Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan – ICF/Wyoming

www.its.dot.gov/index.htm
Final Report — March 14, 2016
FHWA-JPO-16-289

U.S. Department of Transportation

Produced by DTFH6115C00038
U.S. Department of Transportation

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.
The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. FHWA-JPO-16-289	**2. Government Accession No.**	**3. Recipient's Catalog No.**

4. Title and Subtitle
Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan – ICF/Wyoming

5. Report Date
3/14/2016

6. Performing Organization Code

7. Author(s)

Deepak Gopalakrishna (ICF), Vince Garcia (Wyoming DOT), Ali Ragan (Wyoming DOT), Tony English (Trihydro), Shane Zumpf (Trihydro), Rhonda Young (University of Wyoming), Mohamed Ahmed (University of Wyoming), Fred Kitchener (McFarland Management), Nayel Ureña Serulle (ICF), Eva Hsu (ICF)

8. Performing Organization Report No.

Task 4 Report

9. Performing Organization Name And Address
ICF International, 1725 Eye St NW, Washington DC, 20006
Wyoming DOT, 5300 Bishop Boulevard, Cheyenne, WY 82009
Trihydro Corporation, 1252 Commerce Drive, Laramie, WY 82070
McFarland Management, 1015 W. Hays Street, Boise, ID 83702
University of Wyoming, 1000 E University Avenue, Laramie, WY 82071

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFH6115C00038

12. Sponsoring Agency Name and Address
U.S Department of Transportation 1200 New Jersey Ave, SE Washington, DC 20590

13. Type of Report and Period Covered
Safety Management Plan , 12/14/2015 to 3/14/2016

14. Sponsoring Agency Code

15. Supplementary Notes

Kate Hartman (COR), Sarah Khan (CO)

16. Abstract

The Wyoming Department of Transportation's (WYDOT) Connected Vehicle (CV) Pilot Deployment Program is intended to develop a suite of applications that utilize vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication technology to reduce the impact of adverse weather on truck travel in the I-80 corridor. These applications support a flexible range of services from advisories, roadside alerts, parking notifications and dynamic travel guidance. Information from these applications are made available directly to the equipped fleets or through data connections to fleet management centers (who will then communicate it to their trucks using their own systems). The pilot will be conducted in three Phases. Phase I includes the planning for the CV pilot including the concept of operations development. Phase II is the design, development, and testing phase. Phase III includes a real-world demonstration of the applications developed as part of this pilot.

This document presents the Safety Management Plan. It provides guidance material in regards to the identification of safety scenarios and risk mitigation for the ICF/Wyoming Deployment Phase 1. The document is presented based on identifying the safety scenarios at both system-level and application level, assessing the level of risk for each scenario, and providing a safety operational concept for high/ medium risk scenarios. Safety stakeholders were identified, existing safety plans were reviewed, and coordination with emergency responders were incorporated in the Safety Management Plan.

The Pilot Deployment team identified and analyzed 14 potential hazard events. There were no Automotive Safety Integrity Level (ASIL) hazard events identified and none of the measures according to the ASIL as defined in ISO 26262 needed to be applied to achieve safety goals. Therefore, all potential risks will be handled and mitigated using the best practices of system engineering and project management principals during the design of the Safety Pilot Model Deployment infrastructure installation and fleet builds. Coordination between the SMP and other tasks is also discussed.

17. Key Words
CV Technology, I-80 Corridor, Road Weather, Truck Safety, Safety Management Plan

18. Distribution Statement
This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

19. Security Classif. (of this report)	**20. Security Classif. (of this page)**	**21. No. of Pages**	**22. Price**
None	None	48	NA

Acknowledgements

We acknowledge the timely and high-quality support offered by U.S DOT through the project calls, webinars relating to safety management and the white papers provided during this phase of the project. The guidance provided by U.S DOT and the support contractor Noblis is greatly appreciated by the project team in developing the safety management plan.

Table of Contents

List of Figures

List of Tables

1 Scope

1.1 Project Scope

Wyoming Department of Transportation (WYDOT) is one of the first wave of CV (CV) Pilot sites selected to showcase the value of and spur the adoption of CV Technology in the United States. CV Technology is a broad term to describe the applications and the systems that take advantage of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications to improve safety, mobility and productivity of the users of the nation's transportation system.

As one of the three selected pilots, WYDOT is focusing on improving safety and mobility by creating new ways to communicate road and travel information to commercial truck drivers and fleet managers along the 402 miles of Interstate 80 (I-80 henceforth) in the State. For the pilot project, WYDOT will work in a planning phase through September 2016. The deployment process will happen in the second phase (ending in September 2017) followed by an eighteen-month demonstration period in the third phase (starting in October 2017).

Systems and applications developed in the pilot will enable drivers to have 360-degree awareness of hazards and situations they cannot even see. Specifically, WYDOT hopes to improve operations on the corridor especially during periods of adverse weather and when work zones are present. Through the anticipated outcomes of the pilot, fleet managers will be able to make better decisions regarding their freight operations on I-80, truckers will be made aware of downstream conditions and provided guidance on parking options as they travel the corridor, and automobile travelers will receive improved road condition and incident information through various existing and new information outlets.

1.2 Safety Management Plan Introduction

The Safety Management Plan for the ICF/Wyoming CV Pilot is a companion document to the Concept of Operations (ConOps) and is a key element in ensuring the safety of pilot participants and the security of the system data and communications.

This document complies with the ISO 26262 Automotive Safety Integrity Level (ASIL) and applies basic system engineering and project management principles. It describes the underlying needs of the Pilot Deployment to validate the overall safety of the CV Pilot and to understand the impacts of various scenarios at system and application levels such as power outage, communication failures, unintended or malicious attacks, severe crashes, and adverse weather conditions. The concept provides and documents the guidance on designing a safety-critical system that is capable of eliminating hazards from the design, reducing the risks by modifying the design to lower the probability of the occurrence of the hazard, or at minimum, mitigating the impact of the hazard if it does occur.

1.3 Document Overview

This document is an overview of the safety management plan utilized in this pilot. It provides guidance to design a safety-critical system to account for different scenarios that may occur during the demonstration. The team is aware of the importance of safety for the users of CV applications and vehicles. Although systems can be designed and implemented for very few failures, it is not possible to completely eliminate hazards due to unforeseen events. As a pilot for CV technology, the safety management plan needs to be structured as part of the design rather than an afterthought. The development of the CV systems and applications follow fault-tolerant or fail-safe procedures to eliminate or minimize the risk of faults and failures. The success of this pilot depends on the public's acceptance that the Pilot CV users and non-CV users' safety is not endangered.

1.4 Document Organization

This document contains seven additional sections and a reference section. Section 3 explains the overall approach of the safety risk according to ISO 26262. Section 4 provides safety assessment of scenarios at the system level and application level. The safety operational concept is explained in Section 5. This includes the functional safety requirements, safety management plan, and the system-wide fail-safe mode and responses. Section 6 links the safety management plan task with other related tasks. These tasks include: the ConOps, privacy and security management operating concept, system requirements, application deployment plan, human use approval, participant training and stakeholder education, and comprehensive pilot deployment plan. A short summary is provided in section 7, followed by notes/glossary and an acronym list in section 8.

1.5 System Overview

The pilot is intended to develop a suite of applications that utilize V2V and V2I technology to improve truck safety and reduce the impact of adverse weather on, but not limited to, truck travel in the I-80. Specifically, this pilot will target the 402-mile stretch of I-80 that passes through Wyoming's Maintenance Districts 1 and 3 and will be demonstrated for an eighteen month period in 2017-2018. Through the pilot, several CV systems and applications will be developed and provided to equipped commercial vehicle fleets. These applications will support wide area travel advisories, variable speed limit postings, forecast road condition information, spot-specific warnings, detours, emergency alerts, and parking notification.

1.5.1 System Objects

The following objects are of interest to the system:

- Vehicles – Four categories of vehicles will play a role in the pilot.
    - WYDOT Fleet –This group represents vehicles owned by WYDOT (such as snow plows, highway patrol vehicles, and other state-owned vehicles) that will be equipped with onboard equipment (OBE) with Dedicated Short Range Communications

(DSRC) connectivity. The OBE will support communications; generate safety messages; collect and report vehicle, weather, and road condition data; store data; and provide an interface to communicate safety alerts and advisories. WYDOT fleets also have radio-based connectivity with WYDOT centers to support operations

  - Connected Truck – This group represents vehicles owned by commercial vehicle operators that are participating in the pilot. These trucks will be equipped with an OBE with similar functions and capabilities as described for the WYDOT fleet. Connected trucks may have cellular or satellite-based connectivity to their fleet management centers.
  - Private Vehicle – This group of vehicles represent private vehicles who have access to third-party applications on their personal information device (PID).
  - Truck – This group of vehicles represent trucks that are connected to fleet management centers but are not equipped with an OBE for this project.
- Infrastructure – Two infrastructure elements are part of the pilot
  - WYDOT Traditional Intelligent Transportation System (ITS) – This object group includes the existing ITS program devices like 511, Dynamic Message Signs (DMS), and Highway Advisory Radios (HARs).
  - WYDOT Roadside Equipment (RSE) – This object describes the RSEs that will be deployed as part of the system. RSEs include DSRC connectivity, application support, data storage, and other support services to enable CV applications. WYDOT RSEs can be either fixed or portable equipment depending on the use-case.
- Centers/Systems – Three major centers and systems are part of the pilot.
  - WYDOT Transportation Management Center (TMC) – The TMC is planned to be the hub of operations for the CV Pilot collecting information from WYDOT fleet, and partnering fleet management centers. The TMC supports the integration and fusion of CV and non-CV data to developing warnings and advisories. The TMC also provides traveler information services back to the general public and fleet management centers via various means. The TMC is also responsible for various system services that are necessary for the pilot.
  - Fleet Management Centers – This object represents the partnering fleet management centers that both receive and send real-time information to the WYDOT TMC about their firm’s truck operations and corridor conditions.
  - Data Warehouse – A data warehouse capability is planned for the pilot to collect, manage and make available the data collected as part of the pilot for performance management and evaluation.
- External Systems
  - Third Party Information Service Providers (ISPs) – This object represents third-party developers of data and information products for both WYDOT and the end-consumer. These may include weather products that are used by WYDOT TMC to driver-focused applications that use data from the TMC.
  - WYDOT Maintenance Management – This object represents the WYDOT maintenance management systems and functions carried out in the corridor including

winter maintenance, work zone management and other non-winter maintenance activities.

- WYDOT Commercial Vehicle Enforcement- This object represents WYDOT commercial vehicle operations enforcement in the corridor including Port of Entry operations, permitting, and oversize/overweight enforcement.
- Truck Parking Services – This object represents the public and private parking services available in the corridor.
- National Weather Service (NWS) – This object represents the systems and personnel of the NWS offices for the I-80 corridor.
- Adjacent State DOT TMCs – This object represents the systems and personnel at adjacent State DOTs (Colorado, Utah, and Nebraska) necessary for coordinated response to conditions on I-80.

1.5.2 Proposed System Functionality

System capabilities are organized by two categories – the pilot system that describes the center-related capabilities and the mobile distribution system that describes the capabilities relating to field to vehicle and V2V interactions. The system, comprising of the pilot system and the mobile distribution element provides the following capabilities.

- Pilot System – Collect Road and Weather Data: The system shall collect road and weather data from a variety of sources including connected trucks, connected WYDOT fleets, fixed infrastructure sensors like Road Weather Information System (RWIS), NWS, maintenance personnel and adjacent State DOTs. The data collected include both directly observed road and weather conditions or other data (such as vehicle telematics) that will help estimate the conditions of road segments along I-80.
- Pilot System – Collect Work Zone Information: The system shall collect work zone information including location, duration and nature of activity reported by maintenance personnel and centers.
- Pilot System – Collect Dynamic Travel Information: The system shall collect dynamic travel information such as travel speeds, parking availability, and incident notifications
- Pilot System – Share Integrated and Fused Advisories: The system shall fuse travel information, road condition data, and weather data to generate segment-level advisories along I-80. The system shall share advisories with CVs, fleet management centers, traditional ITS channels like DMS/HAR/511 and to partners like truck parking facilities and adjacent State DOTs.
- Pilot System – Provide Dynamic Travel Information: The system shall provide dynamic travel information to both vehicles on-road as well as over a wide area to support travel decisions. Dynamic travel information may relate to variable speed limits, road closures, and truck parking availabilities.
- Mobile Distribution – Share Safety and Road Condition Messages: The mobile distribution aspect of the system shall share safety and road condition messages between CVs and between vehicles and the roadside infrastructure. Safety and road condition information shared by CVs to other CVs include situational awareness of

downstream conditions, speeds, information on slowing traffic or queues. This information will also be relayed to RSE when CVs pass them in the corridor.

- Mobile Distribution – Collect Messages from Other CVs: Connected vehicles shall collect messages from other CVs about situational awareness of conditions and provide the information to the driver in a meaningful format.
- Mobile Distribution – Collect Messages from Infrastructure: Connected vehicles and the pilot system shall collect messages from infrastructure about advisories and alerts including speeds, parking availability, upcoming travel conditions and provide the information to the driver in a meaningful format.
- Mobile Distribution – Generate Emergency Message: Connected vehicles shall have the capability to generate an emergency message while on travel on the I-80 corridor when conditions warrant such a message from that vehicle or about other emergency conditions on the corridor observed by the vehicle.

Where necessary, DSRC will be used to support localized warnings to equipped vehicles as part of the mobile distribution system. This means when connected trucks or WYDOT fleet vehicles approach slowed or stopped traffic, they can receive messages in their vehicle from other equipped vehicles ahead of them to give more reaction time. Or if equipped vehicles pass roadside devices, drivers can receive messages alerting them to hazardous road conditions, crashes ahead, construction zone information, parking recommendations, or other road and travel information. If the equipped vehicle is stranded, the vehicle can send out an emergency notification to the appropriate center for assistance. The use of DSRC technology in the pilot will be guided by the IEEE 1609.2, 1609.3, and 1609.4 standards for Security, Network Services and Multi-Channel Operation (IEEE 1609.2-2016), the SAE J2735 Message Set Dictionary (SAE, 2016a), the emerging SAE J2945/1 V5 Communication Minimum Performance Requirements standard (SAE, 2016c). Relevant sections from SAE J3067 (SAE, 2014) Information Report will also be reviewed as part of systems development. Weather data collection will also be guided by National Transportation Communications for ITS Protocol (NTCIP) 1204.

The system capabilities and functions described in the previous paragraphs are implemented through the following seven applications:

- Road Weather Advisories for Trucks – This application provides the capability of collecting road weather data from WYDOT Fleets and Connected Trucks and using that data to develop short term warnings or advisories that can be provided to individual commercial vehicles or to commercial vehicle dispatchers.
- Automatic Alerts for Emergency Responders – This application provides the capability for connected trucks to transmit an emergency message when the vehicle has been involved in a crash or other distress situation.
- CV-enabled Weather-Responsive Variable Speed Limits (VSLs) – This application uses road weather information from connected trucks and WYDOT Fleet vehicles as well as current and historical data from multiple sources to determine the appropriate current safe speed and other traffic management strategies.

- Spot Weather Impact Warning (SWIW) – This application will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts (e.g., high winds, flood conditions, ice, and fog).
- Work Zone Warnings – This application provides information about the conditions that exist in a work zone to vehicles that are approaching the work zone.
- Situational Awareness – The application determines if the road conditions measured by other vehicles represent a potential safety hazard for the vehicle containing the application.
- Freight-Specific Dynamic Travel Planning – This application provides both pre-trip and en-route travel planning, routing, and commercial vehicle related traveler information for fleet management centers.

2 References

The following table lists the documents, sources and tools used to develop the concepts in this document.

Table 2-1 – References

#	Documents, Sources Referenced
1	CV Reference Implementation Architecture (CVRIA), Version 2.1, www.iteris.com/cvria.
2	Systems Engineering Tool for Intelligent Transportation (SET-IT) Version 2.1.
3	Deliverable Task 2.1 Stakeholder Registry and ConOps Review Panel Roster.
4	Deliverable Task 2.2 Draft User Needs.
5	IEEE. (2016a). 1609.2-2016 - *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages*. IEEE Vehicular Technology Society.
6	IEEE. (2016b). *1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services.* IEEE Vehicular Technology Society.
7	IEEE. (2016c). 1609.4-2016 - *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation.* IEEE Vehicular Technology Society.
8	International Organization for Standardization, ISO 26262 Road Vehicles - Functional Safety: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43464
9	USDOT Federal Motor Carrier Safety Administration (FMCSA), Hazardous Materials (HAZMAT)/ Dangerous Goods Regulations, http://www.fmcsa.dot.gov/regulations/hazardous-materials/hazardous-materialsdangerous-goods-regulations
10	USDOT Federal Emergency Management Agency (FEMA), Operational Lessons Learned in Disaster Response, http://www.usfa.fema.gov/downloads/pdf/publications/operational_lessons_learned_in_disaster_response.pdf

11 USDOT Pipeline and Hazardous Materials Safety Administration, 2012 Emergency Response Guidebook, http://phmsa.dot.gov/pv_obj_cache/pv_obj_id_7410989F4294AE44A2EBF6A80ADB640BCA8E4200/filename/ERG2012.pdf

12 USDOT, National Highway Traffic Safety Administration (NHTSA), Integrated Vehicle-Based Safety Systems (IVBSS) Preliminary Field Operational Test Plan, August 2008, Report No. DOT HS 811 010, http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2008/811010.pdf

13 SAE. (2014). J3067: *Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods.* SAE International.

14 SAE. (2016a). *J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary.* SAE International.

15 SAE. (2016b). J2945/0: *Dedicated Short Range Communication (DSRC) Minimum Performance Requirements.* SAE International.

16 SAE. (2016c). J2945/1: *On-Board System Requirements for V2V Safety Communications.* SAE International.

17 SAE. (2016d). J2945/2: *DSRC Requirements for V2V Safety Awareness*. SAE International.

18 Federal Information Processing Standard (FIPS). (2004). PUB 199: *Standards for Security Categorization of Federal Information and Information Systems.* NIST.

19 FIPS. (2006). PUB 200: *Minimum Security Requirements for Federal Information and Information Systems.* NIST.

20 NIST (2013). 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST.

3 SAFETY RISK PROCESS AND APPROACH

In order to protect pilot user's safety, and any non-pilot motorist, each application leveraged by the pilot was reviewed following the ISO 26262 process and for the testing, deployment, and closeout stages. This was done by reviewing the individual flows that make up each application and the CV systems, identifying hazards, classifying the risk based on the ASILs, and developing risk mitigation plans. This document incorporates steps highlighted in the 10 parts included in the ISO 26262 as shown in Figure 3-1. This will help incorporate safety management plans into the design, procurement, installation, testing, and deployment stages.

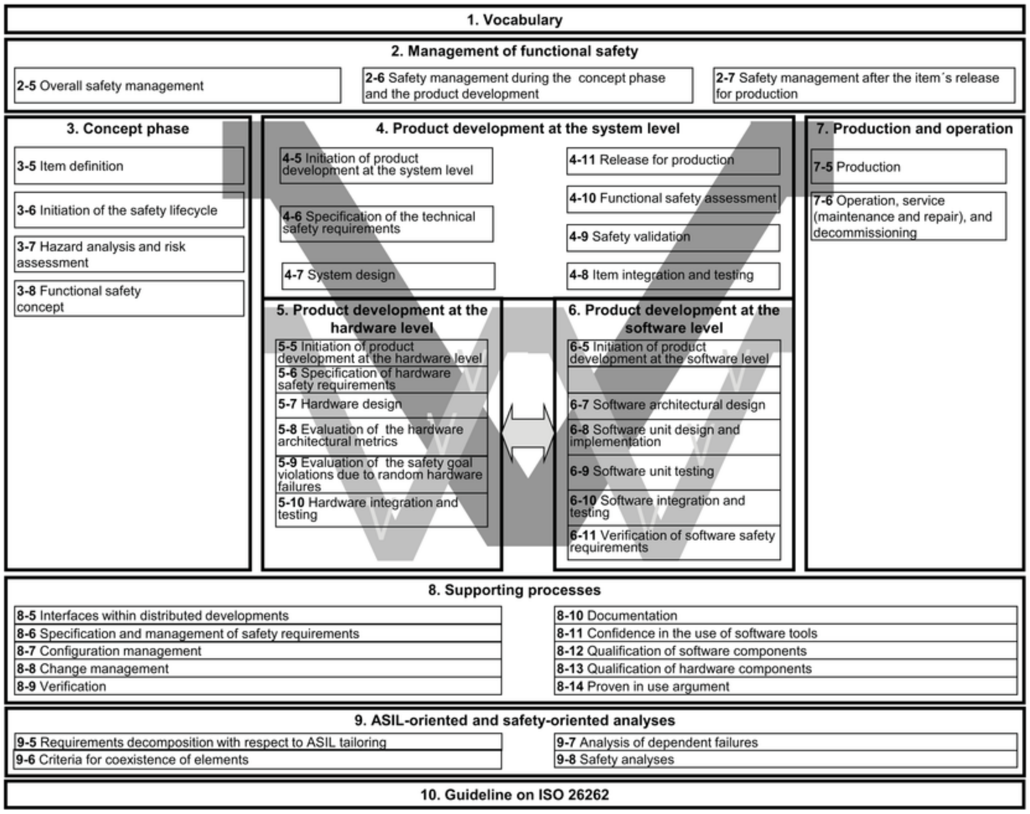
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Figure 3-1. Overview of ISO 26262 (Source: ISO 26262 Road Vehicles - Functional Safety).

3.1 Development Process

The Development Process of the Safety Management Plan follows the process defined in the USDOT guidelines; 1) identify safety scenarios at both system level and application level as defined in the ConOps, 2) assess the level of risk for each safety scenario, and 3) develop a safety operational concept for each scenario if it is identified as high/medium risk. Figure 3-2 illustrates this process.

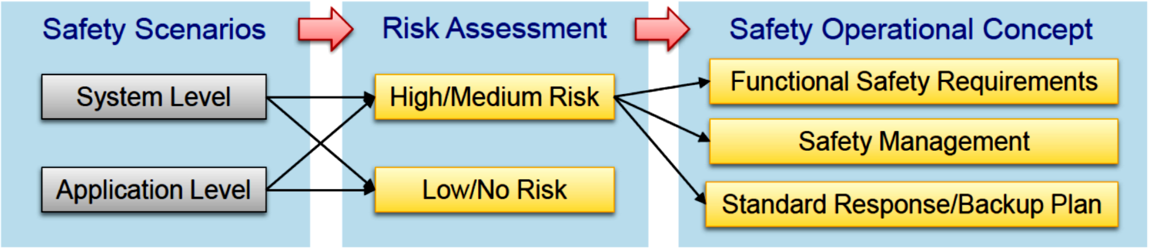

Figure 3-2. Safety Management Plan Development Process (Source: USDOT Guidance Summary on Safety Management Plan)

3.2 Safety Stakeholders

The following are safety stakeholders, in no particular order, for the proposed system:

- USDOT
- WYDOT – Traffic, Construction, Maintenance, Geographic Information System (GIS)/ITS, IT, Telecom Programs (including equipped snow plow drivers).
- Wyoming Highway Patrol
- Truck/ Fleet Managers and Drivers
- Wyoming Trucking Association
- City managers and local traffic and law enforcement officials (Rawlins, Laramie, Cheyenne, Green River, Rock Springs, Evanston)
- NWS
- County Emergency Management (including Hospitals)
- Private Truck Parking Services
- Adjacent State DOTs
- Third party application developers
- System integrators and vendors
- Private vehicle drivers
- Equipped and non-equipped truck drivers
- Tow truck operators

The project team in charge of safety management is composed by Robert Wilson as the Telecommunications manager (responsible for radio and leased telecommunications), James England as the Information Technology (IT) manager (responsible for network equipment personnel), Vince

Garcia as the GIS/ITS manager (responsible for electrical techs), and Kevin Cox as the TMC manager (responsible for monitoring the health of devices). Safety management roles and responsibilities are described in Section 5.3 of this document.

It should be noted that relevant emergency services entities will be based on the counties along the I-80 corridor. Furthermore, services to fix or address problems with CV infrastructure are covered by a service level agreement (SLA) with a 1-hour response time, with technicians located along the corridor.

3.3 Emergency Responder Coordination

Agencies within the State of Wyoming and local cities have their own emergency response plans for various events, such as severe incidents, natural disasters, or planned events. Section 4.3 lists the corresponding agencies for each safety scenario.

The pilot deployment team will coordinate with emergency responders on what actions are expected from both the agencies and the deployment program (e.g., safety manager) in response to the emergency situations identified in this safety management plan.

3.4 Existing Plans

The rural nature and sparse population of Wyoming require creative solutions to provide communications and power to roadside devices. Communication options used by WYDOT include commercial service (principally Digital Subscriber Line (DSL) and a limited number of fiber-based solutions) and systems provided by WYDOT’s Telecommunications Program (Wi-Fi and other radio-based systems). Where possible, systems are powered by commercial power sources (alternating current (A/C)); but, many locations are powered using solar and/or wind generation due to availability and cost considerations. When commercial power sources are not readily available or the cost to get such service is not affordable, WYDOT plans to deploy two forms of direct current (D/C) power generation. All sites, whether A/C or D/C, are supported by battery backup power in the event of a power outage. Special attention in the design of D/C systems is paid to improving battery performance and life by using intelligent charge controlling systems.

Solar and wind generation systems, along with all Internet Protocol-addressable (IP-addressable) ITS, communication systems and other devices on the WYDOT network, are monitored 24 hours per day using the SolarWinds network monitoring tool. In the event of an outage, WYDOT’s TMC operators, GIS/ITS electrical technicians, Telecommunications technicians, and Enterprise Technology technicians all use this network monitoring tool and a shared trouble ticket system to share notes and to relay progress of repairs.

WYDOT’s response to malfunctions with roadside devices, including VSL signs and the communication and power systems that support them, is governed by a SLA agreed to by the GIS/ITS program, the Telecommunications program, and the state’s Enterprise Technology Services agency. The SLA classifies critical devices, such as VSLs, as regulatory devices and assigns them a Priority 1 level. This requires the appropriate technician to be notified of problems immediately upon discovery and for initial response to begin within one hour. If it is necessary to visit the site, dispatch should occur within two hours unless unsafe conditions exist. WYDOT GIS/ITS and Telecommunication technicians have job duties that specifically include responding to problems with ITS devices and communication systems along the I-80 corridor, although all technicians are available to respond when needed. In addition, WYDOT has mutual aid agreements between programs to help reduce response times to critical issues. Most VSL signs along I-80 are in pairs, so if there is a problem with one sign the other can still be used to display the speed limit. In the event neither sign is functioning, the sign will be covered so it does not influence drivers and the previously posted speed limit (i.e., there is a traditional speed limit sign of a VSL) will be in place.

In the event a construction project occurs in a VSL zone, the existing signs are used for reduced work zone speeds. In the event a project affects the functionality of a sign, it is treated similarly to a traditional speed limit sign by being covered so it does not influence drivers and a temporary sign that posts the reduced construction zone speed is deployed to the roadside.

WYDOT's response to malfunctions, power issues, security problems, communications problems, and unforeseen issues associated with critical roadside CV devices will be governed by the existing SLA agreed to by the GIS/ITS program, the Telecommunications program, and the state's Enterprise Technology Services agency for ITS. The SLA classifies critical devices and assigns them a Priority 1 level with response times as noted above.

4 Safety Analysis and Threat Assessment Plan

The main goal of the Safety Analysis and Threat Assessment Plan is to guide the pilot deployment team in designing a safety-critical system to eliminate hazards from the design, or to mitigate the risk if it does occur. The following set of safety scenarios have been identified in relation to the applications and technologies selected for the Pilot Deployment. The safety scenarios included an analysis of likelihood and potential impact as well as mitigation plans.

4.1 Identification and Classification of Safety Critical Events

This section discusses the safety scenarios at system level and application level. The safety scenarios are defined based on system-level and the seven Pilot applications. The safety scenario identification considers the implications of the geographical and weather related features of I-80 corridor.

4.1.1 Identified Pilot-Specific System Safety and Threats

This section reviews and identifies safety threats and risks that affect deployed a CV system. These threats and risks include communications, security, power outages, the impact of other events outside the CV systems, and potential safety risks beyond single application concept and driver perception.

4.1.1.1 *Communications*

Communication failures is considered as a generic system-level scenario that may be applied to the whole Pilot Deployment corridor. The Pilot Deployment corridor has some sections that may have greater implications on the performance of the wireless communication needed for the CV. Communications failure would cover many possible problems; some examples are:

1) Telecommunications provider outage for satellite, cellular, and backhaul (DSL/Fiber/T1/DS3),
2) Wire cut or destroyed that provides communications,
3) Router or switch configuration problem or error,
4) Internet Protocol Security (IPSEC) Virtual Private Network (VPN) failure at the field or head end, and
5) DSRC failures due to jamming, antenna failure, or general congestion.

While there are many types of communications failures that could be intentional or accidental, the result is the same – drivers and the TMC lose or have delayed messages. To help mitigate the communications, links are monitored to reduce the length of outage and the vehicles will maintain a 10-minute log of messages to attempt to resend unreceived relevant ones further down I-80.

4.1.1.2 *Security*

Similar to communication failures, malicious attacks and hacks into the CV's OBE or the RSE systems are considered as a generic system-level scenario that may have an impact at various levels on the system performance. The following are examples of security failures:

- A device that is misbehaving due to someone hacking into the system.
- Someone steals the certificates and pretends to be an After-market Safety Device (ASD), Integrated Safety Device (ISD), or Vehicle Awareness Device (VAD).
- Someone hacks into the backhaul and pretends to be an RSE.

4.1.1.3 *Power Outages*

Power outages is another generic scenario that could be caused by a lightning strike. For instance, the system negatively impacts the VSL controller to causes the VSL sign to go down. This scenario could be applied to other devices such as DMS, RSE, and other devices that would prohibit the TMC to send the OBE important safety and weather messages.

4.1.1.4 *Impacts outside CV System focus*

Adverse weather, challenging roadway geometry, severe crashes, and HAZMAT incidents were identified as factors that may have safety implications outside the CV system focus. Adverse weather may have an impact on different devices such as the RSEs. Awareness of law enforcement, emergency management agencies, and other entities about the safety implications of the CV Pilot is also required for a successful and safe implementation.

4.1.1.5 *Collective environment*

Potential safety risks beyond a single application may be considered as system-level collective environment scenario. A natural disaster such as tornados or severe lightning strikes cause the whole CV system for the Pilot corridor to go down. A CV truck could be stranded without information about weather and road conditions, parking information, or emergency responders.

4.1.1.6 *Users Perceptions*

Misperception or confusion of how the system works, such as high expectation of what the CV technology offers, may have some safety implications. For example, a driver mistakenly thinks that an instrumented CV can take control or take an evasive action to avert the threat. Another example could be a driver expects to receive warnings more often or expects continued warning messages if advised speeds were exceeded.

4.1.1.7 *Operational and Functional Safety*

According to the definition in ISO 26262, functional safety requirement is a safety requirement implemented by a safety-related system or technologies in order to achieve or maintain a safe state for the item taking into account a determined hazardous event. Unforeseen events may cause the system to become dysfunctional.

4.1.2 Identified Pilot Specific Application Safety and Threats

This section reviews the seven applications being used by the pilot and their safety implications. All applications are sensitive to malfunction; installation (e.g., location of device/Driver-Vehicle Interface (DVI)); wrong information; and interaction with non-equipped vehicles, software, and hardware updates required for a device or an application, which impact the overall safety of the driver, vehicle, and application. Although human factors, such as distraction, could be considered as a safety threat, not all applications would be affected in the same manner and therefore should be considered on a case-by-case basis. For example, results from field operational tests on Integrated Vehicle-Based Safety System (IVBSS) and Road-Departure Crash Warning (RDCW) Systems indicated that no safety implications could be related to such systems because of user reliance/perception (Wilson, Stearns, Koopmann, & Yang, 2007; Sayer, et al., 2011).

Descriptions of each application in this Pilot, and any particular safety scenario, are provided in the subsections below.

4.1.2.1 *Road Weather Advisories for Trucks*

This application provides the capability of collecting road weather data from WYDOT Fleets and Connected Trucks and using that data to develop short term warnings or advisories that can be provided to individual commercial vehicles or to commercial vehicle dispatchers. The raw data will be processed in a controlling center (WYDOT TMC) to generate road segment-based data outputs. The processing will also include a road weather commercial vehicle alerts algorithm to generate short time horizon alerts that will be pushed to fleet management systems and available to commercial vehicle dispatchers. In addition, the information collected can be combined with observations and forecasts from other sources to provide medium (next 2-12 hours) or long term (more than 12 hours) advisories through a variety of interfaces including web based and CV-based interfaces. While these advisories are generated for trucks, through existing traveler information portals, road weather advisories can be shared with the general traveling public.

Incorrect or inadequate road weather advisories, planned or unplanned software updates required for the application, and increased driver distraction because of too much information are safety scenarios identified for this application.

4.1.2.2 *Automatic Alerts for Emergency Responders*

This application provides the capability for connected trucks to transmit an emergency message when the vehicle has been involved in a crash or other distress situation. In addition to driver initiation, an automatic crash notification feature transmits key data on the crash recorded by sensors mounted in the vehicle (e.g., deployment of airbags) without the need for involvement of the driver.

Connected trucks would attempt to provide notification via cellular communication in the corridor. In areas with inadequate cellular coverage, the emergency message is broadcast to passing CVs, which can relay the message to other CVs as well as roadside “hotspots.” Once received by WYDOT TMC (either through emergency vehicles or through the RSE), the appropriate response to the vehicle situation can be carried out by emergency response services. This application allows a vehicle to forward mayday requests even in areas where no V2I infrastructure exists.

Safety scenarios for this application are malfunctions that cause the application not to provide notifications in a timely manner, or, in areas with inadequate cellular coverage, insufficiencies in the mass of V2V prevent emergency message getting relayed back to the TMC.

4.1.2.3 *CV-enabled Weather-Responsive Variable Speed Limit*

This application uses road weather information from connected trucks and WYDOT Fleet vehicles as well as current and historical data from multiple sources to determine the appropriate current safe speed and other traffic management strategies. The application provides real-time information on appropriate speeds for current conditions and warns drivers of coming road conditions.

Safety scenarios for this application include potential conflicts of information provided by message signs and in-vehicle devices, as well as the *lack of CV mass interaction, so real-time information speed information is not received.*

4.1.2.4 *Spot Weather Impact Warning*

This application will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts (e.g., high winds, flood conditions, ice, and fog). The application is designed to use standalone weather systems to warn drivers about inclement weather conditions that may impact travel conditions. Real-time weather information is collected via RWIS or via vehicle-based probe data from commercial, specialty or public vehicles. The information is processed to determine the nature of the alert or warning to be delivered and then communicated to CVs. If the warning includes road closure, then diversion information can be provided. For non-equipped vehicles, the alerts or warnings will be provided via roadway signage or through third-party applications.

All safety scenarios for the weather advisories for trucks application apply to this application. Malfunctions or communication issues that cause the application not to provide timely diversion information may result in CV or non-equipped vehicles becoming stranded on the main Pilot Deployment corridor.

4.1.2.5 *Work Zone Warnings*

This application provides information about the conditions that exist in a work zone in relation to vehicles that are approaching the work zone. This application provides approaching vehicles with information about work zone activities that may result in unsafe conditions to the vehicle, such as obstructions in the vehicle's travel lane, lane closures, lane shifts, speed reductions, or vehicles entering/exiting the work zone.

Similar safety scenarios of malfunction, installation, provision of wrong information, and human factors apply to this application as others.

4.1.2.6 *Situational Awareness*

The application determines if the road conditions measured by other vehicles represent a potential safety hazard for the vehicle containing the application. To enable this application, other vehicles broadcast relevant road condition information, such as fog, icy roads, slowing speeds, or brake lights. This application supports the capability for CVs to share situational awareness information even in areas where no roadside communications infrastructure exists. This application can be useful to vehicles that are not fully equipped with sensors, or vehicles entering an area with hazardous conditions.

Safety scenarios of malfunction, installation, provision of wrong information, and human factors apply to this application as others. In addition, the lack of critical mass of CV-vehicles might result in no information being provided.

4.1.2.7 *Freight-Specific Dynamic Travel Planning*

This application provides both pre-trip and en-route travel planning, routing, and commercial vehicle related traveler information. Both real-time and static information can be provided directly to fleet managers, to mobile devices used by commercial vehicle operators, or directly to in-vehicle systems as commercial vehicles approach roadway exits with key facilities such as parking. The application also supports advisories to specific categories of advisories (restrictions on lightweight or high-profile vehicles for example).

Safety scenarios of malfunction, installation, provide wrong information, and human factors apply to this application as others.

4.2 Analysis of Likelihood (Probability/Exposure) and Potential Impact (Severity/Controllability)

Analysis of the probability of each of the identified safety scenario and the level of severity and controllability was conducted following the ISO 26262 ASIL determination matrix, shown in Table 4-1. The Pilot Deployment team examined hazard events related to the installation of the devices for both the vehicle fleets and infrastructure. The security management operating concept provided guidance in regards to security and privacy, as well as mitigation plans for V2V and V2I security breaches regarding confidentiality, integrity, and availability along with the potential threats. In order to qualify a hazard event that would be governed by ISO 26262, the event analysis must result in an ASIL A, B, C, or D. The ASIL level is derived using the following 3 attributes:

1. Classes of Severity
    - S1: light and moderate injuries;
    - S2: severe and life-threatening injuries (survival probable); and
    - S3: life-threatening injuries (survival uncertain), fatal injuries.
2. Classes of probability of exposure regarding operational situations
    - E1: very low probability;
    - E2: low probability;
    - E3: medium probability; and
    - E4: high probability.
3. Classes of Controllability
    - C1: simply controllable;
    - C2: normally controllable; and
    - C3: difficult to control or uncontrollable.

Table 4-1 – ASIL Determination (Adapted from ISO 26262 Part 3: Concept Phase)

		Probability of Exposure	Controllability through the Driver		
			Simply Controllable (C1)	Normally Controllable (C2)	Uncontrollable (C3)
Potential Severity	Light and Moderate Injuries (S1)	Extremely Low Probability (E1)	QM	QM	QM
		Low Probability (E2)	QM	QM	QM
		Medium Probability (E3)	QM	QM	ASIL A
		High Probability (E4)	QM	ASIL A	ASIL B
	Severe and Life-threatening –Survival probable (S2)	Extremely Low Probability (E1)	QM	QM	QM
		Low Probability (E2)	QM	QM	ASIL A
		Medium Probability (E3)	QM	ASIL A	ASIL B
		High Probability (E4)	ASIL A	ASIL B	ASIL C
	Life-threatening –Survival Uncertain (S3)	Extremely Low Probability (E1)	QM	QM	ASIL A
		Low Probability (E2)	QM	ASIL A	ASIL B
		Medium Probability (E3)	ASIL A	ASIL B	ASIL C
		High Probability (E4)	ASIL B	ASIL C	ASIL D

Where:

- Quality Management (QM) = standard quality/ safety management is sufficient
- ASIL x = measures according to ASIL x are to be applied to achieve safety goals

In particular, ASIL D represents likely potential for severely life-threatening or fatal injury in the event of a malfunction and requires the highest level of assurance that the dependent safety goals are sufficient and have been achieved. ASIL D is noteworthy, not only because of the elevated risk it represents and the exceptional rigor required in development. Any product able to comply with ASIL D requirements would also comply with any lower level.

The level QM only means that there are no hazards associated with the given application, so management of safety requirements is not relevant. This is not to say that no controls are required in the development of the product. Even if there are no hazards, there may still be business risk and other risks to manage, and there may be other applicable customer and regulatory requirements for QM.

4.3 ASIL Determination Matrix

Table 4-2 provides the safety and threat analysis for the pilot identifying risk description, the likely impacts of each scenario, the risk response plan, and the overall ASIL determination for each risk. The likely impacts of each scenario are provided on case-by-case basis. To help the Institutional Review Board (IRB) to understand the risk assessment of scenario using the ISO 26262, the following section provides the rational of determining the Severity, Exposure, and Controllability ratings. Severity is defined as percentage classifications of the potential and cascaded/propagated injuries that may be sustained in accidents, as a result of a hazard, to the driver, passengers, and other road users. Severity level 0 means that no injuries will result from the scenario, or will result in Abbreviated Injury Scale (AIS) 0 and less than 10% probability of AIS 1-6. Severity level 1 (S1) which indicates a light and moderate injuries or more than10% probability of AIS 1-6 and not S2 or S3. Severity level 2 means that severe injuries, possibly life-threatening, or survival probable may result from a risk scenario with more than 10% probability of AIS 3-6 and not S3. Severity level 3 (S3) is a life-threatening injuries (survival uncertain) or fatal injuries with a likelihood of 10% of AIS 5-6.

Exposure used in Table 4-2 is defined as the probability of a human‘s exposure to a hazard in terms of time and location in particular scenarios during expectable (mis-)use cases. Exposure level 0 (E0) means that the scenario will never happen, probability is 0%. Exposure level 1 (E1) has a very low probability, or may happen less often than once a year. E2 has a very low probability, may happen a few times a year, or may occur less than 1% of average operating time. E3 has a medium occurrence probability, may happen once or more a month, or has 1%-10% occurrence of average operating time. E4 has a high probability of almost every drive or greater than 10% of average operating time.

Controllability is defined as the probability of being able to withdraw oneself from the severity impact, thereby avoiding or alleviating the injury, once exposed to a hazard. Controllable in general is defined as level 0 (C0). Controllability level 1 (C1) is a scenario that is simply controllable by 99% or more of all drivers. C2 is normally controllable by 90% or more by all drivers while C3 is difficult to control or uncontrollable by more than 90% of all drivers.

The number used in the risk register column corresponds to the overall risk register developed as part of the project management plan and maintained by the pilot team.

Table 4-2 – Safety and Threat Analysis

ID No.	Risk Register Reference	Category	Safety Risk Description	Likely Impacts	Risk Response Plan	E	S	C	ASIL
1	25	Fleet Builds	Independent of the function of the safety system installed on the vehicle, there is a crash/ HAZMAT crash. The equipment installed by the ICF/Wyoming CV Pilot deployer affects the crashworthiness of the production vehicle.	Safety of the participant	-Include lessons learned and best practices from Safety Pilot Model Deployment (SPMD), IVBSS and RDCW in the installation design. -Conduct design review to verify compliance with Federal Motor Vehicle Safety Standards (FMVSS) as applicable. -Coordinate with emergency responders. -Repair problem that affected the crashworthiness by doing a root cause analysis, define the problem and fix across the fleet.	1	2	3	QM
2	26	Infrastructure Installation	Communication failures, or power outages cause a system or application to go down or not sending timely needed information	Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react.	Failsafe will be built in all applications. WYDOT maintains a failover data center that provides critical services including HAR during outages of the primary data center and some levels of load balancing during times both data centers are available. Additionally, FIPS 140-2 level 3 devices will be used for RSE and Snow Plow/Highway patrol equipment with Hardware Security Module (HSM) to harden the devices from bad actor compromise. Monitor communications links so that repairs can be made promptly when failures occur.	1	1	1	QM
3	27	Infrastructure Installation	The CV system negatively impacts the VSL algorithm to cause the roadside VSL system to go down.	The symptom is the same as if a lightning strike caused a power outage. There are failsafe already built into the VSL system and the default mode would be no variable speed limit posted similar to other roadway sections with no VSL system. Therefore, the Pilot Deployment does not increase the potential severity to a driver's normal day-to-day activities.	System monitoring will be used to reduce the length of time for failures. WYDOT maintenance and Network Operations Center (NOC) teams are available 24x7x365 for emergency repairs.	1	1	1	QM

ID No.	Risk Register Reference	Category	Safety Risk Description	Likely Impacts	Risk Response Plan	E	S	C	ASIL
4	28	Infrastructure Installation	The RSE and related equipment are installed such that there is additional damage or harm inflicted in the case of a vehicle crash into the RSE mounting structure.	Safety of the participant	-Include lessons learned and best practices in the design and installation of the RSE equipment. -Conduct a design review of the Infrastructure Installation -Move or repair installation of RSE equipment to address problem.	1	1	1	QM
5	29	Infrastructure Installation	The RSE and related equipment are installed such that there is additional damage or harm inflicted in the case of a HAZMAT crash into the RSE mounting structure.	Safety of the participant	-Include lessons learned and best practices in the design and installation of the RSE equipment. -Conduct a design review of the Infrastructure Installation -Coordinate with emergency responders and follow normal safety precautions and practices in the Emergency Response Guidebook. -After the crash is addressed analyze the root cause of RSE installation, repair across the I-80 installation.	1	1	1	QM
6	30	Infrastructure Installation	Communication failures, or power outages cause a system or application to go down or not sending timely needed information	Failsafe will be built in all applications. Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react.	WYDOT maintains a failover data center that provides critical services including HAR during outages of the primary data center and some levels of load balancing during times both data centers are available. Additionally, FIPS 140-2 level 3 devices will be used for RSE and Snow Plow/Highway patrol equipment with HSM to harden the devices from bad actor compromise. After the failure has been repaired (by fail over to second site or equipment repair), review the cause of the failure and implement measures to mitigate reoccurrence.	1	1	1	QM
7	31	Fleet Builds	Improper installation of the OBE causes a device to misbehave	Safety of the participant. In this case, there is no increase to the potential injuries. Therefore, we designate the potential severity as S0. Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react. University of Michigan Transportation Research Institute (UMTRI) showed	-Include lessons learned and best practices from SPMD, IVBSS and RDCW incorporated in the installation design. -Conduct design review of installation interface. -Verify installation before deployment (institute specific end-of-line testing and checklist procedures). -Analyze cause of device problem and address across fleet.	1	0	1	QM

ID No.	Risk Register Reference	Category	Safety Risk Description	Likely Impacts	Risk Response Plan	E	S	C	ASIL
				with data collected on previous programs, such as IVBSS, that false warnings do not pose a hazard.					
8	32	Security	A device is misbehaving due to someone hacking into the system. For instance, someone steals the certificates and pretends to be an ASD, ISD, or VAD. Another scenario is that they hack into the backhaul and pretend to be an RSE; e.g., issuing faulty or erroneous alerts/advisories/warnings such as higher speed limits for the condition, or “No incident ahead” and causing drivers not to reduce speeds	In this case, there is no increase to the potential injuries. Therefore, the potential severity is S0. It has been determined that these types of "spoofing (masquerading) scenarios" don't pose additional hazard to the driver. Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react. UMTRI showed with data collected on previous programs, such as IVBSS, that false warnings do not pose a hazard.	-Develop smart applications to conduct data integrity checks before messages are sent, also have a services engine that receives messages and verifies integrity at the Center. Log problems for potential misuse, bad actor, or failing equipment review. -Include lessons learned and best practices in the Security Credential Management System (SCMS) and backhaul design. -Establish firewalls that are compliant with industry standards. -Comply with established server installation standards and practices ICF/ Wyoming. -Leverage SCMS certificates to validate messages and smart application to validate messages are within appropriate bounds -Add tamper evident seals to the devices. -If a hacker creates an environment to maintain an announcement of higher speed during a time the TMC has reduced speed due to adverse road conditions, the action plan would be to monitor broadcasts from the RSE on the additional radio from the TMC. This would allow the TMC to see the hack has taken place, take the RSE offline, or repair the code that has been altered. During this time the drivers would still be in control of their vehicles and would be expected to drive with good judgment to be safe. -Review logs to find point of entry and weakness leveraged by hacker. Tighten security to address weakness. Leverage outside group to assist with audit if appropriate. Also do a detailed	1	0	1	QM

ID No.	Risk Register Reference	Category	Safety Risk Description	Likely Impacts	Risk Response Plan	E	S	C	ASIL
					review of software to ensure no backdoors or remaining hacker code is in system.				
9	33	Fleet Builds	Improper installation of the ASD, VAD, or DAS drains the battery, leaving the driver stranded in the middle of the night.	Safety of the test participant	-Include lessons learned and best practices incorporated in the SPMD in the installation design. -Conduct design review to prevent improper installation (ASD/VAD Installation Procedures). -Pilot Deployment Best Practice: During training, participants are instructed to call Pilot Deployment for any issues including accidents or stranding. They are provided a phone number that they can call 24/7. A Pilot Deployment representative will be on call 24/7. If the participant needs roadside assistance, WYDOT will arrange for service to be dispatched. This service is pre-arranged such that they are on-call 24/7 and have a proven response time. Arrival time will be based on their actual location on the pilot corridor. -Define problem that caused the battery drain, address problem across fleet.	2	2	2	QM
10	34	Fleet Builds	Improper installation of the ASD, VAD, or DAS leads to degradation of the Controller Area Network (CAN) bus interface.	Safety of the test participant	-Include lessons learned and best practices from SPMD, IVBSS and RDCW incorporated in the installation design. -Conduct design review of installation interface. -Review resistance degradation of CAN bus or data overload to find cause, update installation or software queries of the CAN to repair problem.	2	2	2	QM
11	35	Driver Training	The driver has a misperception of how the system works. For instance, the driver thinks it is more protective than just a warning system and expects the vehicle to take control and avert the threat.	Safety of the test participant	Incorporate into the driver training plan and checklists.	1	1	1	QM

ID No.	Risk Register Reference	Category	Safety Risk Description	Likely Impacts	Risk Response Plan	E	S	C	ASIL
12	36	Fleet Builds	A piece of Pilot equipment in the cabin becomes loose.	Safety of test participant. Causes driver distraction or occludes the driver's vision, causing an accident.	-Include lessons learned and best practices from SPMD, IVBSS, and RDCW incorporated in the installation design. -Conduct design review of installation interface.	1	3	2	QM
13	37	Fleet Builds	A short in the equipment being installed by the pilot causes overheating.	Safety of test participant or component failure.	-Include lessons learned and best practices from SPMD, IVBSS, and RDCW incorporated in the installation design. -Conduct design review of installation interface.	1	1	2	QM
14	38	Fleet Builds	A driver becomes hurt in the high-bay/ workshop where the OBE/ software will be installed, tested, updated in trucks or other work areas.	Safety of the test participant	-Do not allow participants to drive their vehicle into the work area.	2	1	2	QM
15	39	Backhaul	Someone hacks into the data flow at any point in the system (V2V or V2I)	Malicious software/code installed. Personal information and other information are stolen which may increase risk to personal safety such as tracking individual travels, etc.	-Pilot Deployment will have rigorous design standards in place when developing a new system. -Perform routine information security audits. -Perform root cause analyses of hack, lock down as appropriate, verify the hacker has not left code on the network or devices.	2	0	3	QM
16	40	Infrastructure Installation	Lack of CV mass interaction on the pilot corridor may result in important safety information not relayed at all or in a timely fashion.	Safety of the test participant. Normal procedures of no CV system apply. In this case, there is no increased risk. Therefore, we designate the potential severity as S0. Since these are warning systems, the driver is still in control of the vehicle and will need to assess the situation and determine how to react.	-Lack of CV mass will be treated as failsafe, all applications and systems will be designed to consider insufficient CV mass. -Drivers will be trained to understand the limitations of the system.	3	0	1	QM

4.4 Summary of Risk Assessment

The Pilot Deployment team identified and analyzed various potential hazard events at the system level and application level. The system level included scenarios that may be generated because of communications, security, special events, crashes, weather, perception of users, and risks beyond single application concept, i.e., collective environment. Special considerations for system and software vulnerability are discussed in the Security Management Operating Concept.

There were no ASIL hazard events identified, and none of the measures according to the ASIL as defined in ISO 26262 needed to be applied to achieve safety goals. Therefore, all potential risks will be handled and mitigated using the best practices of system engineering and project management principals during the design of the pilot installation and fleet builds. Furthermore, the items identified have been added to the risk register and will be tracked using the risk management process.

Four examples of best practices that will be implemented for this CV pilot are focused around software development, vendor selection, vehicle retrofit of CV equipment, and network security. A brief explanation of each follows.

Software development within this CV pilot will leverage an Agile software development process. This process promotes strong communications between developers and stakeholders outside the development team, testing, and documentation. This process also allows for flexibility within the development process while maintaining direction based on requirements.

The vendor selection process started with interviews from over 20 vendors; based on these interviews, a short list was complied by evaluating vendor technology compatibility with pilot needs, willingness to work with the CV pilot, and previous experience. This process will continue with testing equipment by evaluating application programming interfaces (API’s) maturity and the capabilities made available by the vendor, and then asking the lead vendors to come on site with equipment to do a more thorough presentation.

Vehicle retrofit of equipment will be an important part to do carefully. Focus will be placed on building a plan to install equipment with lessons learned from the UMTRI Safety Pilot. The pilot will document the installation of equipment to include device type, firmware, software, and serial number. Before vehicle leave the installation bay, they will be tested with a test RSE to ensure the vehicle has operational access to the SCMS and each application is functioning.

Network security is built with a policy of security in depth. This is a process that focuses on building security systems with layers of security from the outside point of a network through to internal devices with security implementations at each point. The pilot will use an external firewall, encrypted VPNs, or private circuits for wide area connectivity, device security updates on network attached equipment, hardware security equipment for tamper evidence and tamper resistance (in Highway Patrol vehicles, snow plows, and RSEs), and monitoring logs and devices for breach attempts to provide security in depth.

5 Safety Operational Concept

5.1 Functional Safety Requirements

The Pilot Deployment safety plan has been developed in compliance with ISO 26262 and the safety activities have been included in the overall project plan, such as the hazard analysis and risk assessment. The systems requirements developed for the pilot will include appropriate functional safety requirements to mitigate the safety scenarios identified in Section 4.3. As an example, Table 4-2 ID 2 has a Safety Risk Description of “Communication failures, or power outages cause a system or application to go down or not sending timely needed information” with a Risk Response Plan of “Failsafe will be built in all applications. WYDOT maintains a failover data center that provides critical services including HAR during outages of the primary data center and some levels of load balancing during times both data centers are available.” Additionally, FIPS 140-2 level 3 devices will be used for RSE and Snow Plow/Highway patrol equipment with HSM to harden the devices from bad actor compromise. Monitor communications links so that repairs can be made promptly when failures occur.”

5.2 Overall Safety Management Plan

Safety scenarios in this Safety Management Plan were developed based on the Pilot Deployment ConOps. The ConOps developed for ICF/ Wyoming Pilot Deployment documents the applications to be deployed and operational practices to be followed in Phases 2 and 3. The safety operational concept was developed contingent on the proposed operational practice in the ConOps.

The Pilot Team Concept Development Lead (Vince Garcia) has been identified and tabbed to be Safety Manager for the pilot. The safety management will focus on four areas:

1. Overall Safety Management
2. Safety Management during Testing & Installation Phase (Infrastructure, fleet deployment, installation, testing)
3. Safety Management during Deployment Phase
4. Deployment Closeout

The Safety Manager shall utilize existing processes to effectively communicate safety anomalies to the responsible persons. Section 4.3 lists additional safety related risks and mitigations that will be added to the existing risks present for WYDOT. Additional risks are associated during development, deployment and operation. These are detailed in section 5.4 and 5.5 and will be add to existing risks. Specifically, the safety hazard events will be added to the risk register as appropriate. Additionally, any safety anomalies that occur will use the change management process described in the Configuration Management Plan of the Project Management Plan for issue resolution.

5.3 Safety Management Stakeholder Roles and Responsibilities

The principles used by WYDOT to support the prompt response to critical ITS will be employed to support roadside CV systems. This includes proper design of power and communication systems, network monitoring, dedicated support of the roadside devices, a service level-based approach and mutual aid strategy for prompt response to failed systems and the use of well-established support and trouble ticket system.

Table 5-1 – Safety Management Stakeholder Roles and Responsibilities.

Responsible Party	Core Function	Safety Management Role
WYDOT Traffic engineers	Roadside electrical systems design	Ensure reliability and robustness of electrical systems and power supply to roadside elements by mitigating power outages to CV Pilot infrastructure
WYDOT ITS electrical technicians	Roadside electrical systems maintenance	Provide quick response repair capabilities to recover from power outages to CV Pilot System Infrastructure
WYDOT Telecommunications Program	Roadside communication systems design	Ensure reliability and robustness of communication systems to roadside and selected onboard elements
	Roadside communication systems maintenance	Provide quick response repair capabilities to recover from communication failures to CV Pilot System Infrastructure
	WYDOT fleet OBE	Safety management during installation, updates, and maintenance of WYDOT fleet OBE
WYDOT GIS/ITS	Roadside network security and Firewalls	Provide overall safety management for application development and testing
State of Wyoming Enterprise Technology Services	State network security and Firewalls	Provide system security for CV Pilot System
Pilot Contractors	Connected Trucks OBE	Provide equipment installation, updates, and testing per specified safety requirements
	RSE installation	Provide equipment installation, updates, and testing per specified safety requirements
	Application development and testing	Provide application, updates, and testing per specified safety requirements

Responsible Party	Core Function	Safety Management Role
	System Integration	Monitor and maintain reliability and stability of overall CV pilot system across all applications and physical objects
	Training	Provide training to pilot participants on CV applications per human use approval plan
	Evaluation	Collect data and evaluation-specific information in accordance with human use approval plan
WYDOT Pilot Safety Manager	Overall safety management	Maintain overall safety plan, risk register, conduct periodic safety meetings, conduct after action reviews, and provide corrective action reports. Coordinate with commercial fleet safety managers to have in place a method of communication should and incident occur. Also coordinate with fleet managers to understand safety needs for the fleets and drivers. Has verification responsibilities for commercial fleets and WYDOT fleets to ensure testing and safety management has happened.
WYDOT Highway Patrol	Emergency response	Provide emergency response and field support services for CV pilot participants in accordance to their existing operational responsibilities

5.4 Safety Management during Testing & Installation Phase (Infrastructure and Fleets)

During the hardware and software installation, turn up, and testing phase the Pilot Deployment Team will have additional safety management concerns. These will be presented from a software, vehicle, and infrastructure prospective. In addition to these specific safety areas, the Pilot Safety Manager will host monthly safety calls to discuss what is planned for the next six weeks for installations and how safety will be managed for these operations. This meeting will also cover an after-actions review of the previous month's operations with a critical eye for safety and what should be maintained and improved.

While testing and installing software the deployment team will leverage vehicle operators with advanced knowledge of the software and system so that as bugs are discovered they will not pose a greater danger to drivers and operators during the pilot. This will be done with a dedicated driver and separate developer/tester working in tandem for road tests. The pilot will also utilize simulation data to test application software in simulated/lab settings prior to on-road deployment. The pilot applications will be carefully architected to protect driver safety and reduce possible driver distraction by developing systems that factor in appropriate human factor considerations.

The software development process will follow an Agile development process to allow for backlog management, thorough testing plans (automated as well as user), and a strong focus on developing the right software to address the pilot requirements. It will be critical to have a deterministic approach to problem resolution and ensure future code releases don't re-introduce previously resolved issues.

While installing OBE in vehicles the pilot team will ensure that modifications to vehicles are engineered to protect the vehicle from damage (e.g., leaking where antennas are installed; power management for battery and alternator use; internal wire routing and sizing to protect from fire hazards; and shielding to prevent interference caused by radio waves with cellular, DSRC, and Global Positioning System (GPS) communications). The team will also need to be careful to ensure modifications and OBE do not come loose during vehicle movement to cause or worsen accidents. The OBE will need to be monitored, updated, repaired and verified during the pilot, these procedures will have to be done with quality assurances so that the drivers' safety is protected by vehicle modifications and loose equipment. This will be done by have a regimented process of installation and use a second person for inspection sign off.

During the installation of infrastructure to support RSE the safety of the installers and the traveling public will need to be protected from falling equipment on roadways, messages delivered to the traveling public during testing (not causing distracted driving or inaccurate messages), underground hazards (call before you dig and all other WYDOT standard operation procedures for road work), coordinated work zones prepared for traffic management during installations, and protections built in for data that traverses the RSE from abuse or misuse. The RSE will have to be monitored, updated and repaired with a consideration of safety for the workers, data and traveling public.

5.5 Safety Management during Deployment

During the deployment and operation phase, the system will still be dynamic and be in need of software updates, hardware upgrades, and repairs. Additionally, the users of the system will need training to use the applications and updates safely. The software updates will have to be carefully tested and vetted by the development team. This will require regression testing against automated tests, lab simulations and road tests. For updates that change the user interface or user interactions the pilot team will also need to vet the changes based on the approved human use approval plan.

Hardware repairs and upgrades (as well software/firmware updates that require physical access to the RSE), will have to follow the Standard Operating Practices for WYDOT repairs to ensure staff and public safety.

User training will be critical to have optimal effect for the CV Pilot. With proper training the driver will get the best use of the presented data from the CV Pilot. This data will be available via a hands free and eyes free interface to reduce driver distraction and the data will be post processed on the vehicle OBE to give the drivers an interface that will just provide very basic data allowing the driver to focus on the road.

The pilot team is looking at three basic levels of communication with the driver.

- Green: All is well or green.

- Yellow Warning: Basic problem (e.g., a bit above recommended speed, or wind is getting high for vehicle profile and weight).
- Red Alert: A real and imminent problem (e.g., nearby accident, ice in the road ahead, or high blow over risk.

The driver training will be a critical part to have the best response. The system will undoubtedly miss some alerts that should be given (false negative) and give alerts when little or no danger is actually present (false positive), so the drivers will need to understand the system to use it effectively and safely. Based on feedback from the user needs the driver interface system will need to work well with operators that have English as a second language and that are color blind.

5.5.1 System-Wide Fail-Safe Mode and Responses

The Pilot Deployment team recognizes no system is failure free. The team has identified components of the system that may function in a fail-safe mode during failures. To help mitigate these failures system monitoring will be used to reduce the length of time for failures. WYDOT electrical and telecommunications maintenance teams are available 24x7x365 for emergency repairs. WYDOT maintains a failover data center that provides critical services during outages of the primary data center and some levels of load balancing during times both data centers are available. Additionally, FIPS 140-2 level 3 devices will be used for RSE and Participating Truck/Snow Plow/Highway patrol equipment with HSM to harden the devices from bad actor compromise. The system wide failures, problems these failures will demonstrate, and mitigations that we are planning for are described below.

Table 5-2 – Failure Mitigation Approaches

Description of failure	Problems	Mitigation
Power or communications failure to RSE	V2I communications with RSE will fail from OBE Data will not be collected or propagated from infrastructure	OBE applications will gracefully degrade with lack of data by not alerting the driver, use previous data when still applicable, or re-establish communications over satellite or cellular. If appropriate notify driver of system communications failure.
Data center communications fails	RSE will not have data to send to OBE and will not be able to forward information from OBE to the Center	RSE will store data and forward it to the Center once it comes back on line, OBE will gracefully degrade with lack of data by not alerting the driver. If appropriate notify driver of system communications failure. If possible failover to redundant data center.

OBE sensor or application compromise	Bad data or no data from OBE for V2V and/or V2I	Develop smart applications to do data integrity checks before messages are sent, also have a services engine that receives messages and verifies integrity at the Center. Log problems for potential misuse, bad actor or failing equipment review.
RSE compromise	Data not processed to Center and/or OBE	Leverage SCMS certificates to validate messages and smart application to validate messages are within appropriate bounds

5.6 Deployment Closeout

While the Pilot components are expected to remain operational post the demonstration period, the nature of the operational elements may change with contractual changes and staffing changes. Similarly, the success of the Pilot may create new opportunities for advancing applications and bringing new partners to the fold. To maintain the continuity of the safety management plan, the safety manager will develop a post-demonstration update to the safety management plan that will identify approaches to bring new partners (fleet operators, new vendors, and consultants) to the same level of safety during the demonstration. These may include specific requirements that may be included in new vendor procurements, and maintenance of documented procedures and guides for installation and training modules for new fleet partners and drivers that are available at the end of the pilot.

6 Coordination with other Tasks

6.1 Task 2: Concept of Operations

Safety scenarios in this Safety Management Plan were developed based on the Pilot Deployment ConOps. The ConOps developed for ICF/ Wyoming Pilot Deployment documents the applications to be deployed and operational practices to be followed in phase 2. The safety operational concept was developed contingent on the proposed operational practice in the ConOps.

6.2 Task 3: Privacy and Security Management Operating Concept

The Privacy and Security Management Operating Concept provides guidance material in regards to security and privacy for the ICF/Wyoming Deployment Phase 1. The document is developed based on identifying the impacts of security breaches regarding confidentiality, integrity, and availability along with potential threats. Additional security analyses are included to cover V2V security, the SCMS, and CV application security needs. Major challenges such as SCMS integration and security for a complex system of systems are considered. The safety scenarios as well as safety operational concept were developed to protect the privacy of users, ensure secure operations, and eliminate the impact of security breaches.

6.3 Task 6: Pilot Deployment System Requirements

The Pilot Deployment System Requirements (SyRs) will identify and specify the requirements following established guidance such as those in the Federal Highway Administration's (FHWA) Systems Engineering for ITS. The requirements will be based on the user needs and system concept developed and documented in the ConOps as part of Task 2. The IEEE Standard 1233-1998, the IEEE Guide for Developing System Requirements Specifications, will be used as the general guide for documentation. Although the IEEE guidance allows significant flexibility in the structuring of requirements, the specification will use the common categories of functional, interface, performance, security, data, and reliability requirements. The end-product of this task will be a Stakeholder SyRS Review Panel (Draft and Final), a SyRs Document (Draft and Final), and a Walkthrough Workbook and Resolution report. Within this format the system requirements will be created to incorporate the Safety and Threat Analysis risks and risk response plan from Table 4-2.

6.4 Task 7: Application Deployment Plan

The Application Deployment Plan will map the identified systems requirements to the standard definitions of the applications as found in the CVRIA to determine the differences and changes in functionality required. It will additionally incorporate the defined risk response plan tasks defined in Table 4-2. During this phase, the impact of these changes in terms of development cost will be investigated. Also included in the application deployment plan will be a consideration of how to use the existing prototypes and software created as part of the Differential Mobility Analysis (DMA) program for the pilot. For the Wyoming pilot, the primary applications of interest are from the Intelligent Network Flow Optimization (INFLO) bundle and the Response, Emergency Staging and Communications, Uniform Management and Evacuation (R.E.S.C.U.M.E.) bundle but requirements from the V2I Safety program and the road weather management performance measurement prototype will be investigated as part of the application development plan.

6.5 Task 8: Human Use Approval Summary

The Human Use Approval Summary shall explain the procedures of protecting the privacy and confidentiality of the participants (e.g., how, where, and for how long the data will be stored; who will have access to the data; and other confidentiality issues). Risks to subjects should be described in detail of any reasonably foreseeable risks or discomforts to the subjects as a result of each procedure/experiment, including discomfort or embarrassment with survey or interview questions, exposure to minor pain, discomfort, injury, or harm from possible side effects from using research equipment. A description of the procedure to obtain informed consent or to provide information to participants will also be included in the proposal. As part of the proposal, we will define the actual consent forms, as well as a description of when and by whom the subjects will be approached, how information will be relayed to subjects, and how collected feedback should be submitted.

6.6 Task 9: Participant Training and Stakeholder Education Plan

The Participant Training and Stakeholder Education Plan divides its efforts between three objectives. For end-users, like the fleet drivers (be it snow plow operators or truckers), the emphasis will be on developing a level of comfort and understanding of the messaging provided to them in-vehicle. Participants may not be aware of the potential safety scenarios and the actions they are expected to take during emergency situations. Therefore, the safety management plan will be included as part of training plan as a key to prevent personnel injury and eliminate the potential impacts. We will develop an end-user training plan, consistent with the human use approval summary that will include training on the truck simulator maintained by the University of Wyoming. The simulator will also look at the concern of distracted driving and help gather feedback on the user-interface design in Phase II.

For stakeholders that are not direct end-users, like fleet managers, trucking association members, and DOT staff, the emphasis will be on demonstrating the value and the functionality of these systems. In accordance with the outreach plan in Task 11, training material will be prepared explaining the pilot objectives and how their operations benefit from the successful pilot. Finally, for partners who will be responsible for the demonstration, training manuals will be developed for different aspects of the system and integrated into existing plans and procedures used by the partners. For example, maintenance of DSRC radios will be factored into WYDOT's maintenance plans for ITS equipment.

6.7 Task 12: Comprehensive Pilot Deployment Plan

The Comprehensive Pilot Deployment Plan will build upon previous task reports and add information on the deployment and demonstration plan, data collection and sharing, performance measurement plan, and a detailed schedule and budget for subsequent phases. This comprehensive plan will be built to incorporate the risk response plan from Table 4-2. After approval of the Comprehensive Pilot Deployment Plan, a webinar will be developed to describe the Comprehensive Pilot Deployment approach to the public, including stakeholders in Wyoming, other CV pilots, and others as defined in the outreach plan.

7 Summary

This document presented the Safety Management Plan. It provides guidance material in regards to the identification of safety scenarios and risk mitigation for the ICF/Wyoming Deployment Phase 1. The document is presented based on identifying the safety scenarios at both system-level and application level, assessing the level of risk for each scenario, and providing a safety operational concept for high/ medium risk scenarios. Safety stakeholders were identified, existing safety plans were reviewed, and coordination with emergency responders were incorporated in the SMP.

The Pilot Deployment team identified and analyzed 14 potential hazard events. There were no ASIL hazard events identified, and none of the measures according to the ASIL as defined in ISO 26262 needed to be applied to achieve safety goals. Therefore, all potential risks will be handled and mitigated using the best practices of system engineering and project management principals during the design of the SPMD infrastructure installation and fleet builds. Coordination between the Safety Management Plan and other tasks was also discussed.

8 Notes and Glossary

The following table defines selected project specific terms used throughout this ConOps document.

Table 8-1 – Glossary of Terms

Term	Definition
Data Distribution	A support application that manages the distribution of data from data providers to data consumers and protects those data from unauthorized access.
Freight-Specific Dynamic Travel Planning	An application that provides both pre-trip and en-route travel planning, routing, and commercial vehicle related traveler information, which includes information such as truck parking locations and current status.
GIS/ITS Program	WYDOT's primary division responsible for ITS.
Location and Time	A support application that shows the external systems and their interfaces to provide accurate location and time to CV devices and systems.
Road Weather Information for Freight Carriers	An application that is a special case of the Road Weather Advisories and Warnings for Motorists application focuses on Freight Carrier users.
Situational Awareness	An application that determines if the road conditions measured by other vehicles represent a potential safety hazard for the vehicle containing the application.
Spot Weather Impact Warning (SWIW)	An application that will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts.
Telecom Program	WYDOT's Telecommunications Program is responsible for the statewide WyoLink radio system, most in-vehicle electronics integration, and various wireless networks including backhaul from roadside electronics devices and Wi-Fi hotspots.
Transportation Management Center (TMC)	Center that collects information and informs the public about changing travel conditions.
Warnings about Upcoming Work Zone	An application that provides information about the conditions that exist in a work zone to vehicles that are approaching the work zone.
WyoLink Radio Network	Statewide digital trunked VHF P-25 compliant public safety land mobile radio communications system, used for voice traffic and secondarily for low-speed mobile data communications.

Table 8-2 – Acronym List

Acronym/Abbreviation	Definition
A/C	alternating current
API	application programming interfaces
ASD	After-market Safety Device
ASIL	Automotive Safety Integrity Level
CAN	Controller Area Network
ConOps	Concept of Operations
CV	Connected Vehicle
CVRIA	Connected Vehicle Reference Implementation Architecture
D/C	direct current
DMA	Differential Mobility Analysis
DMS	Dynamic Message Signs
DSL	Digital Subscriber Line
DSRC	Dedicated Short Range Communications
DVI	Driver-Vehicle Interface
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FMCSA	Federal Motor Carrier Safety Administration
FMVSS	Federal Motor Vehicle Safety Standards
GIS	Geographic Information System
GPS	Global Positioning System
HAR	Highway Advisory Radio
HAZMAT	hazardous materials
HSM	Hardware Security Module
I-80	Interstate 80
INFLO	Intelligent Network Flow Optimization
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISD	Integrated Safety Device
ISP	Information Service Provider
IT	Information Technology

ITS	Intelligent Transportation System
IVBSS	Integrated Vehicle-Based Safety System
NHTSA	National Highway Traffic Safety Administration
NOC	Network Operations Center
NTCIP	National Transportation Communications for ITS Protocol
NWS	National Weather Service
OBE	on-board equipment
PID	personal information device
QM	Quality Management
RDCW	Road-Departure Crash Warning
R.E.S.C.U.M.E.	Response, Emergency Staging and Communications, Uniform Management and Evacuation
RSE	Roadside Equipment
RWIS	Road Weather Information System
SCMS	Security Credential Management System
SET-IT	Systems Engineering Tool for Intelligent Transportation
SLA	service level agreement
SPMD	Safety Pilot Model Deployment
SWIW	Spot Weather Impact Warning
SyRs	System Requirements
TMC	Transportation Management Center
UMTRI	University of Michigan Transportation Research Institute
USDOT	United States Department of Transportation
V2I	vehicle to infrastructure
V2V	vehicle to vehicle
VAD	Vehicle Awareness Device
VPN	Virtual Private Network
VSL	Variable Speed Limit
WAVE	Wireless Access in Vehicular Environments
WYDOT	Wyoming Department of Transportation

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

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-16-289

U.S. Department of Transportation