-v1</td>
<td>Siemens Traffic Signal Controller does not support Signal Priority, as of 04/21/2021.</td>
<td>Medium</td>
<td>Closed</td>
<td>Siemens</td>
<td>The City deployed Econolite Traffic Signal Controllers at intersections that require Signal Priority</td>
<td>The City is still waiting on a firmware update from Siemens</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
4.3. CHANNEL 180 TESTS

As discussed in Section 3.7.2 DSRC Channel Plan, Smart Columbus RSUs are configured to broadcast all messages on Channel 180. To verify proper system operation, specific Channel 180 test objectives were defined in the Test Plan, focusing Channel Congestion. Channel 180 SST was performed in the Demonstration Area, using 1 RSU, 4 ASDs and 1 VAD-Transit OBU. The Test Scenarios are listed in Table 20. The number listed in the cell indicates the number of devices broadcasting the corresponding message. For example, for (test) ID # 1 VAD is broadcasting SRMs and 1 RSU is broadcasting WSA, SPaT, MAP, TIM, and SSM and in ID #10 4 VADs are running the RLVW application while downloading firmware updates OTA, 1 VAD is broadcasting SRM while downloading firmware updates OTA, and 1 RSU is broadcasting WSA, SPaT, MAP, TIM, SSM, while supporting firmware downloads (OBU OTA).

Table 20: Channel 180 Test Scenarios

<table>
<thead>
<tr>
<th>Test Scenarios</th>
<th>ID #</th>
<th>ASD</th>
<th>VAD-Transit</th>
<th>RSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-VAD-Transit broadcasting SRM and logging SSMs with 1-RSU broadcasting SPaT, MAP, TIM, SSM, and WSA</td>
<td>1</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1-VAD-Transit broadcasting SRM and logging SSMs while downloading a firmware update OTA with 1-RSU broadcasting SPaT, MAP, TIM, SSM, and WSA</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1-ASD RLVW application functioning with 1-RSU broadcasting SPaT, MAP, TIM, and WSA</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1-ASD RLVW application functioning while downloading a firmware update OTA with 1-RSU broadcasting SPaT, MAP, TIM, and WSA</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1-ASD RLVW application functioning with 1-VAD-Transit broadcasting SRM and 1-RSU broadcasting SPaT, MAP, TIM, SSM, and WSA</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Test Scenarios

<table>
<thead>
<tr>
<th>Test Scenarios</th>
<th>ID #</th>
<th>ASD</th>
<th>VAD-Transit</th>
<th>RSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-ASD RLVW application functioning with 1-VAD-Transit broadcasting SRM while downloading a firmware update OTA and 1-RSU broadcasting SPaT, MAP, TIM, SSM, and WSA.</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: City of Columbus
Chapter 5. Summary of Results

5.1. TEST METRICS

This section provides summaries of test metrics based on testing activities.

Table 21: Test Cases Passed vs Failed

<table>
<thead>
<tr>
<th>TOTAL</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>140</td>
</tr>
<tr>
<td>Ratio of Pass to Failed</td>
<td>127:4</td>
</tr>
</tbody>
</table>

Source: City of Columbus

Table 22: Test Cases by Test Status

<table>
<thead>
<tr>
<th>TEST CASE STATUS</th>
<th>TOTAL</th>
<th>OBU</th>
<th>OBU Application</th>
<th>RSU-Kapsch</th>
<th>RSU-Danlaw</th>
<th>RSU-Siemens</th>
<th>Message Handler</th>
<th>TSC-Econolite</th>
<th>TSC-Siemens</th>
<th>TCVMS</th>
<th>TrCVMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned</td>
<td>140</td>
<td>28</td>
<td>15</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>14</td>
<td>5</td>
<td>5</td>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>In-Progress</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Passed</td>
<td>127</td>
<td>28</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>11</td>
<td>5</td>
<td>1</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>Failed</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Deferred</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Deprecated</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: City of Columbus
### Chapter 5. Summary of Results

#### Table 23: Defect by Status Type

<table>
<thead>
<tr>
<th>DEFECT STATUS</th>
<th>TOTAL</th>
<th>CRITICAL</th>
<th>HIGH</th>
<th>MEDIUM</th>
<th>LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opened</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Closed</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Canceled</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Resolved</td>
<td>9</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Deferred</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*

#### Table 24: Change Request Status

<table>
<thead>
<tr>
<th>CHANGE REQUEST STATUS</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>14</td>
</tr>
<tr>
<td>Submitted</td>
<td>14</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
5.2. OUTSTANDING ISSUES

This section provides a list of open tests, defects, and change request as well as explanations as to why they are still open. Table 25 contains the list of open tests.

Table 25: Open Issues

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-MH004-v01</td>
<td>Siemens TSC Verify the Message Handler places a priority call to the local Signal Controller based on an authorized SRM</td>
<td>1. Power on RSU and Message Handler</td>
<td>• Test Conductor</td>
<td>FAIL</td>
<td>04/21/2021</td>
<td>Signal Priority is not implemented in the Siemens TSC as of 04/21/2021. The City is still expecting a FW update from Siemens for NTCIP 1211 and will test this functionality if received before project shutdown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Connect a laptop (L1) running Wireshark to the Signal Controller port of the Message Handler (L1 acts as the signal controller)</td>
<td>• Traffic Data Consumer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Configure Wireshark on L1 to capture packets from the Message Handler</td>
<td>• RSU Data Producer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Log received packets on L1</td>
<td>• Vehicle Drivers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Power on OBU1</td>
<td>• Data Recorder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. OBU1 broadcasts SRMs signed with a signal priority certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. In Wireshark on L1, inspect packets coming from the Message Handler to verify received packets contain priority calls from OBU1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Message Handler logs signal priority requests from OBU1 and signal priority calls sent to the Signal Controller (L1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Summary of Results

<table>
<thead>
<tr>
<th>Test Case ID</th>
<th>Objective</th>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
</table>
| CVE-MH006-v01     | Siemens TSC: Verify the Message Handler generates and forwards SAE J2735-032016-2016 SSMs, based on status data received from the local Signal Controller, to the local RSU | 1. Connect a laptop (L1) running Wireshark between the Signal Controller and the Message Handler such that data can flow between the Signal Controller and the Message Handler and Wireshark can monitor the data packets.  
2. Log received packets on L1  
3. Power on the Message Handler  
4. Power on the Signal Controller  
5. Connect a second laptop (L2) running Wireshark to the RSU port on the Message Handler (L2 acts as the RSU)  
6. Configure Wireshark on L2 to capture packets from the Message Handler  
7. Log received packets on L2  
8. Monitor Wireshark on L1 to be sure data is flowing between the Signal Controller and the Message Handler  
9. Inspect packets coming from the Message Handler on L2 to verify they conform to J2735-032016 SSM messages                                                                 | - Test Conductor  
- Traffic Data Consumer  
- RSU Data Producer  
- Vehicle Drivers  
- Data Recorder | FAIL        | 04/21/2021 | Signal Priority is not implemented in the Siemens TSC as of 04/21/2021.  
The City is still expecting a FW update from Siemens for NTCIP 1211 and will test this functionality if received before project shutdown |
## Test Case IDs

### CVE-TSC002-v01

**Objective:** Siemens TSC Verify Traffic Signal Controller processes a signal priority call from the Message Handler

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Power on RSU, Message Handler, OBU1, and Signal Controller</td>
<td>Test Conductor, Traffic Data Consumer, RSU Data Producer, Vehicle Driver, Data Recorder</td>
<td>FAIL</td>
<td>04/21/2021</td>
<td>Signal Priority is not implemented in the Siemens TSC as of 04/21/2021. The City is still expecting a FW update from Siemens for NTCIP 1211 and will test this functionality if received before project shutdown</td>
</tr>
<tr>
<td>2. OBU1 broadcasts SRMs signed with a signal priority certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. RSU forwards SRM to the Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Message Handler sends a signal priority call to the Signal Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Signal controller changes timing based on the priority call</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Data recorder log the time change in the test log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CVE-TSC004-v01

**Objective:** Siemens TSC Verify Traffic Signal Controller sends priority status to the Message Handler

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Tester Role</th>
<th>Test Status</th>
<th>Date Run</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Connect a laptop (L1) running Wireshark between the Signal Controller and the Message Handler such that data can flow between the Signal Controller and the Message Handler and Wireshark can monitor the data packets.</td>
<td>Test Conductor, Traffic Data Consumer, RSU Data Producer, Vehicle Driver, Data Recorder</td>
<td>FAIL</td>
<td>04/21/2021</td>
<td>Signal Priority is not implemented in the Siemens TSC as of 04/21/2021. The City is still expecting a FW update from Siemens for NTCIP 1211 and will test this functionality if received before project shutdown</td>
</tr>
<tr>
<td>2. Log received packets on L1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Power on RSU, Message Handler, OBU1, and Signal Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. OBU1 broadcasts SRMs signed with a signal priority certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. RSU forwards SRM to the Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Message Handler sends a signal priority call to the Signal Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Inspect packets coming from the Signal Controller on L1 to verify the Signal Controller is sending signal priority status data to the Message Handler</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** City of Columbus
All defects and change requests have been addressed.

### 5.3. CHANGE REQUEST LOG

Table 26 contains the Change Requests (CR) that were submitted, evaluated, and instantiated throughout testing.

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
<th>Justification</th>
<th>Defect ID</th>
<th>Requirement</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR001</td>
<td>Deprecate Test Case CVE-RSU011-v01 for Kapsch RSU</td>
<td>Kapsch RSUs do not support reporting “Channel Busy Ratio”. Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>CVE-RSU-DEFECT012-v01</td>
<td>CVE-FN1322-V01 CVE-FN3053-V01</td>
<td>Approved</td>
<td>Since development is required to fully resolve this issue the team decided to accept RSU functionality without reporting “Channel Busy Ratio”. Channel Busy Ratio is not a critical performance metric</td>
</tr>
<tr>
<td>CR002</td>
<td>Deprecate Test Case CVE-RSU011-v01 for Danlaw RSU</td>
<td>Danlaw RSUs do not support reporting “Channel Busy Ratio”. Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>CVE-RSU-DEFECT013-v01</td>
<td>CVE-FN1322-V01 CVE-FN3053-V01</td>
<td>Approved</td>
<td>Since development is required to fully resolve this issue the team decided to accept RSU functionality without reporting “Channel Busy Ratio”. Channel Busy Ratio is not a critical performance metric</td>
</tr>
<tr>
<td>CR003</td>
<td>Deprecate Test Case CVE-RSU011-v01 for Siemens RSU</td>
<td>Siemens RSUs do not support reporting “Channel Busy Ratio”. Development (cost and schedule impacts) is required for RSUs to support this requirement</td>
<td>CVE-RSU-DEFECT014-v01</td>
<td>CVE-FN1322-V01 CVE-FN3053-V01</td>
<td>Approved</td>
<td>Since development is required to fully resolve this issue the team decided to accept RSU functionality without reporting “Channel Busy Ratio”. Channel Busy Ratio is not a critical performance metric</td>
</tr>
<tr>
<td>CR004</td>
<td>Deprecate Test Case CVE-MH007-v01</td>
<td>The Controller Cabinet reporting when the cabinet door is open; Functionality is not required from the Message Handler</td>
<td>CVE-MH-DEFECT015-v01</td>
<td>CVE-FN3045-V01 CVE-FN3046-V01</td>
<td>Approved</td>
<td>No need for duplicate functionality</td>
</tr>
</tbody>
</table>
## Chapter 5. Summary of Results

### Connected Vehicle Environment Test Report – Final Report | Smart Columbus Program | 121

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
<th>Justification</th>
<th>Defect ID</th>
<th>Requirement</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR005</td>
<td>Deprecate Test Case CVE-TSC003-v01 for Siemens Traffic Signal Controller</td>
<td>Siemens Traffic Signal Controllers only support Signal Priority; they do not support Signal Preemption</td>
<td>CVE-TSC-DEFECT016-v03</td>
<td>CVE-FN1515-V01 CVE-FN1517-V01 CVE-FN1513-V01 CVE-FN1516-V01 CVE-FN1508-V01 CVE-FN1500-V01 CVE-IX3262-V01</td>
<td>Approved</td>
<td>The City does not plan to request Siemens develop Signal Preemption functionality for the Controller</td>
</tr>
<tr>
<td>CR006</td>
<td>Deprecate Test Case CVE-TSC005-v01 for Siemens Traffic Signal Controller</td>
<td>Siemens Traffic Signal Controllers only support Signal Priority; they do not support Signal Preemption</td>
<td>CVE-TSC-DEFECT016-v03</td>
<td>CVE-FN1515-V01 CVE-FN1517-V01 CVE-FN1513-V01 CVE-FN1516-V01 CVE-FN1508-V01 CVE-FN1500-V01 CVE-IX3262-V01</td>
<td>Approved</td>
<td>The City does not plan to request Siemens develop Signal Preemption functionality for the Controller</td>
</tr>
<tr>
<td>CR007</td>
<td>Deprecate Test Case CVE-TCVMS009-v01</td>
<td>OBUs cannot effectively utilize RTCM Position Corrections</td>
<td>CVE-FN3078-V01 CVE-FN3079-V01</td>
<td></td>
<td>Approved</td>
<td>Approved</td>
</tr>
<tr>
<td>CR008</td>
<td>Remove e-mail requirement from Test Case CVE-TCVMS018-v01</td>
<td>Smart Columbus Team feels a Dashboard Alert is sufficient</td>
<td>CVE-TCVMS-DEFECT017-v03</td>
<td>CVE-FN1451-V01 CVE-FN3046-V01 CVE-FN3048-V01 CVE-FN3050-V01</td>
<td>Approved</td>
<td>TMC staff agrees that a Dashboard Alert is sufficient</td>
</tr>
<tr>
<td>CR009</td>
<td>Remove e-mail requirement from Test Case CVE-TCVMS019-v01</td>
<td>Smart Columbus Team feels a Dashboard Alert is sufficient</td>
<td>CVE-TCVMS-DEFECT017-v03</td>
<td>CVE-FN1451-V01 CVE-FN3046-V01 CVE-FN3048-V01 CVE-FN3050-V01</td>
<td>Approved</td>
<td>TMC staff agrees that a Dashboard Alert is sufficient</td>
</tr>
<tr>
<td>CR010</td>
<td>Remove e-mail requirement from Test Case CVE-TCVMS020-v01</td>
<td>Smart Columbus Team feels a Dashboard Alert is sufficient</td>
<td>CVE-TCVMS-DEFECT017-v03</td>
<td>CVE-FN1451-V01 CVE-FN3046-V01 CVE-FN3048-V01 CVE-FN3050-V01</td>
<td>Approved</td>
<td>TMC staff agrees that a Dashboard Alert is sufficient</td>
</tr>
<tr>
<td>CR011</td>
<td>Deprecate requirement for OBU to utilize RTCM Position Corrections</td>
<td>OBU Position Accuracy gets worse when using RTCM</td>
<td>CVE-OBU-DEFECT008-v01</td>
<td>CVE-FN3078-V01 CVE-FN3079-V01</td>
<td>Approved</td>
<td>Smart Columbus and Siemens agreed to use the OBU internal GNSS and NOT use RTCM until the GNSS chip provider provides a resolution</td>
</tr>
</tbody>
</table>
### Chapter 5. Summary of Results

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
<th>Justification</th>
<th>Defect ID</th>
<th>Requirement</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR012</td>
<td>Deprecate Test that Message Handler match’s SRM Vehicle Role to 1609.2 Certificate Specific Service Permission (SSP)</td>
<td>Development (cost and schedule impacts) required for all 3 RSU manufacturers to include 1609.2 certificate with SRM Payload Development (cost and schedule impacts) required for CVCP to evaluate SSP if 1609.2 certificate included with SRM</td>
<td>CVE-OBU-DEFECT011-v01</td>
<td>N/A</td>
<td>Approved</td>
<td>There is not a specific CVE requirement for RSUs to include the 1609.2 certificate when forwarding messages. The City did consult with the RSU manufacturers about adding this functionality. The outcome of these discussions was that additional development, compensation, and a delay in schedule, would be required for the RSUs to include the 1609.2 certificate when forwarding SRMs to the Message Handler. Given the RSUs verify SRM certificates, Signal Priority and Preemption are limited to specific corridors and the overall number of OBUS, in general, in the Columbus area is low, the team felt the risk of a non-Smart Columbus OBU requesting and being granted Signal Priority/Preemption was low and determined to move forward without comparing the SRM Vehicle Role to the certificate SSP.</td>
</tr>
</tbody>
</table>
## Chapter 5. Summary of Results

### Connected Vehicle Environment Test Report – Final Report | Smart Columbus Program | 123

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
<th>Justification</th>
<th>Defect ID</th>
<th>Requirement</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR013</td>
<td>Deprecate Requirement for verifying TCVMS can detect unauthorized network activity</td>
<td>Detecting unauthorized network activity is part of the Columbus Department of Technology Network Intrusion Detection System, not part of the CVE TCVMS</td>
<td></td>
<td>CVE-SR1459-V01</td>
<td>Approved</td>
<td>This is not a TCVMS function</td>
</tr>
<tr>
<td>CR014</td>
<td>Deprecate Requirement for verifying TCVMS provides dashboard and e-mail alerts when unauthorized network activity is detected</td>
<td>Providing an alert when unauthorized network activity is detected is part of the Columbus Department of Technology Network Intrusion Detection System, not part of the CVE TCVMS</td>
<td></td>
<td>CVE-FN3050-V01</td>
<td>Approved</td>
<td>This is not a TCVMS function</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
5.4. **EXIT CRITERIA**

Table 27 lists the conditions that were fulfilled to claim testing is complete.

Table 27: Test Exit Criteria

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>MET / NOT MET</th>
</tr>
</thead>
<tbody>
<tr>
<td>All planned test cases and scenarios have been executed</td>
<td>MET</td>
</tr>
<tr>
<td>Test scenarios achieve a 100% pass ratio (in relation to failures)</td>
<td>NOT MET, 4 Test Cases (2 Message Handler and 2 Siemens Traffic Signal Controller) related to the Siemens Traffic Signal Controller <strong>Failed</strong> due to the Siemens Traffic Signal Controller not supporting Signal Priority. See Table 25: <strong>Open Issues</strong></td>
</tr>
<tr>
<td>All defects found have been recorded in the defect management tool</td>
<td>MET</td>
</tr>
<tr>
<td>All high-severity defects have been resolved and retested</td>
<td>MET</td>
</tr>
<tr>
<td>Outstanding issues have a plan and schedule for resolution</td>
<td>MET</td>
</tr>
<tr>
<td>Master Test Plan and Report Summary issued to all stakeholders</td>
<td>MET</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
Chapter 6. Signoff

The information being reported on this document is correct and grants permission for the project to move forward with the production deployment.

Table 28: Acceptance Test Signoff

<table>
<thead>
<tr>
<th>ROLE</th>
<th>NAME</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE Project Manager</td>
<td>Ryan Bollo</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>Test Manager</td>
<td>Frank Perry</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>Data Recorder</td>
<td>Tom Timcho</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>Traffic Data Consumer</td>
<td>Sara Khosravi</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>Transit Data Consumer</td>
<td>Iouri Nemirovski</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>OBU Test Conductor</td>
<td>Amadou Kane</td>
<td>12/18/2020</td>
</tr>
<tr>
<td>RSU Test Conductor</td>
<td>Paul Hill</td>
<td>12/18/2020</td>
</tr>
</tbody>
</table>

Source: City of Columbus
Appendix A. Terminology and Conventions

A.1 NUMBERING CONVENTION

Each testing element is assigned a unique ID for traceability and configuration management. Test cases and scenarios for all projects in the Smart Columbus program will follow the same convention, each element representing an identifiable attribute of the traced metric. The numbering convention is as shown in Figure 13.

![Numbering Convention Diagram]

Figure 13: Numbering Convention
*Source: City of Columbus*

Where:

01 Identifies the Project

02 Identifies the device under test and the test number

03 Identifies the version of the Test

The definitions of the components in Figure 13 are listed in Table 29.
Table 29: Numbering Convention Definitions

<table>
<thead>
<tr>
<th>Octet</th>
<th>Description</th>
<th>Data Type, Casing</th>
<th>Number of Characters or Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Project abbreviation</td>
<td>The designated Smart Columbus project acronym (i.e., CVE)</td>
<td>String, upper case</td>
<td>Variable</td>
</tr>
<tr>
<td>b. Device type code</td>
<td>• OBU: On-Board Unit&lt;br&gt;• App: OBU Application&lt;br&gt;• RSU: Roadside Unit&lt;br&gt;• MH: Message Handler&lt;br&gt;• TSC: Traffic Signal Controller&lt;br&gt;• TCVMS: Traffic Connected Vehicle Management System&lt;br&gt;• TrCVMS: Transit Connected Vehicle Management System</td>
<td>String, upper case</td>
<td>2</td>
</tr>
<tr>
<td>c. Test number</td>
<td>Integer incrementing by 1, indicating the number of Test Cases or Test Procedures</td>
<td>Integer</td>
<td>3</td>
</tr>
<tr>
<td>d. “v” static character</td>
<td>Static letter “v” represents the version for the particular test objective and procedure</td>
<td>Character</td>
<td>1</td>
</tr>
<tr>
<td>e. Version number</td>
<td>Integer incrementing by 1, indicating the number of revisions made to the test element being traced</td>
<td>Integer</td>
<td>2</td>
</tr>
</tbody>
</table>

Source: City of Columbus

An example of a test case for the integration of CVE would be CVE-OBU001-v01.
1. “CVE” is the project abbreviation.
2. “OBU001” is the Test Case #1 for the On-Board Units
3. “v01” is version #1 of Test Case OBU001
Appendix B. Acronyms and Definitions

Table 30 contains project specific acronyms used throughout this document.

Table 30: Acronyms List

<table>
<thead>
<tr>
<th>Abbreviation/Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARC-IT</td>
<td>Architecture Reference for Cooperative and Intelligent Transportation</td>
</tr>
<tr>
<td>ASD</td>
<td>After Market Safety Device</td>
</tr>
<tr>
<td>BSM</td>
<td>Basic Safety Message</td>
</tr>
<tr>
<td>CBR</td>
<td>Channel Busy Ratio</td>
</tr>
<tr>
<td>ConOps</td>
<td>[CVE] Concept of Operations</td>
</tr>
<tr>
<td>COTA</td>
<td>Central Ohio Transit Authority</td>
</tr>
<tr>
<td>CTSS</td>
<td>Columbus Traffic Signal System</td>
</tr>
<tr>
<td>CVE</td>
<td>Connected Vehicle Environment</td>
</tr>
<tr>
<td>CVRIA</td>
<td>CV Reference Implementation Architecture</td>
</tr>
<tr>
<td>CV</td>
<td>Connected Vehicle</td>
</tr>
<tr>
<td>CVTT</td>
<td>Connected Vehicle Test Tool</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short-Range Communications</td>
</tr>
<tr>
<td>EEBL</td>
<td>Electronic Emergency Brake Light</td>
</tr>
<tr>
<td>EV</td>
<td>Emergency Vehicle</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FCW</td>
<td>Forward Collision Warning</td>
</tr>
<tr>
<td>FST</td>
<td>Final System Test</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HDV</td>
<td>Heavy-duty Vehicle</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICD</td>
<td>Interface Control Document</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IMA</td>
<td>Intersection Movement Assist</td>
</tr>
<tr>
<td>IO</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
</tbody>
</table>
## Acronyms and Definitions

<table>
<thead>
<tr>
<th>Abbreviation/Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS</td>
<td>Intelligent Transportation System</td>
</tr>
<tr>
<td>L1</td>
<td>laptop 1</td>
</tr>
<tr>
<td>L2</td>
<td>laptop 2</td>
</tr>
<tr>
<td>LCW</td>
<td>Lane Change Warning</td>
</tr>
<tr>
<td>LDAT</td>
<td>Local Device Assembly Test</td>
</tr>
<tr>
<td>LDV</td>
<td>Light-duty Vehicle</td>
</tr>
<tr>
<td>MAP</td>
<td>SAE J2735 Map Message</td>
</tr>
<tr>
<td>OBUs</td>
<td>On-board Units</td>
</tr>
<tr>
<td>ODOT</td>
<td>Ohio Department of Transportation</td>
</tr>
<tr>
<td>Operating System</td>
<td>[Smart Columbus] Operating System</td>
</tr>
<tr>
<td>OTA</td>
<td>over the air (or over-the-air for adjectival use)</td>
</tr>
<tr>
<td>pcap</td>
<td>Packet Capture file</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RLVW</td>
<td>Red Light Violation Warning</td>
</tr>
<tr>
<td>RSSZ</td>
<td>Reduce Speed School Zone warning</td>
</tr>
<tr>
<td>RSU</td>
<td>Roadside Units</td>
</tr>
<tr>
<td>RTCM</td>
<td>Radio Technical Commission for Maritime Services</td>
</tr>
<tr>
<td>S1</td>
<td>toggle switch</td>
</tr>
<tr>
<td>SAE</td>
<td>Society of Automotive Engineers</td>
</tr>
<tr>
<td>SCMS</td>
<td>Security Credential Management System</td>
</tr>
<tr>
<td>SDD</td>
<td>[CVE] System Design Document</td>
</tr>
<tr>
<td>SPaT</td>
<td>Signal Phasing and Timing</td>
</tr>
<tr>
<td>SRM</td>
<td>Signal Request Message</td>
</tr>
<tr>
<td>SSM</td>
<td>Signal Status Message</td>
</tr>
<tr>
<td>SST</td>
<td>subsystem test</td>
</tr>
<tr>
<td>SyRS</td>
<td>[CVE] System Requirements</td>
</tr>
<tr>
<td>TBD</td>
<td>to be determined</td>
</tr>
<tr>
<td>TCVMS</td>
<td>Traffic Connected Vehicle Management System</td>
</tr>
<tr>
<td>TIM</td>
<td>Traveler Information Message</td>
</tr>
<tr>
<td>TMC</td>
<td>Traffic Management Center</td>
</tr>
<tr>
<td>TrCVMS</td>
<td>Transit Connected Vehicle Management System</td>
</tr>
<tr>
<td>TRL</td>
<td>Test Result Log</td>
</tr>
<tr>
<td>TVIER</td>
<td>Transit Vehicle Interaction Event Record</td>
</tr>
<tr>
<td>USDOT</td>
<td>U.S. Department of Transportation</td>
</tr>
<tr>
<td>Abbreviation/Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle-to-Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle-to-Vehicle</td>
</tr>
<tr>
<td>VAD</td>
<td>Vehicle Awareness Device</td>
</tr>
<tr>
<td>WAVE</td>
<td>wireless access in vehicular environments</td>
</tr>
<tr>
<td>WRA</td>
<td>wireless access in vehicular environments routing advertisement</td>
</tr>
<tr>
<td>WSA</td>
<td>wireless access in vehicular environments service advertisement</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*
## Appendix C. Glossary

Table 31 contains project specific terms used throughout this document.

### Table 31: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CV test tool (CVTT)</td>
<td>The CVTT is a specialized OBU designed to capture DSRC messages for decoding, visualizing DSRC messages (e.g., MAP, TIM), and running CV applications for system acceptance.</td>
</tr>
<tr>
<td>position correction system</td>
<td>A position correction system provides global navigation satellite system (GNSS) data consisting of carrier phase and code range measurements in support of three-dimensional positioning. Correction data are used to improve the precision of GPS data. Enhanced post-processed coordinates approach a few centimeters relative to the National Spatial Reference System, both horizontally and vertically.</td>
</tr>
<tr>
<td>Smart Columbus Operating System</td>
<td>The Operating System collects and archives CV data for distribution to third parties.</td>
</tr>
<tr>
<td>Traffic CV Management Center (TCVMS)</td>
<td>The TCVMS is the operation and maintenance center of the CVE. RSUs are monitored from, and data are archived to, the TCVMS.</td>
</tr>
<tr>
<td>Transit CV Management Center (TrCVMS)</td>
<td>The TrCVMS is the CV data center for COTA. Transit OBUs upload the log files to the TrCVMS and TrCVMS, and staff can review and process transit vehicle log files.</td>
</tr>
</tbody>
</table>

*Source: City of Columbus*