USDOT Guidance Summary for Connected Vehicle Deployments

Safety Management

www.its.dot.gov/index.htm
Final Report – July 2016
Publication Number: FHWA-JPO-16-340

U.S. Department of Transportation

Produced by Noblis, Inc.
U.S. Department of Transportation
Intelligent Transportation Systems (ITS) Joint Program Office

Notice

Cover photo courtesy of ITS JPO Module 13 ePrimer Presentation (Connected Vehicles)

Technical Report Documentation Page

1. Report No. **FHWA-JPO-16-340**	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle USDOT Guidance Summary for Connected Vehicle Deployments: Safety Management		**5. Report Date** July 2016 **6. Performing Organization Code**
7. Author(s) Peiwei Wang (Noblis)		**8. Performing Organization Report No.**
9. Performing Organization Name And Address Noblis 600 Maryland Ave., SW, Suite 755 Washington, DC 20024		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH61-11-D-00018
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code** **HOIT-1**
15. Supplementary Notes Work performed for: Kate Hartman (ITS JPO, CV Pilots Program Manager)		

16. Abstract

This document provides guidance material in regards to safety management plan for the CV Pilots Deployment Concept Development Phase. This guidance provides key concepts and references in developing the Safety Management Plan in Task 4, lists relevant deliverables and the required elements in each deliverables, identifies key challenges the site deployers may encounter with respect to Task 4, and provides a summary of USDOT sponsored technical support events.

This document does not replace or alter the work statement defined in the Broad Agency Announcement (BAA); rather it provides technical guidance to the pilot deployers in completing the tasks and deliverables described in the statement of work.

17. Key Words Connected vehicles, Safety scenario, Emergency response, Risk Assessment	**18. Distribution Statement**

19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 16	**22. Price**

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

Table of Contents

1 Introduction 4

1.1 Purpose of the Report 4

1.2 Organization of the Report 4

2 Background 5

2.1 Development Process 5

2.1.1 Safety Scenarios 5

2.1.2 Risk Assessment 6

2.1.3 Safety Operational Concept 7

2.2 Key References 8

3 Deliverables 10

3.1 Task 4: Safety Management Plan 10

3.2 Relevant Tasks 10

3.2.1 Task 2: Concept of Operations 10

3.2.2 Task 3: Privacy and Security Management Operating Concept 11

3.2.3 Task 6: Pilot Deployment System Requirements 11

3.2.4 Task 7: Application Deployment Plan 11

3.2.5 Task 8: Human Use Approval Summary 11

3.2.6 Task 9: Participant Training and Stakeholder Education Plan 11

3.2.7 Task 12: Comprehensive Pilot Deployment Plan 11

4 Key Challenges 12

4.1 Risk Assessment 12

4.2 Site-Specific Safety Plan 12

4.3 Local Support 12

4.4 Reaction of Participants 12

5 Technical Support Summary 13

References 14

Appendix: List of Acronyms 16

List of Figures

Figure 2.1. Safety Plan Development Process (Source: Noblis, 2015)..... 5

List of Tables

Table 2-1. ASIL Determination (Source: ISO 26262 Part 3: Concept Phase) 7
Table A-1: List of Acronyms 16

1 Introduction

1.1 Purpose of the Report

The purpose of this report is to assist Pilot Deployers in the timely and successful completion of Concept Development Phase deliverables. This includes a synthesis of considerations in key topic areas (e.g., Safety), additional background and guidance materials potentially helpful to the preparation of Concept Development Phase deliverables, and a summary of available technical support resources available to CV Pilots sites. This report covers safety management that may emerge during the pilot deployment and measures that can be taken to ensure a smooth and efficient Concept Development Phase. Using the framework laid out in this report allows for a structured *Safety Management Plan* deliverable.

This document does not replace or alter the work statement defined in the Broad Agency Announcement; it provides technical assistance to the pilot deployers in completing the tasks and deliverables described in the statement of work.

1.2 Organization of the Report

This report contains four additional sections and a references section. Section 2 provides a general background to the concept of safety management plan development process. This includes key concepts to consider, and the most useful references which can be used to learn about safety management. Section 3 walks through the relevant deliverables and how each task must take safety into consideration for a successful draft and final Concept Development Phase *Safety Management Plan*. Section 4 summarizes the key challenges that may arise when dealing with safety in the CV pilots, including methods that can be used to overcome them. Section 5 provides a technical support summary of technical support events provided by USDOT. Finally, documents listed in the Reference section are provided with the URL links if they are available online.

2 Background

The Safety Management Plan (SMP) identifies Safety Scenarios related to the applications and technologies selected for the Pilot Deployment and develops a Safety Operational Concept that describes the actions expected to be taken within the deployment to identify safety scenarios and reduce the likelihood and potential impact of each safety scenario. A safety manager who is responsible for safety management affairs of the deployment site is recommended.

2.1 Development Process

Figure 2.1 illustrates the process of developing a safety plan for a connected vehicle pilot deployment site:

- identify safety scenarios at both system level and application level,
- assess level of risk for each safety scenario, and
- develop a safety operational concept for each scenario if it is identified as high/medium risk.

The following subsections describe the key concepts in Task 4 and provide recommended approaches and examples.

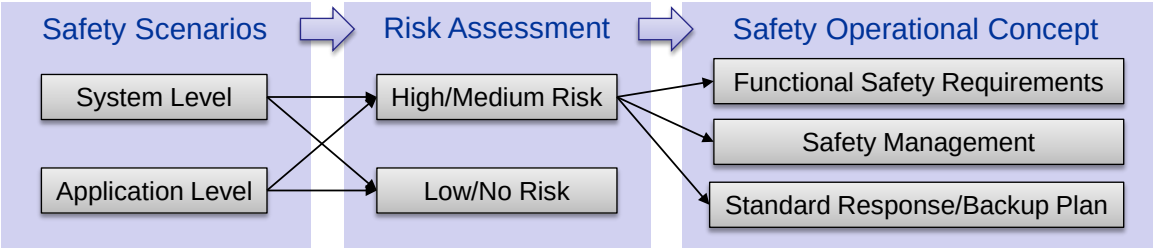

Figure 2.1. Safety Plan Development Process (Source: Noblis, 2015)

2.1.1 Safety Scenarios

Safety Scenarios could be at system level or at application level. Each site deployer will identify its own safety scenarios based on the applications selected and the site, such as geographical and weather related features. Some system-level scenarios are generic and may be applied to all sites, such as power outage, communication failures, system hacks or severe accidents. Other system-level scenarios are unexpected events related to weather or geographical features, such as heavy storms, earthquakes or hurricanes.

Application-level safety scenarios are related to the application selected and deployed. For example, when deploying freight-related applications, one needs to consider a safety scenario of hazardous product delivery. When an application malfunctions, if it involves safety concerns, such as pedestrian crossing detector malfunctions, this scenario will be included in the safety plan. The examples listed here are not an exhaustive list. Each site deployer will develop its own safety scenarios that fit the site and selected applications and technologies.

2.1.2 Risk Assessment

In order to address the most critical safety scenarios, the site deployers will select one risk assessment approach to identify the level of risk associated with the Pilot Deployment. ISO 26262 ASIL is a recommended risk assessment approach listed in the BAA. Other approaches may also be used to identify the level of risk. Depending on the familiarity and suitability, each site deployer will select a risk assessment approach for this task. The nature of these assessment processes will be dependent on the applications selected and the nature of the specific safety risks.

ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems. Automotive Safety Integrity Level (ASIL) refers to an abstract classification of inherent safety risk in an automotive system or elements of such a system. ASIL classifications are used within ISO 26262 to express the level of risk reduction required to prevent a specific hazard, with ASIL D representing the highest and ASIL A the lowest. The ASIL assessed for a given hazard is then assigned to the safety goal set to address that hazard and is then inherited by the safety requirements derived from that goal. ISO 26262 ASIL was also used in the Safety Pilot Model Deployment Program[1] to identify the level of risk. In order to qualify a safety scenario that would be governed by ISO 26262, the event analysis must result in an ASIL level A, B, C or D. The ASIL level is derived using the following 3 attributes:

- 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
- Classes of probability of exposure regarding operational situations
    - E1: very low probability;
    - E2: low probability;
    - E3: medium probability; and
    - E4: high probability
- Classes of Controllability
    - C1: simply controllable;
    - C2: normally controllable; and
    - C3: difficult to control or uncontrollable

Using the ASIL determination table shown in Table 2.1, four ASILs are defined: ASIL A, ASIL B, ASIL C and ASIL D, where ASIL A is the lowest safety level and ASIL D the highest one.

[1] http://www.its.dot.gov/safety_pilot/

Table 2-1. ASIL Determination (Source: ISO 26262 Part 3: Concept Phase)

Severity Class	Probability Class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Where:

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

In terms of these classifications, an ASIL D hazardous event is defined as an event having reasonable possibility of causing a life-threatening or fatal injury, with the injury being physically possible in most operating conditions, and with little chance the driver can do something to prevent the injury. That is, ASIL D is the combination of S3, E4, and C3 classifications. A hypothetical uncontrollable (C3) fatal injury (S3) hazard could be classified as ASIL A if the hazard has a very low probability (E1). The ASIL level below A is the lowest level, QM. QM refers to the standard's consideration that below ASIL A, there is no safety relevance and only standard Quality/Safety Management processes are required[2].

2.1.3 Safety Operational Concept

Safety Operational Concept describes the actions expected to be taken within the deployment to reduce the likelihood and potential impacts in each safety scenario. Mitigating actions taken at various times and locations will be identified for each safety scenario. The Safety Operational Concept also describes a *fail-safe system mode* and associated stakeholder response that can be deployed as a default in the case of unanticipated safety-related events. *Fail-safe system mode* means that a device or a system will not endanger lives or property when it fails. For example, when power outage occurs, traffic signal lights become yellow and red flash lights.

[2] https://en.wikipedia.org/wiki/ISO_26262

According 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. In the Pilot Deployment, functional safety requirements is to ensure safe operation of the application and safety management is to incorporate safety from concept development to monitoring operations. The key management tasks are to plan, coordinate and track the activities related to functional safety.

Some safety scenarios can be addressed or mitigated by the existing response procedures. For example, each state/local agency has its own Emergency Transportation Operations (ETO) plan developed. In this safety operational concept, when a severe accident, a natural disaster or a planned special event occurs, the site deployer will follow the plan developed by the state or local agencies. At the application level, for example, when freight-related applications are selected, the safety operational concept will consist of emergency response procedures for dangerous goods/hazardous materials transportation incidents.

For other identified safety scenarios, the site deployer will develop backup plans to either shut down the deployment so the site is back to the pre-deployment status, or provide a backup detection/ warning system. For example, a pedestrian detection system is planned to be installed at the deployment site. If the risk assessment results show that the risk level is high, another detection technology may be selected as a backup detection system.

2.2 Key References

International Organization for Standardization, ISO 26262 Road Vehicles - Functional Safety

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43464

ISO 26262 can be found and purchased on the ISO website. The ASIL Determination Table (Table 1) and the associated terminologies are listed in Part 3, Concept phase. The Safety Pilot Model Deployment, Test Conductor Team Report discusses how the ISO26262 ASIL was adapted for use in the Safety Analysis and Threat Assessment Plan of the Safety Pilot Model Deployment Program.

USDOT Federal Highway Administration, Emergency Transportation Operations

http://www.ops.fhwa.dot.gov/eto_tim_pse/

http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v6.pdf

Federal Highway Administration (FHWA) sponsored research and the publications of Emergency Transportation Operations (ETO) can be found on the Office of Operations website. The website features information on the ETO for Disasters, Traffic Planning for Special Events (PSE) and Traffic Incident Management (TIM) programs. Through the ETO programs, FHWA provides tools, guidance, capacity building and good practices that aid local and State DOTs and their partners in their efforts to improve transportation network efficiency and public/responder safety when a non-recurring event either interrupts or overwhelms transportation operations. Transportation Research Board (TRB) also published a report titled *Guide for Emergency Transportation Operations* to identify and consolidate related needs and practices to improve management of transportation-related emergencies.

USDOT Federal Emergency Management Agency, Operational Lessons Learned in Disaster Response

http://www.usfa.fema.gov/downloads/pdf/publications/operational_lessons_learned_in_disaster_response.pdf

U.S. Federal Emergency Management Agency (FEMA) released *Operational Lessons Learned in Disaster Response* in June 2015. The report can be found at the FEMA website. The report lists the key factors to successfully response and recover from emergency situations, the key response agencies and their roles, and lesson learned from the past events. The site deployer could refer to the document when developing the safety operational concept.

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

Pipeline and Hazardous Materials Safety Administration (PHMSA) produces and distributes the Emergency Response Guidebook (ERG) for use by firefighters, police, and other emergency services personnel who may be the first to arrive at the scene of a transportation incident involving a hazardous material. It is primarily a guide to aid first responders in quickly identifying the specific or generic classification of materials involved in an incident and protecting themselves and the general public during the initial response phase of an incident. The ERG is updated every three to four years to accommodate new products and technology. Part of the update process includes soliciting feedback from stakeholders through a Federal Register notice concerning the necessary updates.

3 Deliverables

This section describes each individual deliverable by task as explained in the CV Pilots Broad Agency Announcement. While the main deliverable dealing with safety is the *Safety Management Plan* of Task 4, elements of safety management may need to be developed for other deliverables in a number of other tasks. Below are each of the tasks which could include safety concerns. While the examples are not comprehensive, they should give a baseline for what may be considered safety sensitive.

3.1 Task 4: Safety Management Plan

In the BAA, under Task 4, it states:

> ***Safety Needs.*** ***The Contractor shall develop a set of Safety Scenarios related to the applications and technologies selected for the Pilot Deployment. These scenarios shall include an analysis of likelihood and potential impact. Potential mitigating actions taken at various times and locations shall be identified for each scenario. A set of Safety Needs shall be derived from this scenario-based analysis. The Contractor shall identify levels of safety risk associated with the Pilot Deployment, using established processes where possible, (e.g., ISO 26262 ASIL). The nature of these assessment processes will be dependent on the applications selected and the nature of the specific safety risks.***
>
> ***Safety Operational Concept.*** ***The Contractor shall develop a Safety Operational Concept that describes the actions expected to be taken within the deployment to reduce the likelihood and potential impact in each safety scenario. The Safety Operational Concept shall also include a description of a fail-safe system mode and associated stakeholder response that can be deployed as a default in the case of unanticipated safety-related events.***
>
> ***The Contractor shall deliver a draft version of the Safety Management Plan to the COR for review. The Contractor shall prepare a revised document in response to the COR's comments. The COR must accept and approve all comment resolutions before the revised report is considered final.***

3.2 Relevant Tasks

3.2.1 Task 2: Concept of Operations

The *Pilot Deployment Concept of Operations* (ConOps) documents the applications to be deployed and operational practice identified for the deployment site. Safety scenarios will be developed based on the applications and technologies listed in the ConOps. The safety operational concept will also be developed associated with the proposed operational practice in the ConOps.

3.2.2 Task 3: Privacy and Security Management Operating Concept

Task 3 describes the underlying needs of the Pilot Deployment to protect the privacy of users, ensure secure operations, and outline a concept that addresses these needs. One of the safety scenarios could cover the case when privacy or security systems are hacked. This situation could result in personal information being stolen or unreliable messages being sent out through the system and causing a safety issue. A safety operational concept should be developed to eliminate the impact of this safety issue. The concept will also be included in the concept of Task 3.

3.2.3 Task 6: Pilot Deployment System Requirements

Task 6 follows the guidance in IEEE Standard 1233-1998 to include functional requirements, interface requirements, performance requirements, and data requirements. Safety requirements are listed as one of the functional requirements. All the safety operational concepts developed in Task 3 will be included in the system requirements to ensure their inclusion during the installation and deployment phases.

3.2.4 Task 7: Application Deployment Plan

Task 7 describes the additional functionality and/or performance elements required to further develop, tailor, and integrate applications for use within the Pilot Deployment. The safety operational concept associated with application-level safety scenario will be included in the application deployment plan to ensure its inclusion during the installation and deployment phases.

3.2.5 Task 8: Human Use Approval Summary

Task 8 summarizes human use approval regarding human participation within the Pilot Deployment. Safety is the primary factor when dealing with human subjects in scientific trials. Safety scenarios and the associated safety operational concepts need to meet the human use approval. A safety management plan is one of the supporting documents necessary to obtain institutional Review Board (IRB) approval.

3.2.6 Task 9: Participant Training and Stakeholder Education Plan

Task 9 identifies the roles that participants will take during the pilot deployment, including a rough description of their activities and responsibilities, and likely training requirements needed to ensure as-planned execution of the pilot deployment in the operational phase. In the BAA, it states that "*this plan shall be consistent with the outcomes and plans associated with both the Human Use Approval Plan (Task 8) and Safety Management Plan (Task 4).*" The training requirements will include the training of actions expected to be taken within the deployment to reduce the likelihood and potential impact in each safety scenario, as the actions could be the actions of the site safety manager or the participants.

3.2.7 Task 12: Comprehensive Pilot Deployment Plan

The final Comprehensive Pilot Deployment plan is the culmination of the material prepared from tasks 2-11. In the BAA, it states that "*The plan shall describe the steps to be taken to ensure the safety and privacy of participants, and steps to be taken to ensure system security*." Therefore, any safety concerns throughout the entire CV pilot deployment should be covered in this deliverable.

4 Key Challenges

The major challenges in safety management include identifying and estimating the level of safety risk properly, coordinating with various local agencies when executing safety operational concepts, and developing comprehensive safety scenarios that also consider unexpected events and driver reaction to the safety operational concepts. This section of the orientation material will touch upon just the top few major challenges that may arise during the CV pilots, and what can be done to ensure a safety adequate deployment.

4.1 Risk Assessment

Developing a comprehensive safety management plan that includes all possible safety scenarios is a major challenge in this task. This includes identifying safety scenarios and assessing the level of risk for each scenario. It is recommended to follow the development process in Section 2.1 to identify the safety scenario, assess level of risk, and develop safety operational concepts to eliminate or mitigate the impacts. A stakeholder input activity is also recommended to help the site deployer identify and assess safety scenarios associated with the proposed Pilot Deployment.

4.2 Site-Specific Safety Plan

A safety management plan is customized to fit the needs of each site depending on the site's geographic and weather features and applications selected. Therefore, each site will develop its own safety plan that addresses identified safety scenarios and corresponding response actions.

4.3 Local Support

State and local agencies have their own emergency response plans for various events, such as severe incidents, natural disasters, or planned events. The site deployer will list the corresponding agencies for each safety scenario and coordinate with them 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.

4.4 Reaction of Participants

Participants may not be aware of the potential safety scenarios and the actions they are expected to take during emergency situations. Therefore, including the safety management plan as part of training plan is the key to prevent personnel injury and eliminate the potential impacts.

5 Technical Support Summary

A series of USDOT-sponsored webinars were developed to assist early deployers of connected vehicle technologies with Concept Development activities. The webinar described below provides support for the development of the Safety Management Plan.

1. Preparing a Safety Management Plan for Connected Vehicle Deployments

This webinar presents the USDOT perspective on the development of a Safety Management Plan, a key step in the concept development phase for deployment planning. John Harding of the National Highway Traffic Safety Administration describes the design concept and the requirements of a Safety Management Plan, which will address the underlying safety needs associated with the safety of all travelers, subjects, and other personnel associated with connected vehicle deployments. Note that Safety Management planning is critical, yet different from Safety Evaluation. The purpose of Safety Evaluation is to evaluate safety impacts/benefits, while the purpose of the Safety Management Plan is to define approaches/processes for the identification and management/ minimization of the inherent safety risks associated with connected vehicle deployments.

To access the presentation slides and audio recording for this webinar, please visit the technical assistance page of the CV Pilots website: http://www.its.dot.gov/pilots/technical_assistance_events.htm.

References

1. Connected Vehicle Pilot Deployments: Phase 1 Concept Development, Broad Agency Announcement No. DTFH6115R00003, Federal Highway Administration, January 2015. https://www.fbo.gov/index?s=opportunity&mode=form&id=36ac05d6be6db2c92dd77bda3965e245&tab=documents&tabmode=form&tabid=7c71a2c57d27b4c1185c15f069d80180&subtab=core&subtabmode=list&=
2. International Organization for Standardization, ISO 26262 Road Vehicles - Functional Safety: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43464
3. USDOT FHWA, Highway Evacuations in Selected Metropolitan Areas: Assessment of Impediments: http://www.ops.fhwa.dot.gov/eto_tim_pse/reports/2010_cong_evac_study/fhwahop10059.pdf
4. USDOT FHWA, Operational Concept - Assessment of the State of the Practice and State of the Art in Evacuation Transportation Management: http://www.ops.fhwa.dot.gov/publications/fhwahop08020/fhwahop08020.pdf
5. USDOT FHWA, Good Practices in Transportation Evacuation Preparedness and Response: http://www.ops.fhwa.dot.gov/publications/fhwahop09040/fhwahop09040.pdf
6. USDOT Federal Motor Carrier Safety Administration (FMCSA), Hazardous Materials/ Dangerous Goods Regulations, http://www.fmcsa.dot.gov/regulations/hazardous-materials/hazardous-materialsdangerous-goods-regulations
7. USDOT Federal Emergency Management Agency, Operational Lessons Learned in Disaster Response, http://www.usfa.fema.gov/downloads/pdf/publications/operational_lessons_learned_in_disaster_response.pdf
8. 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
9. TRB, NCHRP Report No. 525, Surface Transportation Security Volume 6, Guide for Emergency Transportation Operations, 2005, http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v6.pdf
10. USDOT NHTSA, Safety Pilot Model Deployment, Test Conductor Team Report, June 2015, Report No. DOT HS 812 171, http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2015/812171-SafetyPilotModelDeployDelTestCondrTmRep.pdf

11. USDOT, NHTSA, Integrated Vehicle-Based Safety Systems 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
12. USDOD, Department of Defense Standard Practice – System Safety, May 2012, Report No. MIL-STD-882E, http://www.system-safety.org/Documents/MIL-STD-882E.pdf

Appendix: List of Acronyms

Table A-1: List of Acronyms

Acronym	Meaning
ASIL	Automotive Safety Integrity Level
ETO	Emergency Transportation Operations
FEMA	Federal Emergency Management Agency
IRB	Institutional Review Board
ISO	International Standard Organization
PHMSA	Pipeline and Hazardous Materials Safety Administration
PSE	Traffic Planning for Special Events
TIM	Traffic Incident Management
TRB	Transportation Research Board

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-16-340

U.S. Department of Transportation