Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD)

Department of Public Works
City and County of Denver, Colorado

Concept of Operations (ConOps)

Version	Date	Comments
1.0	September 23, 2019	Final v1

Table of Contents

List of Tables

List of Figures

1. Introduction

This Concept of Operations (ConOps) document is part of the Systems Engineering Process, which provides an interdisciplinary approach for planning, designing, implementing (deploying), and operating a Connected Vehicle (CV) system while managing complexity, reducing risk, and promoting awareness of system/stakeholder needs and interfaces. Described below are a series of documents that will support the planning and implementation of the City and County of Denver's (CCD) Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD) program. Included in this series is the Concept of Operations (this document), which outlines how a system will function in respect to stakeholder needs, goals and objectives.

- **Program Charter**: Signed in February 2018, the charter was an internal document to kick off ATCMTD within CCD and serves as a base setting document for high-level goals, requirements, and description for how the program would run.
- **Program Management Plan** (PMP): A more detailed and thorough description of how the ATCMTD program will be managed. This will be a living document that will evolve with the needs of the program.
- **System Engineering Documentation**: This series of documents will serve as the fundamental architectural design behind the program and projects, including logic and information flow diagrams, and will address security and privacy requirements associated with the program.
    - **Systems Engineering Management Plan** (SEMP): In conjunction with the PMP, the SEMP identifies the systems engineering processes to be used in the project, the project management strategies being employed, and the risks and complexities of the program.
    - **Concept of Operations** (ConOps, this document): The concept of operations will serve as a living document that captures how the projects under ATCMTD will function from the perspective of various users.
    - **System Requirements** (SysRs): The system requirements document details all of the requirements of the system design process to ensure final product selection, software development, and system deployment meets the needs of the program.

1.1 Document Overview and Organization

This ConOps will describe enhancements and new functionality proposed for Denver's traffic management capabilities, with particular emphasis on connected vehicle technologies. More specifically, it will outline how the three ATCMTD projects (Connected Pedestrian, Connected Freight, and Connected Fleet/TMC) will operate to meet the needs of various stakeholders and provide a structure for the design and operational needs of the system. This ConOps will feed into the System Requirements document that will detail out the specifications of the system designs to inform the development of the final systems.

The audience for this document includes stakeholders within CCD who are involved with various aspects of the ATCMTD program and the impacts connected vehicle technology will have on CCD, such as the Traffic Management Center, Fleet Operators, Transportation Maintenance, Traffic Signals and Operations, and Transportation Engineering. External stakeholders include the freight community and FHWA.

The subsequent sections of the ConOps are organized as designated below:

Section 2: Background. This section overviews the ATCMTD program, the specific projects within the program, and their goals and objectives.

Section 3: User Needs. This section lists the primary and secondary users of the systems, and details out their needs from the system.

Section 4: Current Systems and Justification for Change. This section describes deficiencies of the existing conditions as it relates to each project.

Section 5: Scope and Description of Proposed System. This section details the system components, scope, and bounding conditions associated with each project.

Section 6: Assumptions, Policies, and Constraints. This section describes and illustrates the proposed system environments, capabilities, and functions of each project.

Section 7: Modes of Operation. This section describes the states of degradation the system could experience, and consequences of that.

Section 8: Analysis of Proposed System. This section analyzes the benefits, limitations, and evaluation methodologies considered for the system.

Section 9: Appendix, References, and Glossary. This section lists the documents relevant to this project, including any state/federal guidelines or documentation from related existing projects. It also includes definitions for terms, acronyms, and abbreviations used throughout the document.

2. Background

In 2016, CCD was awarded the U.S. DOT ATCMTD grant. The ATCMTD funds cutting-edge transportation technologies to reduce congestion and to improve the safety of our transportation system. This four-year, $12M effort is structured as a $6M Federal grant with $6M Denver matching funds. This program will pilot and demonstrate the value of connected vehicle and infrastructure technology.

2.1 Objectives

The ATCMTD program is broken down into three Connected Vehicle (CV) projects, each of which has a vision statement that provides the highest level of direction for the program team's goals and objectives. The three projects are as follows:

2.1.1 Connected Freight Project Vision

The goal of this project is to provide prioritized signal timing through connected vehicle technology to freight operators operating routes to businesses in and around the Denver metro area. Designated points of origin, and corridors will receive prioritized signal timing that will result in overall transportation operational and safety benefits. This project will provide an incentive to freight operators to take more efficient routes, avoid local neighborhood roads, and reduce congestion.

2.1.2 Connected Traffic Management Center (TMC)/Fleet Project Vision

The goal of this project is to provide the Denver TMC operators with a more advanced understanding of real-time and historical conditions in order to make more informed decisions. This project is intended to support the broader TMC strategic plan and Public Works mission. Connected vehicle technology deployed in City fleet vehicles will provide information on real-time traffic flows across the transportation grid, allowing for interventions from the TMC to reduce congestion. Unlike current traffic data platforms that rely on one-way communication with vehicles, present information via single-use tools or websites, rely on manual review of camera feeds, or use less precise technologies to understand travel flows; this project will use vehicle probe data to improve real-time decision making regarding signal timing, routing, and event and incident notifications. This project will also prepare the TMC for higher volumes of probe data when more CV-equipped vehicles enter the roadway in the future. The system will also provide information back to drivers, starting with signal phase information. Providing information back to the public will better inform drivers of real-time conditions.

2.1.3 Connected Pedestrian Project Vision

The goal of this project is to provide individuals accessing our city system of sidewalks with a safer way to cross the roadway. CCD will deploy adaptive pedestrian crossing technology, at select mid-block locations, that can adapt and respond to real-time conditions and alert oncoming vehicles to pedestrians ahead in the crosswalk to prevent traffic injuries and lower the potential risk of a crash. This project will provide real-time alerts to drivers, making crossing the street safer for all members of the public.

2.1.4 Supporting Technologies

As a part of implementing these CV technologies, Denver will need to build a data architecture that supports the volume of incoming vehicle data, ties disparate systems together, and leverages data to make operational and planning decisions.

3. User Needs

A user is defined as anyone who interacts with a system. Users can be grouped into user classes depending on their distinct modes of interaction with a system. The existing user classes identified below are broken out into two categories: Primary System Users, and Secondary System Users. Primary users are users that interact directly with CCD's systems. Secondary users are ones that interact with the resulting data, evaluate the system, or have some other indirect relationship with the target end user on the roadway. The ATCMTD program's use cases are designed to serve the primary user group first.

Tables 3.1 and 3.2 list the primary and secondary users followed by a brief description of their role within the system(s).

Table 3.1 - Primary System Users

User Group	ID	Owner	Description
Denver Traffic Management Center (DTMC) Operations Staff	DTMC	CCD	Denver staff responsible for monitoring, evaluating, and responding to traffic conditions and events
Denver Fleet and Safety	DFS	CCD	The managers, drivers, and staff that support city fleet operations, including snow plows, trash operations, etc.
Private Freight	PF	Private	The managers, dispatchers, and drivers of private freight companies participating in the program.
Equipped Public Drivers	EPD	Public	Members of the public with vehicles that have CV technology
Pedestrians	PED	Public	Non-vehicular travelers crossing the roadway

Table 3.2 - Secondary System Users

User Group	ID	Owner	Description
Denver Transportation Planners and Engineers	DTPE	CCD	Denver staff who use data to inform transportation plans and designs
Online Public	OP	Public	Private citizens seeking transportation data while driving

3rd Party Application Developers (3AD)	3AD	Private	Software developers building tools and solutions that leverage Denver's data
Colorado Motor Carriers Association (CMCA)	CMCA	Other	Non-government stakeholder group representing the interests of the freight industry
Colorado Department of Transportation (CDOT), Denver Regional Council of Governments (DRCOG), and other local agencies	GOV	Other Gov	State and regional transportation staff that will share information and data
Federal Highway Administration (FHWA)	FHWA	Other Gov	Program sponsor, evaluator, and regional stakeholder and coordinator

3.1 User Needs

In an effort to solve the transportation system challenges identified above, long-known user needs were prioritized. In describing a user need, it's important not to prescribe a solution, but to focus solely on the issue to be solved.

Tables 3.3 through 3.11 identify the user needs broken down by the user groups identified above. As noted above, this document identifies primary and secondary users of the system, allowing the program team to prioritize the use cases that serve the primary users first.

3.1.1 Primary System User Needs

Table 3.3 - User Needs for Denver Traffic Management Center (DTMC) Operations Staff

User Need ID	User Need Title	User Need Description
DTMC 1	Data Capture and Collection	Need the ability to capture, process, and evaluate information from CV and ITS devices for TMC operations
DTMC 2	Real-Time and Historical Comparison	Need to be able to aggregate data to establish a historical baseline, and then use real-time data measured against that historical base to generate alerts for TMC operators

DTMC 3	Performance Management	Need the ability to integrate performance measures from ATCMTD with broader industry evaluation tools like the automated traffic signal performance measures (ATSPM) framework
DTMC 4	Dashboards	Need a visual tool to remotely monitor the health of the devices and system
DTMC 5	Automating manual processes	Need the ability to automate repetitive actions and analysis, particularly for actions involving large datasets
DTMC 6	Data Dissemination	Need the ability to share data with 3rd party companies and the public, including data elements like SPaT

Table 3.4 - User Needs for Denver Fleet and Safety

User Need ID	User Need Title	User Need Description
DFS 1	Ability to see a birds-eye view of signal timing	Denver Police officers need the ability to see a “birds-eye” view (as if from above) of an intersection, to see the timing across multiple approaches and monitor potential traffic infringements.
DFS 2	Signal Priority for Select Fleet Vehicles	Need to be able to request signal priority for select fleet vehicles while in operation
DFS 3	Ability to see signal timing information (dependent on driver type)	Need the ability to more accurately predict the signal phase and timing of an approaching intersection to time acceleration and braking
DFS 4	Fleet Training	Fleet staff need training and information on installing and maintaining CV on-board equipment.
DFS 5	OBE Health Monitoring	Fleet Staff need the ability to check the health of OBE installed in their vehicles.
DFS 6	Distraction Free	Fleet operators need a human-machine interface for CV applications that does not create a distraction or impose a burden on the driver (if desired).

Table 3.5 - User Needs for Private Freight

User Need ID	User Need Title	User Need Description
PF 1	Freight signal priority	Need CCD to be able to modify signal timing to improve travel time for freight vehicles
PF 2	Freight queue management	Need improved signal timing at traffic signals near freight distribution centers for queue management of freight vehicles during high egress or ingress times
PF 3	Statistics on program utilization	Need information on the frequency of signal priority requests accepted for their fleet
PF 4	Shield competitive advantage	Need to ensure safeguards that prevent proprietary industry data from being publicly released to the detriment of private partners

Table 3.6 - User Needs for Equipped Public Drivers

User Need ID	User Need Title	User Need Description
EPD 1	Alerts for upcoming pedestrians in the crosswalk	Need alerts for upcoming pedestrians in a crossing, including out of sight pedestrians, via an in-vehicle alert (if equipped with DSRC) or sign along the roadway

Table 3.7 - User Needs for Pedestrians

User Need ID	User Need Title	User Need Description
PED 1	Extended time available to walk	Need additional protected time when the original time allocated is insufficient
PED 2	Approaching Vehicles Alerted to Pedestrians	Need to have approaching vehicles alerted to a pedestrian’s presence in a crosswalk

3.1.2 Secondary System User Needs

Table 3.8 - User Needs for Denver Transportation Planners and Engineers

User Need ID	User Need Title	User Need Description
DTPE 1	Evaluate historical data	Need to be able to evaluate historical data for trend analysis in coordination with the TMC

Table 3.9 - User Needs for Online Public

User Need ID	User Need Title	User Need Description
OP 1	Visual information in vehicle	Need automaker to provide visual display of warnings and information in an intuitive manner

Table 3.10 - User Needs for 3rd Party Application Developers

User Need ID	User Need Title	User Need Description
3AD 1	Machine-readable transportation data	Need clear, well-documented, and machine-readable data from APIs for any TMC data feed, such as SPaT data
3AD 2	Standard J2735 broadcast for automakers	Need standard broadcast messages for automakers to incorporate into future vehicle interfaces

Table 3.11 - User Needs for Colorado Motor Carriers Association (CMCA)

User Need ID	User Need Title	User Need Description
CMCA 1	Coordination	Need close coordination on logistics and impacts of projects on dispatching, route finding, and timing

Table 3.12 - User Needs for Denver Regional Council of Governors (DRGOC), Colorado Department of Transportation (CDOT), and other local governments (GOV)

User Need ID	User Need Title	User Need Description
GOV 1	Data interoperability	Need data standards and interoperability for regional sharing and collaboration

Table 3.12 - User Needs for Federal Highway Administration (FHWA)

User Need ID	User Need Title	User Need Description
FHWA 1	Data for program evaluation	Need data to prove out findings from project evaluations for performance and impact

4. Current Systems and Justification for Change

This section will describe the current systems associated with each of the three CV projects, and the associated justification for making changes.

4.1 Connected Freight

4.1.1 Current State

Denver's freight system includes highways, rail lines, and a major international airport that delivers goods, creates jobs, and provides economic opportunity to many people in the region, and statewide. Three of Colorado's major highways converge in north Denver: I-76, I-70, and I-25. The north Denver neighborhoods include Globeville, Elyria-Swansea, and Montebello, all of which have high densities of minority populations, low-income households, and high percentages of families with children. Major factories and distribution centers including Pepsi, Purina, Safeway, Swift, Coca-Cola, United Parcel Service (UPS), United States Postal Service (USPS), Suncor, Federal Express (FedEx), and the future Amazon warehouse and National Western Centers can all be found in north Denver. Heavy freight traffic throughout the area subjects these citizens to pollution, noise, and congestion. Additionally, due to continued growth in the area, pressure on the arterial streets is increasing. The Central 70 project will widen I-70 through north Denver, however, construction will greatly impact the north Denver communities for the next 3-5 years.

4.1.2 Justification for Change

The Connected Freight project recognizes the north Denver neighborhoods are disproportionately impacted by the effects of freight congestion. To test improvements to the movement of freight vehicles and their associated impacts on traffic and air quality, the Connected Freight project will target specific freight corridors to implement freight signal priority with participating private firms.

4.2 Connected TMC and Fleet

4.2.1 Current State

Denver operates a TMC five days per week from 6 AM to 7 PM that monitors traffic conditions throughout CCD. Operators in the TMC are responsible for managing and monitoring traffic signals and ITS devices, obtaining information about road and travel conditions, and coordinating with maintenance and incident management personnel to keep Denver's transportation system working safely and effectively. ITS devices that inform TMC operators include over 500 traffic monitoring pan-tilt-zoom (PTZ) cameras, over 800 detection sensors and count stations connected to the TMC via 300 miles of fiber optic cable. This information is supplemented by communications with maintenance personnel, construction teams, and Denver Police. The systems that operate these devices include the following:

- TransSuite - the central traffic signal control program. This platform is the primary tool for TMC operations used to monitor and manage the performance of City traffic signals.

- Skyline - a Variable Message Board control interface is a module that integrates functionality to control messages/graphics posted on CCD variable message signs.

- Bluetoad System - a TrafficCast system used to monitor and analyze travel time data captured from Bluetooth sensors deployed on certain transportation corridors in CCD.

- Camera/PTZ system - a system used to monitor and control the Closed-Circuit Television (CCTV) cameras with Pan, Tilt, and Zoom (PTZ) capabilities deployed throughout CCD; these feeds are shared regionally.

- HAR System - a Highway Advisory Radio (HAR) communications system used to notify motorists of traffic conditions.

- SolarWinds - this system is used for the management and monitoring of IT networks. Denver utilizes SolarWinds to manage its robust fiber network.

- Cartegraph - this is a new system procured by CCD to be its asset management tool that will support the operation and maintenance of Denver’s various assets, including ITS devices.

All of the systems listed above operate with proprietary systems and are not interoperable.

The TMC serves dual functions as the confluence of operations and technology: 1) real-time management of daily operations, unplanned incidents and events, special events, and road work, and 2) collecting data for historical analysis and trend analysis. To effectively accomplish real-time operations management, a high level of situational awareness is required. To meet this need, Denver has an in-house geospatial dashboard for situational awareness, monitors a CCTV system, and collects data from existing field devices. When CV data is added as a resource for the TMC, data collection and processing tools will be necessary to make the data actionable to TMC operators.

Additionally, a fleet of over 1,250 light and heavy-duty vehicles are used in daily operations throughout CCD. These vehicles have the potential to generate large amounts of vehicle probe data that could be used to provide real-time data to TMC operations.

4.2.2 Justification for Change

Denver staff cannot manually monitor the entire system described above. The staff needs a means to automate this data collection. Developing data solutions that establish baseline trend data and automatic alerts when current conditions deviate significantly from the norm will improve TMC operator response time.

Additionally, the TMC would benefit from richer data provided directly by connected vehicles. Leveraging CCD's own fleet vehicles to start this data collection will prepare the TMC for broader CV adoption in the future and improve operations today.

Finally, CCD does not currently disseminate all of the types of real-time information to the traveling public. By investing in data systems that support data collection and dissemination, the TMC will be able to share additional valuable information with the public.

4.3 Connected Pedestrian

4.3.1 Current State

Many pedestrian crossings in Denver are equipped with traffic technology to support the safe crossing of City streets. This technology includes pedestrian walk indicators with walk time countdowns, audio cues for when and where to cross, and signs/signals to alert vehicles of midblock crossings. There is currently no technology deployed in Denver that has the capability of automatically detecting pedestrians in a crosswalk and extending warning signal times for late arriving and slower than average pedestrians. Pilot programs to evaluate Automated Pedestrian Detection are needed, and Denver's existing High-Intensity Activated crosswalk (HAWK) signals provide great opportunity to test the viability of these technologies.

4.3.2 Connected Pedestrian Justification

In 2015, 1,618 crashes involving pedestrians occurred in Denver. Automated Pedestrian Detection and advanced alerting of drivers is a promising opportunity to reduce that number and make pedestrian crossings safer for all users of the system.

5. Scope and Description of Proposed System

Below is the description, system components, and scope for each of the three CV projects, followed by program-wide components, organized as follows:

1. Project Description

2. Major System Components - this subsection includes a primary information flow diagram to illustrate how the major components interface with each other.
    a. Vehicles
    b. Roadside Infrastructure
    c. Operational Data
    d. Personnel
    e. Network Infrastructure

3. Regional ITS Architecture - subsection that describes the relationship of the project to the regional ITS architecture service package(s). The ATCMTD program started with the national CVRIA architecture as its base, and has incorporated regional ITS architecture from the Denver Regional Council of Governments (DRCOG) as well.

4. Bounding conditions of the proposed system - this subsection describes the needs of CCD to make these projects work that are not traced back to a specific user group.

5. Interfaces with external systems - this subsection describes the high-level interfaces between external systems and the specific proposed system.

6. Project risk factors - this subsection outlines the project risk factors that will need to be managed while operating the specific proposed system.

7. Deployment Area - this subsection describes the geographic area for project deployment.

The specific operational scenarios, detailing step by step logical data flows for each use case are being developed in a separate document, "ATCMTD Operational Scenarios" as they will require constant revision as the team begins implementation.

5.1 Project: Connected Freight

5.1.1 Connected Freight Description

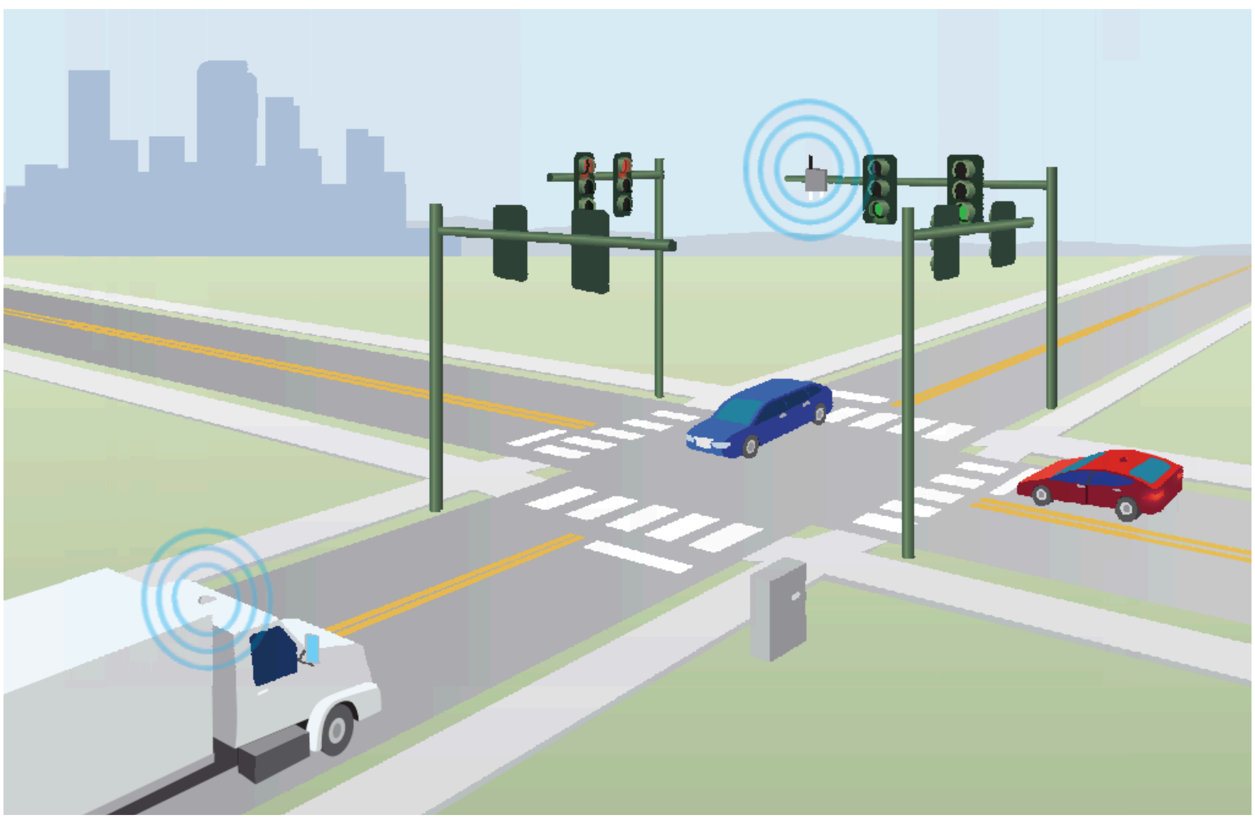
To address the freight congestion issues identified above, Denver plans to test DSRC-based freight signal priority (FSP) on high priority freight routes (Figure 5.3) throughout CCD. The targeted improvement of this project involves effectively moving more freight along selected routes by incentivizing companies with FSP. It is intended that this will reduce interruptive freight movement through neighborhood streets, improve the efficiency of the vehicles along select routes, and reduce travel time. Specifically, the proposed system will:

1. Add capability for an OBU installed on participating freight vehicles to request signal priority on City-designated high priority freight corridors.
2. Add capability for an RSU installed on a freight corridor intersection to provide the signal status for a priority request from a freight vehicle.
3. Store data generated from freight vehicles and controlling systems for performance measurement and evaluation.

5.1.2 Connected Freight System Components

Figure 5.1 illustrates the proposed concept for the Connected Freight project. Following this graphic is a detailed description and a primary information flow diagram of the major system components and their interactions.

Figure 5.1 - Connected Freight Summary Illustration



5.1.2.a Vehicles

Freight vehicles/operators that have opted to participate in this program will be the primary users to interface with the proposed system. Participating vehicles will be equipped with a

DSRC-enabled OBU. The OBU will not be connected to the vehicle's electronic systems, it will only generate the Basic Safety Message (BSM) Part 1 elements. The OBU will be able to generate signal priority requests for equipped intersections.

5.1.2.b Roadside Infrastructure

New equipment to support CV infrastructure will include the RSU, and V2X Hub Linux computer. This equipment will work alongside CCD's current standard for roadside equipment.

5.1.2.c Operational Data

The following bullets outline any Connected Freight project-specific CV message sets beyond the BSM and MAP/SPaT messages, collected in the centers.

- Signal Request Messages (SRM)
    - Messages produced by the OBU requesting priority or preemption from the signal
- Signal Status Messages (SSM)
    - Messages produced by the RSU communicating the status of the priority or preemption request

5.1.2.d Personnel

Three major personnel-related objects interface with the proposed Connected Freight system: freight operators, Denver TMC operations personnel, and Denver maintenance personnel.

- Freight drivers, the primary users of the proposed system, will interact with the proposed system through an OBU installed in their vehicle. The driver may or may not be aware of the benefits the OBU is providing to them, however, logic programmed on the advanced traffic signal controller will grant freight operators signal priority based on predefined conditions. The OBU will send, receive, and log Signal Request Messages (SRM) and Signal Status Messages (SSM). These messages could be conveyed to the freight operator through a driver interface that does not require input from the operator. It is undetermined at this time if the driver will utilize any interface. It is also undetermined if or how freight operators will be responsible for the upkeep or replacement of equipment installed in their vehicles.

- Denver TMC operations personnel will interact through network monitoring and management of the roadside system components, as described in other sections of this document.

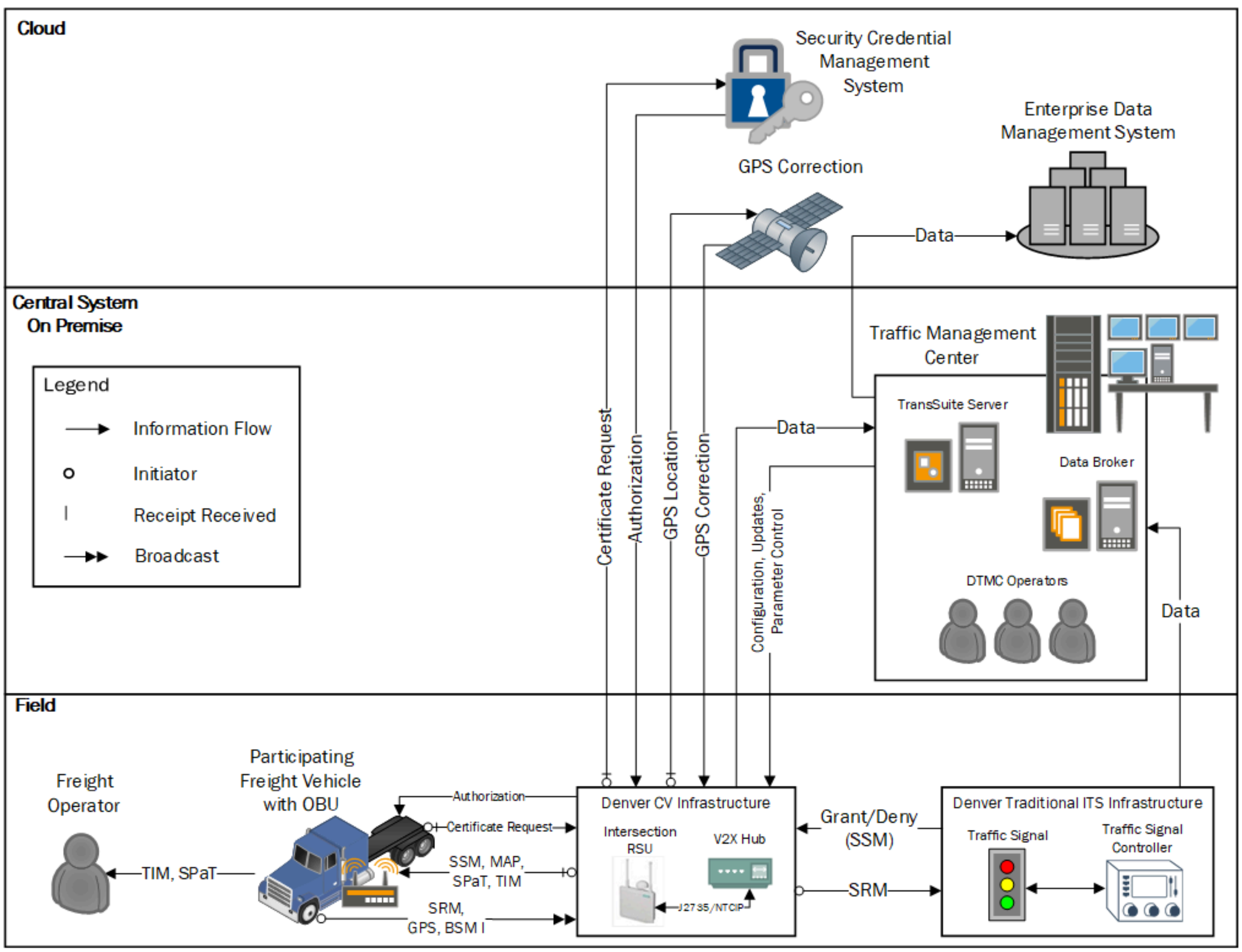
- Denver maintenance personnel will perform installation or maintenance activities appropriate for the roadside equipment (Controllers, V2X Hub, RSUs, etc.). Operations and maintenance procedures will be developed as this technology is deployed.

5.1.2.e Network Infrastructure

All participating intersections will be connected to the TransSuite Central Signal System for monitoring and analysis. RSUs and the accompanying V2X hub processing computer will tie into Denver's fiber-optic network. This will support the collection of signal priority request data and signal performance and timing data for evaluation of the proposed system. The data broker(s) will pull data into the TMC and push it to the Enterprise Data Management (EDM), which will be described in greater detail below, where the data can flow between the two systems.

Figure 5.2 illustrates how each component of the Connected Freight system listed above interacts with each other. This diagram illustrates the primary information flows between major groups of physical objects. There are more detailed flows between objects within each major group that are not shown as part of this diagram.

Figure 5.2 - Connected Freight Primary Information Flow Diagram



5.1.3 Regional ITS Architecture

DRCOG maintains the regions ITS Architecture. For this Connected Freight project, the following service package from DRCOG is applicable:

> ***CVO06-01 Denver Freight Signal Priority*** *- provides traffic signal priority for freight and commercial vehicles traveling in a signalized network with the goal to reduce stops and delays and to increase travel time reliability for freight traffic, while enhancing safety at intersections.*

5.1.4 Bounding Conditions of the Proposed System

The Connected Freight project will utilize unconditional priority to improve freight congestion. This approach minimizes the complexity associated with deploying conditional logic on edge devices, while allowing parameters like time of day, days of the week, and directionality to be configured from a central management system. The freight priority calls into the traffic signal controller will be weighted to balance the demands of other users at the intersection as well, ensuring, for example, preemption calls from emergency vehicles continue to take precedent.

Table 5.1 lists the bounding conditions specific to the Connected Freight project.

Table 5.1 - Connected Freight System Bounding Conditions

ID#	Bounding Condition
BC-CF-01	Freight partners receive training and information on installing CV on-board equipment
BC-CF-02	Freight partners are able to monitor the health of any OBE installed in their vehicles
BC-CF-03	Freight partners receive training and information on how to maintain CV on-board equipment
BC-CF-04	If desired, freight operators could use a human-machine interface for CV applications

5.1.5 Interfaces with Existing Systems

The FSP application will interface with the Traffic Signal Controller for priority requests.

5.1.6 Project Risk Factors

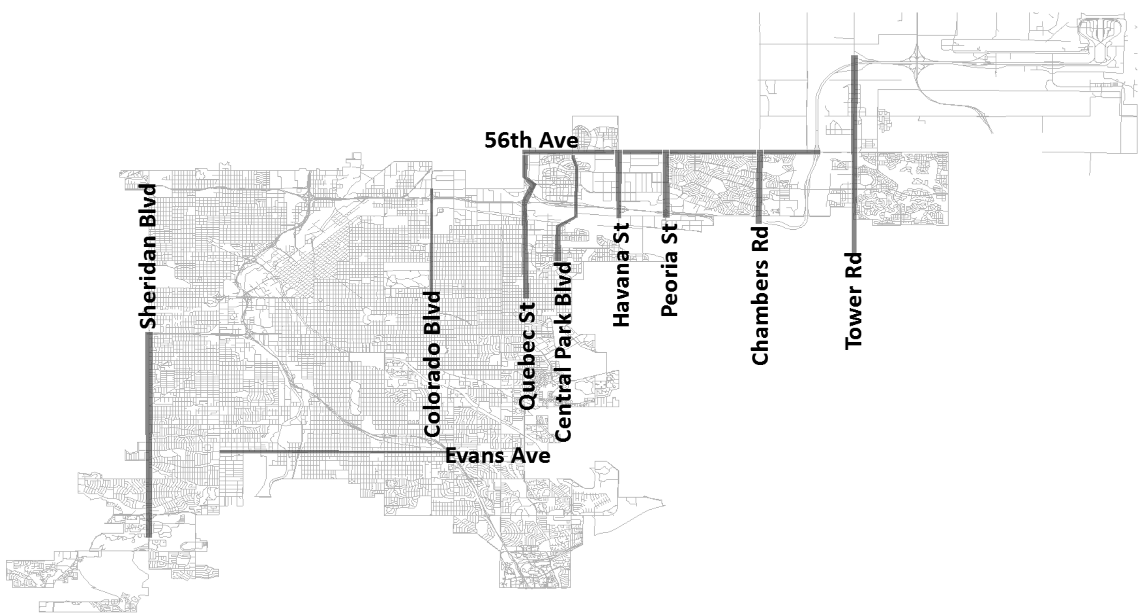
There are four major project-specific risk factors for the Connected Freight proposed system including:

- Lack of benefit to the freight companies leading to lower participation or compliance with the proposed system.
- Difficulties regarding OBU management including maintenance responsibilities, liability, system updates, and reliability.
- Interoperability issues between RSUs and OBUs leading to ineffective use of the CV applications.
- Different implementations of standards and use of proprietary protocols among device manufacturers leading to inaccurate message exchanges or interoperability.

5.1.7 Connected Freight Deployment Area

The connected freight project will focus on providing signal priority to commercial vehicles along designated major freight corridors. The routes were selected based on the geographic concentration of freight distribution centers, arterial roads near highway routes, and feedback from the Colorado Motor Carriers Association to incorporate industry expertise in route selection. The deployment locations were also cross-referenced with CCD's snow plow routes and geographic locations with a high concentration of city vehicles to maximize the value of each RSU placement across the Connected Freight and Fleet projects. CCD's initial deployment plan looks to install DSRC units at 150 intersections on defined corridors, which is subject to change based on field evaluations. Further deployment phases will increase the number of installed units over the life of the program. Figure 5.3 maps out the initial corridors to be implemented:

Figure 5.3 - Proposed RSU Deployment Map



5.2 Project: Connected Traffic Management Center (TMC) and Fleet

5.2.1 Connected Traffic Management Center (TMC) and Fleet Description

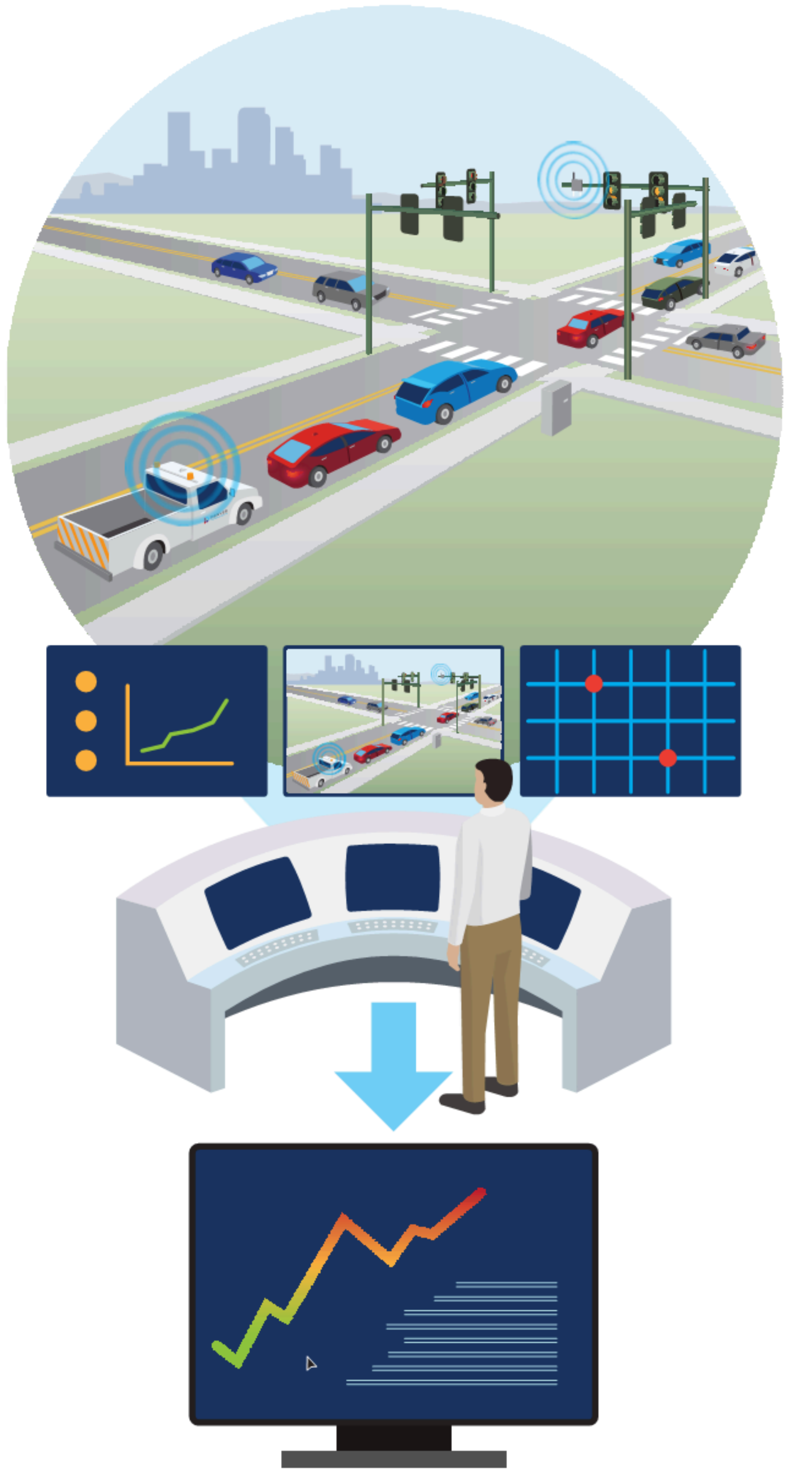
To achieve a greater understanding of real-time traffic conditions, Denver will install DSRC OBUs in up to 1,500 City fleet vehicles. This will allow for the collection of probe data to make more informed decisions regarding signal timing, routing, and incidents. A CV operations environment will be implemented within the TMC to support the collection of this data along with other CV applications. Specifically, the proposed system will:

1. Add capability to collect probe vehicle data from equipped City fleet vehicles for situational awareness via system-generated alerts.
2. Add the capability for snow plows in CCD’s fleet to request signal priority from CV-enabled intersections.
3. Add the capability for select fleet vehicles, specifically police officers, to see a “birds-eye” view of the signal phase and timing of an intersection.
4. Share data with the EDM, and leverage the EDM to share data with third parties and the public as appropriate.

5.2.2 Connected Traffic Management Center (TMC) and Fleet System Components

Figure 5.4 illustrates the proposed concept for the Connected TMC/Fleet project. Following this graphic is a detailed description and primary information flow diagram of the major system components and their interactions.

Figure 5.4 - Connected TMC/Fleet Summary Illustration



5.2.2.a Vehicles

Participating fleet vehicles will be equipped with a DSRC-enabled OBU. The OBU may or may not be connected to the vehicle's electronic systems. If it is, the OBU will be able to provide both BSM Parts 1 and 2, and if not, it will just utilize part 1. The OBU will broadcast its data to nearby RSUs. For snow plow vehicles equipped in the fleet, the OBUs will also be able to request signal priority when the snow plow is actively plowing or applying product to the roadway.

5.2.2.b Roadside Infrastructure

New equipment to support CV infrastructure will include the RSU, and V2X Hub Linux computer. This equipment will work alongside CCD's current standard for roadside equipment, including P cabinets, Hirschmann POE switches, and Intelight traffic signal controllers.

5.2.2.c Operational Data

The following bullets outline any Connected TMC/Fleet project-specific CV message sets in addition to the standard BSM and MAP/SPaT messages, collected in the centers.

- Basic Safety Messages (BSM)
    - BSM data will be collected to support situational awareness insights from connected fleet vehicles. BSM data is continually broadcasted and only picked up by other CVs or RSUs in range of that broadcast.
- Signal Request Messages (SRM)
    - Messages produced by the authorized OBU requesting priority or preemption from the signal.
- Signal Status Messages (SSM)
    - Messages produced by the RSU communicating the status of the priority or preemption request.

5.2.2.d Personnel

Four major personnel-related objects interface with the proposed Connected Fleet/TMC system:

- Fleet drivers will interact with the proposed system through an OBU installed in their vehicle. The driver may or may not be aware of the benefits the OBU is providing to them, however. The OBU may or may not be connected to the vehicle's electronic systems. If it is, the OBU will be able to provide both BSM Parts 1 and 2, and if not, it will just utilize part 1. Logic programmed on the advanced traffic signal controller will grant snow plow operators signal priority if the vehicle is actively plowing or applying product to the roadway. The OBU will send, receive, and log Signal Request Messages (SRM) and Signal Status Messages (SSM). These messages could be conveyed to the snow plow operator through a simple driver interface that does not require input from the operator. It is undetermined at this time if the driver will utilize any interface.

- Denver TMC operations personnel will interact with the Connected Fleet/TMC project to improve real-time situational awareness of the traffic network. With the support of the EDM and its underlying data systems, TMC personnel will have access to the probe data collected by the connected fleet vehicles. This data, in conjunction with current systems and devices, provides better situational awareness for TMC personnel of the traffic network. Improved situational awareness can include back of queue detection, alerts for multiple traction control indicators from a geo-fenced area, rapid decelerations (which may signal an incident has occurred), and speed probe analysis. This data has the potential to be ingested by third-party application developers to get important traveler information to the public.

- The traveling public could interact with the proposed system if a user owns a connected vehicle, equipped with a DSRC-enabled OBU. The driver will be able to receive SPaT/MAP messages at participating intersections equipped with RSUs. Proposed RSUs will also have the ability to receive BSM I/II data from public connected vehicles.

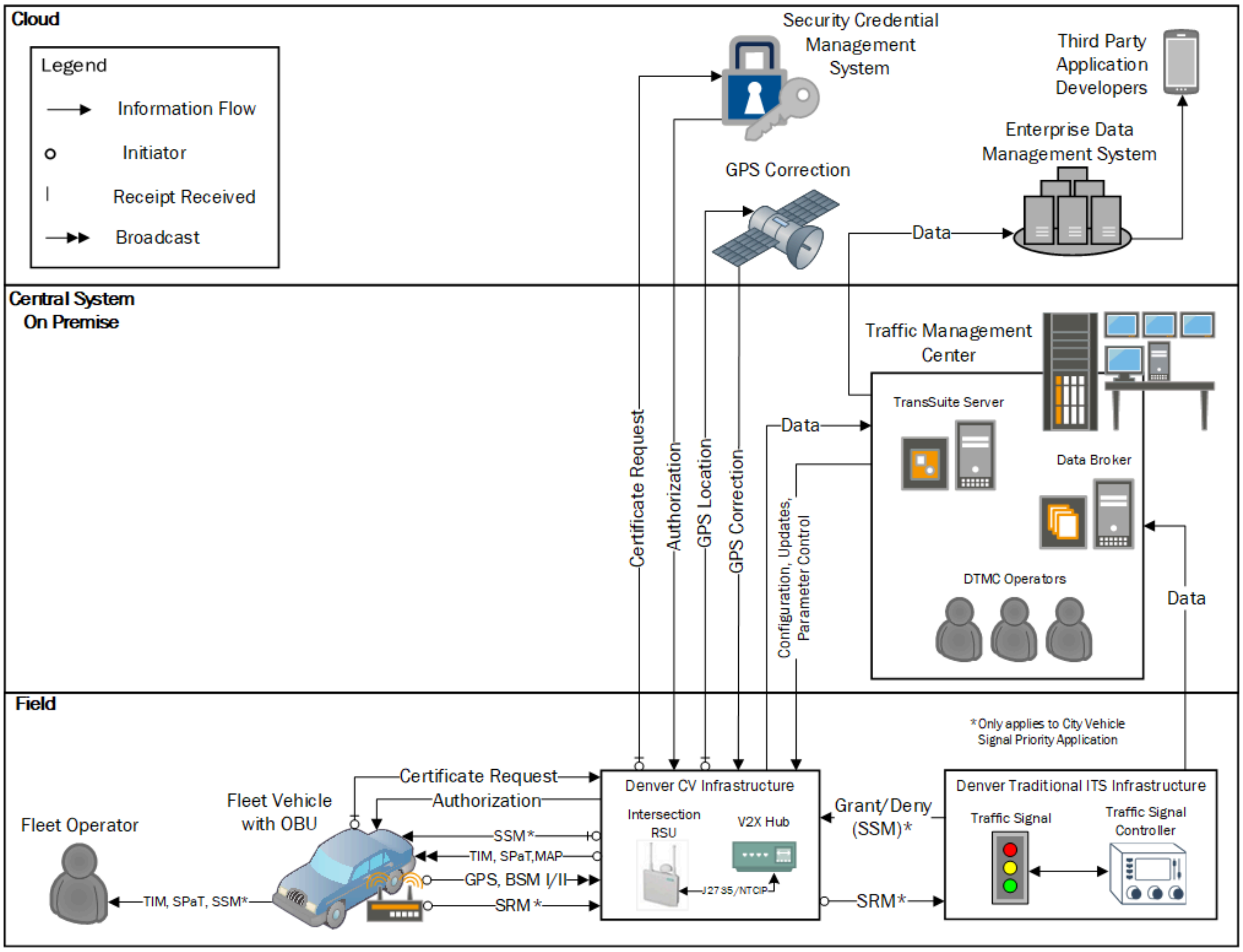
- Third party application developers will have access to APIs developed by CCD that are provided by the TMC and EDM systems. These APIs can be integrated into third-party applications to provide the traveling public with better information regarding the performance of CCD's traffic network. Data expected to be provided currently includes real-time SPaT data.

5.2.2.e Network Infrastructure

All participating intersections will be connected to the TransSuite Central Signal System for monitoring and analysis of advanced traffic signal performance measures. RSUs and the accompanying V2X hub processing computer will tie into Denver's fiber-optic network. This will support the collection of signal priority request data and signal performance and timing data for evaluation of the proposed system. On-premise data broker(s) will funnel data into the TMC and to the EDM where it can flow between the two systems.

Figure 5.5 illustrates how each component of the Connected TMC/Fleet system listed above interacts with each other. This diagram illustrates the primary information flows between major groups of physical objects. There are more detailed flows between objects within each major group that are not shown as part of this diagram.

Figure 5.5 - Connected TMC/Fleet Primary Information Flow Diagram



5.2.3 Regional ITS Architecture

DRCOG maintains the regions ITS Architecture. For this Connected TMC/Fleet project, the following service package from DRCOG is applicable:

> ***TM02-02 Local Jurisdiction Vehicle-Based Traffic Surveillance*** *- supports dedicated short-range communications between passing vehicles and the roadside to provide vehicle operational information and status directly to the traffic management center. This package enables transportation operators and traveler information providers to monitor road conditions, identify incidents, analyze and reduce the collected data, and make it available to users and private information providers.*

5.2.4 Bounding Conditions of the Proposed System

Table 5.2 lists the bounding conditions specific to the Connected TMC/Fleet project. These conditions are specific to CCD fleet vehicles, and may not apply to freight or privately owned vehicles.

Table 5.2 - Connected TMC/Fleet System Bounding Conditions

ID#	Bounding Condition
BC-TF-01	Any CV onboard technologies installed as a part of this project do not interfere with telematics devices
BC-TF-02	Any CV onboard equipment installed as a part of this project is tamper proof to prevent driver interference

5.2.5 Interfaces with Existing Systems

The proposed system could interface with the following existing system:

- ESRI-based Situational Awareness Tool - as the TMC's main tool for visualizing real-time traffic data, the Situational Awareness Tool could benefit greatly from the addition of city probe data.

5.2.6 Project Risk Factors

There are four project-specific risk factors for the Connected TMC/Fleet proposed system including:

- Ineffective in-vehicle driver interface for advisory and alert messages leading to frustration with the system or poor compliance.
- Limited market penetration of private vehicles leading to smaller volumes of data coming into the TMC.
- Limited RSU coverage across CCD leading to a relatively narrow view of real-time conditions.
- Interoperability issues between RSUs and OBUs leading to ineffective use of the CV applications.

5.2.7 Connected Traffic Management Center (TMC) and Fleet Deployment Area

The Connected TMC/Fleet project aims to equip up to 1,500 fleet vehicles with DSRC onboard units to enable probe vehicle data collection, signal priority for select vehicles, and SPaT information for select vehicles. The TMC will leverage this field data to build a baseline of historical data and be able to automatically alert TMC operators to conditions outside the norm when enough data is captured to be statistically significant. The TMC will leverage the EDM for data analysis and distribution, including APIs to third parties. The intersections in Figure 5.3 will serve as the RSU data collection points for CCD's DSRC enabled fleet vehicles.

5.3 Project: Connected Pedestrian

5.3.1 Connected Pedestrian Description

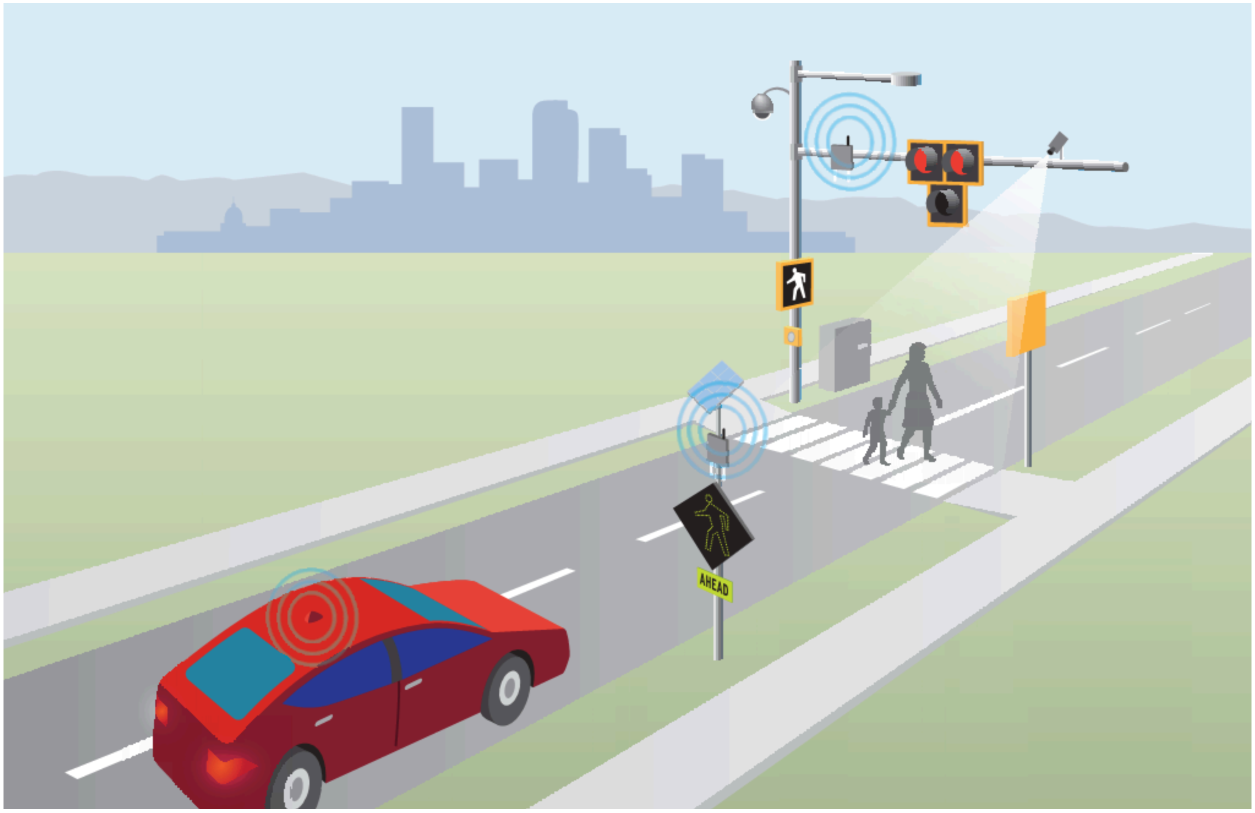
Denver will implement Automated Pedestrian Detection (APD), Advance Warning Signs, and DSRC technology to improve pedestrian and driver interactions at four midblock crossings within CCD. These deployments will act as pilot studies and will work with existing HAWK signals that have already been installed at each location. The DSRC component will also serve as a proof of concept for connected pedestrian warning systems by allowing CCD to collect and disseminate pedestrian crossing information. Specifically, the proposed system will:

1. Add capability to automatically detect pedestrians in a crosswalk.
2. Add capability to collect pedestrian crossing attributes (speed, heading, occupancy, counts).
3. Add capability to extend the wig/wag phase of the HAWK signal to allow a pedestrian to finish crossing if needed.
4. Add capability to warn drivers in advance that there is a pedestrian in a crosswalk.

5.3.2 Connected Pedestrian System Components

Figure 5.6 illustrates the proposed concept for the Connected Pedestrian project. Following this graphic is a detailed description and primary information flow diagram of the major system components and their interactions.

Figure 5.6 - Connected Pedestrian Summary Illustration



5.3.2.a Vehicles

Drivers will be able to interact with the system if their vehicle has DSRC capabilities or not. In both cases, the pedestrian crossing warnings that are presented are added functionality on top of the existing HAWK crossing indicator.

- Vehicles with DSRC-equipped OBUs will be able to receive direct wireless warnings of a pedestrian crossing ahead. The vehicle will also broadcast out its BSM information, which will allow CCD to review driving behavior at these crossings.

- Drivers of vehicles without DSRC will be presented real-time alerts about a pedestrian crossing ahead with a dynamic advance warning sign, which is wirelessly triggered from the intersection.

5.3.2.b Roadside Infrastructure

New equipment to support CV infrastructure will include the RSU, and V2X Hub Linux computer. This equipment will work alongside CCD's current standard for roadside equipment, including P cabinets, Hirschmann POE switches, and Intelight traffic signal controllers.

For this project, the selection of Automated Pedestrian Detection is critical to successfully extend the HAWK Wig/Wag time, and produce a signal for DSRC-enabled devices.

5.3.2.c Operational Data

The following bullets outline any Connected Pedestrian project-specific message sets beyond the standard BSM and MAP/SPaT messages, collected in the centers.

- Pedestrian Detection data (vendor-dependent)
  - Detection elements could include pedestrian speed, heading, occupancy/time in the intersection, and counts.
- High-resolution Traffic Signal Controller Data
  - HAWK signal actuation data, push button utilization.
- BSM data from passing connected vehicles

5.3.2.d Personnel

There are two personnel-related objects that interface with the proposed Connected Pedestrian system:

- Pedestrians, the primary users of the proposed system, will continue to interface with the traditional ITS infrastructure components of the system at participating crosswalks. Pedestrians will use the pedestrian push button (PPB) to activate the HAWK signal and cross. The changes the system makes will be invisible to the pedestrian. If a Pedestrian needs additional time to cross, the Wig/Wag phase will be extended to allow for that time, but this system adaptation won't be apparent to the Pedestrian it benefits.

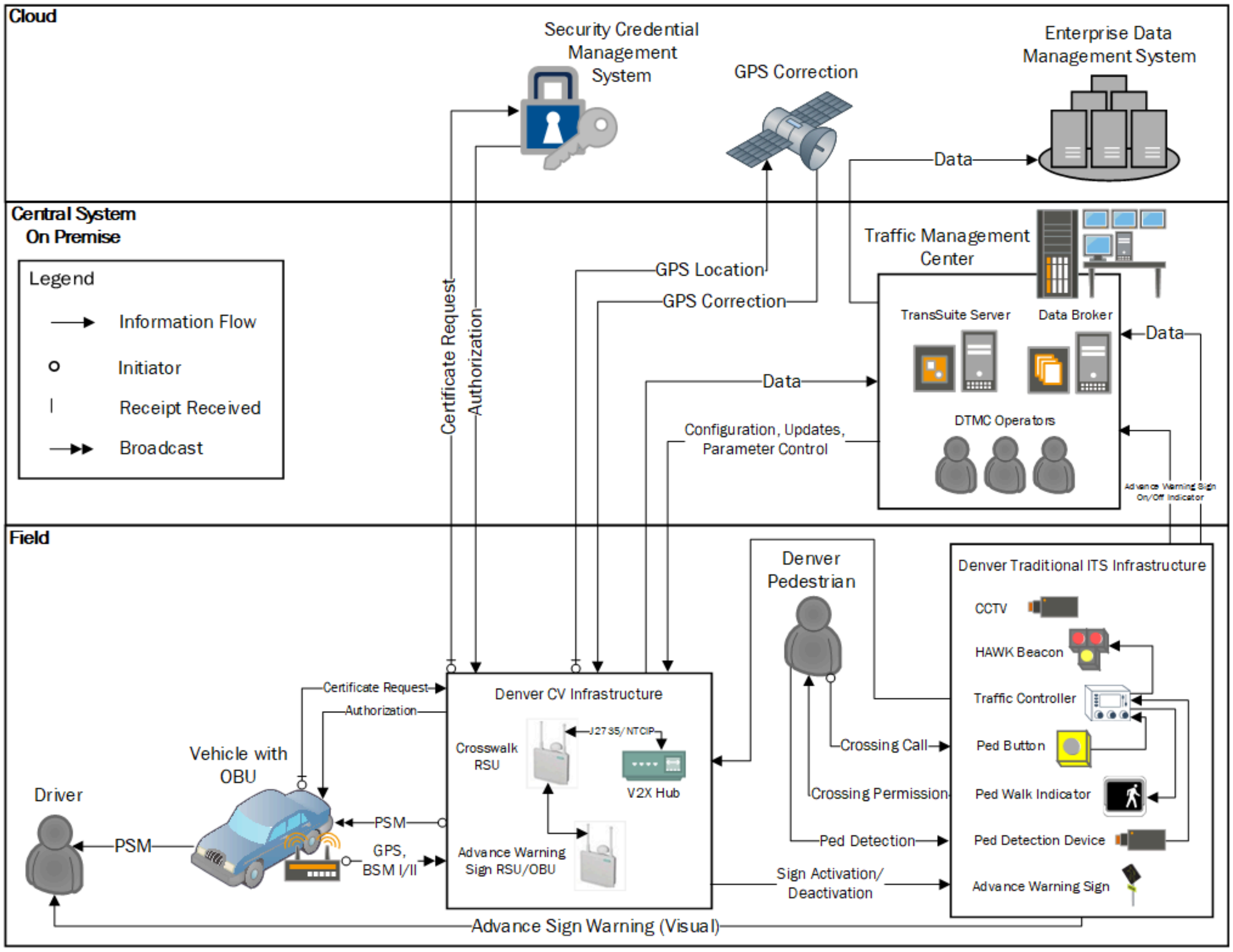
- Drivers in equipped vehicles will receive advance notification of pedestrians in a crosswalk through a PSM sent via the crosswalk RSU to the OBU. Drivers in non-equipped vehicles will be notified of pedestrians in a crosswalk through the advance warning sign and HAWK signal.

5.3.2.e Network Infrastructure

All roadside equipment (RSE), advance warning signs, pedestrian detection devices, and the accompanying V2X hub processing computers will tie into Denver's fiber-optic network. This will support the collection of BSM and pedestrian detections for evaluation of the proposed system. The data broker(s) will funnel data into the TMC and to the EDM where it can flow between the two systems.

Figure 5.7 illustrates how each component of the Connected Pedestrian system listed above interacts with each other. This diagram illustrates the primary information flows between major groups of physical objects. There are more detailed flows between objects within each major group that are not shown as part of this diagram.

Figure 5.7 - Connected Pedestrian Primary Information Flow Diagram



5.3.3 Regional ITS Architecture

DRCOG maintains the regions ITS Architecture. For this Connected Pedestrian project, the following service package from DRCOG is applicable:

> ***VS12-02 Local Jurisdiction Pedestrian and Cyclist Safety*** *- supports the sensing and warning systems used to interact with pedestrians, bicyclists, and other vehicles that operate on the main vehicle roadways, or on pathways which intersect the main vehicle roadways. These systems could allow automated warning or active protection for this class of users.*

5.3.4 Bounding Conditions of the Proposed System

Table 5.3 lists the bounding conditions specific to the Connected Pedestrian project. These bounding conditions apply to the four HAWK locations being used as the first deployment locations, and may not apply when the technology is scaled beyond the initial installation.

Table 5.3 - Connected Pedestrian System Bounding Conditions

ID#	Bounding Condition
BC-CP-01	The advance warning sign is MUTCD compliant
BC-CP-02	Any software plugins created as a part of this project function in coordination with the V2X Hub
BC-CP-03	Any software plugins created as a part of this project run in parallel with other plugins on the V2X Hub

5.3.5 Interfaces with Existing Systems

The proposed system will interface with the existing systems described in the current TMC state section, 4.2.1.

5.3.6 Project Risk Factors

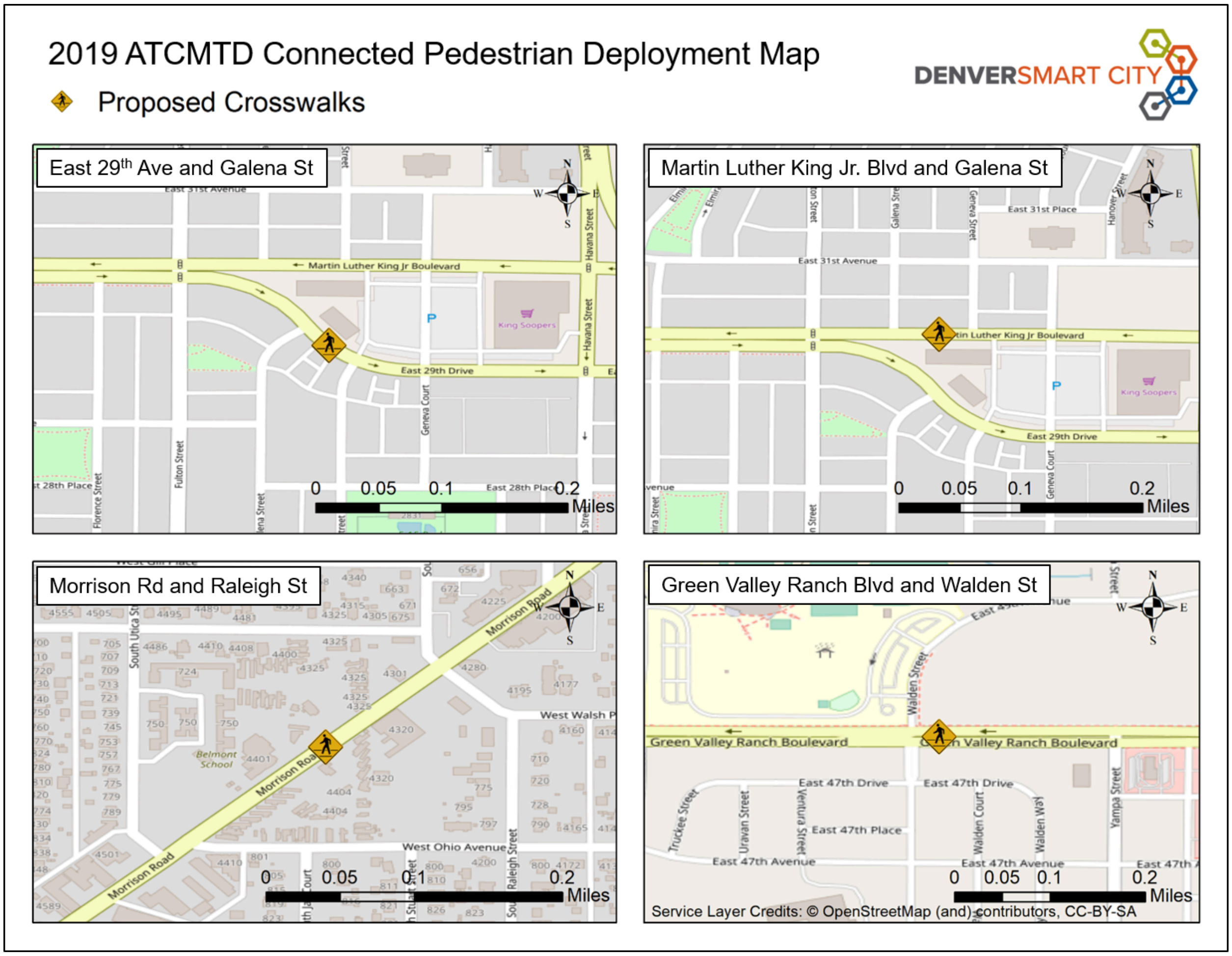
There are four project-specific risk factors for the Connected Pedestrian proposed system including:

- Potential for low pedestrian usage or incorrect usage (i.e. cutting diagonally outside of the detection area) at the proposed HAWK signal locations.
- The relative need for advance warning signs at certain locations given how recently these crossings were installed.
- The DSRC interface between the intersection RSU and the advance warning sign RSU/OBU as a means to activate/deactivate the advance warning sign.
- Insufficient technology propagation in privately owned vehicles to be compatible with the system.

5.3.7 Connected Pedestrian Deployment Area

To demonstrate the connected pedestrian technology, four mid-block crossing locations have been chosen by CCD to receive APD, Advance Warning Signage, and DSRC radios in addition to the pre-existing HAWK signals. These locations were selected because they are relatively controlled environments, with fewer variables to account for compared with a four-way intersection or more complicated crossing. These crossings are relatively new builds for CCD, with fewer upgrades required to support CV technology, and provide good locations for an initial deployment of this technology aimed at supporting safer pedestrian crossings for citizens. If this is successful, the technology could be deployed to a full four-way crossing. The initial four sites are shown on the map in figure 5.8 and are detailed further below:

Figure 5.8 - Connected Pedestrian Deployment Map



East 29th Ave and Galena St

This HAWK signal connects the Stapleton Eastbridge Town Center to the adjoining neighborhood to the south. Unique to this location is the horizontal curve and associated sight distance limitation that will dictate locations of the RSU and Advance Warning Sign.

Martin Luther King Jr. Blvd and Galena St

This crosswalk connects the Eastbridge Town Center to the northern neighborhoods and businesses. This section of road is one-way with clear sight lines to the HAWK signal. Sun glare does affect the visibility of the HAWK signal in the afternoon.

Green Valley Ranch Blvd and Walden St

The HAWK signal at this crosswalk connects the Denver School of Science and Technology (DSST) Middle and High School with the residential neighborhood and retail space east of the campus. This 4-lane roadway is separated by a median island with its own pedestrian push button.

Morrison Road and Raleigh St

This crosswalk connects newly developed apartments and a park generating both pedestrian and vehicle traffic. Morrison road is a two-lane road with bike lanes and parking along both sides. There are no signalized intersections near this crosswalk.

5.4 Enterprise Data Management System

A data processing environment is an important component of the transportation management structure CCD envisions. Currently, it plans for an Enterprise Data Management System (EDM) to serve as a living, intelligent data engine for ingesting disparate data sets from multiple sources and returning digestible information for CCD and the traveling public. The EDM is currently being developed by Denver's Technology Services department. The current architecture of the EDM resides in a cloud environment and is being prepared to support the data needs of the projects as described above. Specifically, this data processing environment will:

- Connected Freight
  - Gather and store data from the V2X Hub, RSUs, advanced traffic signal controllers, and freight OBUs regarding freight signal priority performance.

- Connected TMC/Fleet
  - Gather and store probe traffic data from the V2X Hub and fleet OBUs
  - House an API to communicate TMC transportation data to developers, agencies, and ultimately the traveling public.
  - Analyze and present functional data and alerts to TMC operators to aid in real-time traffic/incident management.

- Connected Pedestrian
  - Gather and store data from the V2X Hub, the APD device and advanced traffic signal controllers regarding pedestrian crossings performance.

5.5 Program-wide Commonalities

5.5.1 Regional ITS Architecture

DRCOG maintains the regions ITS Architecture. In addition to the project-specific service packages listed above, the following service packages from DRCOG are applicable to the overall program:

> ***SU08-02 Denver Security and Credentials Management*** *- used to ensure trusted communications between vehicle devices and roadside devices and protect data they handle from unauthorized access. This service package grants trust credentials to qualified devices in the Connected Vehicle Environments so that these devices may be considered trusted by other devices that receive trust credentials from this service package.*
>
> ***SU07-02 Denver Privacy Protection*** *- provides the privacy protection essential to the operation of connected vehicle applications. Privacy protection obscures the network*

identifiers of devices in order to allow communications with credentials management and other centers.

DM01-04 Denver EDM Data Warehouse *- provides access to transportation data to support transportation planning, condition, and performance monitoring, safety analysis, and research. Configurations range from focused repositories that house data collected and owned by a single agency, district, private sector provider, or research institution to broad repositories that contain multimodal, multidimensional data from various data sources covering a broader region.*

5.5.2 Bounding Conditions of the Proposed System

For the entire program to be deployed successfully, bounding conditions have been developed to meet the more general city needs that span across all three of the CV projects. These conditions are listed in table 5.4.

Table 5.4 - Program-wide Bounding Conditions

ID#	Bounding Condition
BC-PW-01	Any devices installed as a part of this program do not impact base functionality of the traffic signal
BC-PW-02	Installation of an OBU into a vehicle does not affect the normal operation of that vehicle
BC-PW-03	An OBU conforms to all applicable sections of the USDOT RSU 4.1 Spec until a standard from the National Highway Traffic Safety Administration (NHTSA) is available for OBUs
BC-PW-04	A RSU has a direct connection to a V2X Hub processing computer
BC-PW-05	All RSU installers are approved by CCD
BC-PW-06	CCD maintains all new components installed as a part of this program
BC-PW-07	CCD continues to comply with FCC requirements for registering RSUs. (47 CFR, Parts 90, 95)
BC-PW-08	Traffic signal cabinets have sufficient space to house any components installed as a part of this program
BC-PW-09	Traffic signal cabinets have sufficient power to accommodate any components installed as a part of this program
BC-PW-10	Any switches located in participating traffic signal cabinets have sufficient ports to accommodate any components installed as a part of this program

BC-PW-11	Any switches located in participating traffic signal cabinets have sufficient power to accommodate any power over Ethernet (PoE) components installed as a part of this program
BC-PW-12	CCD has the ability to remotely monitor and manage RSUs and V2X Hubs
BC-PW-13	Physical and remote access to any CV devices deployed as a part of this program is secured and segmented from the broader CCD enterprise network
BC-PW-14	Any CV devices that access the traffic and enterprise networks do so on appropriate ports and subnets along appropriate IPv4 or IPv6 protocols
BC-PW-15	Any devices installed as a part of this program are physically secure and tamper proof, including in adverse weather
BC-PW-16	Any data obtained from this program conforms with CCD storage, access, and PII policies
BC-PW-17	All equipment, software, processes, and interfaces comply with applicable and most current SAE, IEEE, UL, NTCIP, and NEMA standards
BC-PW-18	CCD has available transmission bandwidth in their network to support this program in addition to other ITS/Traffic applications

5.5.3 Program-wide Software Needs

Software will support functionality in the field, TMC, and cloud environments. Existing software that will interface with the proposed system is described further down in the document. The following new software packages will be included in the deployment of each project.

- **OBU Software** - OBUs will be equipped with the appropriate vendor software packages to support the applications being used across the projects.
- **RSU Software** - RSUs will be equipped with the appropriate vendor software packages to support the applications being used across the projects.
- **V2X Hub** - the V2X Hub software will reside on a Linux processing computer at each intersection where DSRC is deployed. It will act as a bridge between infrastructure messages and vehicle messages, allowing the two to communicate effectively. Various plugins can be added to the V2X Hub depending on the desired functionality at each deployment.
- **Remote Management Tools** - software systems will be deployed for the remote management of roadside equipment (RSE) including updates, firmware, configuration files, etc.
- **Data Broker(s)** - the data broker(s) will reside in a physical server at the TMC, and will facilitate the transfer of data from the field to other data repositories such as the EDM or current TMC systems.

- **EDM -** as described above, the EDM will aggregate, analyze, process, visualize, and distribute CV data in conjunction with the data broker(s) and backend systems.
- **Security Credential Management System (SCMS)** - an SCMS will be explored during the course of this program. If the concept is proven and an industry solution exists at the conclusion of the program, CCD will deploy a production SCMS before interfacing with privately owned vehicles.
- **Real-time GPS Correction Software** - for fleet vehicles to receive accurate SPaT/MAP messages, lane-level GPS accuracy will be required. In an urban environment, this may require a software plugin that corrects GPS data received from connected vehicles. This plugin can reside on the V2X Hub or within an RSU and will enable accurate SPaT/MAP messages to be sent to fleet vehicles in range of participating intersections.

5.6 Scope Changes from Technical Proposal

Several adjustments to the program scope were made compared to the original technical application.

- **Collaboration with Peloton Technologies** - Peloton Technology was listed as part of the Connected Freight project to increase travel time reliability through a CV platooning application. Although this technology has major benefits for the freight community, it is geared towards freeway applications. The Freight Efficiency Corridor proposed for north Denver consists primarily of major arterials, thus the Peloton Technology was deemed less applicable to the specific needs of this system.

- **Collaboration with Waze** - In the technical application, Waze was listed as the primary partner to consume data produced by the TMC and EDM. As the program has advanced, CCD has adjusted our data dissemination strategy to be platform-agnostic, and aims to use open APIs to make data available to any navigation platform or 3rd party applications.

6. Assumptions, Policies, and Constraints

In deploying the three CV projects, the program will need to account for several assumptions, policies, and constraints.

6.2 Operational Assumptions

Due to the fact that CV technology is new and evolving, some assumptions relevant to all three projects were identified:

- A Security Credentialing Management System (SCMS) can support secure and trustworthy communications for the program when it is ready to move to production after this pilot.
- As DSRC penetration rates grow, the system will be able to support back-end systems and greater data collection.
- DSRC remains the prominent technology used for V2X communications and applications or that the backend system and infrastructure can remain agnostic to the edge devices and communications.
- The Federal Communications Commission will maintain the 5.9 GHz band for transportation uses.

6.3 Policies

Policies regarding the responsibilities of various CCD divisions that play a role in supporting CV equipment will need to be established. The use of DSRC technology will be guided by the following standards:

Table 6.1 - DSRC Technology Policies

Standard	**Year**	**Description**
IEEE 802.11p	2010	Specifies the extensions to existing 802.11 spec to support wireless communications in a vehicle environment
IEEE 1609.0	2013	Provides an overview of the architecture needed to support the system, its components, and operation
IEEE 1609.1	2006	Defines the Wireless Access in Vehicular Environments (WAVE) Resource Manager
IEEE 1609.2	2016	Defines secure message formats and processing
IEEE 1609.3	2016	Defines addressing and routing of data

IEEE 1609.4	2016	Supports multi-channel operations
IEEE 1609.12	2016	Describes the identifiers used in WAVE
SAE J2735	2016	Defines the format and structure of messages, data frames, and data elements
SAE J2945/1	2016	Specifies system requirements for on-board V2V safety communications
SAE J2945/2	2018	Specifies DSRC interface requirements for V2V safety awareness applications
SAE J2945/4	WIP	Aims to extend application of J2735 beyond what is enabled by a Traveler Information Message (TIM)
SAE J2945/9	2017	Provides performance requirements for the Vulnerable Road User safety message
SAE J2945/10	WIP	Aims to define recommendations for MAP/SPaT message deployment
NTCIP 1202 v3	WIP	Defines interface between a controller and an RSU
DSRC RSU v4.1	2017	Sets the minimum requirements for DSRC roadside units
NMEA 0183 v4.1	2008	Defines electrical signal requirements and data transmission protocol for serial data bus

6.4 Constraints

- The vendor community supporting CV technologies remains immature and is experiencing frequent changes. CCD is serving as the systems integrator for these CV projects, and is thus dependent on the rapidly changing vendor environment to enable the use cases.
- The security and privacy frameworks associated with CV technologies is changing. When the ATCMTD program was first proposed, the Security Credential Management System (SCMS) framework was just being proposed. In delivering these projects, Denver will focus deployments on city-owned and controlled assets to reduce broader security risks and emphasize demonstrating value early in deployments.
- Resource limitations in the form of staff and budget are constraining factors for Denver as well. Additional workload or upkeep of the technology and systems deployed as a result of this project will need to be absorbed by existing CCD personnel.

- CCD resources will be required and new responsibilities will be added. New knowledge, skills, and abilities are added due to the implementation of these new systems

6.5 Security

CCD will demonstrate the value of CV technologies by deploying them on top of existing transportation infrastructure, in a manner that does not reduce base functionality. Existing traffic control and ITS devices have redundancy and failover procedures built in that will not be altered by this program. To maintain CCD's security and privacy policies, CCD will:

- Adhere to CCD's current policies, plans, and procedures for cybersecurity and refine as necessary for the requirements of CV deployment.

- Conform to CCD's existing data security and privacy practices and refine as necessary for the requirements of CV deployment.

- Purchase products that have been built with standard, industry-accepted cybersecurity standards in mind, including certified OBUs and RSUs.

- Utilize secure coding practices with the software CCD purchases, develops and deploys to prevent the introduction of security vulnerabilities.

- Maintain current versions of software running on ed-ge devices using over the air (OTA) updates.

- Explore a Security Credential Management System (SCMS) for application to Denver's CV environment.

6.6 Operations and Maintenance Support

CCD is currently bench testing and running integration tests on a variety of CV devices. As the program scales up and deploys larger numbers of devices, it will update it's operations and maintenance procedures to account for these new technologies and increased volume of devices in the field.

- Operations and Maintenance Activities
    - CCD will review the scale and schedule of its CV deployment and compare that to its current staff positions to determine if it is adequate to operate and maintain the current system plus the addition of CV hardware.
    - Equipment and software for configuration, testing, and troubleshooting will also be assessed by CCD to ensure that the tools required by technicians are available. This is expected to include ruggedized field laptops, diagnostic

software, spectrum analyzers, 5.9 GHz DSRC multi-channel tester, bench test equipment, etc.
    - CCD will stock spare equipment of RSUs, PoE midspan injectors, and OBUs for replacing malfunctioning field equipment. Additional units will be reserved for technicians, working in the test bench environment, to perform testing of configuration changes and the stability of these changes prior to active deployment in the field.

- FCC Licensing Activities
    - The FCC's mobile service allocation is limited to DSRC systems operating in the ITS radio service communications frequency band as defined by the FCC in CFR 47 Parts 90 and 95.
    - CCD staff will be responsible for the following:
        - Reviewing FCC service rules, regulations, and technical requirements
        - Licensing administration and ongoing management activities
        - Coordination with existing Federal and non-Federal co-primary users
        - Service channel/application configuration updates and optimization
        - Ongoing coordination with new primary users
        - Ongoing coordination with existing/new DSRC RSU sites and their respective agencies (e.g., CDOT, City of Aurora, etc.)
        - Updates to RF analysis addressing new interference
    - It is important to note for CCD's DSRC deployment that the FCC requires all transponders, transmitters, and transceivers associated with RSUs used in the 5.9 GHz band to be certified by the FCC.
    - In most cases, CCD will need to complete the FCC registration for the RSU prior to construction or installation. CCD will have 12 months to install and begin operating a registered RSU.

7. Modes of Operation

It is expected that users of the proposed systems will continue to follow traffic regulations and respond to traffic control devices as they currently do, but with additional applications that improve safety and mobility under certain circumstances. As described above, the proposed systems will provide functionality in the areas of signal priority, probe data collection, and pedestrian detection and warnings. The modes of operation for the proposed systems are as follows:

- Normal operations - this mode indicates that all systems are functioning as they are intended to, with the full set of CV applications available to system users.

- Degraded operations - this mode indicates that some of the deployed technology is malfunctioning. Depending on the nature of the degradation, functionality can still be accomplished through alternative means. For example, traditional ITS equipment can still be used to receive roadside communications in the event of OBE or RSU malfunctions.

- Operation failure - this mode indicates that the proposed system is not providing one or more functions as intended. Due to the risk associated with a malfunctioning central system, all CV-related uses cases would be suspended and the proposed system(s) would revert back to a pre-CV state of operations. The new system does not replace existing safety systems in place for current operations, thus the base system would continue to operate without the enhanced features provided by the proposed CV technologies. Table 7.1 outlines various scenarios that can result in degraded or failing operations, and how the system/users should respond.

Table 7.1 - System Failure Scenarios

Event	Examples	Description	Response
Traffic Signal System Citywide Outage	Traffic signal controllers at each intersection are unable to communicate with the central system	A problem occurs at the DTMC data center that takes down the traffic signal system servers.	Traffic signal controllers in the field will continue to operate based on a Time of Day (TOD) schedule and SPaT data will still be available through the V2X hub. Real-time high res data from the traffic signal system will not be available to update the EDM.
Communications Network for Traffic and ITS is Offline	Fiber optic communications to the switches at each signalized intersection is unavailable	Fiber optic communications to individual signalized intersections is unavailable due to a major fiber cut in CCD or a failure at the core switch level in the DTMC data center.	The infrastructure at each signalized intersection should be able to operate temporarily depending on the duration of the communications outage, but data from the field to the DTMC will not be transmitted and, over time, the clock on the controller may drift without the time sync from the central system. The existing network design should be evaluated to provide for redundant communications routes. At the core, a redundancy protocol should be considered to establish a fault-tolerant default gateway option.
Diminished CV Communications	Loss of connectivity between roadside infrastructure devices	Some applications rely on connection and communication between multiple devices (i.e., the pedestrian detection, RSU, and advance warning sign). If this	CCD’s field crew will need to be dispatched to check the hardwired and wireless connectivity of infrastructure devices. Initial design of wireless connectivity should include a spectrum analysis to

<table>
<tr><td rowspan="2"></td><td></td><td>communication is lost, alerts/warnings may not be broadcasted, increasing the risk of an incident.</td><td>check for any interference parameters on the DSRC frequency.</td></tr>
<tr><td>DSRC channel congestion</td><td>Broadcasting a high volume of messages from multiple devices has the potential to congest DSRC bandwidths. This can cause messages to not be received or be received too late for a driver to respond.</td><td rowspan="3">In the case of late, inaccurate, or missing messages, drivers would be expected to safely operate their vehicle as they normally would without CV applications. Continuous monitoring of the system will be a key step in recognizing and troubleshooting communication and messaging functionality. Downstream data accuracy in the EDM could also be impacted.</td></tr>
<tr><td rowspan="2">Deficient OBE Data Quality</td><td>Inaccurate GPS data</td><td>Inaccurate positioning or heading information from a vehicle can result in false positive and false negative notification outputs which reduces the system’s effectiveness and credibility.</td></tr>
<tr><td>Inability to process data in a timely manner</td><td>If processing capability is not robust enough for the amount of incoming data, messages/warnings may be delivered too late for a driver to respond.</td></tr>
<tr><td>Security Breach</td><td>Inaccurate messages</td><td>If a security breach occurs, there is the possibility that false messages can be generated and broadcasted to any equipped vehicle in range of a RSU.</td><td>This will require monitoring of the systems and QA/QC processes with a sample of connected intersections. In the case of a security breach, all field CV technology would be shut down remotely (or locally, if needed), along with internal systems and servers. Access to the shared API would be</td></tr>
</table>

	Vulnerability in software code	Software running on the OBU, RSU, or V2X Hub may have been developed without good application development practices, which can lead to security issues.	eliminated, and all users of the system(s) would be expected to revert back to pre-CV conditions until the issues have been resolved and any vulnerabilities appropriately addressed.
Catastrophic Failure of the Entire CV System Due to a Cyberattack	The entire CV system is shut down due to an attack	The traffic signal controllers and existing base traffic management technologies continue to operate as intended. The RSU, V2X Hub, and other CV devices fail to operate. The system continues to operate as if CV technology wasn't deployed.	Perform analysis to determine what has occurred. Continue to share incident information, next steps, and updates with CCD team, including when the incident has been resolved. Implement the incident response plan to neutralize and contain the situation. Once the incident has been resolved, restore the system and network back to a healthy state. Document the incident response process to evaluate the potential for future incidents and for security training purposes. Conduct a post-incident analysis to review what happened, the timeframe for response, the appropriateness of the response, and how long the incident lasted.

8. **Analysis of Proposed System**

8.1 Summary of Improvements

In general, the three proposed projects are focused mainly on safety, mobility, efficiency, and environmental impact improvements throughout CCD's traffic network. While the projects comprising the ATCMTD program share commonalities surrounding system enhancements, each project will have distinct improvements linked to the project's goals and objectives. These project-specific improvements are as follows:

8.1.1 Connected Freight System Improvements

- Improved signal timing for participating freight vehicles alleviating congestion and improving air quality.
- Improved travel time reliability, fuel efficiency, and/or route efficiency for participating freight companies.
- Reduced impact on local neighborhood roads by freight vehicles (although likely unmeasurable).

8.1.2 Connected TMC/Fleet System Improvements

- Improved analysis of and reporting on CCD's traffic network from probe data collected by fleet vehicles and processed by the EDM.
- Improved traffic network situational awareness based on actionable data from DSRC equipped fleet vehicles.
- Provide real-time traffic data to the public and third parties.
- Provide fleet vehicles with SPaT/MAP data and signal priority when applicable.

8.1.3 Connected Pedestrian System Improvements

- Reduced number of conflicts between vehicles and pedestrians.
- Extended wig/wag time for "vulnerable" pedestrians when needed.
- Improved understanding of pedestrian crossing behaviors and characteristics.
- Improved real-time advance warning to approaching vehicles through the placement of advance warning signs and in-vehicle notifications for OBU-equipped vehicles.

8.2 Performance Measurements

This section outlines how each project's performance will be assessed, the performance measures and data sources that will be used, and the appropriate data collection approach. As each project is a demonstration of new technology, success criteria was formed around verification that the system works as intended. Through monitoring of each successfully deployed system, CCD hopes to achieve the network-wide improvements listed above. The exact time frame over which these projects will be evaluated will be determined by the quality and quantity to data received following each project's deployment. A more detailed overview of how each project will be evaluated can be found in Denver's ATCMTD Program Evaluation Plan (May 2018).

8.2.1 Connected Freight Performance Measurement

Evaluating the performance of the Connected Freight project will utilize various data collection techniques and methodologies. For the initial demonstration of the technology, data regarding signal priority requests, and priority status messages will be collected from the traffic signal controller and the V2X Hub. This will give Denver an idea of whether the system is performing as intended and freight operators are actually receiving signal priority.

To analyze the benefits of the signal priority, CCD will look at various analysis tools, including queue analysis, number of priority requests logged, and/or before and after studies to measure the improvements to congestion. If freight companies share data to show the impact of the program on their metrics, that could also be incorporated.

One of the drivers of this project was negative freight impacts on neighborhoods in north Denver. Although CCD would like to see improvements to these impacts, it is a difficult metric to measure and will not be used to evaluate the success of this project.

All of the performance measures are listed below. Some metrics will be measured directly, while others will result from derivative calculations.

- Total number of freight vehicles passing along select corridors
- Total number of signal priority requests
- Total number of signal priority approvals
- Total number of signal priority denials
- Total number of freight routes altered to utilize connected corridors
- Total amount of CO2 reduced by partnering freight companies (derivative calculation)
- Total amount of money saved by partnering freight companies (derivative calculation)
- Total decrease in travel time by partnering freight companies
- Total amount of time taken from other programmed signal phases to allow for freight priority
- Total number of RSUs and OBUs deployed and reporting to the EDM

8.2.2 Connected TMC/Fleet Performance Measurement

The success of the TMC/Fleet system will be measured based on the quality of the data reported by the fleet vehicles to benefit the situational awareness of the TMC. To drive situational awareness insights (speed probe data, multiple rapid decelerations, queue backups), a baseline of data to establish a norm must be set. The quantity of data coming from vehicles will be the first measure to determine how effectively CV data can build that baseline.

After establishing the baseline, the effectiveness of real-time alerting for incidents outside the norm will be measured. This could be measured by usage metrics of the EDM.

To measure the success of data being disseminated to 3rd parties and applications, the EDM can measure the number of calls made against any public-facing APIs it produces.

Snow plow priority signal effectiveness can be measured using priority call records from the V2X Hub and signal controller, and travel time information from fleet management to look at the benefits of signal priority for the plow operator.

All of the performance measures include:

- Total number of fleet vehicles equipped with OBUs
- Total number of signal priority requests, and status message logs or fleet vehicles
- Total number of times the TMC receives an alert triggered by a DSRC device/message
- Total number of times CV data provides enhanced situational awareness (probe speeds, rapid deceleration events, queue backup information)
- Total number of third-party applications accessing CCD's APIs (including SPaT)
- Total number of RSUs and OBUs deployed and reporting data to the EDM

8.2.3 Connected Pedestrian Performance Measurement

Performance analysis of the Connected Pedestrian project centers around how users interact with the system, if the system responds effectively, and whether safety benefits are realized. As a demonstration of DSRC and automated pedestrian detection technology, it is essential to monitor and track the performance of the system along with any safety improvements that occur as a result of successful deployment.

A before and after analysis of the general system usage will be conducted using CCTV footage to evaluate whether the proposed system is operating effectively in regards to each use case. Following deployment of the system, additional performance metrics regarding how users interact with the system and the system's subsequent response will be collected from TransSuite and the V2X Hub. Since the RSU and advance warning sign activate whenever a pedestrian is detected, yet the HAWK signal only activates when the pedestrian push button is used, this delta can be used to better understand pedestrian crossing behavior. Hard actuations of the HAWK signal versus the number of passive detections will demonstrate whether pedestrians manually activating the HAWK signal or simply entering the street. Additionally, the number of times a Personal Safety Message (PSM) is sent and/or the simultaneous activation of the advance warning sign can be compared against CCTV footage in an attempt to measure accuracy of the CV application for public confidence and trust. To validate or adjust the fixed extension time of the HAWK signal, the average crossing speed of vulnerable pedestrians can be calculated. The default extension time will be calculated by finding the delta between cross times at 2.5 ft/s (vulnerable pedestrian) and cross times at 3.5 ft/s (industry standard); however, by calculating the actual average crossing speed of normal and vulnerable pedestrians, more informed rates can be used, resulting in more effective use of the system by both pedestrians and drivers.

Due to the recent installation of the HAWK signals there have been zero reported incidents at these locations. It will not be possible to see a safety benefit using a before/after study as a result. Instead, the metrics identified above will prove out if the technology is able to meet CCD’s requirements, and can then be deployed at additional crossings and more complex intersections.

All of the performance measures include:

- Total number of pedestrians that are detected in the crossing zone
- Total number of RSU/Advance Warning Sign activations, including false activations when a pedestrian was not actually present
- Total number of HAWK Signal actuations versus advance warning sign activations
- Total number of pedestrians that extend the flashing wig/wag time
- Total number of times there is still a pedestrian being detected after max wig/wag completed
- Total number of RSUs and Automated Pedestrian Detection devices deployed and reporting data to the EDM

8.3 Analysis Limitations

Limitations regarding the analysis of each CV system are listed below:

8.3.1 Connected Freight Analysis Limitations

- Proprietary data specific to each participating freight company may limit the performance metrics available to evaluate the system.
- Evaluation of improvements to freight vehicles will depend on the freight companies sharing data.
- Confounding variables, like regional construction projects, may be hard to avoid if comparing the benefits to partnering freight companies.
- OBU malfunctions and/or inability to perform needed OTA updates.

8.3.2 Connected TMC/Fleet Analysis Limitations

- Limited market penetration of private vehicles will reduce the overall volume of data to analyze.
- Limited RSU coverage across CCD will provide a relatively narrow view of real-time conditions.
- Limited access to vehicle data on the CAN bus of a vehicle, for BSM Part II elements

- Limited access to performance metrics associated with V2X Hub plugins, either on a discrete Linux board or with embedded RSU software.

8.3.3 Connected Pedestrian Analysis Limitations

- The HAWK signals are new builds, and do not have any vehicle-pedestrian incidents. The technology will need to be tested in these more controlled HAWK locations before being deployed at more complex intersections.
- Since the participating crosswalks are relatively new builds in CCD, the crossings are not highly trafficked.

8.4 Alternatives and Trade-offs Considered

The proposed systems are being developed as part of the ATCMTD federal grant program to demonstrate connected vehicle technology. As such, at this time, no alternatives or trade-offs are being considered for any of the three CV projects. As the projects advance through the procurement, design, and deployment phases, any alternatives or trade-offs that are considered will be documented here.

9. Appendix, References, and Glossary

Full-page versions of the information flow diagrams are provided [redacted link].

Table 9.1 lists the references used to develop the concepts in this document. As some of the base standards referred to in the list are currently evolving, their identifiers have been temporarily highlighted to indicate that the version may change.

Table 9.1 - Reference Documents

#	Document (Title, source, version, date, location)
1	United States Department of Transportation, Office of the Assistant Secretary for Research and Technology, Intelligent Transportation System Joint Program Office https://www.its.dot.gov/index.htm
2	*Architecture Reference for Cooperative and Intelligent Transportation Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. https://local.iteris.com/arc-it/
3	*1609.0-2013 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture* http://standards.ieee.org/findstds/standard/1609.0-2013.html
4	*1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages* http://standards.ieee.org/findstds/standard/1609.2-2013.html
5	*1609.3-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services* http://standards.ieee.org/findstds/standard/1609.3-2010-Cor_2-2014.html
6	*1609.4-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation* http://standards.ieee.org/findstds/standard/1609.4-2010.html
7	*SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary™*, SAE International, March 30, 2016 https://www.sae.org/standards/content/j2735_201603/
8	*SAE J3067 - Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods*, August 26, 2014 https://www.sae.org/standards/content/j3067_201408/
9	*SAE J2945/1_201603 - On-Board System Requirements for V2V Safety Communications*, SAE International, March 30, 2016 https://www.sae.org/standards/content/j2945/1_201603/
10	*USDOT's Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015-2019*, December, 2014 https://www.its.dot.gov/strategicplan.pdf
11	*Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications Concept of Operations Document*, Final Report —May 29, 2012 FHWA-JPO-13-058, https://www.its.dot.gov/index.htm
12	*Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations, New York City,* Final ConOps —April 8, 2016 FHWA-JPO-16-299, https://www.its.dot.gov/index.htm
13	*Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations, ICF/Wyoming,* Draft Report —December 14, 2015 FHWA-JPO-16-287, https://www.its.dot.gov/index.htm
14	*Connected Vehicle Pilot Deployment Program Phase 1, Concept of Operations, Tampa (THEA)* - Final Report —February 2016 FHWA-JPO-16-311, https://www.its.dot.gov/index.htm

15	*Concept of Operations for the Connected Vehicle Environment for the Smart Columbus Demonstration Program -* Final —August 7, 2018 FHWA-JPO-16-299, https://www.its.dot.gov/index.htm
16	*Improving Vehicle Cybersecurity, ICT Industry Experience & Perspectives* - 2017 Alliance for Telecommunications Industry Solutions (ATIS)-I-0000059, http://www.atis.org/connected-cars/
17	*Denver Traffic Management Center Strategic Plan* - August 2018 City and County of Denver Department of Public Works - Transportation Operations Division
18	Goldman, David*, 'Chrysler Recalls 1.4 Million Hackable Cars',* July 24, 2015, CNN, https://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html
19	Miller, Charlie and Valasek, Chris*, 'A Survey of Remote Automotive Attack Surfaces',* Illmatics http://illmatics.com/remote%20attack%20surfaces.pdf
20	Dmitriew, Stan*, 'Autonomous Cars Will Generate More Than 300 TB of Data per Year*', November 28, 2017, Tuxera, https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/
21	Kwederis, Joe and Boehmer, Greg, *'Cyber Risks Ahead for Connected Cars'*, May 11, 2016, Deloitte & Touche, LLP, https://deloitte.wsj.com/riskandcompliance/2016/05/11/caution-cyber-risks-ahead-for-connected-cars/,.
22	https://informationisbeautiful.net/visualizations/million-lines-of-code/

9.1 Definitions and Acronyms

Table 9.2 and 9.3 define selected project specific terms used throughout this Concept of Operations document.

Table 9.2 - Acronym List

Acronym / Abbreviation	**Definition**
ACL	Access Control List
APDU	Application Protocol Data Unit
ASD	Aftermarket Safety Device
BSM	Basic Safety Message
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CAN	Controller Area Network
CCD	City and County of Denver
CCMS	Cooperative ITS Credentials Management System
CDOT	Colorado Department of Transportation

ConOps	Concept of Operations
CRV	Certificate Revocation List
CV	Connected Vehicle
CVPD	Connected Vehicle Pilot Deployment
CVRIA	Connected Vehicle Reference Implementation Architecture
DAFNE	Denver Area Fiber Network Ecosystem
DNS	Domain Name System
DOT	Department of Transportation
DSRC	Dedicated Short Range Communication
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol (Secured)
I2V	Infrastructure to Vehicle
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITS	Intelligent Transportation System
JPO	Joint Program Office
LCA	Lane Change Warning/Assist
MAP	Map Data Message (a DSRC message)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NHTSA	National Highway Traffic Safety Administration
NTS	Network Time Source
NWS	National Weather Service
OBD	On-board Diagnostics
OBE	On-board Equipment
OBU	On-board Unit

OEM	Original Equipment Manufacturer
OER	Office of Emergency Response
ORDS	Object Registration & Recovery Service
OTA	Over-the-Air
PDU	Protocol Data Unit
PID	Personal Identification Device
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
RA	Registration Authority
RDE	Research Data Exchange
RF	Radio Frequency
RSA	Roadside Alert
RSE	Roadside Equipment
RSU	Roadside Unit
SAE	Society of Automotive Engineers International
SCMS	Security Credential Management System
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSL	Secure Sockets Layer
SSM	Signal Status Message
TBD	To Be Determined
TCP	Transmission Control Protocol
TIM	Traveler Information Message
UPS	United Parcel Service
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructructure
V2V	Vehicle-to-Vehicle
VRU	Vulnerable Road User

WAID	Wide Area Information Distributor
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement

Table 9.3 - Glossary of Terms

Term	Definition
5.9GHz	The frequency reserved for connected vehicle communications and dedicated short-range communications (DSRC).
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Adjacent (A)	Data that is hyper local (relevant to a geographic area within approximately 1 minute travel distance).
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Anonymity	Lacking individuality, distinction, and recognizability within message exchanges.
Anonymous Certificate	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
APDU	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
Application	One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task.
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.
Backup	The ability of one System Element replacing another System Element's functionality upon the failure of that System Element.
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.

Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog.
Cardinality	The characterization of the relationship between the number of sender(s) and receiver(s) of a data exchange. (e.g., broadcast (one-to-many) unicast (one to one)).
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms back office and center are used interchangeably. Center is traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of this ConOps Specification these are considered the same.
Configuration	Data that is used to customize the operational environment for a System Element or System User, or the System as a whole.
Constraint	An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.
Cyber Address	The cyber or network address of a Unified Implementation of the Reference Architecture object.
Data Consumer	A user or system that is receiving or using data from another user or system. Any Unified Implementation of the Reference Architecture object that registers with and subsequently requests and receives delivery of data from a data warehouse.
Data Provider	Any Unified Implementation of the Reference Architecture object that registers with and subsequently deposits data into a data warehouse. A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data.
Data Warehouse	A data storage facility that supports the input (deposit) and retrieval (delivery) of clearly defined data objects. This can be designed and implemented in a variety of ways, including publish/subscribe and a traditional query based database.
Decrypt	To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access..
Dedicated Short Range Communication	Dedicated short-range communications are one-way or two-way short-range to medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards.
Digital Certificate or Signature	A digital certificate is an electronic identification card that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names, and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application

	of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it.
Extensibility	The ability to add or modify functionality or features with little or no design changes.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., dynamic message signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSE and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Geo-referencing	The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space.
Handshake	"DSRC Handshake" or simply "handshake" is a term used within Denver to describe the minimal viable product of getting data to consistently pass through our connected vehicle test site.
Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Integrity	To maintain a system that is secure, complete, and conforming to an acceptable conduct without being vulnerable and corruptible. The property of being certain that a message's contents are the same at the receiver as at the sender.
Issuance	For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Logical Security	Safeguards that include user identification and password access, authentication, access

	rights and authority levels.
Misbehaving User	A user who exhibits misbehavior.
Misbehavior	The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages. etc.; either purposeful or unintended.
Misbehavior Report	Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior.
Non-repudiation	The property whereby a PDU is constructed in such a way that the PDU sender cannot effectively deny having been the sender of that PDU; and the PDU receiver cannot effectively deny having received a particular PDU.
On-board Equipment (OBE)	Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.
Operators	These are the day-to-day users of the System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.
Permission	Authorization granted to do something. From the System's perspective, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the System.
Persistent Connection	A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection.
Physical Security	Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. This can range from simply a locked door to badge entry, with armed security guards.
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively.
Protocol Data Unit (PDU)	A defined data structure that is transferred at a peer level between corresponding software entities functioning at the same layer in the OSI standard model which are operating on different computing platforms that are interconnected via communications media.
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).

Registry	A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.
Repackage Data	Data that is broken down for aggregation, parsing, or sampling.
Research Data Exchange	A web-based data resource provided by the USDOT ITS-JPO's Real-Time Data Capture and Management (DCM) program which collects, manages, and provides archived and real-time multi-source and multi-modal data to support the development and testing of ITS applications.
Scalability	The capability of being easily grown, expanded or upgraded upon demand without requiring a redesign.
Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Secure Transmission	To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications.
Session-oriented Connection	A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection.
States	A distinct system setting in which the same user input will produce different results than it would in other settings. The System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby.
Static	Data that is permanent (relevant at the time of reporting for an indefinite interval).
Subsystem	An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
Synchronization	The act or results of occurrence or operating at the same time or rate.
System	(A) A collection of interacting elements organized to accomplish a specified function or set of functions within a specified environment. Typically the System Elements within the System are operationally self- contained but are interconnected and collaborate to meet the needs of the System and its Users. (B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.
System Element	(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment. (B) An object and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system element includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to

	the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
System Need	A capability that is identified and supported within the System to accomplish a specific goal or solve a problem.
System Performance	This term refers to the measures of effectiveness used by NYCDOT traffic management operations staff on a periodic basis to manage the ongoing operation of the system.
System Personnel	This represents the staff that operates and maintains the System. In addition to network managers and operations personnel, System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployment teams, and Testers.
System User	System Users refers to Mobile, Field, and Center Systems.
Testers	These users verify the System's operation when any changes are made to its operating hardware or software.
Time Synchronization	Calibration adjustment of date, hour, minutes, and seconds for keeping the same time within a system.
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.
Unicast	The sending of a message to a single network destination identified by a unique address.
User	An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions.
Valid	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.