NYC CV Pilot Deployment Program

Safety Management Plan – New York City

www.its.dot.gov/index.htm
Report — April 22, 2016
FHWA-JPO-16-301

U.S. Department of Transportation

Produced by New York City Connected Vehicle Pilot Deployment Program, Phase 1
New York City Department of Transportation
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office.

The cover photo is from the ITS JPO.

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-16-301		

4. Title and Subtitle	5. Report Date
New York City Connected Vehicle Pilot Deployment Program Task 4: Safety Management Plan	April 22, 2016
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Douglas Pape, Battelle Hunter McCracken, Battelle	Task 4 Report

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Battelle 505 King Avenue Columbus, OH 43201	11. Contract or Grant No. DTFH6115C00036

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	Task Report, December 2015 to April 2016
	14. Sponsoring Agency Code

15. Supplementary Notes

Program Manager: Kate Hartman
Contracting Officer's Representative (COR): Jonathan Walker

16. Abstract

This safety management plan identifies preliminary safety hazards associated with the New York City Connected Vehicle Pilot Deployment project. Each of the hazards is rated, and a plan for managing the risks through detailed design and deployment is outlined. The hazards are classified as to whether they apply to one of the individual safety applications or to the system as a whole. To address these hazards, the plan provides design requirements, ongoing safety management policies, or plans to restore normal operation following an event.

This is one of several planning documents for The Connected Vehicle Pilot Deployment Program, Phase 1, project funded by the United States Department of Transportation (U.S. DOT).

17. Key Words	18. Distribution Statement
connected vehicles, DSRC, V2V, V2I, safety, New York City	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	38	

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

Table of Contents

List of Tables

List of Figures

Revision History

Version #	Date	Author	Change Description
1.0	March 25, 2016	Pape and McCracken	Draft
2.0	April 22, 2016	Pape and McCracken	Responds to USDOT comments

Chapter 1 Summary

The New York City Connected Vehicle (CV) Pilot Deployment will be the largest deployment of connected vehicle technology to date. This project brings New York City another step toward reaching the Vision Zero goal of eliminating the injuries and fatalities due to traffic crashes. The purpose of the safety management plan is to minimize the possibility that the deployment introduces appreciable new safety risks to the city's travelers.

This plan identifies scenarios that could pose risks to safety, rates the scenarios, and outlines ongoing steps so that safety is adequately addressed throughout the deployment.

The team adapted the methodology outlined in ISO 26262, an automotive industry standard for managing functional safety. Risks were systematically identified and ranked. Levels of severity, exposure, and controllability were established, generally following ISO 26262. Hazard scenarios and their consequences were evaluated and assigned levels of risk, or Automotive Safety Integrity Level (ASIL).

Hazards receiving an ASIL rating of A, B, C, or D exhibit the possibility of causing harm if not properly managed. Increasing ratings require increasing levels of rigor to ensure safety goals are achieved. Hazard analysis, verification and validation, and testing, will be applied in combination. Scenarios of lesser concern were rated "QM," indicating that harm is possible, but the scenario is handled by normal quality management practices. After thorough evaluation, some scenarios were deemed to pose no risk for harm and assigned a zero rating, excluding them from further analysis.

The Mobile Accessible Pedestrian Signal System (PED-SIG) has the hazards with the highest safety ratings. It is the only application that communicates permission to a traveler to take a particular action.

Safety-related requirements were written for all scenarios with a safety rating. These safety requirements vary between four different categories, with the overarching safety goal associated with each high-ranking hazard scenario mapping to one or more of the categories. The safety goals associated with each hazard scenario dictated which actions should be taken to mitigate the associated risk, resulting in that scenario's safety requirement(s). The safety requirements vary between those that can be applied to a particular component, piece of software, or subsystem; operating rules; fail-safes to pre-deployment conditions; and a standard emergency service response.

Because the deployment is in its concept phase, this analysis should be considered a preliminary hazard analysis. Continued diligence in adhering to this plan as it evolves through the design and deployment phases will be necessary.

Chapter 2 Introduction

This document is the Task 4 deliverable for Phase 1 of the project for the New York City Connected Vehicle Pilot Deployment Program. The program is being funded by the United States Department of Transportation (USDOT). This Safety Management Plan considers the applications to be deployed [1] and is intended to describe the underlying safety needs associated with the safety of all personnel associated with the Pilot Deployment, including travelers in New York who are not direct participants. The plan includes a high-level risk management plan for each of the safety needs, so that safety is not diminished by any aspect of the deployment.

The scope of this document is to develop the safety plan at the system level. The items to be analyzed are defined, a preliminary hazard analysis and risk assessment is performed, and the safety goals are identified.

A number of standard approach to safety management are available, including MIL-STD-882E [2] and ISO 26262 [3]. The New York City team elected to follow the principles and general approach of ISO 26262 in developing the safety management plan. Many standards have a hazard assessment considering the risk in terms of likelihood of occurrence and severity of effects or consequences. ISO 26262 is particularly suited for vehicle-related hazard analysis because it adds a third layer of controllability—the ability of the operator to compensate, at least temporarily, for a failure.

This document cannot claim compliance with ISO 26262, because the standard's scope is "series production passenger cars with a maximum gross vehicle mass up to 3,500 kg" (7,700 lb). The applications inherently include components beyond the vehicle; many of the vehicles in the deployment are not passenger cars, and the pedestrians are not vehicles at all. While the systems in this pilot deployment are outside the scope of ISO 26262, the team followed the guidance of ISO 26262 in developing this safety management plan. This document was written according to the general principles of ISO 26262—Part 2 for the management of functional safety and ISO 26262—Part 3 with respect to item definition, hazard analysis and risk assessment, and development of the safety goals.

The guidance summary on safety management [4] called for a broad interpretation of safety. The key management tasks are to plan, coordinate, and track the activities related to functional safety. Specifically, in the Pilot Deployment,

- functional safety requirements are to ensure safe operation of the application and
- safety management is to incorporate safety from concept development to monitoring operation.

Guidance called for the safety management plan to address all aspects of safety. This includes

- Operational safety of the city—enhancing the safe transportation of people and freight through New York City
- Functional safety of the equipment—performing as intended and reverting to a safe state in the event of a malfunction

- Emergency safety—tending to immediate needs and restoring operation according to a backup plan, following an unusual event.

Every a V2V or V2I application is an “item” for analysis as in ISO 26262. Not all vehicles in the study will have the same applications; pedestrians will have their own unique applications. Many common elements will be shared across applications.

The safety management plan considers disruptions that could come from any source, including

- Inadequate design, including software flaws and inadequate power supplies
- Natural causes, such as storms and power outages
- Improper use, from installation, to operation, to maintenance

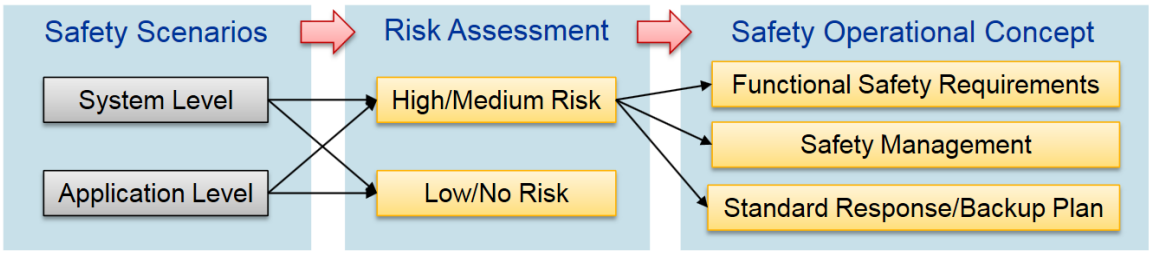
Although safety goals were developed for a comprehensive list of threats, not all of the goals will be managed under the safety management plan. Some of the needs identified in this process will be transferred to other activities. For example, unjustified pedestrian signal requests and sophisticated attacks on the communications channels will be exported to security.

The safety management plan will continue to be a living document throughout the deployment. It will incorporate new input and findings from other stakeholders and team members. Implementation of the plan, of course, also continues throughout the project.

Chapter 3 Safety Risk Process and Approach

The approach was an adaptation of the steps in ISO 26262 for developing a safety plan in the concept phase. In Phase 2 of this project, the safety-related requirements will be developed, implemented, and verified according to this plan.

The steps are outlined in Figure 3-1. The safety scenarios are developed in Section 5.2 of this document and the risk assessment is in 5.3. The safety operational concept is developed in Chapter 6.



Source: NHTSA [5]

Figure 3-1. The overall Process of Developing the Safety Management Plan has Three Steps.

3.1 Application of ISO 26262

The steps that the team followed in developing this plan were generally according to the following clauses of ISO 26262:

Part 2: Management of functional safety
- 6.4.3 Planning and coordination of the safety activities
- 6.4.4 Progression of the safety lifecycle
- 6.4.5 Tailoring of the safety activities

Part 3: Concept phase
- 5 Item definition
- 6 Initiation of the safety lifecycle
- 7 Hazard analysis and risk assessment
- 8 Functional safety concept

Part 8: Supporting processes
- 6 Specification and management of safety requirements

The safety applications to be deployed in New York City were defined in the concept of operations [1]. For the purpose of this safety management plan, an "item" whose safety is to be assured is one of the applications.

The hazard identification collected input from numerous sources—U.S. DOT guidance, communication with stakeholders, a prior model deployment, and the experience of the project team. The list included hazards at both the system level (e.g., communications, weather) and the application level (e.g., installation, software algorithm). The hazards were assigned to one or more of the applications that they might affect.

The hazard analysis and risk assessment used the three-aspect approach of ISO 26262-3, Clause 7. It considered the exposure, the severity, and the controllability of each hazard. Safety goals were developed and rated following the general principles of ISO 26262-3, clause 7.4.4 and ISO 26262-8, clause 6.

The current contract is for the first year, which is the concept phase of the deployment. The design, development, and testing are scheduled for Phase 2. The high-level safety goals developed in this plan will be flowed down to technical safety requirements and programmatic safety policies in the next phase. ISO 26262-9, Clause 5.2 provides that functional safety requirements be allocated during the design and development phase. Phase 1 of the JPO contract includes only concept development, so this document extends no further than that. An important part of the project plan for Phase 2 will be to carry out the safety management during the design, development, and deployment of the systems. During that phase and the planned subsequent operational phase, additional portions of ISO 26262 will be adapted.

The Safety Operational Concept calls for four classes of action. Many scenarios were addressed by writing Functional Safety Requirements, which will be flowed down to activities during the second or third phase. For example, a certain application may be required to have false positive and false negative rates below specific values. The second class of action is Safety Management. These will be operational policies and procedures that are in place during the subsequent phases. They may, for example, call for testing signal control boxes at regular intervals. Backup plans will be developed to recover from disruptions. These will range from restoring service following a system-wide failure to recalling Aftermarket Safety Devices (ASDs) in the event of an essential upgrade. Finally, the emergency response plans will be to call 911 in the event of a crash.

3.2 Departures from ISO 26262

The hazard analysis and risk assessment took a significant departure from ISO 26262 in the definitions of severity and exposure. A “harm” as defined in ISO 26262-1 is a “physical injury or damage to the health of persons.” Any event that does not result in an injury, including a property-damage-only crash, is assigned a severity of S0 in the standard (ISO 26262-3, Appendix C.1) and is not assigned an ASIL for further analysis.

When this analysis identified a scenario that could impair mobility or increase congestion, the scenario was assigned a severity of S0a to aid tracking. These scenarios will be exported to the project’s tasks for general requirements development and will no longer be considered part of the safety analysis. The team recognizes that congestion or unexpectedly stopped traffic can lead to a crash, but crashes that are secondary to congestion caused by a hazard were excluded from the safety analysis.

Severity levels S1, S2, and S3 correspond to progressively more severe injury levels. S2 and S3 were not changed from ISO 26262; S1 was expanded to include property damage crashes because of the difficulty in estimating impact speeds at this stage of the analysis.

The definitions of the severity levels used in developing this safety management plan are in Table 3-1.

The exposure classes in ISO 26262 apply at the vehicle level and are not scaled according to the number of vehicles expected to be produced. The exposure classes for this document were based on those in ISO 26262-3 Appendix C.3, but they are applied over the planned duration of the deployment. A poor design that affects an application (such as an inappropriate threshold) is deemed to occur every time that application should generate a message. The exposure definitions are in Table 3-2.

The characterization of controllability was also tailored for this project, because most of the apps produce only warnings. A mere distraction is C0 in ISO 26262-3 Table B.4; it is C1 in this analysis. See Table 3-3.

Table 3-1. Classes of Severity for the Hazard Analysis and Risk Assessment

Class of Severity	S0	S0a	S1	S2	S3
Definition	No degradation in service	Traffic is slowed or congestion is increased	Any impact of a vehicle with another vehicle, an infrastructure element, or a pedestrian, with a severity lower than S2.	More than 10% probability of AIS 3-6 (and not S3)	More than 10% probability of AIS 5-6
Description	Mobility is as it is without the application. The system, or a part of it, may cease to function, but mobility is no worse than it would have been without the system.	Movement of vehicles or pedestrians is noticeably impaired	Any crash is deemed to be at least S1.	S2 is defined as in ISO 26262.	S3 is defined as in ISO 26262.

Source: Battelle

Table 3-2. Classes of Probability of Exposure for the Hazard Analysis and Risk Assessment

Class of Probability of Exposure	E0	E1	E2	E3	E4
Definition	Incredible. Unlikely to happen in 2 years	Expected to happen fewer than 10 times during the two-year deployment	Expected to happen once daily during the deployment	Expected to happen once per hour at some location in the deployment region.	Expected to happen in almost every trip by every participant in the deployment.
Description	Less than 1% probability of happening anywhere during the deployment	Severe storms are an example of rare but expectable events.	Once daily to a vehicle, pedestrian, or piece of infrastructure at some location in the deployment region.	Events that will occur more than daily.	Will occur thousands of times daily during the deployment period.

Source: Battelle

Table 3-3. Classes of Controllability for the Hazard Analysis and Risk Assessment

Class of Controllability	C0	C1	C2	C3
Definition	No unusual action is required of the participant or another driver or pedestrian.	99% of participants will be able to make a timely, correct response to the situation.	90% or more of participants will be able to make a timely, correct response to the situation	Less than 90% of all drivers or traffic participants will be able or barely able to avoid harm.
Description	Participant will notice nothing unusual, and normal movement is the proper course.	The response may be normal steering, braking, or perhaps no change in course. A participant is readily able to recognize an incorrect message or overcome a distraction and to execute the proper maneuver.	At least 90% of drivers would have the skills necessary to recognize the situation and avoid a crash. At least 90% of participants would overcome an incorrect or misleading or ambiguous message in a timely manner.	Harm that occurs regardless of driver response is not controllable. Any system feature (static equipment or inappropriate message) that leads a driver to take harm-causing action is in this class.

Source: Battelle

Chapter 4 Safety Stakeholders

The safety stakeholders ultimately include all who travel in New York City. All travelers who share the streets and crosswalks with project participants have an interest in the equipment behaving safely. Organizations associated with the travelers, from the New York City Department of Transportation to the Taxi and Limousine Commission, have an indirect interest in project safety. The ConOps [1] has a complete list of stakeholders.

Project leadership consulted with the team members (e.g., UPS and New York State Motor Truck Association) to hear their concerns. One desire raised by representatives of drivers was that the alerts be sent only for actual safety-sensitive situations. Alerts that are too numerous could become distracting or ultimately ignored. Stakeholders wanted alerts to be loud enough to get the attention of the driver (perhaps by muting the radio) and distinguishable from other sounds in the cab. One suggested that some variability in audio volume may be needed depending on risk condition. Similarly, alerts have to be clear in what they mean. Also, the team should address how the drivers might behave over the duration of the deployment. Stakeholders were concerned that drivers might become dependent on the technology and fail to practice defensive driving skills. Maintaining equipment health over the deployment was mentioned.

This input was included in the list of safety scenarios and handled accordingly.

Chapter 5 Safety Needs

Identifying the safety needs of the New York City Connected Vehicle Pilot Deployment project requires a firm understanding of the technologies being implemented, a heavy reliance on the past experience of the research team, and the diligent adherence to industry standard safety plan development.

Scenarios resulting in a detriment to the transportation system of the city and, more important, to the safety of its people, can be found in every application, system level, and application level. Scenarios were developed for each of these areas to provide the most comprehensive list of possible hazards and ranked based on their severity, potential exposure, and controllability by human subjects. This ranking provides a detailed list of scenarios that pose the most potential for disruption and harm, and should therefore be most thoroughly analyzed and prevented with safety requirements.

5.1 List of Connected Vehicle Applications

The safety needs were considered as they apply to the applications to be deployed. Each application will be provided by a system of hardware and software. Each application will have interfaces to other specialized equipment to be in the deployment, with existing infrastructure, and with humans. The application could present a hazard due to an internal failure of one of its components, or because of failures in one of the external elements with which it interfaces.

The application must perform its function in a way that does not introduce new harms. It must do so when it is operating as intended, when it is malfunctioning due to internal failures, external failures, and foreseeable misuse.

The applications, sorted by need area as in Table 11 of the ConOps [1], are

Manage Speed
1) Speed Compliance
2) Curve Speed Compliance
3) Speed Compliance in Work Zones

Reduce Vehicle-to-Vehicle Crashes
4) Forward Crash Warning (FCW)
5) Emergency Electronics Brake Lights (EEBL)
6) Blind Spot Warning (BSW)
7) Lane Change Warning (LCW)
8) Intersection Movement Assist (IMA)
9) Red Light Violation Warning
10) Vehicle Turning Right in Front of Bus Warning

Reduce Vehicle-to-Pedestrian Crashes
11) Pedestrian in Signalized Crosswalk Warning
12) Mobile Accessible Pedestrian Signal System (PED-SIG)

Reduce Vehicle-to-Infrastructure Crashes
13) Oversized Vehicle Compliance

Inform Drivers of Serious Incidents

14) Emergency Communications and Evacuation Information

5.2 Identified Safety Scenarios (i.e., Hazards)

The safety scenarios are potential sources of harm—things that could go wrong during the pilot deployment. The scenarios came from a wide variety of sources, including project staff experience, prior projects, and stakeholder concerns. The scenarios were categorized in two levels. System-level scenarios are those that affect the entire operation and essentially all safety applications, such as a weather disruption. Application-level scenarios affect only a single application or a class of similar applications. Examples would be a hardware failure on equipment in a vehicle or an incorrectly coded work zone location. The scenarios are described at a high level in groups in this section of the main text. The individual scenarios are listed and analyzed in Appendix C.

5.2.1 System Level

System-level scenarios are events that could affect the entire pilot deployment system.

Perhaps the simplest to understand are those related to weather. If a storm causes a power failure, messages originating from deployment vehicles that are transmitted to traffic signals will be lost. Even a localized failure would prevent a portion of the system from working. Similarly, outdoor components are exposed and vulnerable to vandalism.

The entire connected vehicle concept depends on Dedicated Short-Range Communication (DSRC) messages being continuously broadcast and received by the infrastructure, vehicles, and pedestrians. Anything that interferes with the reliable and timely transmission will degrade system performance. Any number of causes could disrupt DSRC signals: weather, poor antenna placement, inadequate processing speed in devices, multipath transmission (reflections from tall buildings), electromagnetic interference from construction equipment, and deliberate attacks through breaches of security.

The system will not work properly if those who install equipment and those who operate it do not understand it. The cause of the poor comprehension could be a poor design that is difficult to grasp, or it could be inadequate training. Poorly installed equipment could cause a fire, distract a driver, or prevent the equipment from functioning. Drivers and pedestrians who do not interact properly with equipment could fail to realize benefits or take inappropriate action and cause a crash.

Software on any device that does not perform as intended may present hazards. In-vehicle devices (i.e., ASDs) will have supervisory software to handle inbound and outbound DSRC messages, GPS signals, and communication with the vehicle and driver. In addition, ASDs will have a number of software modules executing the safety applications. All of these software components need to function properly together according to an established interface. They must accommodate failures in hardware or in adjacent software modules in a way that does not pose hazards. Similarly, software in fixed structures must interface with signal controllers, NYCWiN, and DSRC messages from travelers.

In-vehicle devices will use the OBDII port for vehicle-related information, which poses a number of hazards to consider. Many of New York City's vehicles already have a device plugged in the OBDII port, so a splitter needs to be developed and tested to ensure that the CV equipment performs properly and does not interfere with the other equipment or with the vehicle itself. If the device is removed from the port so a mechanic can read engine codes, then the participant or mechanic will need to be informed of the necessity of and procedure for reinstalling the CV equipment.

As with other CV studies, the vagaries of precision GPS location need to be understood and mitigated. That will be more complicated in the urban canyon in Manhattan.

Mechanics and technicians who install equipment (indoors, outdoors, and on vehicles) for the deployment will be subject to the normal hazards of their jobs. The deployment is not expected to change the safety level of their tasks, and their normal safety practices are expected to be sufficient for deployment-related work. Safety hazards to personnel who build or install equipment are not part of this analysis.

5.2.2 Application Level

Application-level scenarios are hazards that might arise from the malfunctioning of a single application or a group of similar applications. The list of applications is in Section 5.1 of this document. Some of the scenarios are unique to a particular application while other scenarios are common to a group of applications sharing a similar characteristic. When a scenario affects more than one application, the analysis may be identical for all applications, or it may be different. The discussion here pertains to the application-level scenarios at a high level; the complete analysis for every application is in Appendix C.

A concern raised by stakeholders is that the safety messages might be presented too often and annoy the driver. This concern pertains mostly to the V2V safety applications, such as EEBL and FCW, where the device alerts the driver of a developing situation. In these applications, it is not only necessary to set the message threshold at the proper level, but also to formulate the decision algorithm properly to recognize the threat, and to ensure that all components of the system are functioning as intended. Tolerance and prevalence of alarms will differ between the types of vehicles in the deployment. Threshold setting and perhaps algorithm tuning will need to be handled individually for all applications and all fleets.

Thresholds that are set too high (or algorithms that systematically miss certain conditions) would deny an application the opportunity to advise a driver of a potentially dangerous situation. Worse, inconsistent performance could allow a driver accustomed to the messages to respond too late to avoid a crash. Proper design for reliable performance is essential, as is training that the safety applications are intended only to supplement the driver's own senses and good judgement.

The PED-SIG application (which will provide verbal information regarding the signal state) clearly has the greatest potential for injury. If the system malfunctions or a pedestrian responds to it improperly, a pedestrian is likely to be struck. Occupants of vehicles will be protected by the vehicle in moderate crashes, but pedestrians are inherently exposed and subject to serious injury from even minor impacts. Hazards related to these applications have the highest severity ratings and consequently the highest ASIL ratings in the analysis. Therefore, they will require the greatest attention during design and the greatest rigor in testing. Training will be important for all users during the deployment, so that they understand the capabilities and limits of the equipment and are aware of their role and their proper response to messages. Training will be especially important for pedestrians, for how to input data and receive data from the applications. Visually impaired pedestrians are a vulnerable population less able to correct for malfunctioning equipment than are most other users.

The mobility applications (such as Speed Compliance) have the fewest safety concerns. Intended only to improve traffic flow, they are not expected to affect safety. These applications do not operate in near-crash situations, and any safety hazard associated with these applications would be secondary to the possibly increased congestion caused by a malfunction.

The V2I safety applications will prove beneficial only if they broadcast correct, timely information. If work zone locations are out of date, then drivers will be provided information that is, at best, confusing. This could be a serious safety issue if a driver becomes reliant on the system for periodically changing information. Initial data entry needs to be carefully verified, and ongoing safety management has to include periodic checks of roadside equipment (RSE) performance and information.

Nearly all of the applications have hazards related to the driver vehicle interface. If information is not transferred clearly and interpreted properly, the application will fail to accomplish its goal. An opportunity for improvement in safety or mobility may be lost; at worst, an improper user action could lead to a crash. Requirements flowing from these hazards are for proper interface design and proper training. Because the exact information to be transmitted is unique to each application, this common hazard has to be addressed individually for every application.

5.3 Classification of Hazardous Events (or of Safety Scenarios)

A key step in developing any safety plan is the hazard analysis and risk assessment. Each of the hazards that has been identified has to be given a rating for how likely it is to occur and what are the consequences if it does occur. ISO 26262 provides for a third level of classification, which is the ability of the human operator to compensate for the malfunction.

In Appendix C, each of the hazards is assigned an exposure level, a severity, and a controllability according to Table 3-1, Table 3-2, and Table 3-3. Rules were written to assign the ratings, and the appendix records which rule was applied in each case. The ratings and the rules for assigning them were reviewed by stakeholders with a variety of perspectives and disciplines on the deployment team.

The principles used to guide the rating process and the analysis of classes of hazards are discussed here, and examples are presented.

5.3.1 Analysis of Severity

The pedestrian-related safety applications were assigned the highest levels of severity. While vehicle occupants are protected by their vehicle in crashes, pedestrians are exposed directly to the impact. These injuries could be fatal, so they were assigned a severity of S3. This is consistent with research on pedestrian injuries that found a risk of severe injury (AIS 4 or above) of over 25 percent at a speed of 25 mph [6]. ISO 26262:3 defines S3 as a 10 percent probability of AIS 5 or 6 injury.

Historical research found a ten percent probability of injury at AIS 3 or above at an impact speed of 25 mph [7]. That is a speed limit on streets in Manhattan, and ten percent probability of AIS 3 or above is S2 in ISO 26262. To be conservative, vehicle-to-vehicle crashes in most of the deployment area are assigned a level of S2. Crashes where the speed limit is above 25 mph are rated S3.

Hazards assigned a severity of S2 for serious injuries that do not threaten life were those where hardware in the vehicle causes an injury. Electrical fires are in this category. In-vehicle equipment could cause an injury in a crash, but properly located and secured equipment will not cause such injuries. These hazards were listed for the purpose of generating requirements on equipment mounting.

Many hazards were operator error exacerbating a situation and causing a minor crash. These were rated S1.

If the safety application misses an opportunity to prevent a crash, and a crash occurs that would have occurred without the system, this analysis does not consider that hazard. If an operator overreacts or reacts inappropriately to the system, and the operator's inappropriate actions cause a crash, that is a hazard. The applications do not assume control of a vehicle, nor do they provide specific instructions to drivers. The system directly causes a crash only in cases where it prevents a driver from obtaining information that would otherwise be available (such as blocking a view or masking an exterior sound). The system may indirectly lead to a crash by distracting driver.

Malfunctions of the mobility applications that increase, rather than decrease, congestion were assigned a severity of S0a. S0a was a special rating for this analysis, for hazards that impair mobility but do not cause physical harm. This rating also applied to hazards where a safety application would lead a driver to unnecessarily brake the vehicle and slow traffic.

The rules that were used to assign severity levels are in Table B-1 in Appendix B.

5.3.2 Analysis of Probability of Exposure

The highest exposure ratings (E4) were assigned to systematic errors that will affect everyday driving. Examples are equipment that blocks a driver's view and ambiguous messages for applications that will be activated on almost every trip for many vehicles.

The second highest exposure rating (E3) is for events that are expected to occur approximately once per hour at some location in the deployment region. The level was assigned primarily to systematic flaws that would manifest themselves less frequently.

The next exposure rating (E2) is for events that are expected to occur approximately daily at some location in the deployment region. This level was assigned to hazards that would not occur on every trip because they require a combination of contributing factors, but the combination is plausible and can be expected to occur with some regularity. The rating is also applied to hazards associated with new drivers or maintenance staff entering the fleets in the deployment; with a workforce the size of those of stakeholder organizations, the project must plan for turnover.

The lowest rating of plausible hazards (E1) is for those events that will occur at most a few times during the two-year deployment. Extreme weather events are an example of this rating. Also, serious crashes of participant vehicles, from any cause, are an exposure to the hazard where deployment equipment could exacerbate an injury or delay medical response.

The rating of E0 refers to incredible events that were considered but are not expected to occur. One example is overloading the ampacity of signal boxes. The power supplies for the boxes are sufficient for incandescent signal lamps, but LEDs have been installed, leaving plenty of power for deployment equipment.

The Modified Emergency Communication and Evacuation application is unlikely to be exercised even once during the two-year deployment. However, scenarios associated with this application were assigned E1, expected to occur at least once, so that they could be carried through the analysis.

The rules that were used to assign exposure levels are in Table B-2 in Appendix B.

5.3.3 Analysis of Controllability

Controllability is the human operator's ability to compensate for a malfunctioning application.

The primary function of the applications is to provide information to the driver. Many, such as speed compliance in work zones, merely call the driver's attention to information that should have been already available. A few, such as EEBL, tell the driver information that would not be available otherwise.

No application takes even partial control of project vehicles, and the driver has at least as much information available with a malfunctioning application as with no application. However, when the driver must assess the validity of information and may mistakenly include incorrect information in a rapidly-made decision, the controllability cannot be C0.

The effect of inappropriate alerts on distraction and performance degradation must be considered.

The large number of applications poses the possibility of a high combined rate of nuisance alarms. The mental workload of interpreting and deciding whether to heed an alert is a distraction. The possibility that a driver startled by a message would inappropriately brake and disrupt traffic cannot be entirely discounted. Research has shown that an unreliable system reduces the accuracy of drivers' initial responses by as much as 40% compared to a reliable system [8]. Another study indicated that false alarms caused drivers to slow down or make inappropriate responses, such as braking [9]. Therefore, hazards of frequent incorrect messages were assigned C1. A driver so accustomed would unwittingly ignore an appropriate message from the offending application.

A driver who misunderstands the purpose of the system and believes that the proper response to a message is different than what it should be will respond inappropriately, justifying a rating of C3 for operator misunderstanding.

The highest controllability rating of C3 was assigned to erroneous messages from the PED-SIG application. A visually impaired pedestrian would rely on the message and have little or no external corroboration. The driver cannot compensate for poor training, and the controllability is C3.

In-vehicle electrical fires were assigned C2; a driver would smell smoke and know to leave the vehicle but might not be able to stop safely and immediately.

The rules that were used to assign controllability levels are in Table B-3 in Appendix B.

5.4 Determination of ASIL Levels

According to ISO 26262, every scenario is assigned an Automotive Safety Integrity Level (ASIL) according to its severity, exposure, and controllability. The table for doing so, adapted from ISO 26262-3 is in Figure 5-1. Hazards with a rating of E0 (not expected to happen at all), S0 (would cause no harm), or C0 (can definitely be controlled by any driver or pedestrian), are not assigned a safety rating and are excluded from further analysis.

The ASIL ratings are listed in the table in the appendix. Some of the hazards received an ASIL rating of A, B, C, or D because they have the possibility of causing real harm if they are not properly handled. More than half of the hazards were rated as "QM," indicating that normal quality management practices will suffice in preventing harm. Safety-related requirements were written for all

scenarios with one of these ratings. The different ratings apply to different levels of rigor in developing the safety requirements and testing to ensure the requirements have been met.

The nine scenarios that were assigned a zero rating can be excluded from further analysis. This applies if a scenario cannot happen, causes no harm, or can be unquestionably handled by any participant. In these cases, that assessment is documented and no safety requirements are needed. These items are listed as "--" in the table in the appendix.

The PED-SIG application poses hazards with ASIL D—the highest rating. The mobile device will communicate audible walk indicators to a visually impaired pedestrian. It will be absolutely essential for the system to correctly discern the pedestrian's position and intended cross direction and to provide unfailingly correct and timely permission to cross. The highest levels of hardware and software development will be employed, and the verification methods will be most rigorous.

		Controllability		
Severity	**Exposure**	**C1**	**C2**	**C3**
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**

Source: NHTSA [5]

Figure 5-1. The ASIL Level is Determined from the Severity, Exposure, and Controllability.

The only other hazard with the D rating is equipment positioned so it blocks a driver's view. A driver with an obstructed view can be expected to strike a pedestrian and cause serious injuries. Requirements for clear visibility must be applied and rigorously verified to all vehicles.

5.5 Summary of the Hazard Analysis and Risk Assessment

Of the more than 70 hazards that have been listed at this point in the concept phase, more than 25 were assigned an ASIL. The Safety Manager and a team of safety professionals will continue to track these hazards, as described in the next chapter on the Safety Operational Concept.

An ASIL of A, the lowest, was assigned to 12 scenarios. The safety team, operating independently of the design team, will review the respective design or procurement requirements to ensure that they address the hazards and will confirm that the verification is adequate and has been performed. Items with an ASIL of B will receive the same scrutiny as those with an ASIL of A, with the additional step that they be verified at least at the system level, or the vehicle level if necessary. Hazards at the higher levels, C and D, will be additionally verified by an independent safety team at New York City Department of Transportation or another member of the contractor team as appropriate. Some of the hazards are addressed by design requirements that are met when they are verified. Other hazards will require ongoing diligence in safety management throughout the deployment.

Chapter 6 Safety Operational Concept

Every safety goal will map to one or more safety requirements. They may be

- Design requirements to be applied to a component, software, subsystem, user interface, or training module in Phase 2
- Operating rules
- Simple reversion to pre-deployment conditions
- Emergency response

Many of the scenarios listed in Appendix C are addressed by writing requirements on the design of components or systems, as discussed in Section 6.1. Other scenarios are addressed by implementing policies to govern the deployment and implementing safety management practices to ensure those policies are followed. Finally, in the case of a partial or complete failure, there will be plans in place to limit any damage and to restore normal deployment operation. One of the three approaches to providing safety is selected in the Type column in the Risk Response Plan of Table C-2.

6.1 Functional Safety Requirements

This section describes the groups of the functional safety requirements; the complete list is in Appendix C. The requirements in the appendix will be flowed down to the design and development activities. Some of the requirements will be combined because they overlap between scenarios. Other requirements will be split because they apply differently to different applications.

The most important functional safety requirements will be performance requirements and testing for the safety applications. Many of the requirements are to develop proper algorithms and thresholds. Where possible, hazards will be eliminated so they are no longer a consideration.

The deployment system will consist of equipment and software from many sources, including existing New York City infrastructure, commercially obtained ASDs and RSEs, and specially designed hardware and software. Properly documenting the interfaces between these systems and ensuring that all components adhere to their interface requirements will be a significant portion of the safety requirements.

Most of the applications affect traffic flow only through driver actions, so human interfaces are a key link in the flow of information. High-level safety requirements for these applications will be that certain information be made available to the driver without delay, ambiguity, or distraction from driving tasks and awareness. These will flow down to more specific requirements on the nature and design of the interface of each application. In the cases of hazards with higher ASIL ratings, quantitative failure rates (such as mean time between hazardous events, MTBHE) will allocated to subsystems, such as signal controllers and communication channels. A separate hazard analysis will be developed for subsystems and their interfaces.

Participants in the study will have new duties. If nothing else, they will need to respond to alerts. Many of the scenarios have requirements for training one group or another. As with everything else, training curricula need to be tested to ensure that the proper understanding is imparted.

6.2 Safety Management

Safety management is overseeing all of the activities necessary to ensure the safe execution of the deployment. That includes writing this document and ensuring the team follows through with the plans.

As the deployment transitions from Phase 1 to Phase 2, the team will ensure that functional safety requirements are met. Requirements will be flowed down to the appropriate design and acquisition activities. Suitable verification and validation activities will be performed and documented.

Safety management also includes policies that need to be carried out during the deployment phase, such as ensuring equipment is calibrated and new work zones are recorded and entered.

During the deployment in Phase 3, safety management has two main roles. The first is to ensure that safety-related practices are put into effect. This would include training and inspections. The second role is to monitor any anomalies, near-misses, or crashes that occur. Examination of reports of incidents may reveal shortcomings and adjustments that need to be made. Sources of information may be participant interviews, data downloads, police reports, and repair records as are appropriate for the incident.

Battelle's Doug Pape will be appointed Safety Manager for Phase 2 and 3. The safety manager's role will be to work with project leadership, suppliers, systems engineers, and other stakeholders. The purpose of the ongoing safety team will be to see that the elements of the risk response plan are implemented and documented. Mr. Pape has developed safety plans for unusual vehicle studies, including crash tests of hydrogen-fueled vehicles and run-off-road recovery experiments with a tank semitrailer. He has worked with connected vehicle safety applications and is comfortable dealing with drivers, engineers, and executive-level leadership. He is a Senior Research Engineer with over 30 years of experience at Battelle..

6.3 Fail-Safe Modes

There will be design requirements that systems revert to a fail-safe mode when they are unable to perform their intended function. The team will have procedures in place for instances where the connected vehicle system, or a part of it, enters a fail-safe mode. The procedure will provide for removing the reason for the failure and for restoring normal operation. These procedures will include restoring power after a blackout, re-booting the system after a disruptive software glitch, and repairing equipment damaged by bad maintenance, tampering, or mishap. In all but the lowest hazards, a failure diagnosis and analysis will be performed, in case the present minor failure is an indicator of a more serious underlying problem.

Many of the weather-related hazards call for a similar response. The first defense against a lightning strike is a good ground. Should that be inadequate, damaged equipment needs to be replaced and restarted. New York City has existing procedures for weather events; response to weather events affecting connected vehicle operations will be patterned after and blended with those procedures.

Individual devices in vehicles or pedestrians' hands will also have fail-safe modes when they suffer an internal failure or detect an anomaly. Part of safety management will be to periodically test for these conditions and to follow established procedures when they occur.

6.4 Emergency Response

Finally, should a vehicle or pedestrian in the deployment be involved in a crash due to any cause, the response will be to follow existing emergency response procedures. As with any emergency situation involving a vehicle or pedestrian, an available person will call 911, and New York City's emergency responders will perform according to their standard training.

Chapter 7 Coordination with other Tasks

Part of safety management is coordinating with other tasks in the deployment so that safety needs are addressed throughout the project.

This safety management plan followed the Concept of Operations developed in Task 2 [1]. The overall functional goals of the deployment led to the high-level safety goals. Likely implementations of the Concept Of Operations led to the more specific safety requirements that are in the hazard analysis.

Security (protection from deliberate attacks) and safety (protection from malfunctions and errors) are distinct, but they have considerable overlap in their high-level objectives.

A large portion of the safety operational concept is developing requirements to be flowed to the design and development tasks. Therefore, this task coordinated closely with the system requirements in Task 6. The safety management activities will continue to be closely integrated with the system requirements activities during the design and development in Phase 2, ensuring that the safety-related requirements are applied at the proper points of design and development and that tests verifying compliance are properly planned, conducted, and documented. Similarly, requirements for initial and ongoing participant training are coordinated with Task 9 on participant training and stakeholder education.

The safety operational concept also calls for ongoing safety management during deployment. Ongoing management is coordinated with Task 7, the application deployment plan, and Task 12, the comprehensive deployment plan, so that safety management is an integral part of overall deployment management.

Chapter 8 Conclusions

The safety hazards of the New York City Connected Vehicle Pilot Deployment are manageable. The conservative approach of delivering only alerts and not permissive messages means that many applications will naturally fail to a safe condition. The prominent exception is PED-SIG, which does grant permission to proceed by indicating the signal phase to a pedestrian. Training of all participants, from mechanics to drivers, will be necessary for the system to perform. Careful attention to details in design, combined with diligent testing, will address many of the hazards that were identified. Ongoing safety management throughout the remainder of the project will ensure follow-through.

The PED-SIG application, where a blind pedestrian needs help being oriented to the crosswalk and the mobile application will notify the pedestrian when to start the crossing, raises the most serious safety concerns. It is the only application that gives permission to a traveler to take action, so its development must be to the highest levels of safety standards. The requirements themselves need to be verified to be correct, all subsystems and interfaces must have independent verification and validation, and full-system testing will be conducted.

As the ConOps and requirements are finalized in the remainder of Phase 1 and in Phase 2, refined analysis will lead to more safety scenarios being identified. They will be rated and tracked along with those already identified.

Some of the hazards are to be addressed by writing safety requirements and verifying designs to those requirements. They will be tracked through design and development in Phase 2. Other hazards will require ongoing safety management through the duration of the deployment in Phase 3. A named safety manager will lead a safety team to continue to follow all of the scenarios. The purpose will be to document verification of safety-related requirements and to coordinate safety-related activities of all stakeholders, under the direction of New York City Department of Transportation.

As the project proceeds to detailed design, safety requirements will be allocated to systems and subsystems, and to their interfaces. Evidence that requirements have been met will be collected, scrutinized, and documented. The level of documentation and independent review will be in accordance with the rating of each hazard.

Chapter 9 Supporting Documents

[1] Steve Galgano, Mohamad Talas, David Benevelli, Robert Rausch, Samuel Sim, Keir Opie, Mark Jensen, Chris Stanley, New York City Department of Transportation, Bureau of Traffic Operations. "Connected Vehicle Pilot Deployment Program Phase 1: Concept of Operations (ConOps)—New York City." FHWA-JPO-16-299. April 8, 2016.

[2] USDOD, Department of Defense Standard Practice – System Safety, May 2012, Standard No. MIL-STD-882E, http://www.system-safety.org/Documents/MIL-STD-882E.pdf

[3] Road Vehicles—Functional Safety. International Standard ISO 26262. 2011.

[4] Peiwei Wang, "USDOT Guidance Summary for Connected Vehicle Pilot Site Deployers: Safety Management." Contract No. DTFH61-11-D-00018. September 2015.

[5] John Harding, "Preparing a Safety Management Plan for Connected Vehicle Deployments." December 7, 2015.

[6] Brian C. Tefft, "Impact Speed and a Pedestrian's Risk of Severe Injury or Death." AAA Foundation for Traffic Safety. September 2011. https://www.aaafoundation.org/sites/default/files/2011PedestrianRiskVsSpeed.pdf

[7] Transportation Research Board, Managing Speed: Review of Current Practice for Setting and Enforcing Speed Limits. Special Report 254. 1998. http://onlinepubs.trb.org/onlinepubs/sr/sr254.pdf

[8] Angela W.L. Ho, M. L. Cummings, Enlie Wang, Louis Tijerina, Dev S. Kochhar, "Integrating Intelligent Driver Warning Systems: Effects of Multiple Alarms and Distraction on Driver Performance." November, 15, 2005.

[9] Maltz M, Shinar D., "Imperfect in-vehicle collision avoidance warning systems can aid drivers." Human Factors: The Journal of the Human Factors and Ergonomics Society, Summer 2004.

APPENDIX A. List of Abbreviations

AIS	Abbreviated Injury Scale
ASD	Aftermarket Safety Device
BSW	Blind Spot Warning
CV	Connected Vehicle
DSRC	Dedicated Short-Range Communication
EEBL	Emergency Electronic Brake Lights
FCW	Forward Crash Warning
GPS	Global Positioning System
IMA	Intersection Movement Assist
I-SIG	Intelligent Traffic Signal System
ISO	International Organization for Standardization
IVBSS	Integrated Vehicle-Based Safety System
LCW	Lane Change Warning
PED-SIG	Mobile Accessible Pedestrian Signal System
RSE	Road Side Equipment
SVA	Stationary Vehicle Ahead
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
U.S. DOD	United States Department of Defense
U.S. DOT	United States Department of Transportation

APPENDIX B. Rules for Assigning Severity, Exposure, and Controllability

The Rule Numbers in these three tables are used in Table C-1 to indicate the rationale for a particular rating. The meanings of the ratings are in Section 3.2 of the main text.

Table B-1. These Rules were Used to Assign Levels to Severity.

Rule Number	Description	Rating
S-A	Any incident where a vehicle strikes a pedestrian is severe.	S3
S-B	A malfunction that cannot lead to a vehicle striking a vehicle, a pedestrian, or a fixed object is at most an inconvenience. Pedestrians are assumed to be able to avoid fixed objects and one another.	S0a
S-C	A low speed crash is assumed to cause minor injuries	S1
S-D	Vehicle-to-vehicle or vehicle-to-fixed-object crashes where the speed limit is 25 mph or below cause moderate injuries.	S2
S-E	Vehicle-to-vehicle or vehicle-to-fixed-object crashes where the speed limit is above 25 mph can cause severe injuries.	S3
S-F	Fires in vehicles are S2.	S2
S-G	Existing policy or tested equipment prevents a scenario and it can be argued that the deployment will not disrupt the existing protections.	S0
S-H	The severity of a missed message depends on the application. A preliminary severity will be resolved later.	S3

Source: Battelle

Table B-2. These Rules were Used to Assign Levels to Exposure.

Rule Number	Description	Rating
E-A	Existing policy or tested equipment prevents a scenario and it can be argued that the deployment will not disrupt the existing protections.	E0
E-B	Extreme weather events, such as lightning strikes, hurricane landfall, and deep snow	E1
E-C	Storms, such as rain or ice are also rated E1, though they may actually occur more frequently.	E1
E-D	Vandalism of protected equipment happens.	E1
E-E	All organizations will experience staff turnover. Scenarios related to new employees are E2, except those associated with management or key staff or other rationale may be E1.	E2
E-F	School begins and ends every year. Work zones are established, moved, and cleared.	E2
E-G	Periodic maintenance occurs for all fleet vehicles, so maintenance itself is at least daily. Random instances of incorrect maintenance will be less often, E1 or E1.5	E2
E-H	A systematic error that affects every trip or an application expected to activate on every or nearly every trip	E4
E-I	A systematic error that affects applications expected to activate only occasionally	E3
E-J	A systematic error that is manifested only when unusual circumstances occur is rated at the frequency of those circumstances.	E2
E-K	A systematic error that is manifested only when unusual circumstances occur is rated at the frequency of those circumstances.	E1
E-L	Difficulties in radio transmission, at least at a minor level, are expected daily, unless historical data shows a different frequency.	E2
E-M	Even with training, a few participants can be expected to misunderstand their role or forget a function used infrequently.	E1
E-N	Project equipment does not deliver permissive messages.	E0
E-O	Crashes involving fleet vehicles are expected a few times during the deployment.	E1
E-P	Delayed DSRC messages are rare.	E0

Source: Battelle

Table B-3. These Rules were Used to Assign Levels to Controllability.

Rule Number	Description	Rating
C-A	Frequent unwarranted messages create a distraction and can degrade performance.	C1
C-B	Ignoring or missing a message that calls for action is an incorrect response.	C3
C-C	Failure to present an advisory message when a message is warranted will not degrade the performance of a normal driver with all ordinary information (sights and sounds) available. Missed alerts are rated C1 to account for the case of a driver who has become accustomed to them and expects to be alerted to developing situations.	C1
C-D	Distractions other than frequent unwarranted messages, such as displays that are difficult to interpret or loose equipment, can cause the driver to miss important external information.	C2
C-E	A message with incorrect information, even if it be only an advisory, is rated as less controllable than a missing message or a spurious message. The incorrect message will, at a minimum, require cognitive effort to discount, and may yield an incorrect response.	C2
C-F	A driver who misinterprets a signal or misunderstands the desired response will definitely behave inappropriately.	C3
C-G	Traffic signals will be obeyed by drivers and pedestrians, so any improper operation by traffic signals cannot be overcome by travelers.	C3
C-H	System-wide malfunctions that can be recognized by staff at the Traffic Management Center can be controlled by those staff. Rank C1 instead of C0 because TMC staff will take time to respond and travelers will be affected until response is complete.	C1
C-I	A driver confronted with a fire can stop and exit the vehicle, but must do so promptly.	C2
C-J	A driver stranded by a disabled vehicle is wholly unable to use the vehicle to continue the trip.	C3
C-K	Equipment or wiring in the wrong place should not be moved by the driver while in motion and will slow emergency responders	C3
C-L	Any defect that exacerbates injury during a crash or impairs rescue following a crash is wholly uncontrollable by the driver	C3
C-M	Participant will notice nothing unusual, and normal movement is the proper course.	C0
C-N	Harm that occurs regardless of driver response is not controllable.	C3
C-O	Any system feature (static equipment or inappropriate message) that leads a driver to take harm-causing action is not controllable.	C3
C-P	Avoiding a crash requires skills beyond what is expected in most drivers. Professional drivers would be challenged beyond their ordinary skill to avoid a crash.	C3
C-Q	The response may be a more sudden steering or a harder braking.	C2
C-R	Removing information from a driver (e.g., blocking a view) is not controllable.	C3

Source: Battelle

APPENDIX C. Hazard Analysis and Risk Assessment with the Risk Response Plans

Table C-1. Preliminary Hazard Analysis and Risk Assessment.

The Rule Numbers and associated ratings are explained in Appendix B. The ratings are used to determine the ASIL according to Figure 5-1 in the main text.

			Exposure		Severity		Controllability		
ID	Description	Effects	Rule	Rating	Rule	Rating	Rule	Rating	ASIL
1	Threshold is too low. False positives (unwarranted messages) occur frequently.	Truly important messages are ignored by the operator	E-H	E4	S-H	S3	C-A	C1	B
2	Threshold is too high.	False negatives occur, and alerts are not transmitted to the driver.	E-H	E4	S-H	S3	C-C	C1	B
3	PED-SIG misinterprets pedestrian's intended direction.	Signal presents a Walk signal to the wrong direction and not to the desired direction.	E-H	E4	S-A	S3	C-O	C3	D
4	Pedestrian incorrectly signals intended direction.	Signal presents a Walk signal to the wrong direction and not to the desired direction.	E-M	E1	S-A	S3	C-O	C3	A
5	PED-SIG presents a walk signal for the wrong direction	Visually disabled pedestrian enters oncoming traffic stream	E-H	E4	S-A	S3	C-O	C3	D
6	PED-SIG presents a delayed or early walk signal	Visually disabled pedestrian enters oncoming traffic stream	E-H	E4	S-A	S3	C-O	C3	D
7	Delayed message transmits incorrect phase	Driver approaching a red signal is not alerted.	E-P	E0	S-A	S3	C-C	C1	--
8	Local speed limit is wrong	False positive or false negative warnings are issued	E-H	E4	S-C	S1	C-E	C2	A
9	Location of a curve, work zone, school, size restriction, or other special condition is wrong	False positive AND false negative warnings are issued	E-H	E4	S-A	S3	C-E	C2	C
10	Time of work zone or school zone is wrong	False positive AND false negative warnings are issued	E-H	E4	S-A	S3	C-E	C2	C
11	Valid alerts occur too frequently.	Truly important messages are ignored by the operator	E-H	E4	S-B	S0a	C-C	C1	--
12	Audible messages are too quiet.	Messages are not heeded by the operator	E-H	E4	S-H	S3	C-B	C1	B
13	Audible messages are indistinguishable from other sounds.	Messages are not heeded by the operator	E-H	E4	S-H	S3	C-B	C1	B
14	Drivers (or pedestrians) become too dependent.	Drivers (or pedestrians) do not practice necessary defensive driving skills.	E-M	E1	S-D	S2	C-C	C1	QM
15	Meaning of messages is unclear	Driver takes the wrong action.	E-J	E2	S-D	S2	C-F	C3	A
16	Messages are too terse to clearly convey the situation	Driver takes the wrong action.	E-J	E2	S-D	S2	C-F	C3	A
17	Messages are too complicated to be parsed in time	Driver takes the wrong action or acts too late.	E-H	E4	S-D	S2	C-D	C2	B
18	Vehicle dimensions coded in an ASD are too big.	Unwarranted alerts are sent to the driver.	E-H	E4	S-C	S1	C-E	C2	A
19	Vehicle dimensions coded in an ASD are too small.	Necessary alerts are not sent to the driver.	E-H	E4	S-H	S3	C-C	C1	B
20	Roadway dimensions coded in an RSE are too big	Necessary alerts are not sent to the driver.	E-H	E4	S-H	S3	C-C	C1	B
21	Roadway dimensions coded in an RSE are too small.	Unwarranted alerts are sent to the driver.	E-H	E4	S-D	S2	C-E	C2	B
22	Bad indicator design (Poor choice of color, icon shape, location, or sound)	Driver is confused and responds inappropriately to messages.	E-J	E2	S-D	S2	C-F	C3	A
23	Bad indicator design (Poor choice of color, icon shape, location, or sound)	Driver is frustrated and ignores messages.	E-J	E2	S-D	S2	C-B	C1	QM
24	Bad indicator design (Poor choice of color, icon shape, location, or sound)	Driver is distracted and misses external cues and causes a crash.	E-J	E2	S-D	S2	C-D	C2	QM
25	Poor design puts the ASD wiring in a precarious location	Electrical fire starts	E-H	E4	S-F	S2	C-I	C2	B
26	Poor design overloads a circuit in the vehicle	Electrical fire starts	E-H	E4	S-F	S2	C-I	C2	B
27	Rain or fog interferes with DSRC.	DSRC messages are not transmitted	E-C	E1	S-H	S3	C-C	C1	QM
28	Lightning interferes with DSRC.	DSRC messages are not transmitted	E-B	E1	S-H	S3	C-C	C1	QM
29	Electromagnetic interference from construction equipment or electrical distribution	DSRC messages are not transmitted	E-L	E2	S-H	S3	C-C	C1	QM
30	Sun interferes with DSRC	DSRC messages are not transmitted	E-C	E1	S-H	S3	C-C	C1	QM
31	Multipath transmission degrades DSRC messages.	Some messages are dropped	E-L	E2	S-H	S3	C-C	C1	QM
32	Packet collisions because high congestion overwhelms BSM receivers	Some messages are dropped; system may break down	E-L	E2	S-H	S3	C-C	C1	QM
33	Bad design of the ASD, VAD, or DAS permits it to drain the battery	Driver is stranded in the middle of the night.	E-H	E4	S-B	S0a	C-J	C3	--
34	Bad design of the ASD, VAD, or DAS leads to degradation of the CAN bus interface	Vehicle performs poorly or not at all	E-H	E4	S-C	S1	C-J	C3	B
35	Improper installation of the ASD, VAD, or DAS drains the battery.	Driver is stranded in the middle of the night.	E-E	E2	S-B	S0a	C-J	C3	--
36	Improper installation of the ASD, VAD, or DAS leads to degradation of the CAN bus interface	Vehicle performs poorly or not at all	E-E	E2	S-C	S1	C-J	C3	QM
37	Improper installation puts the ASD wiring in a precarious location	Electrical fire starts	E-E	E2	S-F	S2	C-I	C2	QM

Table C-1. Preliminary Hazard Analysis and Risk Assessment. **(Cont.)**

			Exposure		Severity		Controllability		
ID	Description	Effects	Rule	Rating	Rule	Rating	Rule	Rating	ASIL
38	Improper installation overloads a circuit in the vehicle	Electrical fire starts	E-E	E2	S-F	S2	C-I	C2	QM
39	Component-level failure causes board to misbehave	Signals are incorrect or missing	E-K	E1	S-H	S3	C-E	C2	QM
40	Component-level failure causes board to misbehave	Fire starts	E-K	E1	S-F	S2	C-I	C2	QM
41	Board-level failure causes device to misbehave	Signals are incorrect or missing	E-K	E1	S-H	S3	C-E	C2	QM
42	Board-level failure causes device to misbehave	Fire starts	E-K	E1	S-F	S2	C-I	C2	QM
43	Power-level failure	Fire starts	E-K	E1	S-F	S2	C-I	C2	QM
44	Incoming messages are misinterpreted by the ASD	Incorrect messages are presented to the driver	E-H	E4	S-H	S3	C-E	C2	C
45	Broadcast messages are incorrect	Another vehicle or the infrastructure behaves improperly	E-H	E4	S-H	S3	C-Q	C2	C
46	ASD misinterprets messages from the CAN bus	Incorrect messages are presented to the driver	E-H	E4	S-H	S3	C-E	C2	C
47	ASD misinterprets messages from the CAN bus	Improper BSMs are broadcast, so another vehicle or the infrastructure behaves improperly	E-H	E4	S-H	S3	C-Q	C2	C
48	Inadequate or confusing training	Inappropriate response to messages	E-I	E3	S-H	S3	C-F	C3	C
49	Inadequate or confusing training	Driver has extra confidence and ignores standard visual and auditory cues, causing a crash	E-I	E3	S-E	S3	C-F	C3	C
50	Frustration with the device leads to tampering or its unauthorized removal	Cues to the driver are lost and messages to other vehicles are lost	E-K	E1	S-H	S3	C-C	C1	QM
51	In-vehicle computers cannot process high density of messages quickly enough.	Alerts are delayed or missed.	E-J	E2	S-H	S3	C-C	C1	QM
52	Outdoor components damaged by vandalism	Messages are not transmitted	E-D	E1	S-H	S3	C-C	C1	QM
53	Outdoor components damaged by weather	Messages are not transmitted	E-C	E1	S-H	S3	C-C	C1	QM
54	Power line in the signal control box is overloaded the power line	Inadequate voltage for the controller or blown fuse or damage the traffic controller	E-A	E0	S-D	S2	C-G	C3	--
55	Untrained maintenance personnel fail to re-install project equipment or install it incorrectly	Messages are not transmitted inward or outward	E-E	E2	S-H	S3	C-C	C1	QM
56	Controller firmware is upgraded or other maintenance is performed without regard to our equipment	Controller fails	E-G	E2	S-D	S2	C-G	C3	A
57	Project equipment causes one signal controller to malfunction	Signal displays four-way green.	E-A	E0	S-D	S2	C-G	C3	--
58	Project equipment causes one signal controller to malfunction	Amber phase is unreasonably short.	E-A	E0	S-D	S2	C-G	C3	--
59	Project equipment causes one signal controller to malfunction	Signal controller locks or becomes unreasonably slow	E-A	E0	S-D	S2	C-G	C3	--
60	Temporary failure of the NYCWiN backhaul floods the backhaul network	Impaired coordination impedes traffic flow	E-J	E2	S-B	S0a	C-G	C3	--
61	Project equipment causes a failure of an adjacent controller	Impaired coordination impedes traffic flow	E-J	E2	S-B	S0a	C-G	C3	--
62	Incorrect signals to Traffic Control System cause inappropriate action to be taken	Midtown traffic is slowed	E-K	E1	S-B	S0a	C-G	C3	--
63	Location from GPS is incorrect to an ASD or PID	Inappropriate message is transmitted to the driver or pedestrian.	E-L	E2	S-A	S3	C-E	C2	A
64	Equipment on the exterior of a vehicle protrudes beyond the normal envelope	Pedestrian is hurt	E-I	E3	S-A	S3	C-N	C3	C
65	Internal equipment not mounted securely	Becomes loose over time and distracts the driver	E-I	E3	S-D	S2	C-D	C2	A
66	Internal equipment not mounted securely	Becomes loose over time and blocks driver's line of sight	E-I	E3	S-E	S3	C-R	C3	C
67	Internal equipment not mounted securely	Becomes loose during a crash and injures the occupant	E-O	E1	S-D	S2	C-D	C2	QM
68	Internal equipment has hard surfaces or sharp corners near an occupant	Struck by an occupant during a crash and increases injury.	E-H	E4	S-D	S2	C-L	C3	C
69	Internal equipment blocks driver's view	Driver misses external cues and causes a crash	E-H	E4	S-E	S3	C-R	C3	D
70	CAN interference degrades active restraints	Occupant injury is exacerbated	E-O	E1	S-E	S3	C-L	C3	A
71	Wiring or devices in the vehicle interfere with extrication	Emergency medical service is delayed	E-O	E1	S-E	S3	C-L	C3	A
72	Processing algorithms take too long	Messages are not timely	E-H	E4	S-H	S3	C-E	C2	C
73	Multiple events occur nearly simultaneously	System locks or displays a low-risk or otherwise inappropriate message.	E-L	E2	S-H	S3	C-E	C2	A

Source: Battelle

Table C-2. Risk Response Plan.

ID	Description	ASIL	Type	Action
1	Threshold is too low. False positives (unwarranted messages) occur frequently.	B	Functional Safety Requirements	Develop and test algorithms and thresholds.
2	Threshold is too high.	B	Functional Safety Requirements	Develop and test algorithms and thresholds.
3	PED-SIG misinterprets pedestrian's intended direction.	D	Functional Safety Requirements	Develop requirements on the accuracy of interpreting pedestrian's intended directions.
4	Pedestrian incorrectly signals intended direction.	A	Functional Safety Requirements	Develop training requirements for PED-SIG application
5	PED-SIG presents a walk signal for the wrong direction	D	Functional Safety Requirements	A safety-critical requirement will be that PED-SIG application cannot advise pedestrian to walk in a direction when "do not walk" is displayed. Verify to 1 in a billion.
6	PED-SIG presents a delayed or early walk signal	D	Functional Safety Requirements	A safety-critical requirement will be that PED-SIG application cannot advise pedestrian to walk in a direction when "do not walk" is displayed. Verify to 1 in a billion.
7	Delayed message transmits incorrect phase	--	--	--
8	Local speed limit is wrong	A	Functional Safety Requirements	Write a requirement for verifying data entry. Test an installed prototype.
9	Location of a curve, work zone, school, size restriction, or other special condition is wrong	C	Functional Safety Requirements	Write a requirement for verifying data entry, comparing the device to the primary source of data. Test an installed prototype. Write a procedure to periodically check non-fixed objects (e.g., moving work zone).
10	Time of work zone or school zone is wrong	C	Safety Management	Write a requirement for verifying data entry. Write procedure for checking periodically for changes and planning for schedule changes (e.g., the end of the school year)
11	Valid alerts occur too frequently.	--	Export	Develop thresholds
12	Audible messages are too quiet.	B	Functional Safety Requirements	Develop vehicle-specific design guidelines, followed by testing in a realistic traffic environment
13	Audible messages are indistinguishable from other sounds.	B	Functional Safety Requirements	Develop vehicle-specific design guidelines, followed by testing in a realistic traffic environment
14	Drivers (or pedestrians) become too dependent.	QM	Safety Management	Periodically spot check driver attitudes through their feedback.
15	Meaning of messages is unclear	A	Functional Safety Requirements	Write a requirement for verifying data entry. Test an installed prototype.
16	Messages are too terse to clearly convey the situation	A	Functional Safety Requirements	Write a requirement for verifying data entry. Test an installed prototype.
17	Messages are too complicated to be parsed in time	B	Functional Safety Requirements	Write a requirement for verifying data entry. Test an installed prototype.
18	Vehicle dimensions coded in an ASD are too big.	A	Safety Management	Write procedures for confirming dimensions when an ASD is installed in a truck, and when one is re-installed.
19	Vehicle dimensions coded in an ASD are too small.	B	Safety Management	Write procedures for confirming dimensions when an ASD is installed in a truck, and when one is re-installed.
20	Roadway dimensions coded in an RSE are too big	B	Safety Management	Write a requirement for verifying data entry. Test an installed prototype.
21	Roadway dimensions coded in an RSE are too small.	B	Safety Management	Write a requirement for verifying data entry. Test an installed prototype.
22	Bad indicator design (Poor choice of color, icon shape, location, or sound)	A	Functional Safety Requirements	Write requirements for interface design; test before production
23	Bad indicator design (Poor choice of color, icon shape, location, or sound)	QM	Functional Safety Requirements	Write requirements for interface design; test before production
24	Bad indicator design (Poor choice of color, icon shape, location, or sound)	QM	Functional Safety Requirements	Write requirements for interface design; test before production
25	Poor design puts the ASD wiring in a precarious location	B	Functional Safety Requirements	Write requirements for wiring location.
26	Poor design overloads a circuit in the vehicle	B	Functional Safety Requirements	Write a requirement for maximum power demand of installation; test before production
27	Rain or fog interferes with DSRC.	QM	Functional Safety Requirements	Write requirements that outdoor equipment withstand 50-year weather events
28	Lightning interferes with DSRC.	QM	Functional Safety Requirements	Write requirements that outdoor equipment withstand 50-year weather events
29	Electromagnetic interference from construction equipment or electrical distribution	QM	Functional Safety Requirements	Characterize EMI from the worst likely equipment; write a requirement that the ASDs can work in that environment.
30	Sun interferes with DSRC	QM	Functional Safety Requirements	Write requirements that outdoor equipment withstand 50-year weather events
31	Multipath transmission degrades DSRC messages.	QM	Functional Safety Requirements	Write requirements that DSRC receivers can handle the urban environment.
32	Packet collisions because high congestion overwhelms BSM receivers	QM	Functional Safety Requirements	Write requirements that DSRC receivers can handle the anticipated throughput rate.
33	Bad design of the ASD, VAD, or DAS permits it to drain the battery	--	Export	Write requirements to design against these hazards.
34	Bad design of the ASD, VAD, or DAS leads to degradation of the CAN bus interface	B	Functional Safety Requirements	Write requirements to design against these hazards.
35	Improper installation of the ASD, VAD, or DAS drains the battery.	--	Export	Write clear installation instructions; test the training or inspect the installations.
36	Improper installation of the ASD, VAD, or DAS leads to degradation of the CAN bus interface	QM	Functional Safety Requirements	Write clear installation instructions; test the training or inspect the installations.
37	Improper installation puts the ASD wiring in a precarious location	QM	Functional Safety Requirements	Write requirement for the design of the location of the wiring.

Table C-2. Risk Response Plan. (Cont.)

ID	Description	ASIL	Type	Action
38	Improper installation overloads a circuit in the vehicle	QM	Functional Safety Requirements	Write a requirement for maximum power demand of installation; test before production
39	Component-level failure causes board to misbehave	QM	Functional Safety Requirements	Write requirements on design and testing for the customized electronics.
40	Component-level failure causes board to misbehave	QM	Functional Safety Requirements	Write requirements on design and testing for the customized electronics.
41	Board-level failure causes device to misbehave	QM	Functional Safety Requirements	Write requirements on design and testing for the customized electronics.
42	Board-level failure causes device to misbehave	QM	Functional Safety Requirements	Write requirements on design and testing for the customized electronics.
43	Power-level failure	QM	Functional Safety Requirements	Write requirements on design and testing for the customized electronics.
44	Incoming messages are misinterpreted by the ASD	C	Functional Safety Requirements	Write clear interface documents for BSMs, TIMs, etc.
45	Broadcast messages are incorrect	C	Functional Safety Requirements	Write clear interface documents for BSMs, TIMs, etc.
46	ASD misinterprets messages from the CAN bus	C	Functional Safety Requirements	Refer to the CAN manuals for every vehicle; test every vehicle for every message in many situations.
47	ASD misinterprets messages from the CAN bus	C	Functional Safety Requirements	Refer to the CAN manuals for every vehicle; test every vehicle for every message in many situations.
48	Inadequate or confusing training	C	Functional Safety Requirements	Write clear and exhaustive objectives for training; test the training;
49	Inadequate or confusing training	C	Functional Safety Requirements	Write clear and exhaustive objectives for training; test the training;
50	Frustration with the device leads to tampering or its unauthorized removal	QM	Safety Management	Provide ongoing feedback channels; respond promptly to concerns
51	In-vehicle computers cannot process high density of messages quickly enough.	QM	Functional Safety Requirements	Write a requirement for the minimum requirement for on-board computer processing capabilities
52	Outdoor components damaged by vandalism	QM	Standard Response or Backup Plan	Develop a plan for periodic functional tests and direction inspection, with necessary repairs
53	Outdoor components damaged by weather	QM	Standard Response or Backup Plan	Develop a plan to recover from adverse weather
54	Power line in the signal control box is overloaded the power line	--	--	--
55	Untrained maintenance personnel fail to re-install project equipment or install it incorrectly	QM	Safety Management	Write a requirement for checking after maintenance is performed to ensure equipment is functioning properly.
56	Controller firmware is upgraded or other maintenance is performed without regard to our equipment	A	Safety Management	Write a requirement for checking after updates and maintenance are performed to ensure equipment is functioning properly.
57	Project equipment causes one signal controller to malfunction	--	--	--
58	Project equipment causes one signal controller to malfunction	--	--	--
59	Project equipment causes one signal controller to malfunction	--	Functional Safety Requirements	If the controller makes this truly impossible, we need not track the hazard further.
60	Temporary failure of the NYCWiN backhaul floods the backhaul network	--	Export	Follow interface documents for NYCWiN
61	Project equipment causes a failure of an adjacent controller	--	Export	Follow interface documents for existing controllers
62	Incorrect signals to Traffic Control System cause inappropriate action to be taken	--	Export	Apply rules for traffic flow (probably this will involve adding extra branches to an existing FMEA or FTA and then deriving new requirements)
63	Location from GPS is incorrect to an ASD or PID	A	Functional Safety Requirements	Write requirements on GPS accuracy and detection of when the accuracy is not achieved.
64	Equipment on the exterior of a vehicle protrudes beyond the normal envelope	C	Functional Safety Requirements	Write rules on the envelope and shape of external equipment.
65	Internal equipment not mounted securely	A	Functional Safety Requirements	This one will become part of the next, which has a higher ASIL.
66	Internal equipment not mounted securely	C	Functional Safety Requirements	Write rules for installation
67	Internal equipment not mounted securely	QM	Functional Safety Requirements	This one will become part of the previous, which has a higher ASIL.
68	Internal equipment has hard surfaces or sharp corners near an occupant	C	Functional Safety Requirements	Position interior equipment out of the way, or make its surfaces compliant with FMVSS 201.
69	Internal equipment blocks driver's view	D	Functional Safety Requirements	Write requirements for driver's vision
70	CAN interference degrades active restraints	A	Functional Safety Requirements	Follow industry guidelines on CAN use.
71	Wiring or devices in the vehicle interfere with extrication	A	Functional Safety Requirements	Develop requirements on the location of in-vehicle components
72	Processing algorithms take too long	C	Functional Safety Requirements	Develop requirements on the timeliness of messages. Flow them down to DSRC latency, hardware and software handling of BSMs and TIMs, etc.
73	Multiple events occur nearly simultaneously	A	Functional Safety Requirements	Develop threat arbitration rules. Rules may need to be specific to vehicles or travelers

Source: Battelle

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-16-301

U.S. Department of Transportation