Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan – Tampa (THEA)

www.its.dot.gov/index.htm
Final Report — April 6, 2016
FHWA-JPO-16-313

U.S. Department of Transportation

Produced by
Tampa Hillsborough Expressway Authority (THEA)
Connected Vehicle Pilot Deployment Program Phase 1
U.S. Department of Transportation, ITS-JPO

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-16-313		

4. Title and Subtitle	5. Report Date
Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan – Tampa (THEA)	April 2016
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Sara Beresheim (HNTB), Steven Johnson (HNTB), Gregory Kreuger (HNTB), Joe Waggoner, Executive Director (THEA); Robert Frey, Planning Director (THEA)	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Tampa Hillsborough Expressway Authority 1104 East Twiggs Street, Suite 300 Tampa, Florida 33602	11. Contract or Grant No. DTFH6115R00003

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation ITS Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes

Govind Vadakpat, COR; Sarah H. Khan, CO

16. Abstract

This document presents the Safety Management Plan for the THEA Connected Vehicle (CV) Pilot Deployment. The THEA CV Pilot Deployment goal is to advance and enable safe, interoperable, networked wireless communications among vehicles, the infrastructure, and travelers' personal communications devices and to make surface transportation safer, smarter, and greener. The purpose of this document is to identify the major safety risks associated with the implementation of the THEA CV Pilot Deployment and lay out a preliminary plan to promote the safety of the participants and surrounding road users including pedestrians, bicyclists, and transit riders. The plan describes the potential safety risk scenarios identified related to the system and applications proposed, assesses the level of risk for each safety scenario using the Automotive Safety Integrity Level (ASIL) process defined by ISO 26262, and provides the safety operational concept for the THEA Connected Vehicle Pilot Deployment, including the functional safety requirements for the system and applications, the safety management proposed, and response plans.

17. Key Words	18. Distribution Statement
Intelligent Transportation Systems, Intelligent Vehicles, Crash Warning Systems, Connected Vehicle Pilot Deployment, Collision Avoidance, V2V, V2I, Vehicle Communication, Safety Scenario, Risk Assessment	No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	28	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

List of Tables

List of Figures

1 Safety Management Plan Documents

1.1 Referenced Documents

The following table lists the references used to develop the concepts in this document.

Table 1-1 References

#	Document (Title, source, version, date, location)
1	FHWA, USDOT, Broad Agency Announcement No. DTFH6115R00003, January 30, 2015.
2	THEA, Connected Vehicle Pilot User Oriented Concept of Operations, February 2016
3	THEA, Project Management Plan, October 2015.
4	THEA, The Connected Vehicle Pilot Deployment Program, Phase 1, March 2015
5	THEA, Privacy and Security Management Operating Concept (SMOC), March 2016
6	International Organization for Standardization, ISO 26262 Road vehicles – Functional safety, January 2011
7	What is the ISO 26262 Functional Safety Standard?, National Instruments, April 2014
8	City of Tampa Standard Operating Plan 23.2, Traffic Signal Timing, July 2015
9	City of Tampa Standard Operating Plan 23.2.1, Special Events, July 2015
10	City of Tampa Standard Operating Plan 23.4, Maintenance, July 2015
11	City of Tampa Comprehensive Emergency Operations Plan, February 2013
12	Tampa Bay Catastrophic Plan, September 2010
13	Hillsborough County Comprehensive Emergency Management Plan (HCCEMP), December 2014
14	State of Florida Emergency Operations Plan, October 2008
15	State of Florida Comprehensive Emergency Management Plan, 2014
16	FDOT, Contraflow Plan For The Florida Intrastate Highway System, June 2005

1.2 Version table

Table 1-2 Versions

Version	Amendments made	Author(s)	Date
Draft	Initial draft release for USDOT review and comment	THEA	2/15/16
Revision 1	Updated to reflect USDOT comments	THEA	3/15/16
Revision 2	Updated to reflect USDOT comments	THEA	3/28/16
Final	Updated to reflect USDOT comments	THEA	4/6/16

1.3 Safety management system document control

We will ensure our Safety Management Plan (SMP) documents are readable, identifiable and traceable to our activities.

In order to achieve this, our Safety Management Plan documents will be:

- reviewed by Jim Barbaresso, QC Reviewer, and revised where necessary.
- signed off as adequate by Jim Drapp, PE, Principal, QC/QC Manager.
- current and available in a secure, fireproof, air-conditioned centralized data center provided by team member HNTB.
- protected from unauthorized changes, deletion and publication and backed up to the data center on a nightly basis. The system includes built-in power supply and storage redundancies, both on local hardware as well as on the data center hardware. Additionally, there are hardware maintenance agreements in place with 24x7 coverage and 4 hour (clock hours) turnaround time, covering both local and data center hardware.
- controlled by Steven Johnson, CVP, Project Management Lead as to how and where.
- removed from circulation if obsolete or marked clearly that they are not to be used.

Archived copies and other safety-related records will be kept for seven years in a secure, fireproof, air-conditioned centralized data center provided by team member HNTB.

2 Introduction

2.1 Description

This section provides information about the Tampa Hillsborough Expressway Authority (THEA) Connected Vehicle (CV) Pilot Deployment and provides context to our Safety Management Plan.

2.2 Background

The THEA CV Pilot is funded by a federal grant awarded in September of 2015 by the United States Department of Transportation (USDOT, Joint Program Office (JPO)). The pilot is one of three selected from more than forty applicants and continues the efforts to generate a body of research data from tested utilization of CV applications to address real world issues impacting Safety, Mobility, Environment and Agency Efficiency. Phase 1 of the Pilot began in mid-September 2015 and will run for one year. If all approvals are granted, Phase 2 and 3 would run three more years until November 2019.

The THEA Pilot is based on traffic studies within the pilot area that identified six use cases; issues that can potentially be mitigated through the use of CV technology. These issues were chosen based on availability of historic data demonstrating current untreated scenarios, their impacts to the community, and the ability to measure the performance of the applied technology versus the current, untreated conditions.

The use cases selected for this Pilot are identified below along with their locations.

- The intersection of **Twiggs Street and Meridian Avenue at the entrance/exit to the Selmon Expressway Reversible Express Lanes (REL)** has long queues during the morning rush hour due to poor signal progression and right turns onto Twiggs immediately followed by a second right turn onto Nebraska Avenue. This causes the queue to back up onto the Selmon Expressway REL exit and into the curve where rear end crashes and other incidents are occurring. Potential CV technologies proposed for this location are V2I (i.e., Curve Speed Warning [CSW] and Intelligent Traffic Signal System [I-SIG]) and V2V (i.e., Emergency Electronic Brake Light [EEBL] and Forward Collision Warning [FCW]).
- The **Entrance/Exit point of the REL at Meridian Avenue and Twiggs Street** is a potential site for wrong-way entries. Wrong-way drivers have become a significant problem in the Tampa Bay area and are a major safety concern at the State level as well. Potential CV technologies proposed for this location are V2I (I-SIG and Probe Enabled Traffic Monitoring) and V2V (i.e., Intersection Movement Assist [IMA]).

- **Twiggs Street at the Hillsborough County Courthouse** has a mid-block pedestrian crossing combined with no protected left turn into the parking garage for the courthouse. This creates pedestrian safety issues as they traverse Twiggs Street. Additionally, pedestrians are crossing at unmarked locations, further complicating the pedestrian safety concern. Potential CV technologies proposed for this location are: V2I (Pedestrian in Signalized Crosswalk Warning, Mobile Accessible Pedestrian Signal, and I-SIG), and V2X (Smart Phone to Roadside Unit).
- Hillsborough Area Regional Transit Authority (HART) operates express, local and Bus Rapid Transit (BRT) routes **along and across the downtown city streets to the Marion Street Transit Station**. BRT routes offer efficiency gains in moving more people; however, during peak periods, the BRT service suffers from poor transit travel time and travel time reliability due to poor signal progression from heavy pedestrian and passenger vehicle volumes and passenger vehicles blocking access to bus stops. Potential CV technologies proposed for this location are V2I (Transit Signal Priority [TSP] and I-SIG).
- **The Amalie Arena/Channelside Drive Area** is a tourist destination and event area. Channelside Drive experiences many types of safety and mobility challenges due to being a part of morning and afternoon peak travel routes, special events, the streetcar trolley and stations and activities associated with the cruise terminal at the Port of Tampa. Depending on the time and day, at least two of the issues identified above have a negative impact on overall travel safety and mobility in the area. One critical potential for conflicts is the TECO Line Trolley that runs through this area. In many cases, the trolley runs parallel to vehicle lanes with a common approach to traffic control signals. The signal will be red for all vehicle phases during the trolley crossing. However, right turn on red is typically a legal move, which may cause a motorist, unaware of the trolley's presence, to turn right into the trolley's path. Similar scenarios occur with the significant pedestrian/bicycle traffic in this area. Potential CV technologies proposed for this location are V2I (I-SIG), V2V (Vehicle Turning Right in Front of Bus Warning), and V2X (Vehicle to Smart Phone).
- The **area of downtown Tampa from the Selmon Express Lanes along Twiggs Avenue to Marion Street and along Meridian Avenue to Channelside Drive** has a significant amount of queuing and congestion during the morning peak periods as well as during special events. Potential CV technologies proposed for this location are V2I (Probe Enabled Traffic Monitoring and I-SIG).

The purpose of the THEA CV Pilot Deployment is to improve the safety and mobility of users of the system. The implementation of the Pilot needs to be designed and implemented in such a manner as to ensure that the treatments being applied to the vehicles and the infrastructure do not cause undue safety issues. The purpose of this document is to identify the major safety risks associated with the implementation of the THEA CV Pilot Deployment and lay out a preliminary plan to promote the safety of the participants and surrounding road users including pedestrians, bicyclists, and transit riders.

There are thirteen main documents being developed in the planning phase of the THEA CV Pilot Deployment. In addition to the Safety Management Plan, they include: the Project Management Plan, the Pilot Deployment Concept of Operations, the Security Management Operating Concept, the Performance Measurement and Evaluation Support Plan, the Pilot Deployment System Requirements, the Application Deployment Plan, the Human Use Approval Summary, the Participant

Training and Stakeholder Education Plan, the Partnership Status Summary, the Deployment Outreach Plan, the Comprehensive Pilot Deployment Plan, and the Deployment Readiness Summary.

The Safety Management Plan is one of the initial documents that is being developed in the planning phases of the THEA CV Pilot. The plan is developed based on the use cases described above and defined in more detail in the Concept of Operations. The concepts developed in the Safety Management Plan will be incorporated in the remainder of the documents as described in a later section of this report.

3 Safety Risk Process and Approach

3.1 Introduction

This section describes the safety risk process for the THEA CV Pilot Deployment and the procedures we will use to manage safety risks.

3.2 Safety Risk Process and Approach

The THEA CV Pilot Deployment will take a structured approach to identifying the safety risks and mitigating those risks to help ensure the safety of the participants. This approach is on-going – as the pilot program proceeds from planning to design and implementation to operations and maintenance, it is likely that new safety risks will be identified and the safety risks currently identified will either be mitigated completely or their status will change. The process developed and utilized by the team will result in the risk assessment table being continuously updated and mitigation efforts identified and implemented throughout the project as needed.

The safety risk approach that has been developed and implemented is based on the following core principles:

- Safety risks are identified, assessed and controlled.
- Team members are involved in the safety management process.
- Technical experts are involved in the process of identification and assessment
- Safety risks and control measures are constantly monitored, and regularly reviewed.
- All team members, participants, contractors, and emergency response agencies will be informed of safety procedures.
- All equipment, software, processes, and interfaces are compliant with applicable regulations and tested before deployment.

An overview of the safety risk process is shown below in Figure 3-1. The safety risk process begins with identifying a potential safety scenario that may occur as part of the THEA CV Pilot Deployment. A risk assessment is then performed for each safety scenario. The risk assessment assigns a level of risk associated with each safety scenario. The safety scenarios developed and the risk assessment performed for the THEA CV Pilot are included in Chapter 5. If the safety scenario is rated as low risk, standard safety management practices are required to be followed. If the safety scenario is rated as medium or high risk, measures are taken to eliminate and/or minimize the risk by the steps detailed in Figure 3-1. The safety management procedures for the identified safety scenarios for the THEA CV Pilot are detailed in the following chapters. If a new safety scenario is identified during any phase of the THEA CV Pilot Deployment, this safety risk process will be completed for each new safety scenario identified.

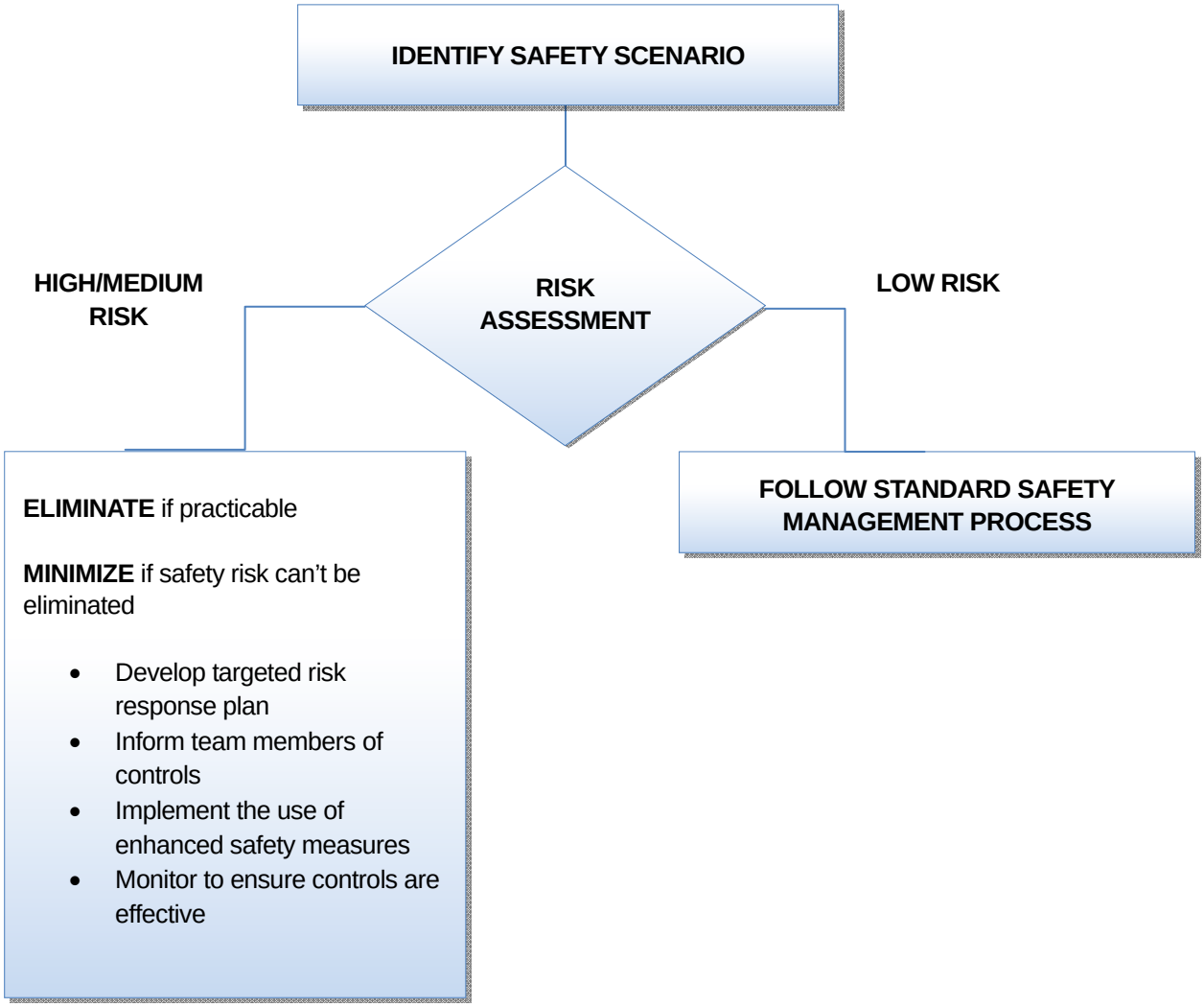

Figure 3-1 Safety Risk Process
Source: HNTB

3.2.1 Safety Risk Control

The THEA CV Pilot Deployment team has performed a preliminary safety risk analysis that is the basis of our initial mitigation strategy. The THEA CV Pilot Deployment team will manage and control each potential risk by taking all practicable steps to eliminate or minimize their potential impact. Controls may reduce the significance of a potential risk or the likelihood of it causing harm to participants or others. All of the identified safety risks have been added to the project risk assessment to ensure that each safety risk is identified, tracked, the potential impacts considered, and the necessary steps taken to implement the response plan at the appropriate time during the schedule. Risk managers will provide status updates on their assigned risks in the monthly status project team meetings when the meetings include their safety risk's planned timeframe. Upon the completion of the project, during the closing process, the Project Management Lead and Safety Manager will analyze each risk as well as the safety risk management process. Based on this analysis, the Project

Management Lead, Systems Development Lead, and Safety Manager will identify any improvements that can be made to the risk management process for future projects. These improvements will be captured as part of the lessons learned knowledge base.

The THEA CV Pilot Deployment team is using the Automotive Safety Integrity Level (ASIL) process to determine the level of safety risk associated with the deployment. ASIL is a risk classification scheme defined by ISO 26262. A risk assessment table, including each potential safety scenario, their identified ASILs, and risk response plans is included in Table 5-1.

3.2.2 Safety Risk Monitoring

The effectiveness of the safety risk controls will be monitored to identify and mitigate any unforeseen shortfalls. We ensure safety risk controls are effective and new safety risks are identified by:

- periodic checks during operation on the equipment, software, interfaces, and processes
- seeking information from participants
- reporting and reviewing incidents
- keeping up to date with best practices and lessons learned
- coordination with other CV Pilot sites
- coordination with identified emergency response agencies
- internal reviews
- regular safety communications and updates with the deployment team

Safety risk monitoring will be tracked and documented utilizing three main methods. The first type of monitoring deals with the communication and coordination with various parties and agencies. This will be documented during our monthly and bi-weekly coordination meetings, meeting minutes, and meeting notes. Safety reviews, such as periodic checks and internal reviews will be documented utilizing the methods detailed in Chapter 6 and the Safety Review Template included in Appendix B. Incidents will be reviewed following the procedures in Chapter 6 and documented utilizing the Incident Report Form in Appendix A.

4 Safety Stakeholders and Existing Risk Response Plans

4.1 Introduction

This section identifies the parties responsible for responding to the identified safety incidents within the areas of the THEA CV Pilot Deployment and describes their existing response plans that are applicable to the safety needs for the THEA CV Pilot Deployment. The Safety Manager will be responsible for ensuring these safety response stakeholders are informed about the deployment activities, protocols, and timeline. This will occur through the safety risk monitoring activities detailed in Chapter 3 and the procedures outlined in Chapter 6.

4.2 Identified Safety Response Stakeholders

The following safety response stakeholders have been identified for the THEA CV Pilot Deployment:

Table 4-1 Safety Response Stakeholders

Agency	Response Hours
HART/TECO Line Streetcar	Mon-Fri 6am-8pm, Sat-Sun 8am-5pm
City of Tampa (COT) Police	24x7
City of Tampa Fire Rescue	24x7
City of Tampa Emergency Medical Services (EMS)	24x7
Hillsborough County Sheriff's Office (HCSO)	24x7
Hillsborough County (HC) Fire Rescue	24x7
Hillsborough County Emergency Medical Services	24x7
Florida Highway Patrol (FHP)	24x7
THEA/COT Traffic Management Center (TMC)	Mon-Fri 5am-6:30pm
Florida Department of Transportation (FDOT) District 7 TMC	24x7
COT Traffic Operations and Maintenance	24x7
THEA Operations and Maintenance	Mon-Fri 5am-6:30pm

4.3 Existing Response Plans

4.3.1 Signal Equipment

The signal equipment hardware and software involved in the THEA CV Pilot Deployment is maintained and operated by the City of Tampa from the THEA/COT TMC. The City of Tampa monitors the condition and operability of the signal equipment and completes maintenance activities and repairs, as necessary. There is a phone number available to report any issues with damaged signal equipment or signals that are not functioning properly. Signal technicians are on standby 24x7 to respond to calls. Emergency calls after hours are dispatched through the Tampa Police Department. The City of Tampa receives these reports and responds accordingly as part of their standard policies and procedures under COT SOP 23.4. If a repair is too large for the available staff to handle, the City of Tampa utilizes a signal contractor that is contracted for quick-response emergency work. If signal equipment is damaged or malfunctioning, the existing fail safes and procedures will take effect, and participants are to follow Florida law in their driving procedures.

4.3.2 Signal Timing and Operation

The City of Tampa monitors the signal timings, operation, and progression of traffic through the signal system for the THEA CV Pilot Deployment from the Traffic Management Center centrally located within the heart of the THEA CV Pilot Deployment area. In the case of signal timing problems or poor progression, these issues are identified and timings are adjusted from the Traffic Management Center, as necessary. The City of Tampa signal technicians and retained contractor are on call to respond to operational issues just as they are for the signal equipment needs under COT SOP 23.2. All participants are required to follow Florida law in their driving procedures with respect to traffic signal timing. The participants will be directed to follow the indication on the traffic signal head during the participant training program.

4.3.3 System Security

The THEA Operations and Maintenance staff and the City of Tampa Traffic personnel maintain the security of the THEA system and the signal system, respectively. These agencies have existing system security protocols in place to ensure the data is secure and to prevent damage or interruption by bad actors or external forces. The THEA CV Pilot Deployment system security procedures are detailed in the Privacy and Security Management Operating Concept. This document includes provisions for secure data and continuity of operations for the system deployment. In the event of a security breach, the existing procedures for THEA and the City of Tampa will be followed along with the Privacy and Security Management Operating Concept for the THEA CV Pilot.

4.3.4 Collisions

If a participant vehicle or a pedestrian participant is involved in a collision, the parties involved in the crash will be directed to follow existing Florida law. If appropriate, 911 will be called for emergency response. The City of Tampa and Hillsborough County have all emergency services available 24x7 for crashes within their jurisdictional boundaries, and Florida Highway Patrol assists with law enforcement on Florida's interstates and toll facilities. The FDOT District 7 TMC provides support to assist with incidents after hours and on weekends on THEA's facilities. In the case of a participant crash, the participant will also call the number provided to them in the driver training; and the Safety Manager will assign someone from the deployment team to inspect the vehicle and THEA CV Pilot

Deployment equipment. The incident will be tracked and investigated utilizing the steps detailed in the Safety Incident Reporting section of this plan and it will be determined if any new mitigation measures need to be developed or if a new safety scenario needs to be added to the risk assessment table. If a participant is unable to notify the deployment team at the time of the incident, the event would be revealed during the next regularly scheduled data download and investigated accordingly. All crashes that occur within the deployment area will be evaluated during the annual safety assessment, and overall trends will also be analyzed.

4.3.5 Special Event Traffic

The Tampa Bay area experiences special events on a consistent basis that causes traffic to be rerouted or heavier than normal in certain areas. These typically include downtown Tampa, which is within the THEA CV Pilot Deployment limits, and the areas around Raymond James Stadium, the Mid-Florida Credit Union Amphitheatre, and the Florida State Fairgrounds, which are within the surrounding area of the THEA CV Pilot Deployment. The City of Tampa is responsible for a majority of the event routing, followed by Hillsborough County, and Florida Highway Patrol. These groups have existing special event plans, including COT SOP 23.2.1, that are followed for each of these areas and events, and 24x7 response capabilities. During special events, the existing procedures will be followed and the communication plan contained within the THEA CV Pilot Deployment Project Management Plan will ensure coordination with the Safety Manager. The communication plan will be followed to include all stakeholders and ensure the Safety Manager and deployment team are informed of all special events that may affect the THEA CV Pilot Deployment.

4.3.6 Emergency Evacuation

During an emergency evacuation, all of the identified safety stakeholders may be involved to some extent. Emergency evacuations affect the entire THEA CV Pilot Deployment limits and beyond. The City of Tampa personnel, Hillsborough County staff, Florida Highway Patrol, and THEA have existing evacuation plans, including the Hillsborough County Comprehensive Emergency Management Plan (HCCEMP), they have developed in coordination with each other, and 24x7 response capabilities. These groups have representatives that meet on a regular basis to keep the plans up to date and properly coordinated with all agencies involved. If the THEA CV Pilot Deployment area experiences an emergency evacuation during the deployment, the existing procedures will be followed and the communication plan will ensure open communication and coordination between the Safety Manager and response agencies. All participants will be required to follow guidance and evacuation information provided by these agencies as some of the emergency evacuation procedures may not be appropriate for the application (such as reverse flow on a freeway or toll road). Traffic control equipment such as signs, signals, and structures placed within a ten mile boundary from the coastline is designed and constructed in accordance with specific hurricane standards to maximize safety during major storms. All connected vehicle equipment installed in this area will be installed in accordance with those same hurricane standards. In the event of a major weather emergency (i.e. hurricane), the THEA CV Pilot Deployment team will inspect all infrastructure deployed on the roadway or within the right-of-way and will inspect the in-vehicle components on publicly owned fleet vehicles to ensure that the equipment did not sustain any damage during the event and that the installation is still secure.

5 Safety Needs

5.1 Identified Safety Scenarios

The intent of the safety scenarios is to identify and document potential safety risks associated with the THEA CV Pilot Deployment through a systematic analysis process that includes system hardware, software, interfaces, human behavioral factors, intended applications, operational environment, weather events, external factors, data security, user abilities, and infrastructure. The scenarios take into account the entire life of the project and are categorized as either system level or application level. The potential safety impacts of each scenario are then documented so mitigation measures may be developed. The initial analysis identified twenty-five potential safety risks for the THEA CV Pilot Deployment. These are listed in Table 5-1 at the end of this chapter.

5.1.1 System Level

Safety scenarios identified at the system level may apply to the entire deployment area or specific areas. The system level safety scenarios include: power outage; communication failure; external, malicious impacts on the system; heavy storms; hurricanes; emergency evacuation; and special events.

5.1.2 Application Level

Safety scenarios identified at the application level apply to the specific application selected and deployed. The application level safety scenarios include: bus rapid transit signal priority, signal progression, reversible express lanes, incorrect or non-issuance of warnings, trolley warning, improper installation, vehicle crashes, pedestrian detection, driver distraction, and driver misconception.

5.2 Risk Assessment

A risk assessment was performed for each of the identified safety scenarios. The intent of the risk assessment is to identify potential safety risks and analyze methods of response to eliminate safety risks from the design, or minimize the risks to the fullest extent possible. This can be achieved by reducing the probability of the safety risk occurring or minimizing the safety impact if exposure does occur.

An Automotive Safety Integrity Level (ASIL) is a risk classification scheme defined by ISO 26262. An ASIL was determined for all of the safety scenarios identified. To determine the appropriate ASIL level, the Exposure (E) Level, the Severity (S) Level, and the Controllability (C) Level for each safety scenario are assessed using the descriptions below. Using our roadways as a driver, passenger, bicyclist, pedestrian, or transit rider includes inherent risk. This evaluation takes into account any increased risk road users may experience as part of the THEA CV Pilot Deployment. Figure 5-1 depicts the ASIL classification procedure.

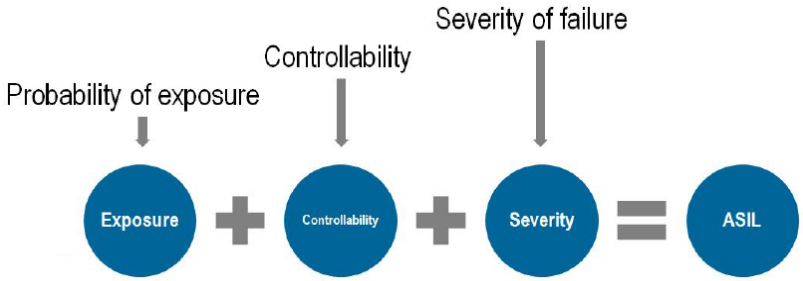

Figure 5-1 ASIL Process
Source: National Instruments

It should be noted that the risk assessment is an on-going effort throughout the life of the THEA CV Pilot. The THEA CV Pilot Safety Manager will be responsible for ensuring the deployment is continuously monitored to determine if the safety risks identified in the initial risk assessment have been accurately classified or fully mitigated. Additionally, if new safety risks are identified, the Safety Manager will ensure that they are assessed through the safety risk process detailed in Chapter 3, added to the safety risk assessment in Table 5-1, and appropriately classified.

5.2.1 Analysis of Likelihood

Exposure is defined as the probability of exposure to the situation associated with the safety scenario. To assign the appropriate exposure level for a scenario, the likelihood of the safety risk occurring is determined. There are four ASIL levels of exposure:

- E1: Extremely low probability
- E2: Low probability
- E3: Medium probability
- E4: High probability

For the THEA CV Pilot Deployment, the probability of exposure for each scenario was based on the frequency that similar events have occurred for similar equipment, conditions, and/or occurrences within the Pilot Deployment area. For example, the number of cases per year that the Pilot Deployment area typically experiences a heavy storm, hurricane, evacuation, special event, power outages, communication failures, etc. Also for similar devices and systems, the frequency of security failures, device errors, or system malfunctions was considered.

5.2.2 Analysis of Potential Impact

Severity is defined as the direct harm inflicted upon a person as a result of the safety scenario. To assign the appropriate severity level for a scenario, the potential level of injury is determined. There are four ASIL levels of severity:

- S0: No injuries
- S1: Light and moderate injuries
- S2: Severe and life-threatening injuries – survival probable
- S3: Life-threatening injuries – survival uncertain

For the THEA CV Pilot Deployment, the severity for each scenario was based on the level of injury most likely to be sustained as a result. This is based on historical trends for the Pilot Deployment area, including frequent crash types, crash rates, weather, typical travel speeds, and crime and injury statistics for the roadways within the THEA CV Pilot Deployment area. These preliminary ratings will be vetted for reasonableness and completeness with local safety stakeholders and those who are most familiar with the existing and planned operation when the design and operational details have been determined as part of our on-going safety management.

5.2.3 Analysis of Controllability

Controllability is defined as the ability to control the safety scenario once the person is exposed to the safety risk. To assign the appropriate controllability level for a scenario, the level of control we hold over the potential situation is determined. There are three ASIL levels of controllability:

- C1: Simply controllable
- C2: Normally controllable
- C3: Difficult to control or uncontrollable

For the THEA CV Pilot Deployment, the controllability for each scenario was based on the overall level control we have over the outcome for each scenario. While we cannot prevent weather events, evacuations, congestion, special events, security attacks, malfunctions, device failures, or outages from occurring, our training, prevention, and mitigation measures and response plans are under our control and exert influence the outcome of each safety scenario. The combination of these determines the level of controllability assigned.

These three dimensions were utilized to assign an ASIL to each safety scenario. Figure 5-2 depicts the method used to perform the ASIL decomposition.

Severity	Exposure	Controllability

		C1	C2	C3
S0	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	QM
	E4	QM	QM	QM
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 5-2 ASIL Decomposition
Source: ISO 26262

There are four ASIL ratings identified: ASIL A, ASIL B, ASIL C, and ASIL D. Safety risks that are identified as QM, or "Quality Management", do not require specific mitigation measures to be developed. These require a standard quality management system. Safety risks that are determined to be ASIL D have the highest safety risk and need the highest level of mitigation measures, while those that receive ratings of ASIL A have the lowest level of testing requirements per ISO 26262. Using the methodology illustrated above, none of the potential safety scenarios were classified as ASIL hazard events, therefore, generally accepted quality management practices are acceptable for the THEA CV Pilot Deployment. The quality management practices to be performed are detailed in Chapter 6 and include provisions for equipment procurement, device installation, a fail-safe system mode, quality training, safety management, safety reviews, and safety incident reporting and tracking.

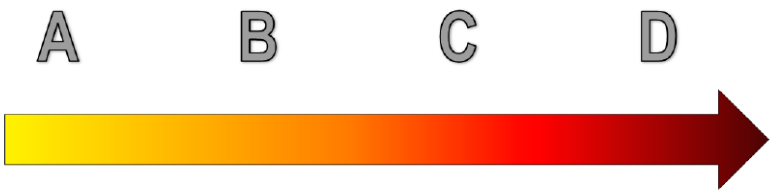

Figure 5-3 ASIL Ratings
Source: National Instruments

A national, multi-disciplinary team comprised of experienced professionals was assembled to identify and assess each safety scenario, and develop the corresponding safety risk response plans. The results of this safety risk process are detailed in Table 5-1 below. Table 5-1 details each safety scenario identified, the associated safety impacts anticipated, the safety risk response plan developed, the ASIL dimensions assigned, and the resulting ASIL rating.

Table 5-1 Summary of Risk Assessment

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
1	Application Level	The Bus Rapid Transit Signal Priority and Progression malfunctions causing poor progression and increased route times.	Safety of the transit users. Riders may be stranded at bus stop locations longer than anticipated without alternate transportation options. This may result in riders stranded unexpectedly at night in a dangerous situation.	Include lessons learned and best practices in the design. Perform reviews and verify communication software and equipment before deployment, including testing and checklists.	Bus driver participants will be provided a phone number to call any time to report issues and gain assistance. An estimated time of arrival will be provided to passengers as well as a phone number to call any time to report issues.	COT SOP 23.2 Vendor QM Plan (Section 6.1.1) HART, THEA, COT	S0	E2	C1	QM
2	Application Level	The signal progression malfunctions resulting in poorly coordinated signals and increased congestion.	Safety of the participant and nearby road users, including transit riders. Increased congestion and delay can result in increased risk-taking for drivers resulting in an increase in vehicular conflicts. With congestion comes longer than normal queues causing the potential for rear end collisions. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform reviews and verify software and equipment before deployment, including testing and checklists.	The Traffic Management Center monitors traffic progression and signal coordination continuously, and will respond with a quick response timing plan for any abnormal traffic congestion.	COT SOP 23.2 Vendor QM Plan THEA, COT	S1	E2	C1	QM
3	System Level	The system installed conflicts with the signal operation or malfunctions and causes the traffic signal to shut down.	Safety of the participant and other road users, including transit riders and pedestrians. Loss of communication would result in the failure of warnings to be issued when appropriate. The fail safe in the signal controller defaults to flashing operation if there is a malfunction. The conflict monitor within the signal cabinet prevents conflicting green signals from displaying. Complete loss of power results in the intersection to default to an all-way stop condition.	Ensure uninterruptible power supply units are installed at all signal controller cabinets with sufficient holdup time to implement response plan. Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	The Traffic Management Center monitors the traffic signal operation and will respond to a malfunction of the system. Driver Use Training, described in Section 6.1.4, will ensure the participants are informed that a dark signal should be treated as an all-way stop.	COT SOP 23.4 Vendor QM Plan THEA, COT	S1	E1	C1	QM
4	System Level	A heavy storm or hurricane results in damage to the signal equipment and power loss.	Safety of the participant and other road users, including transit riders and pedestrians. The fail safe in the signal controller defaults to flashing operation if there is a malfunction. The conflict monitor within the signal cabinet prevents conflicting green signals from displaying. Complete loss of power results in the intersection to default to an all-way stop condition.	Ensure signal equipment located within the 10-mile coastal boundary meets standards and uninterruptible power supply units are installed at all signal controller cabinets with sufficient holdup time to implement response plan.	The Traffic Management Center monitors the traffic signal operation and will respond to repair signal equipment. Driver Use Training will ensure the participants are informed that a dark signal should be treated as an all-way stop.	COT SOP 23.4 HCCEMP THEA, COT	S1	E2	C2	QM

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
5	System Level	A heavy storm or hurricane results in loss of communications and power to the CV system.	Safety of the participant and other road users, including transit riders and pedestrians. Loss of communication would result in the failure of warnings to be issued when appropriate. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists. Ensure uninterruptible power supply units are installed at all signal controller cabinets with sufficient holdup time to implement response plan.	The Traffic Management Center monitors the traffic signal operation and will respond to repair damaged signal equipment. Driver Use Training will reinforce that the warnings are based on MUTCD and Florida law takes precedence over lack of warning or incorrect warnings.	COT SOP 23.4 HCCEMP THEA, COT	S0	E2	C2	QM
6	System Level	An emergency event or hurricane results in evacuation and abnormal traffic routes, such as contraflow.	Safety of the participant and nearby road users. This may cause the driver to take a problematic route resulting in an unsafe situation. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Establish and follow communication plan that includes all parties. Ensure all relevant stakeholders are aware of the traffic plans in place for emergency evacuation.	Gates and emergency responders ensure contraflow points are well marked and wrong way entry blocked. Driver Use Training will ensure participants are instructed to follow marked emergency evacuation routes.	FDOT Contraflow Plan For The Florida Intrastate Highway System, HCCEMP THEA, COT, FDOT, FHP, HCSO	S1	E2	C2	QM
7	System Level	Events in the area such as hockey games, events at Amalie Arena, cruise ships in port, events at the convention center results in unusual routes and traffic patterns.	Safety of the participant and nearby road users, including pedestrians. This may cause the driver to take a problematic route resulting in an unsafe situation. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Establish and follow communication plan that includes all stakeholders. Ensure all relevant stakeholders are aware of the traffic plans in place for special events.	Driver Use Training will ensure participants are instructed to follow marked special event routes. Participants call a phone number any time for roadside assistance, in case of an accident or to report any issues.	COT SOP 23.2.1 THEA, COT, FDOT, FHP, HCSO	S0	E3	C1	QM
8	Application Level	Any device failure for any reason where device is not operating as user was instructed that it should.	Safety of the participant and nearby road users, including transit riders and pedestrians. This may cause driver distraction and/or misinformation which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Incorporate into the Driver Use Training and Informed Consent Form.	The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device repaired and report any issues.	Installation QM Plan (Section 6.1.2) Driver Use Training Vendor QM Plan THEA, COT, FHP, HCSO	S1	E1	C1	QM
9	Application Level	Incorrect information is provided to the participant concerning the current direction of the reversible lanes.	Safety of the participant and nearby road users. This may cause the driver to attempt to enter the reversible lanes in the wrong direction. However, the reversible lanes are blocked by gates at reversible access points to prevent wrong way entries, and special signing and pavement markings are present near each access point to direct motorists to the correct direction.	The current gate access system provides protection against wrong way entries onto the reversible lanes. Current system and fail safes must be maintained. Information concerning the direction of the reversible lanes must be correct and verified in communication plan.	Driver Use Training will ensure the participants are informed that the warnings are based on MUTCD and Florida law takes precedence over lack of warning or incorrect warnings. Participants are to follow the traffic controls on the roadway. Participants call a phone number any time for roadside assistance, in case of an accident or to report any issues.	Driver Use Training Installation QM Plan COT SOP 23.4 Vendor QM Plan THEA, COT, FHP, HCSO	S1	E1	C1	QM

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
10	Application Level	Improper installation causes device to issue incorrect warnings or issue warnings when no hazard is present.	Safety of the participant and nearby road users. This may cause driver distraction which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	Driver Use Training will ensure the participants are informed that the warnings are based on MUTCD and Florida law takes precedence over lack of warning or incorrect warnings. Participants are to follow the traffic controls on the roadway and report any issues.	Installation QM Plan Driver Use Training Vendor QM Plan THEA, COT, FHP, HCSO	S1	E1	C1	QM
11	Application Level	The device fails at a trolley crossing, failing to issue a warning when appropriate.	Safety of the transit users and nearby road users, including pedestrians. However, these are warning systems and the operator is still in control of the trolley and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	Reinforce within Trolley Driver Training to verify Signal Status message and to perform observations of pedestrians and nearby traffic. Participants are to follow the traffic controls on the roadway and report any issues.	Trolley Driver Training Installation QM Plan Vendor QM Plan THEA, HART, COT	S1	E1	C1	QM
12	Application Level	The device installed inside the cabin of the vehicle may detach and cause damage or harm in the case of a crash.	Safety of the participant. A minor increase to potential injury due to the relatively small size/weight of the device.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device reinstalled or report any issues.	Installation QM Plan THEA, COT, FHP, HCSO, HART	S1	E1	C1	QM
13	Application Level	Problematic location of on board unit device installation.	Safety of the participant and nearby road users. This may cause driver distraction or block the vision of the driver which could result in a crash.	Include lessons learned and best practices in the design, including human use factors. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists. Incorporate into participant training plan.	The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device reinstalled or report any issues.	Installation QM Plan THEA, COT, FHP, HCSO, HART	S1	E1	C1	QM
14	Application Level	The device installed inside the cabin of the vehicle detaches while the vehicle is in normal operation.	Safety of the participant and nearby road users. This may cause a driver distraction that may result in a crash. However, the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device reinstalled or report any issues.	Installation QM Plan THEA, COT, FHP, HCSO, HART	S2	E1	C2	QM
15	Application Level	The test vehicle and participant are involved in a severe (or any) accident, causing injury and/or damage to the device. The resulting damage to the device causes it to malfunction or be improperly placed within the vehicle.	Safety of the participant and nearby road users, including transit riders and pedestrians. Malfunction of the device and poor placement may cause driver distraction which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists.	Perform complete inspection of test vehicle including all reviews, testing, and checklists incorporated with initial installation after all accidents involving the test vehicle. The driver/pedestrian/ bicyclist to notify THEA TMC at time of incident or later if necessary. HART drivers to follow HART protocol to report incident.	Installation QM Plan THEA, COT, FHP, HCSO, HART	S1	E2	C2	QM

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
16	Application Level	There is a short in the equipment installed and causes overheating.	Safety of the participant or component failure including smoke inside the vehicle.	Include lessons learned and best practices in the installation design. Ensure properly sized fuses are utilized in the design and installation.	Participants call a phone number any time for roadside assistance, in case of an accident or stranding. The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get a repair and report any issues.	Installation QM Plan THEA, HART	S1	E1	C2	QM
17	Application Level	Improper installation causes device to drain the battery of the test vehicle.	Safety of the participant. The vehicle would not operate, resulting in the participant being without their primary means of transportation at the time and place of the malfunction.	Include lessons learned and best practices in the installation design. Perform design review of installation. Incorporate into driver training. Investigate cut-off device when battery capacity drops to a prescribed level.	Participants call a phone number any time for roadside assistance, in case of an accident or stranding. The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device reinstalled and report any issues.	Installation QM Plan THEA, HART	S1	E1	C1	QM
18	Application Level	The detection at the pedestrian crossings malfunctions failing to issue a warning to either a participating pedestrian or a participating driver.	Safety of the pedestrian. Failure to issue a warning may result in a pedestrian-vehicle collision. However, these are warning systems and the driver and pedestrians are still in control and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists. Incorporate into Driver Use Training to prepare drivers. Since the Pilot area is limited, participants will travel outside of the Pilot area frequently where hazards are present without warnings, keeping participants in the practice of traveling unassisted.	Driver Use Training and smart phone app training reinforce that the warnings are based on MUTCD and Florida law that takes precedence over lack of warning or incorrect warnings. Participants call a phone number any time for roadside assistance, in case of an accident, and to report any issues to get the device repaired. The incident will be reviewed throughout the Incident Review Process and additional Driver Use Training may be issued.	COT SOP 23.4 Vendor QM Plan THEA, COT	S1	E2	C1	QM
19	Application Level	Communication failure causes device to issue incorrect warnings or not to issue a warning when a hazard is present.	Safety of the participant and nearby road users. This may cause driver distraction which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform reviews and verify communication software and equipment before deployment, including testing and checklists. Reinforce within Driver Use Training and smart phone app training that the warnings are based on MUTCD and Florida law that takes precedence over lack of warning or incorrect warnings.	Participants are to follow the traffic controls on the roadway and report any issues. Participants call a phone number any time for roadside assistance, in case of an accident. The Informed Consent Form will include instruction details as to how to contact the THEA TMC, so the participant can get instructions on how to get the device repaired.	COT SOP 23.4 Driver Use Training Vendor QM Plan THEA, COT, FHP, HCSO, HART	S0	E1	C1	QM

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
20	Application Level	A misconception by the participant results in the participant believing the system takes control of the vehicle in case of a hazard.	Safety of the participant and nearby road users, including transit riders and pedestrians, which may result in a crash.	Incorporate into the Driver Use Training and Informed Consent Form that the driver is in full control of the vehicle and ultimately responsible to obey MUTCD and Florida law.	Participants call a phone number any time for roadside assistance, in case of an accident. Repeat any applicable Driver Use Training as a result of incident and Incident Review Process.	Driver Use Training THEA, COT, FHP, HCSO	S2	E1	C1	QM
21	Application Level	The driver is distracted by the device information and warnings.	Safety of the participant and nearby road users, including transit riders and pedestrians. This may cause driver distraction which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately.	Include human use lessons learned and best practices in the design and perform a design review of installation to prevent issues with driver distraction. Incorporate into Driver Use Training.	Participants call a phone number any time for roadside assistance, in case of an accident. Repeat any applicable Driver Use Training as a result of incident and Incident Review Process.	Driver Use Training THEA, COT, FHP, HCSO	S1	E2	C1	QM
22	System Level	The security of the system fails and the system is hacked into. The data flow is accessed by unauthorized personnel.	Personal information of the participant is stolen. This may result in the participant being targeted for a crime.	Include lessons learned and best practices in the security measures. Perform routine information security audits. Avoid collecting unnecessary or sensitive information from participants. Insure adherence to wireless message standards. Private vehicles have no identification (BSM). Public and commercial Vehicle Identification Numbers are authenticated (SRM).	The pilot is reliant on the SCMS to assist in the prevention of hacking the data stream. See the procedures in the SMOC for response to security threats.	SMOC THEA, COT, HART	S0	E2	C3	QM
23	System Level	The security of the system fails and the system is hacked into. This may result in false warnings or warnings not issued when appropriate.	Safety of the participant and nearby road users, including transit riders and pedestrians. This may cause driver distraction which could result in a crash. However, these are warning systems and the driver is still in control of the vehicle and must assess the situation and react appropriately. Inaccurate data may be provided to one or more of the participants devices fooling the device into thinking the location of another device is not where it is.	Include lessons learned and best practices in the design. Establish firewalls and install server compliant with industry standards and practices. Use tamper evident seals for the devices and utilize security measures for accessing equipment, such as locks on signal cabinets and building security at the TMC. Insure adherence to wireless message standards. Private vehicles have no identification (BSM). Public and commercial Vehicle Identification Numbers are authenticated (SRM).	The pilot is reliant on the SCMS to assist in the prevention of hacking the data stream. See the procedures in the SMOC for response to security threats.	SMOC THEA, COT, HART	S0	E1	C1	QM

ID Number	Level	Description	Safety Impacts	Safety Risk Response Plan			S	E	C	ASIL
				Prevention/Mitigation Measures	Safety Incident Response Plans	QM Plan/ Response Agencies				
24	Application Level	The participant becomes dependent upon the application to warn them of safety risks.	Safety of the participant and nearby road users, including transit riders and pedestrians. This may result in a crash if there is not a warning issued for a hazard and the participant has become dependent on the system for safety warnings.	Incorporate into Driver Use Training and Informed Consent Form that the driver is ultimately responsible to obey MUTCD and Florida law. Driver Use Training will inform participants Florida law takes precedence over lack of warning or incorrect warnings. Drivers will operate their vehicles outside of the Pilot area frequently where many hazards are present without warnings, which will decrease the likelihood of a dependency developing.	Participants call a phone number any time for roadside assistance, in case of an accident. Participants are to follow the traffic controls on the roadway. The incident will be reviewed throught the Incident Review Process and additional Driver Use Training may be issued.	Driver Use Training THEA, COT, FHP, HCSO	S2	E2	C2	QM
25	Application Level	The driver participant reacts to the warning messages in an undesirable way, such as hard braking, swerving, becoming distracted or startled and causing a crash.	Safety of the participant and nearby road users, including transit riders and pedestrians.	Driver Use Training and Informed Consent Form inform the driver they are ultimately responsible to obey MUTCD and Florida law. Include human use lessons learned and best practices in the design and perform a design review of installation to prevent issues with driver reactions.	Participants call a phone number any time for roadside assistance, in case of an accident. The incident will be reviewed throught the Incident Review Process and additional Driver Use Training may be issued, or issues addressed with the interface or installation.	Driver Use Training THEA, COT, FHP, HCSO, HART	S2	E2	C2	QM

6 Safety Operational Concept

6.1 Functional Safety Requirements

This section defines the functional safety requirements for the THEA CV Pilot Deployment. These are requirements to ensure safe operation of the application and the actions to be taken within the deployment to reduce the likelihood and potential impact for the safety scenarios. Since all of the safety scenarios identified resulted in ASIL QM, specific safety requirements are not necessary for each safety scenario. Standard quality management procedures will be followed.

6.1.1 Equipment Procurement

The THEA CV Pilot Deployment will utilize quality equipment by requiring all of the suppliers to provide and follow an approved quality management process in designing, constructing and producing their devices, referred to herein as a Vendor QM Plan. This will help to ensure the equipment provided is properly assembled to assist with safe operations in addition to device certification. If certification is not available by one of the three USDOT contracted certification bodies (Omni Air, DanLaw, or Layer7), manufacturer self-certification may be utilized. In this scenario, the acceptable QM plan for these devices will include the submission and approval of: test plans; test procedures; and test results. The manufacturers will also identify which other manufacturers their equipment in interoperable with. A safety review of the proposed operator interface will be performed. We will include lessons learned and best practices in the design. Safety checks for OBU's and RSU's will comprise the equipment reset functions, redundancy, security, and actions upon power loss and restoration. We will also ensure uninterruptible power supply units with sufficient holdup time to implement the response plans will be installed at all signal controller cabinets.

6.1.2 Device Installation

We will ensure that the equipment is properly installed to minimize the risks associated with equipment installation by requiring all of the installers to provide and follow a quality management process in installing the equipment. Installer/maintainers will be comprised of manufacturer approved vendors or THEA CV Pilot partner personnel who have been sufficiently trained by manufacturer approved vendors. We will include lessons learned and best practices in the installation procedures as part of the final documentation and we will coordinate with the other pilot sites in real-time to both share lessons that have been learned in the THEA CV Pilot Deployment as well as incorporating their lessons learned in the THEA CV Pilot. A design review of the installation will be performed and safety checks will be completed for the installation that consider the condition of the vehicle, bypasses, manual shutdown, security, possible overload conditions and a safety review of the proposed location of the on-board unit. We will verify installation before deployment, including specific end-of-line testing and checklists. The draft installation QM plan will be developed as part of the Application Deployment Plan and finalized during Phase 2 of the deployment once the design has been completed.

6.1.3 Fail-Safe System Mode

A fail-safe system mode will be provided for the THEA CV Pilot Deployment. This guarantees that in the event of a system failure, the system and devices will respond in a way that will cause no harm to the system, devices, participants, or other road users. It is a safeguard put in place that will not endanger lives or property if failure occurs. The design mitigates unsafe consequences of the system's failure. The THEA CV Pilot Deployment system default position may be the fail-safe mode in which the user does not receive any safety or mobility feedback from the unit and must drive unassisted. Therefore, in the event of a failure, the system and devices return to the default mode in which the participant will be familiarized with during the participant training program. The fail-safe system mode is presented in more detail in Pilot Deployment System Requirements. There are components of the existing system that currently have fail-safe modes (i.e. traffic signals). The THEA CV Pilot Deployment will not modify those existing systems in any way that would negatively impact the existing fail-safe mode or safety features.

6.1.4 Quality Training

All participants, system operators, system maintainers, installer/maintainers and owners of a response plan included referenced herein will receive adequate, approved training based on their point of interface with the system. This training will be documented as it occurs as part of the THEA CV Pilot Deployment. The participant training is referred to herein as the Driver Use Training, and will be included in the Participant Training and Stakeholder Education Plan.

6.2 Safety Management

This Safety Management Plan has been prepared to enable the THEA CV Pilot Deployment to advance and enable safe, interoperable, networked wireless communications among vehicles, the infrastructure, and travelers' personal communications devices and to make surface transportation smarter and greener in a safe manner, and to comply with applicable regulations.

The objective of safety management is to minimize safety risks associated with the THEA CV Pilot Deployment, including protecting access to the system and the participants' personal information, and minimizing the risk of participants being stranded or rerouted resulting in dangerous situations.

6.2.1 Safety Management Responsibilities

Gregory Krueger, PE is the Safety Manager with the responsibility of the ongoing overall safety management, including safety coordination for the following key areas:

- Leadership and direction in safety procedures
- Ensuring compliance with applicable regulations and the Safety Management Plan
- Incorporating safety into design, deployment, and operational phases
- Guidance for equipment procurement and acceptance
- Oversight for device certification, testing and installation
- Safety leadership for maintenance and updates

- Operational safety and monitoring
- Safety documentation and training
- Incident reporting, documentation, and investigation
- Maintaining and updating safety processes and the Safety Management Plan
- Safety coordination with other entities and task leads

6.2.2 Safety Reviews

Safety reviews support our focus on safety, ensure compliance with the Safety Management Plan, and identify opportunities to improve safety. *Regular* assessments help to identify any new safety risks and develop the appropriate control measures.

When we conduct safety reviews we will ensure that:

- reviews are conducted by the appropriate technical experts and team members
- opportunities for improvement are identified
- outcomes are communicated to the team members
- actions arising from reviews are implemented
- on-going monitoring is maintained to ensure that our operations comply with the Safety Management Plan

Reviews will be conducted at the following key points:

- Safety review for each project deliverable in phase 1 to determine if there are any impacts to the safety risk assessment and to ensure that any risks that can be mitigated through that deliverable are included
- Safety review of the design
- Design review before installation
- Safety review before deployment
- System security review before deployment
- Equipment, software and process check before deployment
- Periodic equipment, software, and process checks during operation
- Regular safety communications and updates
- Safety investigation after an incident
- Following a critical event or significant change that may impact safety
- After a complaint of a safety nature is received from participants, team members, or others
- Following a change in the applicable standards and codes of practices

6.2.3 Safety Incident Reporting

The intent of a safety incident reporting process is to identify improvements that can be made to prevent a recurrence of that incident. The following safety incident reporting policy will be followed.

- Safety incidents will be reported and recorded by the participants and team members using the draft Incident Report Form in the Appendix.
- Participants will receive guidance on safety reporting during their training.
- Safety incidents will be investigated and the underlying causes identified.
- Serious harm incidents will prompt a review of the Safety Management Plan.
- A regular review of all safety incidents occurs to identify any trends.

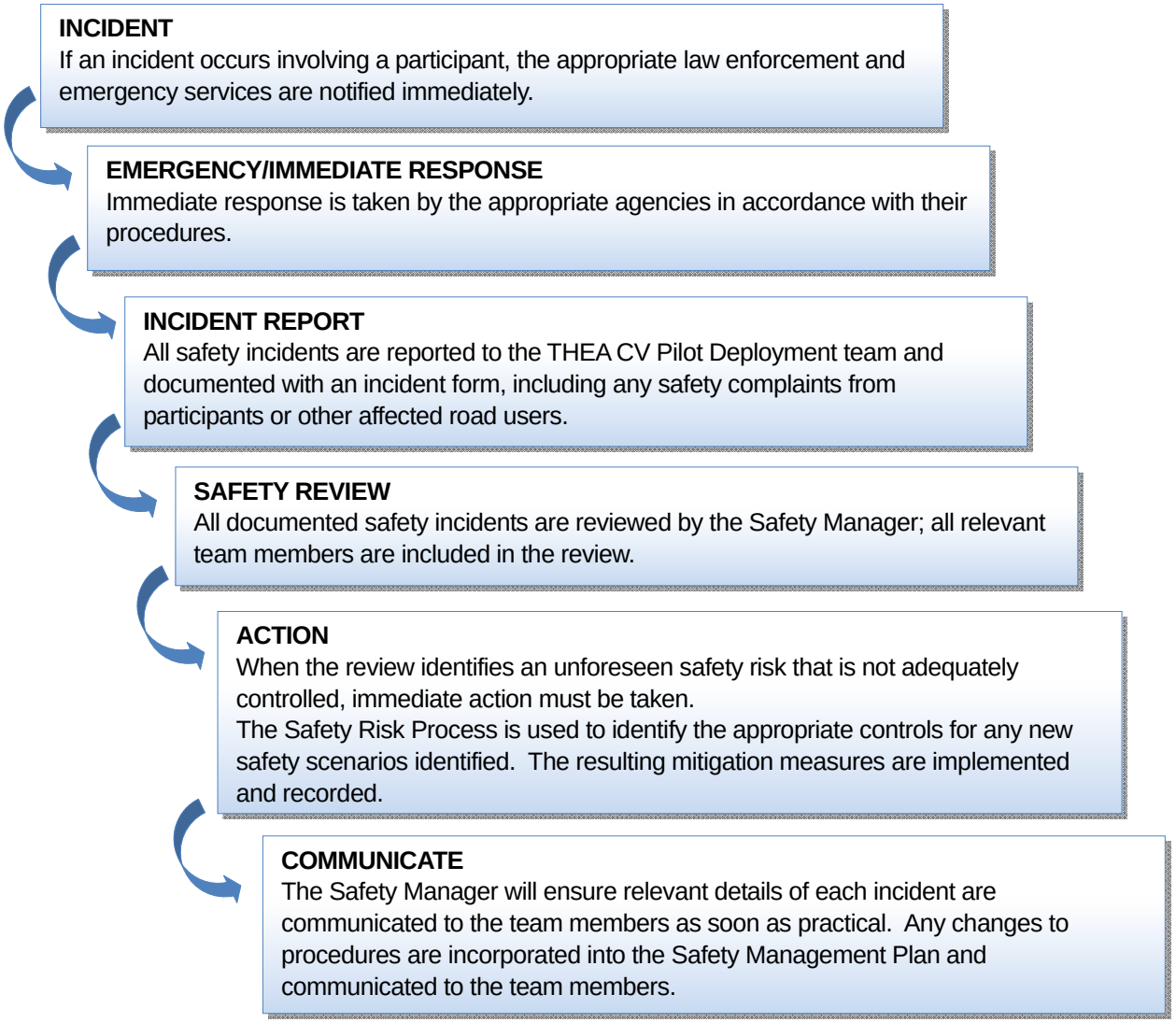

Figure 6-1 Safety Incident Process
Source: HNTB

7 Coordination with other Tasks

7.1 THEA CV Pilot Deployment Team Safety Responsibilities

This Safety Management Plan is one of the THEA CV Pilot Deployment documents developed early in the planning process. The safety needs and the safety operational concept detailed in this Safety Management Plan will be incorporated into the remainder of the program by the team members and task leaders. The task leads coordinate during the monthly progress meetings. THEA CV Pilot Deployment team responsibilities have been assigned as follows.

Steven Johnson, CVP, is the Project Management Lead and also responsible for the **Deployment Readiness Summary** which utilizes all of the previous tasks. He is responsible for developing the Quality Management Plan, the Risk Management Plan, Risk Register, and providing technical reviews for all phases.

Steve Bahler, PE is a QC Reviewer and also responsible for the Pilot Deployment **Task 2: Concept of Operations**. He will assist with detailed QC reviews and also ensure the **Concept of Operations** includes safety considerations. The Safety Management Plan utilizes the Concept of Operations to develop the safety scenarios based on the applications and technologies listed in the Concept of Operations, and the safety operational concept in the Safety Management Plan was developed associated with the proposed operational practice identified for the deployment in the Concept of Operations.

Dominie Garcia, PhD is responsible for the Pilot Deployment **Task 3: Privacy and Security Management Operating Concept** (SMOC) and ensuring it includes provisions for secure data and protection against unintentional or malicious bad actors or external forces. The Safety Management Plan utilizes the Privacy and Security Management Operating Concept to mitigate the safety risk for the safety scenarios that involve the privacy of the participants and security of the system since it describes the needs of the deployment to protect the privacy of the users and ensure secure operations.

Stephen Reich is responsible for the Pilot Deployment **Task 5: Performance Measurement and Evaluation Support Plan** and ensuring it includes safety in the performance measures and evaluation. The methods and processes detailed in the Performance Measurement and Evaluation Support Plan need to be consistent with the safety operational concept in the Safety Management Plan.

Steve Novosad is responsible for the **Task 6: Pilot Deployment System Requirements and Task 12: Comprehensive Pilot Deployment Plan** and ensuring they include provisions for safety. The Pilot Deployment System Requirements include functional requirements, interface requirements, performance requirements, and data requirements. One of the functional requirements are safety requirements, therefore, the safety operational concepts will be included in the system requirements. The Comprehensive Pilot Deployment Plan is comprised of material prepared from the previous tasks,

including the steps to be taken to ensure the safety and privacy of the participants and system security described in the Safety Management Plan.

Gustave Cordahi is responsible for incorporating safety considerations into the Pilot Deployment **Task 7: Application Deployment Plan.** The Application Deployment Plan will include a draft installation quality management plan for the deployment. The safety operational concepts developed that are application level safety scenarios will be included in the Application Deployment Plan.

Victor Blue, PE, PhD is the QA Coordinator and Back-checker and responsible for Quality Control and specifically for establishing implementing and monitoring the Quality Control Plan. The QA Coordinator will be responsible for ensuring the completeness of the technical review; will certify that each submittal has been prepared and checked in accordance with sound engineering practices and represents a quality product; and will certify that the project is in compliance with requirements cited in the Scope of Services. The QA Coordinator will monitor the project as it progresses. He is also responsible for the Pilot Deployment **Task 8: Human Use Approval** and ensuring it includes safety measures for the participants. The Safety Management Plan with safety scenarios and associated safety operational concepts are necessary to obtain Institutional Review Board (IRB) approval.

Mary Hamill is responsible for the Pilot Deployment **Task 9: Participant Training and Stakeholder Education Plan** that identifies the roles that participants will take during the deployment, their activities, responsibilities, and training requirements. The Participant Training and Stakeholder Education Plan will be consistent with the actions described in the Safety Management Plan to reduce the likelihood and potential impact of each safety scenario.

Figure 7 depicts the THEA CV Pilot Deployment team safety relationships and process.

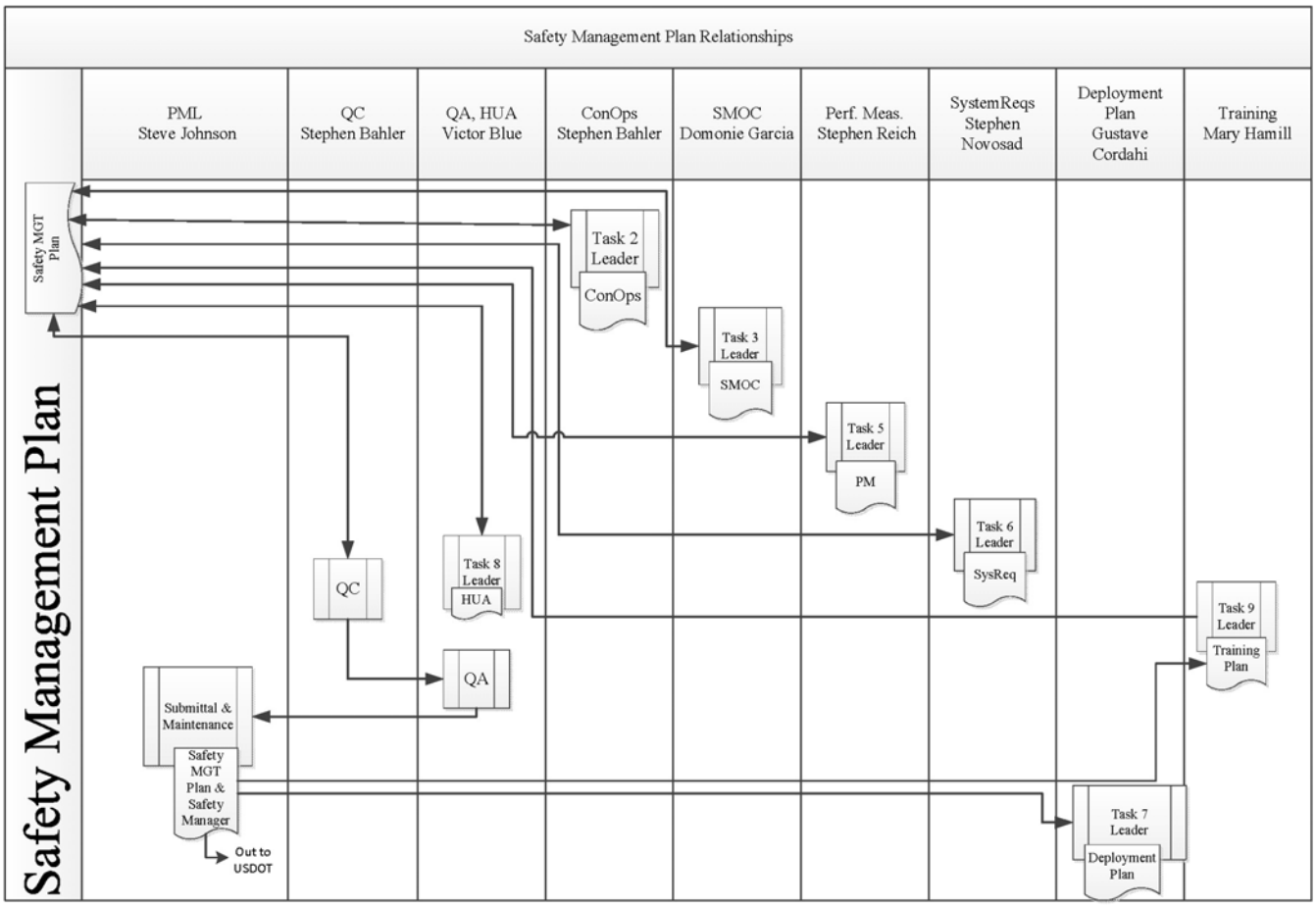

Figure 7-1 Safety Management Plan Relationships
Source: HNTB

Appendix A – Incident Report Form

Part A : (Safety Manager to complete with Participant)

Information about the person who had the incident:

Name:_____ Participant / Team Member / Visitor / Contractor *(please circle one)*

Participant's Mode of Travel *(Personal Vehicle/Bus/Trolley/Bicycle/Pedestrian)*:_____

Contact Telephone: Work:_____ Mobile:_____ Home:_____

What type of incident was it? *(please circle one)*

Near Miss Collision Property Damage Property Loss

When did the incident happen?

Date: **Time:**

Where did the incident happen?

Location:

What happened?

Description: *(include details of any device involved, other vehicles involved, property lost or damaged)*

Was a known safety hazard involved? *(please circle one)* YES NO

If **YES** – what was the safety hazard?

Names and contact information of any witnesses:

What injury or injuries were sustained, and to whom?	**Was law enforcement notified?**
Is this a serious harm injury? (*please circle one*) YES NO	**Name of agency:**
Was first aid or emergency care provided? (*please describe*)	

Declaration: The above report provides a true, accurate and complete account of the accident / incident / near miss / malfunction

_____ _____ _____

Participant Name *(please print)* Signature Date

Part B: (Safety Manager to complete with Participant)				
Were there any contributing factors to this incident?		**Safety Hazard Identification:** Is this a new safety hazard? YES NO It is a significant safety hazard? YES NO If **YES** identify the hazard management process to be done (eg: update risk register and put in **recommended actions** below)		
Recommended Actions		**Individual Responsible**	**By when**	**Date completed**
Has the Risk Management Process been completed for this safety scenario? YES NO (please circle)	What has been done?			
Is a review of Safety Management Plan required? YES NO (please circle)	Which part?			
Other Recommended Actions		**Individual Responsible**	**By when**	**Date completed**
Specific actions to prevent recurrence				
Specific actions to prevent recurrence				
Communications		**Individual Responsible**	**By when**	**Date completed**
All relevant team members and participants have received information regarding the incident, changes of operation / procedures.				
Was the incident related to a malfunction of the device or system? *(please circle)* YES NO If yes, describe the malfunction. Was the incident related to an issue with the installation of the device? *(please circle)* YES NO If yes, describe the installation issue.		**Overall comments**:		

Safety Manager's Name *(please print)* _____ Signature _____ Date _____

Appendix B – Safety Review Template

Safety Review Template

Name of Reviewer:_____ **Date of Review:**_____

What type of review was it? *(document, deliverable, deployment, etc)*

Purpose of the review: *(General Safety Review, Pre-Installation/Deployment Review, Equipment Check, Periodic Check, etc)*

Version of the Risk Assessment that was used:

Revision: ***Date:***

Review Notes:

Were there any new safety issues identified? *(please circle one)* YES NO

If **YES** – Describe the issue:

If **YES** – Describe recommended mitigation action:

Were any new safety issues identified that should be included on the risk register for future reviews? *(please circle one)* YES NO

If **YES** – What was the issue identified?

If **YES** – Has the Safety Manager (or deputy safety manager) been contacted to include the risk? *(please circle one)* YES NO

_____ _____ _____

Name *(please print)* Signature Date

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-16-313

U.S. Department of Transportation