Phase 1 Safety Management Plan (SMP)

Buffalo ITS4US Deployment Project

www.its.dot.gov/index.htm

Draft Report – August 31, 2021
Publication Number FHWA-JPO-21-873

COMPLETE TRIP
ITS4US

U.S. Department of Transportation

Produced by (Name of Contract)
U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office
Federal Highway Administration
Office of the Assistant Secretary for Research and Technology
Federal Transit Administration

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-21-873		

4. Title and Subtitle	5. Report Date
Phase 1 Safety Management Plan (SMP) – Buffalo NY ITS4US Deployment Project	August 31, 2021
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Deepak Gopalakrishna (ICF), Nayel Urena Serulle (ICF), Cindy Peck (ICF), Adel Sadek (UB), Robert Jones (NFTA), Jordana Maisel (UB), Victor Paquet (UB), Edward Stanfield (UB), Polly Okunieff (ICF), Chunming Qiao (UB), Stephen Still (UB), Rahul Dagli (ICF), Katie O'Sullivan (ICF), Xin Liu (UB) Yunpeng Shi (UB)	Task 4 - SMP

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
ICF International, 9300 Lee Highway, Fairfax, VA 22031 University at Buffalo, Amherst, NY 14228 Open Doors Organization, 8600 W. Catalpa Avenue, Chicago, IL 60656 RSG, 55 Railroad Row, Suite 101, White River Junction, VT 05001 ETCH, 4696 Smothers Road, Westerville, OH 43081 BNMC, 640 Ellicott Street, Buffalo, NY 14203 NFTA, 181 Ellicott Street, Buffalo, NY 14203	**11. Contract or Grant No.** 693JJ321C000005

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	Safety Management Plan
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

Elina Zlotchenko (USDOT ITS-JPO) is the Contracts Officer Representative (COR) and Amalia Rodezno (USDOT) will be the Contracting Officer (CO).

16. Abstract

The Buffalo NY ITS4US Deployment Project seeks to improve mobility to, from and within the Buffalo Niagara Medical Campus by deploying new and advanced technologies with a focus on addressing existing mobility and accessibility challenges. Examples of the technologies to be deployed are electric and self-driving shuttles, a trip planning app that is customized for accessible travel, intersections that use tactile and mobile technologies to enable travelers with disabilities navigate intersections, and Smart Infrastructure to support outdoor and indoor wayfinding. The deployment geography includes the 120-acre Medical Campus and surrounding neighborhoods with a focus on three nearby neighborhoods (Fruit Belt and Masten Park) with underserved populations, older adults, and persons with disabilities. This document describes the Safety Management Plan (SMP) for Phase 1 of the Complete Trip Deployment in Buffalo, NY. The plan identifies the safety needs and scenarios, conducts a risk assessment analysis, and identifies safety operations scenarios to mitigate identified risks.

17. Keywords	18. Distribution Statement
ITS4US; Complete Trip; Deployment; ITS; Intelligent Transportation Systems, Safety, and AV safety.	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		85	

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

Revision History

Name	Date	Version	Summary of Changes
ICF	July 26, 2021	0.1	Initial Draft.
ICF	Aug 23, 2021	0.2	Edited based on comments received from USDOT.
ICF	Aug 31, 2021	0.3	Edited based on second round of comments received from USDOT.

Table of Contents

1 Introduction 1

1.1 Document Overview 1

1.2 Project Background 2

1.3 References 3

2 Safety Overview and Relationships 5

2.1 Related Project Tasks 5

2.2 Safety Stakeholders 6

2.3 Safety Risk Process and Approach 9

2.3.1 Safety Needs and Hazard Identification 10

2.3.2 Safety Risk Assessment 10

3 Safety Needs and Scenarios 13

3.1 Safety Needs & Hazards for UC 1 – Register Profile & Preferences 14

3.2 Safety Needs & Hazards for UC 2 – Generate Trip Plan and Book a Trip 14

3.3 Safety Needs & Hazards for UC 3 – Public Transportation Services 16

3.4 Safety Needs & Hazards for UC 4 – Navigation 17

3.5 Safety Needs & Hazards for UC 5 – Reporting & History 20

3.6 Safety Needs & Hazards for UC 6 – Ride hailing, Reservation, and Dispatch 20

3.7 Safety Needs & Hazards for UCs 7 & 8 – Passenger Pick-up, Securement, Travel and Drop-off via an SDS / HDS 21

3.8 Safety Needs & Hazards for UC9 – Manage Incidents 25

3.9 Safety Needs & Hazards for UC10 – PedX Request 27

4 Assessment of Safety Risks 29

4.1 User Safety Risk Assessment 30

4.1.1 Risk SF-U-1 – Contradictory preferences 30

4.1.2 Risk SF-U-2 – Preference/notification selection mismatch with end user's device 31

4.1.3 Risk SF-U-3 – No trip plan generated 31

4.1.4 Risk SF-U-4 – Unintended destination 32

4.1.5 Risk SF-U-5 – Traveler trips 32

4.1.6 Risk SF-U-6 – Traveler early exit 33

4.1.7 Risk SF-U-7 – Traveler misses exit 33

4.1.8 Risk SF-U-8 – Traveler health emergency 34

4.1.9 Risk SF-U-9 – HDS driver health emergency 34

4.1.10 Risk SF-U-10 – SDS steward health emergency 35

4.1.11 Risk SF-U-11 – Emergency stop button misusage 35

4.2 System Safety Risk Assessment 36
4.2.1 Risk SF-S-1 – No trip booking available 36
4.2.2 Risk SF-S-2 – No return trip booking available 37
4.2.3 Risk SF-S-3 – Mismatched vehicle to traveler needs 37
4.2.4 Risk SF-S-4 – Delayed vehicles....37
4.2.5 Risk SF-S-5 – No-show vehicles 38
4.2.6 Risk SF-S-6 – Delayed notifications about late shuttles / PAL 38
4.2.7 Risk SF-S-7– Inaccessible directions 39
4.2.8 Risk SF-S-8 – Inaccurate directions 39
4.2.9 Risk SF-S-9 – Orientation inaccuracy....40
4.2.10 Risk SF-S-10 – Positional inaccuracy....40
4.2.11 Risk SF-S-11 – Inaccurate sidewalk data....41
4.2.12 Risk SF-S-12 – Inaccurate indoor facility data 41
4.2.13 Risk SF-S-13 – Traveler mobile device not linking with indoor/outdoor Smart Signs....42
4.2.14 Risk SF-S-14 – Inaccurate or delayed dynamic information about work zone and obstructions....42
4.2.15 Risk SF-S-15 – Insufficient shuttle availability 43
4.2.16 Risk SF-S-16 – Unavailable special equipment's occupancy information 43
4.2.17 Risk SF-S-17 – Inaccurate pick-up/drop-off information 44
4.2.18 Risk SF-S-18 – SDS/HDS accessibility equipment malfunction....44
4.2.19 Risk SF-S-19 – Pick-up, Drop-off location occupied 45
4.2.20 Risk SF-S-20 – SDS/HDS moves before traveler is secured 45
4.2.21 Risk SF-S-21 – SDS/HDS sudden stops....46
4.2.22 Risk SF-S-22 – SDS driving environment beyond ODD....47
4.2.23 Risk SF-S-23 – Traveler misses connection trip 47
4.2.24 Risk SF-S-24 – Delay or missed stop caused by re-route....48
4.2.25 Risk SF-S-25 – V2X connection lost....48
4.2.26 Risk SF-S-26 – SDS Hardware/physical element malfunction....49
4.2.27 Risk SF-S-27 – SDS/HDS accessibility/securement mechanisms malfunction....49
4.2.28 Risk SF-S-28 – Driver/steward abandonment....50
4.2.29 Risk SF-S-29 - SDS/HDS rear-ended collision 50
4.2.30 Risk SF-S-30 - SDS-pedestrian collision....51
4.2.31 Risk SF-S-31 - SDS frontal collision 51
4.2.32 Risk SF-S-32 – Failing linking traveler’s mobile device with Ped request signal 52
4.2.33 Risk SF-S-33 – Dropped request at intersection....52
4.2.34 Risk SF-S-34 – Incorrect Ped-X signal direction 53
4.2.35 Risk SF-S-35 – Inaccurate Ped-X signal timing 53
4.2.36 Risk SF-S-36 – Delayed Ped-X signal alert....54

5 Safety Operational Concept 55
5.1 Safety Design Elements 55
5.2 Safety Operational Processes 57
5.3 Mitigations and Fail-Safes 58
5.4 Safety Responses 59
5.5 Safety Reporting 60
6 Safety Management Summary 61
6.1 Safety Risk Summary 61
6.2 Continuing Safety Planning 69
Appendix A. Acronyms and Glossary 71

List of Tables

Table 1. References Used 3
Table 2. Safety Stakeholders List 7
Table 3. Modified ASIL Determination (Adapted from ISO 26262) 11
Table 4. Safety Needs and Scenarios (Hazards) associated with UC1. 14
Table 5. Safety Needs and Scenarios (Hazards) associated with UC2. 15
Table 6. Safety Needs and Scenarios (Hazards) associated with UC3. 16
Table 7. Safety Needs and Scenarios (Hazards) associated with UC4. 18
Table 8. Safety Needs and Scenarios (Hazards) associated with UC6. 20
Table 9. Safety Needs and Scenarios (Hazards) associated with UCs 7 & 8. 22
Table 10. Safety Needs and Scenarios (Hazards) associated with UC9. 25
Table 11. Safety Needs and Scenarios (Hazards) associated with UC10. 27
Table 12. Risk Assessment of the Contradictory Preferences Hazard. 31
Table 13. Risk Assessment of the Preference/notification Selection Mismatch with End User's Device Hazard. 31
Table 14. Risk Assessment of the No Trip Plan Generated Hazard. 32
Table 15. Risk Assessment of the Unintended Destination Hazard. 32
Table 16. Risk Assessment of the Traveler Trips Hazard. 33
Table 17. Risk Assessment of the Traveler Early Exit Hazard. 33
Table 18. Risk Assessment of the Traveler Misses Exit Hazard. 34
Table 19. Risk Assessment of the Traveler Health Emergency Hazard. 34
Table 20. Risk Assessment of the HDS Driver Health Emergency Hazard. 35
Table 21. Risk Assessment of the SDS Steward Health Emergency Hazard. 35
Table 22. Risk Assessment of the Emergency Stop Button Misusage Hazard. 36
Table 23. Risk Assessment of the No Trip Booking Available Hazard. 36
Table 24. Risk Assessment of the No Return Trip Booking Available Hazard. 37
Table 25. Risk Assessment of the Mismatched Vehicle to Traveler Needs Hazard. 37
Table 26. Risk Assessment of the Delayed Vehicles Hazard. 38
Table 27. Risk Assessment of the No-show Vehicles Hazard. 38
Table 28. Risk Assessment of the Delayed Notifications about Late Shuttles Hazard. 39
Table 29. Risk Assessment of the Inaccessible Directions Hazard. 39
Table 30. Risk Assessment of the Inaccurate Directions Hazard. 40
Table 31. Risk Assessment of the Orientation Inaccuracy Hazard. 40
Table 32. Risk Assessment of the Positional Inaccuracy Hazard. 41
Table 33. Risk Assessment of the Inaccurate Sidewalk Data Hazard. 41
Table 34. Risk Assessment of the Inaccurate Indoor Facility Data Hazard. 42
Table 35. Risk Assessment of the Traveler Mobile Device Not Linking with Indoor/outdoor Smart Signs Hazard. 42
Table 36. Risk Assessment of the Inaccurate or Delayed Dynamic Information about WZ and Obstructions Hazard. 43
Table 37. Risk Assessment of the Insufficient Shuttle Availability Hazard. 43
Table 38. Risk Assessment of the Unavailable Special Equipment Occupancy Information Hazard. 44

Table 39. Risk Assessment of the Inaccurate Pick-up/Drop-off Information Hazard. 44
Table 40. Risk Assessment of the SDS/HDS Accessibility Equipment Malfunction Hazard. 45
Table 41. Risk Assessment of the Pick-up or Drop-off Hazard. 45
Table 42. Risk Assessment of the SDS/HDS Moves before Traveler is Secured Hazard 46
Table 43. Risk Assessment of the SDS/HDS Sudden Stops Hazard. 46
Table 44. Risk Assessment of the SDS Driving Environment beyond ODD Hazard. 47
Table 45. Risk Assessment of the Traveler Misses Connection Trip Hazard. 47
Table 46. Risk Assessment of the Delay or Missed Stop Caused by Re-route Hazard. 48
Table 47. Risk Assessment of the V2X connection lost Hazard. 48
Table 48. Risk Assessment of the SDS Hardware/physical Element Malfunction Hazard. 49
Table 49. Risk Assessment of the SDS/HDS Accessibility/securement Mechanisms Malfunction Hazard. 49
Table 50. Driver/steward Abandonment Hazard. 50
Table 51. Risk Assessment of the SDS/HDS Rear-ended Collision Hazard. 50
Table 52. Risk Assessment of the SDS-pedestrian Collision Hazard. 51
Table 53. Risk Assessment of the SDS Frontal Collision Hazard. 51
Table 54. Risk Assessment of the Failing Linking Traveler's Mobile Device with Ped Request Signal Hazard. 52
Table 55. Risk Assessment of the Dropped Request at Intersection Hazard. 52
Table 56. Risk Assessment of the Incorrect Ped-X Signal Direction Hazard. 53
Table 57. Risk Assessment of the Inaccurate Ped-X Signal Timing Hazard. 53
Table 58. Risk Assessment of the Delayed Ped-X Signal Alert Hazard. 54
Table 59. Safety Scenarios that will be addressed by Adding Safety Design Elements 56
Table 60. Safety Scenarios that will be addressed by Safety Operational Processes 57
Table 61. Safety Scenarios that will be addressed by Mitigation and/or Fail-Safe Strategies 59
Table 62. Safety Scenarios that will be addressed by Safety or Emergency Response Plans 60
Table 63. Safety Risk Management Summary 61
Table 64. Acronyms used in the SMP 71

List of Figures

Figure 1. Relationship between the SMP Task and Other Tasks of the Project. 5

1 Introduction

Buffalo, New York (NY) is one of five sites selected for the U.S Department of Transportation (USDOT) Complete Trip - ITS4US Deployment Program, which seeks to integrate innovative technologies to improve mobility and accessibility. The Buffalo, NY project plans to deploy an integrated set of travel support services and systems within neighborhoods surrounding Buffalo Niagara Medical Campus (BNMC).

The Phase 1 Safety Management Plan (SMP) describes the planning and preparation undertaken by the Buffalo NY ITS4US project to identify potential hazards and safety needs, assess their risk, and develop strategies and countermeasures to minimize their risk, manage and respond to potential safety issues. Some clear safety issues will likely emerge from the introduction of innovative technologies, such as self-driving feeder shuttles. However, there are also more subtle safety challenges to account for, such as recommending routes that may not be safe (e.g., routing pedestrians with disabilities through work zones). The SMP categorizes these safety scenarios for their risks, severity, exposure, and controllability. The risks are categorized based on the framework established by processes such as the International Standard ISO 26262, entitled "Road vehicles – Functional safety", that defines the functional safety of electrical and/or electronic systems that are installed in serial production road vehicles.

1.1 Document Overview

The primary purpose of the SMP documented herein is to identify the safety needs associated with the deployment of the different system components making up the proposed Buffalo, NY ITS4US Deployment project, assess their risk and propose mitigation and management strategies. The document communicates the safety management effort to the system's stakeholders including the system developer, the agencies and organization who will own and operate the system, as well as the end user. Besides this introductory section, which is intended to provide background information about the project and a listing of the references used in developing the SMP, this document is divided into the following sections:

- Section 2 describes the relationship between the SMP and the other planned tasks of the project. Specifically, the section describes the output from other tasks of the Buffalo ITS4US Phase 1 project which served as an input to the SMP. In addition, the section discusses what other tasks of the project would need input from the SMP developed in this document. This section also describes the approach followed in identifying and accessing the safety risks.

- Section 3 identifies the safety needs and potential hazards of the Buffalo NY ITS4US deployment.

- Section 4 assesses the risk of the hazards identified in section 3, by adapting the methodology outlined in the functional safety standard for road vehicles, ISO 26262, developed the International Organization for Standardization (ISO).

- Section 5 then provides an overview of the safety approaches that will be adopted to avoid, mitigate, and respond to the potential safety impacts of the hazards identified and assessed in sections 3 and 4.

- Section 6 provides a summary of the overall areas of risks identified and describes how the team plans to continue monitoring and managing the safety of the Buffalo NY ITS4US Complete Trip Deployment project.

1.2 Project Background

Buffalo is striving toward a sustainable future at all levels of society, incorporating actions in the community, government, and private entities in the area. Enabling community mobility and access to jobs, healthcare, and services to traditionally underserved populations is the primary motivation for all the regional partners involved in this deployment.

The Complete Trip - ITS4US Deployment Program is an effort led by the Intelligent Transportation System (ITS) Joint Program Office (JPO) and supported by Office of the Secretary (OST), Federal Highway Administration (FHWA), and Federal Transit Administration (FTA) to identify ways to provide more efficient, affordable, and accessible transportation options for underserved communities that often face greater challenges in accessing essential services. The program aims to solve mobility challenges for all travelers with a specific focus on underserved communities, including people with disabilities, older adults, low-income individuals, rural residents, veterans, and limited English proficiency travelers. This program will enable communities to build local partnerships, develop and deploy integrated and replicable mobility solutions to achieve complete trips for all travelers.

As one of the selected sites, the Buffalo, NY ITS4US deployment concept addresses:

1. **Providing transit access to healthcare and jobs** to underserved residents including persons with disabilities and allowing them to share in the economic development in downtown Buffalo.
2. **Leveraging technology to work in support for accessible transportation**, integrating accessible transportation technology, transit, and connected automation to solve a transportation need.
3. **Developing a scalable model** for considering accessibility and universal design in transportation technology projects.

The Buffalo, NY ITS4US project will be completed in three phases:

- Phase 1- Concept Development

- Phase 2- Design and Test

- Phase 3- Operation and Evaluation

To achieve the ITS4US Complete Trip Program objectives, the project seeks to deploy an integrated suite of technologies chosen to address identified needs of users and gaps within the systems and services provided. The main components of the proposed system are:

- **A Complete Trip Platform Application** (CTP) – an Open Trip Planner based transit trip planning app that is customized for accessible travel. This app will address user needs around improved transit planning and travel support.

- **Community Shuttle Service** – a shuttle service that is integrated with the CTP and provides circulation in BNMC campus and Fruit Belt area. This service will be based on both human-operated and self-driving shuttles (with an on-board assistant/steward). This component addresses user needs around BNMC local circulation (travel between partner sites and support for first- and last-mile transit connections).

- **Smart Infrastructure** – improvements to digital features in the area of interest (within and around BNMC), particularly along the public rights-of-way. These include adding communication, connectivity, and traveler information technologies to the sidewalks and their adjacent loading/parking areas for transportation vehicles, bus shelters, intersections, and wayfinding technologies in indoor and outdoor venues. This component addresses user needs around outdoor and indoor mobility and wayfinding for travelers.

- The previous components are monitored through a **Performance Dashboard**, which will be able to ingest log files from the other component and external data sources, as well as store, analyze, and provide visualization tools to display and access current and historic data sets produced by the proposed system.

1.3 References

Table 1 list the documents, sources and tools used to develop the SMP for the project.

Table 1. References Used

#	Documents Referenced
1)	Gopalakrishna et al. (2021). Phase 1 Concept of Operations (ConOps) – Buffalo NY ITS4US Deployment Project. US Department of Transportation, Report No. FHWA-JPO-21-860.
2)	Fraser, S. (2020). Adopting Functional Safety: An Executive-Level View. LHP Engineering Solutions.
3)	Pape, D. and McCracken, H. (2016). New York City Connected Vehicle Pilot Deployment Program - Task 4: Safety Management Plan. US Department of Transportation, Report No. FHWA-JPO-16-301
4)	Wang, P. (2016). USDOT Guidance Summary for Connected Vehicle Deployments Safety Management. US Department of Transportation, Report No. FHWA-JPO-16-340.
5)	Becker, C., Nasser, A., and Brewer, J. (2020). Hazard and Safety Analysis of Automated Transit Bus Applications, Final Report. Federal Transit Administration. FTA Report No. 016111.
6)	Timpone, K. (2021). Complete Trip ITS4US Task 4 Training: Safety Management Plan. US Department of Transportation. ITS Joint Program Office.
7)	Harlow, T. (Feb 10, 2021). University Researchers Test Street-Crossing App for the Blind. Star Tribune (Minneapolis) Distributed by Tribune Content Agency, LLC. https://www.govtech.com/education/higher-ed/university-researchers-test-street-crossing-app-for-the-blind.html

#	Documents Referenced
8)	Niagara Frontier Transportation Authority (NFTA). (2021). *NFTA Metro Agency Safety Plan. Revision 1.0.* 181 Ellicott Street, Buffalo, NY 14203.
9)	New York State Department of Transportation (NYSDOT). (2018). Emergency Traffic Control and Scene Management Guidelines. Albany, NY.

2 Safety Overview and Relationships

2.1 Related Project Tasks

The SMP constitutes an integral task of the overall Phase I Buffalo ITS4US Deployment project. As such, the development of the SMP is driven by the products from other tasks of the project, primarily by the Concept of Operations (ConOps) document. The output from the SMP will serve as input to other tasks of the project (e.g., the Systems Requirement and the Enabling Technology Readiness Assessment task). Figure 1 shows the inter-relationship between the SMP task and the other tasks of the Buffalo ITS4US Deployment project.

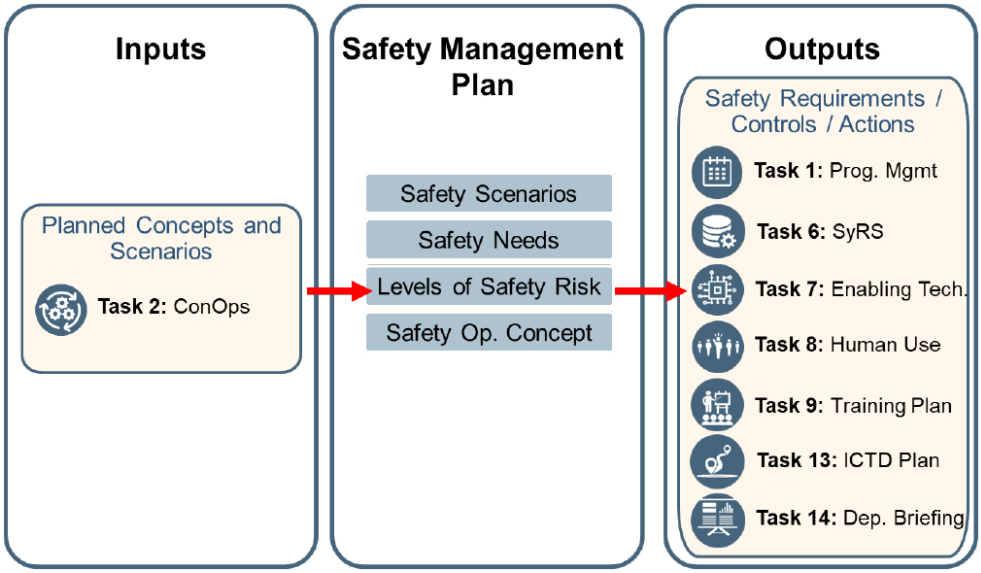

Figure 1. Relationship between the SMP Task and Other Tasks of the Project.
Source: Timpone, K. (2021). Complete Trip ITS4US Task 4 Training: Safety Management Plan.

Task 1 – Project Management. The primary goal of the project management task is to maintain the integrity of the systems engineering approach to the phase I development of the proposed Buffalo ITS4US system, while adhering to the scope, schedule, and cost of the project. By identifying the safety hazards associated with the deployment, the SMP could help identify any additional risks that could affect the project cost and schedule, and which may need to be added to the *risk registry*. The plan also could help identify additional safety stakeholders that should be added to the *stakeholder registry*.

Task 2 – Concept of Operations (ConOps). As explained above, the concepts, and in particular the scenarios or use cases, identified in the ConOps formed the basis for identifying the safety needs and hazards associated with the proposed deployment. This will be explained further in Section 3 of this document.

Task 6 – Deployment System Requirements. The purpose of the Deployment System Requirements task is to define requirements that are clearly mapped to the user needs. Well-defined requirements will support the development of procurement packages, testing strategies and will enable future interoperability. Many of the identified hazards and safety needs will require the development of safety-specific system requirements. As such, the SMP will serve as a critical component guiding the development of those safety requirements in Task 6.

Task 7 – Enabling Technology Readiness Assessment. A key objective of the Enabling Technology Readiness Assessment task (task 7) is to ensure that the Buffalo ITS4US Deployment can adequately procure equipment and software that meets the defined system requirements, including the safety related requirements mentioned above. Given this, the SMP is expected to play a significant role in assessing the readiness of available technologies and in identifying the ones that meet the requirements and safety needs of the project.

Task 8 – Human Use Approval. Any activity conducted as part of the deployment should minimize the risk to human participants, ensure participants consent, and fully inform them of the possible risk associated with the research. Given this, the SMP will provide essential input that would facilitate the approval of the project's human subject protocol and guarantee that safety risks receive due attention and mitigation.

Task 9 – Participant Training and Stakeholder Education Plan. As a part of the participant training and stakeholder education plan, participants and stakeholders need to be made aware of the potential hazards and safety needs of the project, and the mitigation and response plans that will be put in place to address them. The SMP will provide the information needed to address those aspects as part of the training and educational efforts.

Task 13 – Integrated Complete Trip Deployment Plan. The Integrated Complete Trip Deployment Plan is a culmination of all the activities in Phase 1. As such, the SMP will constitute a key element of Integrated Complete Trip Deployment Plan, addressing issues related to managing safety throughout the life cycle of the project.

Task 14 – Deployment Readiness Summary Briefing. The Deployment Readiness Summary Briefing is intended to display the team's fulfillment of all USDOT requirements of Phase 1. Given that the SMP is a critical element of Phase 1 activities, the plan will constitute a part of the briefing.

2.2 Safety Stakeholders

Table 2 lists the stakeholders of the project that relate to safety planning and management, as well as their roles and responsibilities. In that regard, it is to be noted that a safety management committee will be formed to oversee the process of identifying potential hazards and putting in place safety procedures and mitigation strategies to address them. The committee will include members with pertinent expertise relevant to the different safety aspects of the project including the safety of: (1) travel to and from BNMC; (2) persons with disabilities (PWDs) utilizing the Buffalo ITS4US system; (3) the Community Shuttle; and (4) the Self-Driving Shuttle (SDS). This committee will meet regularly to address any identified hazards, and to review progress toward addressing them.

Table 2. Safety Stakeholders List

Name	Organization	Expertise / Roles	Responsibilities
Jamie Hamann-Burney	BNMC Transportation Operations Council	Transportation Planning; Safety Management Committee Member	Identifying hazards associated with travel to, from and within BNMC; suggesting mitigation strategies; monitoring safety during deployment & operations; and reporting safety related concerns
Joe Sonnenberg	Buffalo Hearing and Speech Center	Safety needs of people who are hard at hearing	Identifying hazards and safety needs of people who are hard at hearing and suggesting mitigation strategies for that group; monitoring and reporting safety concerns from that group
Jordana Maisel & Victor Paquet	Center for Inclusive Design and Environmental Access	Safety needs of persons with disability/ies (PWDs) and vulnerable populations. Safety Management Committee Member	Identifying safety needs of PWDs, and suggesting appropriate mitigation strategies based on latest research
Tammy Owen / Ray Zylinski	VIA (formerly Olmsted Center for Sight)	Safety issues of persons who are blind or have low vision.	Identifying hazards of persons who are blind or have low vision; suggesting appropriate mitigation strategies; implementing such strategies; continuing to monitor impacts
Nolan Skipper, Julie Fetzer, and Eric Schmarder	City of Buffalo	Safety needs associated with smart and inclusive infrastructure	Identifying hazards resulting from user interactions with city infrastructure, suggesting mitigation strategies, monitoring safety during deployment & operations related to user interactions with city infrastructure
Blaise DiBernardo	NYS Department of Motor Vehicles	Safety needs associated with the SDS permitting and operations	Developing and approving the law enforcement safety interaction plan governing the deployment and operations of the SDS
Kevin Bruen	NYS State Police	Safety needs associated with vehicle operations including SDS	Developing and approving the law enforcement safety interaction plan governing the deployment and operations of the SDS and the overall safety needs of the Buffalo ITS4US Deployment Project

Name	Organization	Expertise / Roles	Responsibilities
Rob Jones	NFTA	Safety needs of the Community Shuttle, Safety Management Committee Member	Identifying hazards associated with the operations of the Community Shuttle, suggesting mitigation strategies; monitoring safety during deployment & operations; and reporting safety related concerns
Human-Driver Shuttle (HDS) Drivers	NFTA	Safety Issues related to Community Shuttle Operations	Addressing safety and health-related incidents and emergencies for travelers onboard the shuttle, and helping PWDs as they board and get-off the shuttle
Director of Health, Safety and Environmental Quality (Chief Safety Officer)	NFTA	Safety Issues related to Community Shuttle Operations	Addressing safety-related issues of the Community Shuttle Operations
Shuttle Operations Center (SOC) personnel	TBD/NFTA	Safety Issues related to Community Shuttle Operations	Addressing safety and health-related emergencies associated with shuttle operations
Adel W. Sade, Chunming Qiao, and Stephen Still	University at Buffalo (UB)	Autonomous Vehicle Safety and Operations; Safety Management Committee Members	Safety issues associated with the Operations of the SDS; Defining the safe Operations Design Domain (ODD) for SDS; monitoring safety concerns, near misses, incidents of disengagement when the human steward must assume control, identifying root causes of incident of disengagement and near misses, working on refining self-driving algorithms to address identified deficiencies
TBD	NFTA, UB or Third Party (vendor) depending upon the provider of the SDS service and the business model	Overseeing SDS operations while driving autonomously	Monitoring any hazards, assuming control when driving environment goes beyond the safe ODD
Andrew Bartlett	Niagara International Transportation Technology Coalition (NITTEC)	Transportation Incident Management and Response	Identifying and monitoring traffic conditions that may have an impact on the operations and safety of the ITS4US system and its users

Name	Organization	Expertise / Roles	Responsibilities
Robert Limoges	NYSDOT Main Office	Traffic Safety	Advisory role on overall safety of ITS4US Deployment Project, especially aspects related to user interaction with transportation infrastructure
Joe Buffamonte	NYSDOT Region 5	Traffic Safety and Operations	Overall safety of ITS4US Deployment Project especially on aspects related to Smart infrastructure and intersection crossing
TBD	Roswell Park Comprehensive Cancer Center	Public Safety	Identifying hazards associated with travel to, from Roswell Park, a major health care center and employee on BNMC; suggesting mitigation strategies; monitoring safety during deployment & operations; and reporting safety related concerns
Kevin Wild	Kaleida Health	Public Safety	Identifying hazards associated with travel to and from the campus building of the Kaleida Health System, suggesting mitigation strategies; monitoring safety during deployment and operations and reporting safety related concerns
TBD	City of Buffalo Police	Public Safety	Incident management and emergency response
TBD	NFTA Police	Public Safety	Incident management and emergency response
TBD	NYS Police	Public Safety	Incident management and emergency response

2.3 Safety Risk Process and Approach

The current project adapted the safety risk and management approach outlined in the ISO 26262 standard to the specific nature of the Buffalo ITS4US Deployment project. Following the ISO 26262 standard, our process consists of the following three steps: (1) safety needs and hazard identification; (2) safety risk assessment; and (3) safety operational concept. Each of these steps are briefly described in the following subsections.

It should be noted that our focus in this document is on exploring the safety concerns and hazards associated with the Concepts described in the system's Concept of Operations, and not with specific technologies. Naturally, the safety risks and mitigation strategies would depend upon whether implementing such technologies would require procuring Commercial-off-the-Shelf

(COTS) technologies or would require development by the project team. COTS technologies tend to be naturally more mature, and therefore safety risks associated with them are typically better-defined and understood compared to the risks associated with new software or technology development. At the same time, however, the project team will tend to have more control over technologies that the team will develop by themselves. The differences between these two approaches will be considered in the coming phases of the project (e.g., as part of the Enabling Technology Risk Assessment task).

2.3.1 Safety Needs and Hazard Identification

The focus of this step is to identify the major hazards, along with their safety needs, associated with the deployment and operations of the proposed Buffalo IST4US system. As will be explained in more detail in Section 3, this step starts with the ***Use Case*** scenarios identified in the project's ConOps document and identifies the potential hazards resulting from the ***travelers' or operators'*** interactions with the different ***functions of the system***. The identified hazards are then validated through input from the project's stakeholders, owners, and operators.

2.3.2 Safety Risk Assessment

Following the ISO 26262 safety risk assessment procedure, our process assesses the risk of each hazard identified in the safety needs and hazard identification step along the three dimensions of severity, exposure and controllability as briefly outlined below. However, it is worth noting here a few differences between our approach and the ISO 26262 standard. First, while the ISO 26262 was primarily intended for assessing road vehicle functional safety, our system involves many other components other than vehicles including pedestrians, transit riders, and smart/inclusive infrastructure. These other components required significant adaptation to the method in terms of defining the three dimensions, especially the dimensions of severity and controllability. We also include the "0" level for each dimension (i.e., S0 for severity level 0, E0 for level 0 for exposure, etc.). For example, for the severity dimension, level S0 refers to cases where a traveler from a vulnerable population feels afraid or abandoned (psychological harm) but suffers no physical injuries. The application of this step to the identified hazards is described in some detail in Section 4 of this document.

2.3.2.1 Severity

Severity refers to the worst possible consequences of each scenario being described. In our study, we will consider the following four levels and their definitions:

- **S0** - feeling afraid or abandoned but no injuries.
- **S1** - situations that may lead to light to moderate injuries.
- **S2** - severe injuries but survivable probable.
- **S3** - life-threatening and fatal injuries.

2.3.2.2 Exposure

Exposure refers to the probability of the system being in the operational scenario described in the hazardous event when the hazard occurs. For example, a safety scenario involving a passenger getting on or off the bus is very likely (high exposure) in our project, since this scenario will occur each time the shuttle stops at a stop for picking-up or dropping off a passenger. Another example

is related to scenarios involving inclement weather or snow. While significant snow is a rare event in the southern parts of the United States, for example, it is quite likely to occur at the site of the Buffalo ITS4US project, given that Buffalo is well-known for its harsh winters and significant snow fall. We will use the following levels in this project:

- **E0** - Extremely low probability, incredible, unlikely to happen 1 time yearly.
- **E1** - Rare or very low probability, expected to happen fewer than 12 times yearly.
- **E2** - Low probability or expected to happen approximately once a day.
- **E3** - Medium probability, expected to happen once hourly at some locations.
- **E4** - High probability, expected to happen on almost every trip by every participant. It could occur hundreds of times daily.

2.3.2.3 Controllability

Controllability refers to the ability to avoid a given hazard or damage through either the timely and correct application of actions by the person involved in the operation of the system, or the system's control and mitigation, depending on the characteristics of the specific hazard or damage. The level of ease or difficulty in applying such actions is used to categorize the controllability into the following four levels or categories:

- **C0** - Controllable in general, no need for mitigation strategies.
- **C1** - Simply controllable.
- **C2** - Normally controllable.
- **C3** - Difficult to control or uncontrollable.

2.3.2.4 Automotive Safety Integrity Level Overall Rating

Following the assessment of the severity, exposure and controllability of the identified safety scenarios or hazards, the last step in the risk level assessment process is to assign the hazard an overall rating safety integrity level. This is referred to as the Automotive Safety Integrity Level (ASIL) in the ISO26262. Table 3 shows the modified ASIL determination used for this project. We refer to the ASIL's we utilize herein as "modified ASIL", because: (1) they are based on modified definitions for the three dimensions of severity, exposure and controllability, and (2) they incorporate the "0" Level for each dimension. Notwithstanding those two adaptations, the combination of the three ratings for severity, exposure and controllability, to result in an ASIL determination, is the same as in the ISO standard. For any scenario involving a "Level 0" in any one dimension, a designation of "QM" or regular quality management is assigned, as can be seen in Table 3.

Table 3. Modified ASIL Determination (Adapted from ISO 26262)

Severity Class	Probability of Exposure Class	Controllability Class			
		C0	C1	C2	C3
S0	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	Modified ASIL A
	E4	QM	QM	Modified ASIL A	Modified ASIL B

S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	Modified ASIL A
	E4	QM	QM	Modified ASIL A	Modified ASIL B
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	ASIL A
	E3	QM	QM	Modified ASIL A	Modified ASIL B
	E4	QM	Modified ASIL A	Modified ASIL B	Modified ASIL C
S3	E0	QM	QM	QM	QM
	E1	QM	QM	QM	Modified ASIL A
	E2	QM	QM	Modified ASIL A	Modified ASIL B
	E3	QM	Modified ASIL A	Modified ASIL B	Modified ASIL C
	E4	QM	Modified ASIL B	Modified ASIL C	Modified ASIL D

where:

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

As can be seen, several combinations of severity, exposure and controllability are assigned an overall rating of QM. Such a rating refers to cases where typical Quality Management (QM) practices and procedures will be adequate to address the hazard. QM refers to cases when appropriate quality management techniques in the production of system components should be sufficient to eliminate unreasonable risk; this includes appropriate testing and verification of the developed or deployed components. Ratings of modified ASIL A, B, C, and D are the ones that require putting safety measures and mitigation strategies in place, with the overall risk increasing from level A to level D. As will be discussed briefly in Section 5 of this document, those strategies can be broadly categorized into the following four classes: (1) design functional requirements; (2) safety operations processes; (3) mitigation and fail-safe strategies; and (4) emergency response practice and procedures. Section 5 of this document provides some high-level details about those strategies.

3 Safety Needs and Scenarios

The first step in the safety management process adopted in this study is the identification of the potential safety scenarios or hazards, along with their corresponding safety need. Safety scenarios or hazards are potential sources of harm, which may result because of a system malfunction, misuse, hacking, or other extreme events (e.g., severe weather).

There are different approaches that have been suggested in the literature to accomplish this step. For example, the Hazard and Operability Analysis Method starts with an analysis of the system functions. Hazards are then identified as resulting from deviations of the system's functions from their design intent.

In this document, instead of starting with the system functions, we have chosen to use the Use Cases (UC) identified in the project's ConOps as a starting point since the UCs describe how the user is expected to interact with the different system functions (i.e., user function). For each use case, we then identified the potential safety scenarios or hazards that may cause harm because of a user function malfunction, user misuse or abuse, an external event. The identification process was based on information collected from the project team's prior experience with similar applications, communications, and feedback from the project's stakeholders, as well as with end users, system owners, and operators. We also reviewed other safety management plans developed for other projects involving transportation technology including the recent Connected Vehicle pilots. The associated safety need is also listed for each identified scenario.

Before describing each identified safety scenario or hazard, we would like to point out that safety scenarios are sometimes classified into system-level hazards or application-level hazards. System-level hazards affect the entire system, often in diverse ways. An example of a system-wide hazard is a severe weather event, which may impact the operations of the community shuttle, causes sidewalks to become slippery, and knock down communications towers. Such an event could result in significant hazards. Application-level hazards, on the other hand, pertain to the malfunction or misuse of a specific application or project component (e.g., the signalized intersections or the community shuttle).

It is important to note that instead of listing the identified safety needs and safety scenarios by project component, we would list them by use cases and note to which project component the safety need/scenario pertain to. Throughout this document, each safety need is assigned a unique identifier, designated with a formatted reference name and number. The referencing convention is as follows: **SF-<S/U>-<unique number>,** where **SF** refers to Safety Need, **S** refers to System, and **U** refers to User, and **unique number** is a sequential number starting from 1 for each user or system need.

3.1 Safety Needs & Hazards for UC 1 – Register Profile & Preferences

This use case describes the processes and interactions with travelers to set up a Complete Trip Platform user account. The function enables the account holder to select their travel preferences for types of navigation triggers, wayfinding notifications and alert communications. The functions also enable users to identify their preferences for mode, accessibility needs, and link other accounts with their CTP account. Table 4 lists the identified safety scenarios (hazards), the corresponding safety need, the safety scenario (or hazard) description, and its likely impacts.

Table 4. Safety Needs and Scenarios (Hazards) associated with UC1.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-U-1	Contradictory preferences.	Need to guide users to input adequate preference combinations for the system.	Traveler requests conflicting or too many preferences that prevent a coherent trip plan from being generated.	The traveler has difficulty generating a trip plan, and as a result may miss an important trip, or become stranded on return trip without any alternative transportation modes.
SF-U-2	Preference / notification selection mismatch with end user device.	Need to ensure users' device compatibility with the app.	Preferences and notification selections do not match the capabilities of the traveler's end user device(s), and the traveler cannot receive navigation, wayfinding, and notifications.	The traveler is unable to start the trip or end up being led to wrong places because of the inability to receive the needed navigation, wayfinding, and notifications as a result of the mismatch with the traveler's device. This may leave the traveler in unexpected and/or unfamiliar places at night in a dangerous situation.

3.2 Safety Needs & Hazards for UC 2 – Generate Trip Plan and Book a Trip

This use case consists of functions for a traveler to plan a trip by inserting their origin and destination. They may customize this trip by selecting general preferences (e.g., modes, maximum walking distance, shortest trip, fewest transfers), or if they log in to their account use an

existing trip plan or set of preferences for travel and notification. The traveler can also adjust their trip preferences and save the updated trip plan. In addition, as an account holder authorized to use registered mobility services such as PAL or Shuttle, the traveler can generate a complete trip plan with a trip leg that includes reservations and confirmation with the mobility service (PAL Direct or Shuttle). Table 5 lists the identified safety scenarios (hazards), the corresponding safety need, the safety scenario (or hazard) description, and its likely impacts.

Table 5. Safety Needs and Scenarios (Hazards) associated with UC2.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-U-3	No trip plan generated.	Need to inform users the error reason when trip plan is not generated.	No trip plan is generated because preferences selected are too many and there are no itineraries or enough data in the network descriptions to route the traveler.	User is unable to generate a trip plan, and as a result may miss an important trip that may have safety implications (e.g., missing a trip for medical appointment), or become stranded on return trip.
SF-S-1	No trip booking available.	Need to guarantee reservation availability or appropriate notification.	Traveler requests a Shuttle or PAL reservation, and the system cannot access either reservation service.	User is unable to complete a trip booking, and as a result may miss an important trip, or become stranded at current location without any alternative transportation modes.
SF-S-2	No return trip booking available.	Need to ensure reservation availability for return trips.	Traveler assumes that they will be able to book a return trip, but no shuttle or PAL vehicle is available for their return trip request, to that end, the traveler is stranded.	Users may be stranded at their current location (away from home) without any alternative transportation modes.

3.3 Safety Needs & Hazards for UC 3 – Public Transportation Services

This use case describes the information provisions associated with accessing public transit mode options. These include NFTA bus, light rail, and PAL Direct, as well as Shuttle options that are included in these services. The services consist of hailing, boarding, traveling in, and alighting these public transport vehicles. Table 6 lists the identified safety scenarios (hazards), the corresponding safety need, the safety scenario (or hazard) description, and its likely impacts.

Table 6. Safety Needs and Scenarios (Hazards) associated with UC3.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-S-3	Mismatched vehicle to traveler needs.	Need to appropriately accommodate users' needs.	Shuttle arrives without the appropriate accommodation for the traveler(s). Another possibility is that an accessible vehicle is dispatched, but the wheel chair securements are in use, or malfunctioning.	Traveler cannot get on the current shuttle because of the lack of vacant securement equipment (e.g., according to NFTA, wheelchair securement occupancy information could be inaccurate, and bike rack is not equipped with sensors). This may leave the traveler at the shuttle stop at night in a dangerous situation either waiting for the next shuttle or looking for alternative transportation options.
SF-S-4	Delayed vehicles.	Need to follow schedule as much as possible, and when there must be a delay, notify the users.	Travelers will be stranded or left to wait in the "weather" when shuttle or PAL vehicles are delayed.	The traveler is stranded at the shuttle stop longer than anticipated and may be exposed to a dangerous situation at night or when there are inclement weather conditions.

SF-S-5	No-show vehicles.	Need to inform and help users when the shuttle cannot present (no-show).	The shuttle does not arrive at certain stops because of either “weather”, vehicle malfunction, or other unexpected problems.	The traveler is stranded at the shuttle stop until the next scheduled shuttle comes, or even for hours if the no-show vehicle is the last shuttle of the day and no-show notification is not received by the traveler. The traveler may be exposed to a dangerous situation at night or when there are inclement weather conditions.
SF-S-6	Delayed notifications about late shuttles / PAL.	Need to ensure users receive notifications about shuttle schedule changing.	Travelers are inconvenienced or left to wait in the "weather" when notifications of late arrivals of their public transport are not generated, sent, and received by the traveler.	Traveler is stranded at the shuttle stop waiting to be picked up and may be exposed to a dangerous situation at night or in inclement weather conditions.

3.4 Safety Needs & Hazards for UC 4 – Navigation

This use case describes wayfinding and navigation on pathways to complete a trip. This use case consists of the use of the CTP when traveling including crossing intersections, traversing sidewalks, wayfinding to and through indoor facilities. Table 7 lists the identified safety scenarios (hazards), the corresponding safety need, the safety scenario (or hazard) description, and its likely impacts.

Table 7. Safety Needs and Scenarios (Hazards) associated with UC4.

Need #	Scenario Name	Safety Need	Scenario Description/Hazard	Likely Impacts
SF-S-7	Inaccessible directions.	Need to ensure the trip generated meets traveler's preferences.	The navigation instructions provide directions along routes that do not meet traveler preferences (e.g., rough surface) and hence travelers cannot traverse the trip segment.	The traveler may be stranded at his/her current location and miss the next trip segments. The traveler may be exposed to danger if he/she persists to traverse trip leg (e.g., over rough surface).
SF-S-8	Inaccurate directions.	Need to ensure accuracy and clarity of navigation instructions.	The navigation instructions provide directions that are not accurate hence confusing and direct travelers to wrong turns or dangerous locations.	The traveler is guided to an unfamiliar and/or dangerous location. In locations where some movements are restricted (e.g., intersection legs that prohibit pedestrian crossing), inaccurate guidance may lead travelers to perform dangerous actions and/or into vehicle-pedestrian accidents and get severely injured.
SF-S-9	Orientation inaccuracy.	Need to keep the traveler at the right orientation when the traveler’s mobile device does not provide sufficient accuracy.	The traveler’s mobile device does not provide sufficient orientation accuracy to the traveler. As a result, travelers who are visually impaired are incapable of accurately orienting themselves to the correct direction of travel.	The traveler may be wrongly guided away from the correct route or to dangerous locations. The traveler may run into obstacles or vehicles and get injured. This is particularly dangerous when crossing a street or in confined spaces, near stairwells, etc., and for people with visual impairment.
SF-S-10	Positional inaccuracy.	Need to keep the traveler at the right direction when the mobile device does not	The travel mobile device does not provide sufficient positional accuracy to provide step by step	The information given to the traveler is faulty and the traveler misses the correct route. The traveler does not know where

Need #	Scenario Name	Safety Need	Scenario Description/Hazard	Likely Impacts
		provide sufficient positional information.	directions particularly for travel through doorways, into elevators, indoor wayfinding, and more.	she/he is or is led to believe that she/he is in a different location, which may expose them to potentially hazardous situations. For travelers with accessibility needs (e.g., wheelchair accessible), positional inaccuracies may result in directing them to locations where the accessibility needs are not accommodated.
SF-S-11	Inaccurate sidewalk data.	Need to acquire accurate sidewalk data.	The sidewalk data in the system is not accurate.	The travelers may be led to pedestrian restricted areas, places where traveler with accessibility needs cannot traverse. There is also the potential of being struck by traffic, if there is actually no sidewalk, which may result in serious or even fatal injuries.
SF-S-12	Inaccurate indoor facility data.	Need to acquire accurate indoor facility data.	The indoor facility data in the system is not accurate.	The traveler may be led to wrong locations, and/or feel lost and afraid if the traveler is guided to indoor restricted areas.
SF-S-13	Traveler mobile device not linking with indoor / outdoor Smart Signs.	Need to link traveler mobile device with smart signs.	Traveler's mobile device is not linking with indoor/outdoor Smart Signs.	The traveler may feel lost or be stranded at current location, being uncertain about their location.
SF-S-14	Inaccurate or delayed dynamic information about work	Need to acquire accurate and timely dynamic information about work zones and obstructions.	The dynamic information about work zones and obstruction is inaccurate or delayed.	The traveler may be stranded being uncertain about how to cross by or injured if crossing a work zone or obstruction without information or knowledge.

Need #	Scenario Name	Safety Need	Scenario Description/Hazard	Likely Impacts
	zone and obstructions.			
SF-U-4	Unintended Destination.	Need to ensure that the correct / intended destination address and internal building location is entered into the CTP.	The CTP app may have issues in destination confirmation, or the traveler may mistakenly input the wrong destination into the user profile or the app.	The traveler will be directed to the wrong destination and feel lost about their location.

3.5 Safety Needs & Hazards for UC 5 – Reporting & History

This use case describes information provided to the traveler on the CTP that is available for account holders about trips they completed. In addition, the traveler can submit trip obstacles and improvements made during their journey. This provides a crowd-source approach to collecting information on accessibility status, like elevator outages, paths in the trip plan, etc. There are **no safety needs or hazards presented in this use case** because this use case is more related to the data management rather than safety needs and hazards.

3.6 Safety Needs & Hazards for UC 6 – Ride hailing, Reservation, and Dispatch

This use case describes several of the processes and functions of the SOC, and especially those that will be applied and activated when receiving a traveler requests service by the shuttles system. Table 8 lists the safety needs and scenarios for this use case.

Table 8. Safety Needs and Scenarios (Hazards) associated with UC6.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-S-15	Insufficient shuttle availability.	Need to ensure service availability.	No HDS or SDS shuttle is available to satisfy the trip request,either because all vehicles of the community shuttle fleet have reached	The traveler assumes shuttle service is available but is unable to book a trip. As a result, the traveler may be stranded at his/her

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
			capacity or because no vacant HDS or SDS is available for service, based on the preferences and time window requested by the user.	current location without any other transportation mode options feeling afraid or abandoned. The traveler may be exposed to a dangerous situation at night.
SF-S-16	Unavailable special equipment's occupancy information.	Need to ensure accurate information about equipment's occupancy.	The user needs special equipment to accommodate a disability need (e.g., wheelchair securement device), but information about the occupancy status of those equipment (e.g., real-time number of vacant equipment) are not available. All of NFTA's current fixed-route shuttles and paratransit bus are wheelchair accessible, but the occupancy status is not always available or accurate.	The traveler's need (e.g., wheelchair securement device) is not met. If the traveler chooses to wait for the next shuttle or look for alternative transportation modes at the shuttle stop, he/she may be exposed to a dangerous situation at night. If the traveler insists to ride without the need being addressed properly, he/she may be exposed to danger (e.g., falling).
SF-S-17	Inaccurate pick-up or drop-off information.	Need to ensure correct address for pick-up or drop-off locations.	Wrong address for pickup or drop-off. As a result, either the traveler misses the trip or is dropped at a location different from the traveler's desired destination.	The traveler misses an important appointment, such as a medical appointment which has safety implications, and/or is left in an unfamiliar location that may impose the traveler in danger.

3.7 Safety Needs & Hazards for UCs 7 & 8 – Passenger Pick-up, Securement, Travel and Drop-off via an SDS / HDS

These two use cases describe several of the processes and functions of the Shuttles Subsystem, which will be applied and activated when a traveler boards an SDS or HDS, secures him/herself

onboard the vehicle, travels on the SDS/HDS, and finally gets off the SDS/HDS at their final or intermediate destination. Table 9 lists the safety needs and scenarios for this use case.

Table 9. Safety Needs and Scenarios (Hazards) associated with UCs 7 & 8.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-U-5	Traveler trips while boarding or alighting.	Need to prevent travelers from tripping.	The traveler trips while getting on or off the shuttle.	Traveler may fall and hurt him/herself.
SF-S-18	SDS/HDS accessibility equipment malfunction.	Need to maintain the functionality of accessibility equipment.	The traveler is unable to get on the SDS/HDS nor be secured onboard because of a malfunction in the SDS accessibility equipment (e.g., ramp, door, mobility device and person securement system).	Traveler may be stranded at the shuttle stop location without alternative transportation mode. This may result in traveler stranded unexpectedly at night in a dangerous situation.
SF-S-19	Pick-up, Drop-off location occupied.	Need to safely load and unload passengers when the pick-up or drop-off point is blocked.	The pick-up or drop-off point is temporarily blocked because of construction, snow accumulation, slippery surfaces because of weather.	The traveler has difficulty getting on/off the shuttle due to snow and/or slippery surfaces present in the loading area. Some travelers may miss the shuttle at the desired stop if the shuttle does not find any nearby loading locations and forces to skip the stop. This also may expose traveler to danger, as they try to force their way to get on/off the shuttle ignoring the obstacles (snow/ slippery surfaces), potential injuries may occur due to oncoming traffic.
SF-S-20	SDS/HDS moves before the traveler is secured.	Need to ensure necessary securement	SDS/HDS moves before the necessary securement process is completed (e.g.,	Rider who requires securement but has not been secured falls as SDS/HDS moves, or a standee, which is possible in some shuttle designs,

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
		before moving.	wheelchair securement).	especially SDS, falls when the shuttle moves, especially if the SDS acceleration / deceleration profiles are different from traditional shuttles travelers are used to.
SF-S-21	SDS/HDS sudden stops.	Need to prevent traveler injury from sudden stops.	SDS/HDS stops suddenly to avoid a driving hazard and a rider falls.	The rider is injured because of the falling.
SF-S-22	SDS driving environment beyond the ODD.	Need to ensure operations of SDS within the ODD.	A dynamic change in conditions (e.g., caused by weather, incident, etc.) results in a driving environment that is beyond the SDS ODD, a steward will be available to take over control anytime when necessary.	The SDS stops automatically or manually by steward, traveler may be injured (e.g., falling) in the braking process. In extreme conditions such as winter storms, SDS loses traction and control (e.g., brake), and the steward is not able to control the shuttle. This may injure the rider and steward and/or damage the shuttle by crashing into objects or flipping.
SF-U-6	Traveler early exit.	Need to ensure traveler gets off at correct stop.	The traveler is confused due to misinformation and gets off at the wrong drop-off location.	The traveler may wait at the closest pick-up location for the next available shuttle or look for alternative transportation mode. This may result in traveler waiting in unfamiliar place at night in a dangerous situation.
SF-U-7	Traveler misses exit.	Need to ensure traveler gets off at the correct stop.	A traveler fails to get off at the correct drop-off location and misses the stop due to misinformation or lack of notification.	The traveler may get off at the next available stop and either wait for an opposite direction shuttle or look for alternative transportation mode. This may result in traveler waiting in unfamiliar

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
				place at night in a dangerous situation.
SF-S-23	Traveler misses connection trip.	Need to ensure timely transfer at multi-modal connections.	A traveler attempting to make a connection to another transportation mode for the next leg in the trip misses the next leg, because the other mode does not arrive, and is stranded.	The traveler strands at his/her current location and has the probability of missing the next leg in the trip. This may result in travelers stranded at night without alternative transportation mode in a dangerous situation.
SF-S-24	Delay or missed stop, caused by re-route.	Need to minimize impact of traffic incidents on time and location of pick-up or drop-off.	An incident requires SDS to re-route, causing delays or missed pick-up and/or drop-off points.	Traveler stands at a pick-up or drop-off point longer than anticipated (determining what is an acceptable wait time will be based on feedback from users, to be collected during the coming phases of the project). Travelers at missed pick-up or drop-off point may stand for a very long time and find out the shuttle is not coming to their location. This may result in traveler being stranded (perhaps in a dangerous location or at night with limited visibility).
SF-S-25	V2X connection lost.	Need to ensure communicatio n network availability.	V2X connection lost caused by hazardous weather (e.g., snowstorm) or power outage.	The SDS or HDS driver is unable to receive traffic and safety information provided by the infrastructure, which may lead to unsafe operations of the shuttle. The SDS may lose communication with the Shuttle Operations Center (SOC).

3.8 Safety Needs & Hazards for UC9 – Manage Incidents

This use case describes the processes and functions that will be activated by the shuttles subsystem to manage shuttle-related incidents. Examples of such incidents include a severe snowstorm that prevents an autonomous shuttle from operating, a malfunction of sensors onboard the SDS, a medical emergency involving a rider onboard the shuttle, or a traffic incident along the path of the shuttle.

Table 10. Safety Needs and Scenarios (Hazards) associated with UC9.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-S-26	SDS hardware/ physical element malfunction.	Need to address system malfunctioning.	A malfunction of a hardware is designed to be semi- or fully-automated that does not require the intervention of a human operator.	Person using the accessibility/securement feature may be unable to take the shuttle, thus is stranded at the bus stop, which may expose the traveler to a hazardous situation especially during inclement weather conditions. If the securement mechanism malfunctions during the ride, the traveler using such mechanism may be exposed to danger during the ride, especially when the shuttle accelerates or brakes.
SF-U-8	Traveler health emergency.	Need to ensure prompt emergency response to traveler health emergencies.	A traveler has a health emergency onboard the shuttle.	The traveler health emergency may get worse if not treated promptly and correctly.
SF-U-9	HDS driver health emergency.	Need to ensure prompt response to HDS driver’s health emergencies.	An HDS driver has a health emergency while operating the shuttle.	The HDS driver cannot continue to drive. The driver's condition may worsen if not treated promptly. If the shuttle is moving, there is the potential of crashing which may injure the riders.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-U-10	SDS steward health emergency	Need to ensure prompt response to SDS steward's health emergencies.	An SDS steward has a health emergency while standby or operating the shuttle.	The SDS steward cannot continue to monitor or steward the shuttle. The steward's condition may worsen if not treated promptly. If the shuttle is moving and the steward is controlling the shuttle, there is the potential of crashing which may injure the riders.
SF-U-11	Emergency button misusage.	Need to ensure proper application of emergency button.	A traveler accidentally presses the emergency button, which triggers a full strength braking of the SDS.	Travelers may fall, hit objects onboard the shuttle, and get injured.
SF-S-28	Driver / steward abandonment	Need to protect travelers if driver/steward abandons the shuttle.	A steward/driver receives a call/text from family about an emergency, the steward/driver just stops the shuttle from where it stands. For SDS, if the steward does not manually terminate the autonomous mode, the SDS may keep going.	Passengers may be stranded in the shuttle without a driver for HDS or safety steward for SDS. If autonomous mode is not turned off, it may be dangerous for SDS to continue going without a safety steward. (A steward should NEVER leave the SDS without terminating the autonomous mode).
SF-S-29	SDS/HDS rear-ended collision.	Need to prevent rear-ended accidents and protect travelers.	SDS/HDS stops suddenly and is rear-ended by another vehicle.	A passenger is injured because of the crash, or because of falling off the shuttle seat because of the impact.
SF-S-30	SDS-pedestrian collision.	Need to prevent vehicle-pedestrian accidents and	SDS stops suddenly and strikes a pedestrian.	The pedestrian may be seriously injured. A passenger may be injured because of falling off the shuttle seat

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
		protect travelers.		caused by the sudden stop or the impact.
SF-S-31	SDS frontal collision.	Need to prevent frontal collision accidents and protect travelers.	SDS stops suddenly and strikes a vehicle in front.	A passenger from the shuttle or front vehicle is injured because of the crash, or a shuttle passenger is injured because of falling off the shuttle seat because of the impact.

3.9 Safety Needs & Hazards for UC10 – PedX Request

This use case describes the transmission of a PedX request message from the CTP to the traffic signal controller. Specifically, the use case will allow a travel to communicate, “hands free” request for a crossing message to the signal controller at the intersection. The request will behave in a similar fashion as a request button except for several additional features including indicating the specific street to cross and requesting that the duration of the crossing phase be enough to accommodate the walking speed for that particular user. Table 11 lists the safety needs and scenarios for this use case.

Table 11. Safety Needs and Scenarios (Hazards) associated with UC10.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-S-32	Failing linking traveler’s mobile device with Ped request signal.	Need to ensure proper connection between traveler’s mobile device and signal controller.	The traveler's mobile device fails to connect with Ped request signals.	The traveler is unable to make Ped request nor receive signal status via mobile device. For traveler who make travel options solely relying on the mobile device navigation (e.g., having difficulty find or use the physical push button), he/she may be stranded at the intersection feeling afraid and not knowing what to do. If that traveler chooses to cross the intersection without the mobile device, a potential vehicle-pedestrian accident is probable.

Need #	Scenario Name	Safety Need	Scenario Description / Hazard	Likely Impacts
SF-S-33	Dropped request at intersection.	Need to protect traveler when walk signal does not receive requests.	Walk signal is never actuated because no request was initiated, and traveler is stuck at the intersection.	The traveler assumes that a crossing request is made via mobile device, but actually no request was initiated. For traveler who make travel options solely relying on the mobile device navigation (e.g., having difficulty find or use the physical push button), he/she may be stranded at the intersection feeling afraid and not knowing what to do. If that traveler chooses to cross the intersection without the mobile device, a potential vehicle-pedestrian accident is probable.
SF-S-34	Incorrect PED-X signal direction.	Need to protect traveler when PED-X provides the incorrect direction at a pedestrian crossing to CTP app.	Traveler is alerted that signal changes and start to travel toward the wrong direction against traffic.	The traveler walks in the wrong direction of the crosswalk where vehicles face a green light. The traveler is likely to be crashed by a vehicle.
SF-S-35	Inaccurate PED-X signal timing.	Need to protect traveler when PED-X provides inaccurate signal timing to CTP app.	Traveler is alerted that signal changes and begins crossing before actual signal changes.	The traveler starts traveling before the actual signal changes. The traveler is likely to be involved in a vehicle-pedestrian accident.
SF-S-36	Delayed PED-X signal alert.	Need to protect traveler when PED-X provides delayed alert to CTP app.	Traveler is alerted that signal changes later than the actual change, thus does not have sufficient time to cross safely, but does not know it.	The traveler starts walking too late and may be involved in a vehicle-pedestrian accident.

4 Assessment of Safety Risks

As mentioned in section 2.3.2, the safety risk assessment process followed in this project evaluated each hazard along three dimensions or risk classes severity, exposure, and controllability. The severity rating assesses the gravity of the consequences if the hazard does materialize. The exposure gauges how likely it is to occur. Finally, the controllability measures the ability of the system owners, operators, and/or users to compensate for the malfunction. Before describing the different levels for each dimension, it is quite important to note that in our evaluation, we considered the "worst case scenario" for a given situation, by considering the user group who would be most at risk for a given hazard. For example, travelers who are blind or have low vision are most at risk when crossing an intersection for example. On the other hand, travelers with cognitive disabilities would be most affected if stranded or when getting off at a wrong shuttle stop. The advantage of the "worst case scenario" approach is that it provides consistency across the different use cases. Moreover, the applicable mitigation strategies developed in such a fashion should have a positive impact on all other user groups.

In terms of severity, three levels were used as mentioned before:

1. **Severity Level 0 (S0)** refers to situations where a traveler may feel inconvenienced, afraid or abandoned, but there are no physical injuries involved.

2. **Severity Level 1 (S1)** is used to refer to situations that result in moderate injuries. An example of this could be when a traveler onboard the shuttle falls off her/his seat, when the shuttle applies the brakes suddenly, and as a result suffers a light or mild injury.

3. **Severity Level 2 (S2)** refers to incidents where a traveler may incur severe injuries but where survival is probable. This may refer to cases where, for example, a vehicle rear-ends the shuttle, but because the shuttle will always be traveling at a low speed (between 15 mph and 25 mph), the injuries resulting are NOT expected to be life threatening.

4. **Severity Level 3 (S3)** refers to incidents that may result in life-threatening injuries. This typically includes cases where there is a risk for a vehicle to hit a pedestrian crossing an intersection. As is typical with vehicle-pedestrian crashes, these crashes unfortunately often result in life-threatening and fatal injuries.

In terms of exposure, four levels are utilized.

1. **Exposure level 0 (E0)** refers to hazardous situations that are extremely rare or incredible. The probability of occurrence is less than once a year.

2. **Exposure level 1 (E1)** refers to hazardous situations that are rare or of a very low probability. The situations are expected to happen approximately 12 times a year (once a month).

3. **Exposure Level 2 (E2)** refers to scenarios whose probability of occurrence is approximately once a daily.

4. **Exposure Level 3 (E3)** refers to scenarios that are of medium probability, these scenarios are expected to happen approximately once in an hour at some locations.

5. **Exposure Level 4 (E4)** refers to scenarios that are of high probability which are expected to happen in almost every trip. It could occur hundreds of times a day.

In determining the exposure level, there are cases where the probability of hazard occurrence is somewhere between two levels. In such a situation, the higher level is chosen for being conservative.

In terms of controllability, we use four levels.

1. **Control Level 0 (C0)** refers to scenarios that do not require no specific action to control the situation or to mitigate the hazard.

2. **Control Level 1 (C1)** refers to cases where it can be safely assumed that there are simple ways to compensate for the malfunction.

3. **Control Level 2 (C2)** is also controllable but is more involved than C1.

4. **Control Level 3 (C3)** refers to scenarios where the hazard is not controllable or is difficult to control.

Finally, following the assignment of levels to the safety risk assessment classes of severity, exposure and controllability, the safety scenario or hazard can be assigned an overall modified ASIL rating according to Table 3 above. As previously discussed, several combinations of the ratings for severity, exposure, and controllability result in a modified ASIL rating of Quality Management or “QM”, which indicates that all what is needed for such scenarios is to ensure that the system is developed and deployed according to the requirements. For such scenarios, no other specific mitigation strategy is required. Modified ASIL ratings of A, B, C, and D, are the ones that require applying one of the safety operational concepts discussed in Section 5. The following subsections asses the safety risk of each of the hazards identified in Section 3. For this project, hazards are divided into two groups: 1) user safety hazards; and 2) system safety hazards.

4.1 User Safety Risk Assessment

4.1.1 Risk SF-U-1 – Contradictory preferences

Table 12 describes the assessment of the risk of the SF-U-1 or the contradictory preferences safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.1 for UC1 scenario description.

Table 12. Risk Assessment of the Contradictory Preferences Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S0	A vulnerable user being stranded without alternative transportation mode, feeling afraid or abandoned. Considering that users usually book trips, while at home or in a safe building, S0 is selected.
Exposure	E2	It is somewhat likely that a traveler's requests may conflict or that a traveler indicates too many preferences.
Controllability	C1	By setting up a choice system that will inform travelers when preferences are conflicting, and possibly having customer service available, it should be quite possible to control such hazard.
Modified ASIL Overall Rating	QM	

4.1.2 Risk SF-U-2 – Preference/notification selection mismatch with end user's device

Table 13 describes the assessment of the risk of the SF-U-2 or the Preference/notification selection mismatch safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.1 for UC1 scenario description.

Table 13. Risk Assessment of the Preference/notification Selection Mismatch with End User's Device Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A vulnerable user being stranded for hours, or wrongly travelling to unfamiliar or dangerous places, may lead to severe injury.
Exposure	E2	It is somewhat likely that the preference/notification selection would mismatch with end user's device, considering that this would mostly happen to first time users, E2 is assigned.
Controllability	C1	By setting appropriate device compatibility checks and warning notifications in the app, travelers should know any device mismatch problem when using the app and be aware of any inconvenience this may bring.
Modified ASIL Overall Rating	QM	

4.1.3 Risk SF-U-3 – No trip plan generated

Table 14 describes the assessment of the risk of the SF-U-3 or the no trip plan generated safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.2 for UC2 scenario description.

Table 14. Risk Assessment of the No Trip Plan Generated Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S0	A vulnerable user feeling afraid or abandoned. Considering that users usually book trip in safe nonemergency conditions, S0 is selected.
Exposure	E3	It is likely that a traveler inputs combination of preferences does not generate a trip plan, the traveler may succeed in generating a trip plan after changing the combination.
Controllability	C1	By limiting the number of preferences and/or informing users which combinations of preferences are unavailable, users should be able to re-do the trip generation process and generate a feasible trip plan. In addition, customer service would also mitigate the risk.
Modified ASIL Overall Rating	QM	

4.1.4 Risk SF-U-4 – Unintended destination

Table 15 describes the assessment of the risk of the SF-U-4 or the unintended destination safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 15. Risk Assessment of the Unintended Destination Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	In this case, the traveler may be guided to unfamiliar/dangerous and unintended destinations. For some vulnerable users, this may lead to severe injuries.
Exposure	E2	It is possible but somewhat unlikely that the traveler enters the wrong address and or wrong internal destination into the CTP.
Controllability	C1	By confirming the desired address and final location with the user, the possibility of the hazard occurring should be minimized.
Modified ASIL Overall Rating	QM	

4.1.5 Risk SF-U-5 – Traveler trips

Table 16 describes the assessment of the risk of the SF-U-5 scenario, which involves the case when the traveler trips while getting on or off the shuttle safety scenario. The table also describes the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 16. Risk Assessment of the Traveler Trips Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A traveler who trips during boarding may experience lead to severe injuries. This especially would be the case for some user groups.
Exposure	E4	Getting on and off the shuttle occurs at almost every stop, thus, very high probability. However, the probability of trip/stumble in the process of boarding is low.
Controllability	C1	Appropriate design and warning signs at all entrance/exit doors of the shuttle may aid in making travelers aware of the elevation difference and move carefully.
Modified ASIL Overall Rating	Modified ASIL A	

4.1.6 Risk SF-U-6 – Traveler early exit

Table 17 describes the assessment of the risk of the SF-U-6 or the traveler early exit safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 17. Risk Assessment of the Traveler Early Exit Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	For some user groups, exiting at the wrong location or wrong intersection may lead to severe injury, especially in inclement weather conditions.
Exposure	E2	It is somewhat probable that the traveler gets off at the wrong drop-off location.
Controllability	C1	The traveler may walk to the destination if it is close to the traveler's current location and the traveler is capable; or the traveler may check shuttle schedule and wait for the next shuttle. Arrival notification could be sent to travelers to reduce the probability of such hazard.
Modified ASIL Overall Rating	QM	

4.1.7 Risk SF-U-7 – Traveler misses exit

Table 18 describes the assessment of the risk of the SF-U-7 or the traveler misses exit safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 18. Risk Assessment of the Traveler Misses Exit Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	For some user groups, exiting at the wrong location or wrong intersection may lead to severe injury, especially in inclement weather conditions.
Exposure	E2	It is somewhat probable that the traveler misses the correct stop.
Controllability	C1	The traveler may have to get off at the next stop, walk to the destination if it is close to the traveler's current location and the traveler is capable; or the traveler may wait for an opposite direction shuttle. Arrival notification could be sent to travelers to reduce the probability of such hazard.
Modified ASIL Overall Rating	QM	

4.1.8 Risk SF-U-8 – Traveler health emergency

Table 19 describes the assessment of the risk of the SF-U-8 or the traveler health emergency safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 19. Risk Assessment of the Traveler Health Emergency Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Traveler health emergency could be life-threatening.
Exposure	E2	Should be E1 because it is rare that the passenger has a health emergency. However, considering that the shuttle serves around medical facilities, there might be more patients riding the shuttle, and therefore we raised the exposure level to E2.
Controllability	C3	Health emergency is not controllable. However, having a health emergency button in the shuttle and training the driver/steward to take the proper actions to handle the health emergency would minimize the risk to the traveler who experiences the health emergency.
Modified ASIL Overall Rating	Modified ASIL B	

4.1.9 Risk SF-U-9 – HDS driver health emergency

Table 20 describes the assessment of the risk of the SF-U-9 or the HDS driver health emergency safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 20. Risk Assessment of the HDS Driver Health Emergency Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Driver health emergency could be life-threatening, passengers may be injured if the driver is not able to stop the shuttle properly, which could result in a vehicle-to-vehicle crash or vehicle-pedestrian accident.
Exposure	E1	It is rare that the HDS driver has health emergency during service.
Controllability	C3	Health emergency is not controllable. However, proper driver training on how to handle such a situation would minimize the safety risk for both the driver and passengers onboard.
Modified ASIL Overall Rating	Modified ASIL A	

4.1.10 Risk SF-U-10 – SDS steward health emergency

Table 19 describes the assessment of the risk of the SF-U-10 or the SDS steward health emergency safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 21. Risk Assessment of the SDS Steward Health Emergency Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	SDS steward health emergency could be life-threatening, passengers may be injured if the steward does not stop the shuttle properly in manual mode, which may result in a vehicle-to-vehicle crash or vehicle-pedestrian accident.
Exposure	E1	It is rare that the SDS steward has health emergency during service. Most of the time the SDS is on autonomous mode, and thus, the safety risk for passenger injury due to manual mode crash is extremely rare.
Controllability	C3	Health emergency is not controllable. However, proper steward training on how to handle such a situation would minimize the safety risk for both the steward and passengers onboard. Also, remote monitoring of the SDS could be very beneficial in such cases.
Modified ASIL Overall Rating	Modified ASIL A	

4.1.11 Risk SF-U-11 – Emergency stop button misusage

Table 22 describes the assessment of the risk of the SF-U-11 or the emergency stop button misusage safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 22. Risk Assessment of the Emergency Stop Button Misusage Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S1	The passenger falls off the seat or crashes into an object onboard the shuttle. This may lead to light to moderate injuries.
Exposure	E2	It is somewhat likely that the emergency stop button is pushed, especially as most travelers are not familiar with SDS. The probability is between E1 and E2.
Controllability	C1	Warning signs with the proper explanation of when and how to use the emergency button should be posted near the button.
Modified ASIL Overall Rating	QM	

4.2 System Safety Risk Assessment

This section will assess the system safety risks identified in section 3. System risks are those that result from a malfunction of a system or subsystem component. Examples of such risks include: (1) risks associated with a delay or no showing of the Community Shuttle, leaving the traveler stranded; (2) risks resulting from the system providing inaccurate navigation information to travelers; and (3) risks associated with the CTP app on a traveler mobile device failing to communicate with the traffic signal controller at an intersection crossing.

4.2.1 Risk SF-S-1 – No trip booking available

Table 23 describes the assessment of the risk of the SF-S-1 or the No Trip Booking Available safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.2 for UC2 scenario description.

Table 23. Risk Assessment of the No Trip Booking Available Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S0	This may result in a user feeling afraid or abandoned. Considering that users usually book trips in safe surroundings and nonemergency conditions, S0 is selected.
Exposure	E1	It is unlikely that the system cannot access reservation services.
Controllability	C2	Technicians should be available and fix the issue if the system cannot access either shuttle or PAL reservation service as soon as possible.
Modified ASIL Overall Rating	QM	

4.2.2 Risk SF-S-2 – No return trip booking available

Table 24 describes the assessment of the risk of the SF-S-2 or the No Return Trip Booking Available safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.2 for UC2 scenario description.

Table 24. Risk Assessment of the No Return Trip Booking Available Hazard.

Risk Assessment Class	Rating	Rationale
Severity	2	Users being stranded somewhere away from home may lead to severe injury, especially at dangerous locations, at night, or in inclement weather conditions.
Exposure	E2	Depending on the time of day/week/year and weather conditions, travel demand may largely vary. It is somewhat probable that a return trip is not available to the user.
Controllability	C3	It is difficult to control such hazard in a timely manner. From an operational perspective, shuttle distribution optimization may minimize the probability of this hazard.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.3 Risk SF-S-3 – Mismatched vehicle to traveler needs

Table 25 describes the assessment of the risk of the SF-S-3 or the Mismatched vehicle to traveler needs safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.3 for UC3 scenario description.

Table 25. Risk Assessment of the Mismatched Vehicle to Traveler Needs Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Users with special needs may be stuck at the bus stop not being able to ride the shuttle, this may lead to severe injury in inclement weather conditions.
Exposure	E2	It is not very likely that the shuttle would arrive without appropriate accommodations for the traveler. The probability is somewhere between E1 and E2. E2 is selected.
Controllability	C1	By applying appropriate shuttle assignment and fleet management algorithms, all traveler needs should be accommodated appropriately.
Modified ASIL Overall Rating	QM	

4.2.4 Risk SF-S-4 – Delayed vehicles

Table 26 describes the assessment of the risk of the SF-S-4 or the Delayed vehicles safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.3 for UC3 scenario description.

Table 26. Risk Assessment of the Delayed Vehicles Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Traveler waiting extra time at bus stop may be severely injured (e.g., may experience hypothermia), especially during inclement weather conditions.
Exposure	E3	It is likely that the shuttle could be delayed due to all sorts of occasions, especially in inclement weather or snow, which is quite likely to occur in Buffalo during the winter.
Controllability	C2	Delayed vehicles are not controllable. However, by sharing real-time shuttle location and/or sending out delay notifications to the users, users should be able to adjust their travel plans.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.5 Risk SF-S-5 – No-show vehicles

Table 27 describes the assessment of the risk of the SF-S-5 or the No-show vehicles safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.3 for UC3 scenario description.

Table 27. Risk Assessment of the No-show Vehicles Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Traveler may wait at bus stop for hours. In inclement weather conditions, this may be life-threatening for the traveler, especially if the shuttle is the last one of the days and the traveler has no alternative transportation mode.
Exposure	E1	Mechanical malfunction and inclement weather conditions or snow may be the main cause of a no-show situation. Although such weather conditions are quite likely to occur in Buffalo during the winter, no-show would still be unlikely.
Controllability	C3	No show vehicles are not controllable. However, by sharing real-time shuttle location and/or sending out no show notifications to the users, the user's safety risks should be minimized.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.6 Risk SF-S-6 – Delayed notifications about late shuttles / PAL

Table 28 describes the assessment of the risk of the SF-S-6 or the Delayed notifications about late shuttles safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.3 for UC3 scenario description.

Table 28. Risk Assessment of the Delayed Notifications about Late Shuttles Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A user waiting extra time at a bus stop may be severely injured, especially during inclement weather conditions.
Exposure	E2	It is somewhat likely that the notifications about shuttle delays are not received by the user.
Controllability	C1	With a well-maintained notification system, and regularly reminding users to enable the app notification function, users should be able to receive delay notifications properly.
Modified ASIL Overall Rating	QM	

4.2.7 Risk SF-S-7– Inaccessible directions

Table 29 describes the assessment of the risk of the SF-S-7 or the inaccessible directions safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 29. Risk Assessment of the Inaccessible Directions Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A vulnerable user traveling through inaccessible route (e.g., rough surface) may be severely injured.
Exposure	E2	It is not very likely that the navigation provides directions that do not meet traveler's preferences. The probability would be between E1 and E2, E2 is selected.
Controllability	C1	By ensuring that the map database contains pertinent information to travelers' preferences (e.g., surface type, stairs, elevators, and ramps) on all travel way segments included within the scope of the ITS4US system, the navigation instruction generated should be able to meet travelers' preferences.
Modified ASIL Overall Rating	QM	

4.2.8 Risk SF-S-8 – Inaccurate directions

Table 30 describes the assessment of the risk of the SF-S-8 or the inaccurate directions safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 30. Risk Assessment of the Inaccurate Directions Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Inaccurate directions may incorrectly direct the user to a hazardous location, which may result in vehicle-pedestrian accidents that can be fatal to pedestrians.
Exposure	E3	There are many sources of error that may creep in, resulting in inaccurate directions for navigation. The probability is between E2 and E3, E3 is selected.
Controllability	C3	It may be difficult to correct the inaccuracies while a trip is being executed, but with appropriate feedback mechanisms, this could be corrected for future trips.
Modified ASIL Overall Rating	Modified ASIL C	

4.2.9 Risk SF-S-9 – Orientation inaccuracy

Table 31 describes the assessment of the risk of the SF-S-9 or the orientation inaccuracy safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 31. Risk Assessment of the Orientation Inaccuracy Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	This may expose the user to a hazardous location, which may result in vehicle-pedestrian accidents that can be fatal to pedestrians.
Exposure	E3	It is likely that the traveler's mobile device may fail to provide enough orientation accuracy from time to time, especially when the traveler's speed is very low.
Controllability	C1	As the traveler walks, the positional displacement in a very short period would be sufficient for the system to identify the walking direction of the traveler. Additionally, the navigation could provide additional information about landmarks along the way. (e.g., large signs or stores in the correct direction of travel).
Modified ASIL Overall Rating	Modified ASIL A	

4.2.10 Risk SF-S-10 – Positional inaccuracy

Table 32 describes the assessment of the risk of the SF-S-10 or positional inaccuracy safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 32. Risk Assessment of the Positional Inaccuracy Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S1	Positional inaccuracies may cause some user groups, especially those who are highly dependent on the CTP app for navigation, to wrong locations which may cause some users to feel lost, afraid or abandoned.
Exposure	E3	Indoor wayfinding and similar functions require quite high mobile device positional accuracy. Thus, insufficient positional would be very probable.
Controllability	C2	Technologies exist that can significantly improve positional accuracy.
Modified ASIL Overall Rating	QM	

4.2.11 Risk SF-S-11 – Inaccurate sidewalk data

Table 33 describes the assessment of the risk of the SF-S-11 or inaccurate sidewalk data safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 33. Risk Assessment of the Inaccurate Sidewalk Data Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	This may expose some user groups to severe hazards and could result in a vehicle-pedestrian crash which could be fatal.
Exposure	E2	It is somewhat likely that sidewalk data is inaccurate, especially in the beginning of the deployment.
Controllability	C2	The user could use the map and signs near current location as additional reference, anyone who experiences this situation should report it to the transportation authority.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.12 Risk SF-S-12 – Inaccurate indoor facility data

Table 34 describes the assessment of the risk of the SF-S-12 or inaccurate indoor facility data safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 34. Risk Assessment of the Inaccurate Indoor Facility Data Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S1	This may result in some users feeling lost, afraid or abandoned.
Exposure	E2	It is somewhat likely that indoor facility data is inaccurate, especially at the beginning of the project's deployment.
Controllability	C2	The user could use the map and signs near current location as additional reference, or ask others for directions, anyone who has this situation should report to the transportation authority.
Modified ASIL Overall Rating	QM	

4.2.13 Risk SF-S-13 – Traveler mobile device not linking with indoor/outdoor Smart Signs

Table 35 describes the assessment of the risk of the SF-S-13 or traveler mobile device not linking with indoor/outdoor Smart Signs safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 35. Risk Assessment of the Traveler Mobile Device Not Linking with Indoor/outdoor Smart Signs Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S1	This may result in a vulnerable user feeling lost, afraid or abandoned.
Exposure	E2	It is somewhat likely that the mobile device may fail to link to the Smart Signs, either because of incompatibility issues between the mobile device and the smart signs, or because a Smart Signs malfunction.
Controllability	C1	By applying an appropriate device management system, and regular maintenance and tests to the smart signs, the probability of linking problems should be minimized.
Modified ASIL Overall Rating	QM	

4.2.14 Risk SF-S-14 – Inaccurate or delayed dynamic information about work zone and obstructions

Table 36 describes the assessment of the risk of the SF-S-14 or inaccurate or delayed dynamic information about work zone (WZ) and obstructions safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.4 for UC4 scenario description.

Table 36. Risk Assessment of the Inaccurate or Delayed Dynamic Information about WZ and Obstructions Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A person who crosses a work zone or obstruction without notice might be severely injured.
Exposure	E1	It is not very likely that dynamic information about work zones and obstruction is inaccurate or delayed.
Controllability	C1	By keeping good communication with the city, NYSDOT and other agencies that might be involved in setting work zones and constructions, as well as by ensuring a timely updating of the dynamic information about those work zones, the probability of such hazard occurring should be minimized.
Modified ASIL Overall Rating	QM	

4.2.15 Risk SF-S-15 – Insufficient shuttle availability

Table 37 describes the assessment of the risk of the SF-S-15 or the insufficient shuttle availability safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.6 for UC6 scenario description.

Table 37. Risk Assessment of the Insufficient Shuttle Availability Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A user being stuck at his/her current location may lead to severe injury, especially at dangerous locations, at night, or in inclement weather conditions.
Exposure	E2	Depending on the time of day/week/year and weather conditions, travel demand may largely vary. No shuttle available is somewhat probable.
Controllability	C3	Insufficient shuttle availability is not controllable while the trip is being executed. The app may recommend travelers to use other transportation modes (e.g., ride sharing). If there are a lot of requests during certain times and/or on certain routes, new service may need to be added in the future.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.16 Risk SF-S-16 – Unavailable special equipment's occupancy information

Table 38 describes the assessment of the risk of the SF-S-16 or the unavailable special equipment occupancy information safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.6 for UC6 scenario description.

Table 38. Risk Assessment of the Unavailable Special Equipment Occupancy Information Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Users using special equipment may be stuck at the bus stop not being able to ride the shuttle, this may lead to severe injury in inclement weather conditions.
Exposure	E2	It is somewhat likely that information about the special equipment's occupancy status might not be available. Problems include lost connectivity between the SOC and shuttle, sensor error, or a shuttle not equipped with such sensing capability.
Controllability	C2	If a communication error or sensor malfunction occurs, technicians could perform emergency repair. If the shuttle has no vacant equipment, the traveler may need to wait for the next shuttle for safety.
Modified ASIL Overall Rating	QM	

4.2.17 Risk SF-S-17 – Inaccurate pick-up/drop-off information

Table 39 describes the assessment of the risk of the SF-S-17 or the inaccurate pick-up/drop-off information safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.6 for UC6 scenario description.

Table 39. Risk Assessment of the Inaccurate Pick-up/Drop-off Information Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A traveler being left at an unfamiliar/dangerous location at night and/or in inclement weather condition may be severely injured.
Exposure	E2	It is somewhat likely that either the traveler inputs the wrong address when booking or fails to update the address in her profile, or the PAL driver makes a mistake on the pick-up or drop-off address.
Controllability	C1	This scenario is simply controllable. PAL driver can directly contact the traveler or request SOC to contact the traveler and correct the address. Furthermore, confirmation could be sent to the traveler and driver to verify the address to minimize the probability of using the wrong address.
Modified ASIL Overall Rating	QM	

4.2.18 Risk SF-S-18 – SDS/HDS accessibility equipment malfunction

Table 40 describes the assessment of the risk of the SF-S-18 or the SDS/HDS accessibility equipment malfunction safety scenario, and the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 40. Risk Assessment of the SDS/HDS Accessibility Equipment Malfunction Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A traveler who needs to use the accessibility features and cannot do that because of the equipment malfunction, may be stuck at the pick-up location, and deprived from riding the shuttle. This may expose the traveler to a dangerous situation, especially at night or during inclement weather, and may result in severe injury.
Exposure	E1	SDS accessibility equipment malfunction is not very likely.
Controllability	C2	Technicians should be able to perform emergency repairs. Regular maintenance of the accessibility equipment should minimize the probability of malfunction.
Modified ASIL Overall Rating	QM	

4.2.19 Risk SF-S-19 – Pick-up, Drop-off location occupied

Table 41 describes the assessment of the risk of the SF-S-19 or when the pick-up or drop-off locations are occupied safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 41. Risk Assessment of the Pick-up or Drop-off Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	User gets on/off the bus on snow/slippery surface may slip or fall. In the worst case, may be involved in a fatal vehicle-pedestrian accident with an oncoming vehicle.
Exposure	E3	Constructions, snow accumulation, and/or slippery surfaces that blocks the pick-up or drop-off point due to weather conditions are quite probable in Buffalo during winter.
Controllability	C3	Pick-up or drop-off locations being blocked is not controllable in occasions such as construction. However, timely snow plowing and ice removal would reduce the frequency of blockage. In addition, planning alternative pick-up and drop-off locations, during construction, and warning passengers about current conditions (e.g., snow/slippery surfaces) through digital signs or mobile device notifications will minimize the inconvenience and potential injuries.
Modified ASIL Overall Rating	Modified ASIL C	

4.2.20 Risk SF-S-20 – SDS/HDS moves before traveler is secured

Table 42 describes the assessment of the risk of the SF-S-20 safety scenario, which describes the hazard occurring when SDS/HDS moves before the traveler is appropriately secured. It also

explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 42. Risk Assessment of the SDS/HDS Moves before Traveler is Secured Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S1	A Traveler who requires securement falls or crashes into objects inside the shuttle as a result. This may lead to moderate injury.
Exposure	E1	It is rare that SDS/HDS would move before necessary securement is completed. The main cause would be SDS malfunction or HDS driver not following safety protocols, which both are unlikely.
Controllability	C3	SDS/HDS moves before a traveler who uses accessibility feature is secure may be a system/sensor error or a human driver mistake which is difficult to control when the hazard actually occurs. However, proper driver/steward training, regular maintenance, and routine equipment checking, and inspection can reduce the possibility of occurrence
Modified ASIL Overall Rating	QM	

4.2.21 Risk SF-S-21 – SDS/HDS sudden stops

Table 43 describes the assessment of the risk of the SF-S-21 or the sudden SDS/HDS stops safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 43. Risk Assessment of the SDS/HDS Sudden Stops Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Traveler falls or crashes into objects inside the shuttle due to sudden stops may lead to severe injury.
Exposure	E4	It is quite likely that the shuttle would perform sudden stops in the driving process to avoid a driving hazard.
Controllability	C2	Although most of the shuttle sudden stops cannot be avoided. By informing the travelers about the possibility of sudden stops and reminding the travelers to take proper safety procedure (seated when possible, grabbing a pole for standee) through broadcasting inside the shuttle, the possibility of injury should be minimized.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.22 Risk SF-S-22 – SDS driving environment beyond ODD

Table 44 describes the assessment of the risk of the SF-S-22 or the SDS driving environment beyond Operational Design Domain (ODD) safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 44. Risk Assessment of the SDS Driving Environment beyond ODD Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	In extreme cases such as snowstorms, SDS may lose control and crash, or even flip to cause fatal injuries to the passengers and steward.
Exposure	E2	It should be a rare occurrence that the SDS would encounter a driving environment beyond its properly defined ODD. However, considering that Buffalo is likely to have inclement weather and snow during winter, the probability of this hazard would be slightly higher (hence raising the exposure level to E2).
Controllability	C3	It is not controllable that the driving environment is beyond SDS ODD. However, proper steward training and digital messages or broadcastings that remind passengers to take proper safety procedures may reduce the possibility and the severity of injury.
Modified ASIL Overall Rating	Modified ASIL B	

4.2.23 Risk SF-S-23 – Traveler misses connection trip

Table 45 describes the assessment of the risk of the SF-S-23 or the traveler misses connection trip safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 45. Risk Assessment of the Traveler Misses Connection Trip Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Traveler may miss an important appointment, and/or get stuck at the bus/shuttle stop. Traveler may be severely injured, especially in inclement weather conditions.
Exposure	E2	It is somewhat likely that a traveler misses the connection trip due to weather or scheduling factors. (e.g., delay of the prior leg in the trip).
Controllability	C1	Real-time shuttle status should be available for traveler. If such a hazard occurs, the traveler could make another reservation, and determine if there is sufficient connection time. If not, the traveler could find an alternative transportation mode. (e.g., ride sharing).
Modified ASIL Overall Rating	QM	

4.2.24 Risk SF-S-24 – Delay or missed stop caused by re-route

Table 46 describes the assessment of the risk of the SF-S-24 or the delay or missed stop caused by re-route safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 46. Risk Assessment of the Delay or Missed Stop Caused by Re-route Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A traveler may be waiting at the bus stop for extra time which may cause severe injury in inclement weather conditions.
Exposure	E2	It is somewhat likely that a shuttle re-routes, which may result in delays due to weather or traffic factors (e.g., snowstorm, traffic accident that blocks the street).
Controllability	C1	By ensuring that the notifications of potential delays or missing stops are sent to travelers who may be affected, as soon as the re-route is decided, the travelers should be able to plan accordingly.
Modified ASIL Overall Rating	QM	

4.2.25 Risk SF-S-25 – V2X connection lost

Table 47 describes the assessment of the risk of the SF-S-25 or the V2X connection lost safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.7 for UC7&8 scenarios description.

Table 47. Risk Assessment of the V2X connection lost Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	May cause life-threatening injuries if V2X lost is related to pedestrian crossing at traffic signals.
Exposure	E1	It is rare for V2X to lose communication. Furthermore, it is extremely rare that lost communication could cause accidents or incidents.
Controllability	C2	Technician could perform emergency repair to the malfunction element. If the lost V2X contains essential safety information, SDS or the safety steward should stop the vehicle and wait for technician or instructions from SOC. Iin the HDS case, the HDS driver should be notified the situation instantly.
Modified ASIL Overall Rating	QM	

4.2.26 Risk SF-S-26 – SDS Hardware/physical element malfunction

Table 48 describes the assessment of the risk of the SF-S-26 or the SDS hardware/physical element malfunction safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 48. Risk Assessment of the SDS Hardware/physical Element Malfunction Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Hardware (e.g., LiDAR/radar sensor) malfunction may cause vehicle-to-vehicle or vehicle-to-pedestrian accident that is fatal.
Exposure	E1	It is not very likely that the hardware or physical element on board the SDS malfunction.
Controllability	C2	Technician could perform emergency repair to the malfunction elements. Proper safety steward training on identifying and controlling dangerous situations, as well as regular shuttle maintenance will minimize the probability of malfunction during service.
Modified ASIL Overall Rating	QM	

4.2.27 Risk SF-S-27 – SDS/HDS accessibility/securement mechanisms malfunction

Table 49 describes the assessment of the risk of the SF-S-27 or the HDS accessibility/ securement mechanisms malfunction safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 49. Risk Assessment of the SDS/HDS Accessibility/securement Mechanisms Malfunction Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	A person using the accessibility/securement feature may be stuck at the shuttle stop not being able to take the ride. This could result in severe injury in inclement weather conditions. In addition, malfunction during the ride could result in severe injury to the passenger who is using such mechanisms.
Exposure	E1	It is not very likely that HDS accessibility/securement mechanisms would malfunction.
Controllability	C1	HDS driver would be able to fix simple malfunction, technician could perform emergency repair to the malfunction mechanism. Regular maintenance will minimize the probability of malfunction during service.
Modified ASIL Overall Rating	QM	

4.2.28 Risk SF-S-28 – Driver/steward abandonment

Table 50 describes the assessment of the risk of the SF-S-28 or the driver/steward abandonment safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 50. Driver/steward Abandonment Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	Passengers may be stranded in the shuttle not knowing the situation, nor how to open the door, feeling afraid or abandoned. This may cause panic and potential severe injuries to passengers (e.g., as a result of running and falling when panic occurs).
Exposure	E1	It is rare that the steward/driver abandons the vehicle even after receiving text/call related to an emergency.
Controllability	C1	By setting appropriate driver/steward training, driver/steward abandonment should be preventable. In addition, having an available backup driver in the system in service hours would mitigate the risk of abandonment.
Modified ASIL Overall Rating	QM	

4.2.29 Risk SF-S-29 - SDS/HDS rear-ended collision

Table 51 describes the assessment of the risk of the SF-S-29 safety scenario, or when the SDS or HDS is involved in a rear-end collision. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 51. Risk Assessment of the SDS/HDS Rear-ended Collision Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	The speed limit in some parts of the deployment area exceeds 25 mph (though the SDS itself would be always restricted to traveling at speeds LOWER than 25 mph). Because of this, a speeding car rear-ending the SDS could cause severe injury, or even result in a fatality, to the passengers (especially considering the population of interest) when crashing.
Exposure	E0	It is very rare that SDS would be rear-ended by another vehicle. This is estimated to potentially occur less than once per year.
Controllability	C3	An SDS being involved in a rear-ended collision is not controllable, because it could be the result of the human error of the driver of the other vehicle. However, notification that reminds passengers to always follow the safety procedures (e.g., seated when possible, always grabbing a pole for standees) may reduce the possibility and the severity of injury.

Modified ASIL Overall Rating	QM

4.2.30 Risk SF-S-30 - SDS-pedestrian collision

Table 52 describes the assessment of the risk of the SF-S-30 or the SDS-pedestrian collision safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 52. Risk Assessment of the SDS-pedestrian Collision Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	The SDS maximum speed in ODD is 25 mph, which could cause severe injury to both the pedestrian and the passengers onboard, when involved in a vehicle-pedestrian collision.
Exposure	E0	It is very rare that SDS would be involved in a pedestrian collision incident, considering the SDS is very conservative in driving. Furthermore, the safety steward will monitor the driving situation at all times and always has the capability to stop the shuttle.
Controllability	C2	With proper steward training on emergency operation in such a situation, the probability of the incident occurring, and the severity of the injuries should be minimized.
Modified ASIL Overall Rating	QM	

4.2.31 Risk SF-S-31 - SDS frontal collision

Table 53 describes the assessment of the risk of the SF-S-31 or the SDS frontal collision safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.8 for UC9 scenario description.

Table 53. Risk Assessment of the SDS Frontal Collision Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S2	The SDS maximum speed in ODD is 25 mph, which could cause severe injury, or even a fatality, to the passengers when involved in a frontal collision.
Exposure	E0	It is very rare that SDS would be involved in frontal collision, considering that SDS is very conservative in driving. Additionally, the safety steward will monitor the driving situation at all times and always has the capability to stop the shuttle.
Controllability	C2	With proper steward training on emergency operation in such a situation, the probability of the incident occurring, and the severity of the injuries should be minimized.
Modified ASIL Overall Rating	QM	

4.2.32 Risk SF-S-32 – Failing linking traveler's mobile device with Ped request signal

Table 54 describes the assessment of the risk of the SF-S-32 or the failing linking traveler's mobile device with Ped request signal safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.9 for UC10 scenario description.

Table 54. Risk Assessment of the Failing Linking Traveler's Mobile Device with Ped Request Signal Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	A Traveler who solely depends on the app but tries to cross without making crossing request may be involved in a fatal vehicle-pedestrian accident.
Exposure	E2	It is somewhat likely that the traveler's device would fail to link with Ped request signal due to mobile device signal instability or Ped request signal malfunction.
Controllability	C2	The traveler can try to press the crossing request button. This may be more difficult for some users. A warning could be sent to a traveler's mobile device when a link lost is discovered. Anyone who experiences such a situation should report it.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.33 Risk SF-S-33 – Dropped request at intersection

Table 55 describes the assessment of the risk of the SF-S-33 safety scenario, or the dropped request at intersection. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.9 for UC10 scenario description.

Table 55. Risk Assessment of the Dropped Request at Intersection Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	A traveler who assumes the request is received, and starts crossing based on the traffic flow direction, may be struck by an incoming vehicle, which may result in fatality.
Exposure	E1	It is not very likely that the passing request is dropped.
Controllability	C2	The traveler can try to press the crossing request button. This may be more difficult for some users. If the signal is not triggered in two cycles, then a repair is needed. Any user who experiences this situation should report it.
MODIFIED ASIL Overall Rating	QM	

4.2.34 Risk SF-S-34 – Incorrect Ped-X signal direction

Table 56 describes the assessment of the risk of the SF-S-34 or the incorrect Ped-X signal direction safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.9 for UC10 scenario description.

Table 56. Risk Assessment of the Incorrect Ped-X Signal Direction Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Traffic accident with pedestrian may be fatal.
Exposure	E2	A recent study of PedNav in downtown Stillwater (Harlow, 2021) shows that there was about 95 percent accurate in accessing traffic signal control systems and sending correct auditory and visual messages to tell pedestrians when it was safe to cross the street. Therefore, it is still somewhat probable to have incorrect Ped-X signal direction.
Controllability	C2	A message reminding traveler to pay attention to the actual pedestrian signal as well as surrounding traffic could be sent or shown in the traveler's app before crossing the street. Anyone who experiences errors should be able to report it.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.35 Risk SF-S-35 – Inaccurate Ped-X signal timing

Table 57 describes the assessment of the risk of the SF-S-35 or the Inaccurate Ped-X signal timing safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.9 for UC10 scenario description.

Table 57. Risk Assessment of the Inaccurate Ped-X Signal Timing Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Traffic accident with pedestrian may be fatal.
Exposure	E2	Similar to SF-S-34, it is somewhat probable that Ped-X provides inaccurate signal timing.
Controllability	C2	A message reminding traveler to pay attention to the actual pedestrian signal as well as surrounding traffic could be sent or shown in the traveler's app before crossing the street. Anyone who has the error should be able to report it for further investigation.
Modified ASIL Overall Rating	Modified ASIL A	

4.2.36 Risk SF-S-36 – Delayed Ped-X signal alert

Table 58 describes the assessment of the risk of the SF-S-36 or the delayed Ped-X signal alert safety scenario. It also explains the rationale behind the ratings assigned to that hazard. See Section 3.9 for UC10 scenario description.

Table 58. Risk Assessment of the Delayed Ped-X Signal Alert Hazard.

Risk Assessment Class	Rating	Rationale
Severity	S3	Traffic accident with pedestrian may be fatal.
Exposure	E2	Similar to SF-S-34, it is somewhat probable that Ped-X would provide delayed signal alert.
Controllability	C2	A message reminding traveler to pay attention to the actual pedestrian signal as well as surrounding traffic could be sent or shown in traveler's app before crossing the street. Anyone who has the error should be able to report it for further investigation.
Modified ASIL Overall Rating	Modified ASIL A	

5 Safety Operational Concept

To avoid, mitigate, and respond to the potential safety impacts of the hazards identified in the previous sections, four major approaches are suggested. The first approach attempts to address the hazards by including appropriate design requirements to be applied to a subsystem, a component, software, or user interface. The second approach includes policies and operating rules that are put in place during the deployment and evaluation phases of the project. These include approaches such as the regular maintenance of the community shuttle vehicles, accessibility and securement mechanisms, the SDS sensors, etc. It also includes appropriate training and education programs to ensure the proper use of the system, and the analysis of the data collected to reveal any safety deficiencies and to suggest approaches to address them. The third category includes approaches for simple reversion to pre-deployment conditions, or fail-safe modes, when a system or subsystem component fails. Finally, to address some safety impacts, it may require the implementation of emergency response plans.

The previous section (section 4) has evaluated the risks of 11 user safety scenarios ***and*** 36 system safety scenarios, for a total of **47 overall safety scenarios or hazards**. The detailed risk assessment described in section 4 has resulted in a total of **29 scenarios** or hazards assigned the rating of "**QM**" or "Quality Measures", and a total of **18 scenarios** or hazards receiving a higher modified ASIL rating **of Modified ASIL A, B, or C** (there were no scenarios identified that received the most serious rating of D in our study). As discussed before, for those scenarios receiving the "QM" rating, the typical systems engineering principles which will be followed in designing, developing and deploying the system, and which are intended to ensure that the deployed system meets the quality measures and design specifications established, should be adequate to address those safety scenarios (i.e., the 29 scenarios rated as "QM"). On the other hands, the scenarios that were rated as modified ASIL A, B, or C (a total of 18 scenarios as just mentioned) were further examined to identify which of the aforementioned four safety operational concepts (i.e., design elements, operational processes, mitigation and/or emergency response) would be most effective in improving safety and addressing the potential hazard identified.

In the following paragraphs, we briefly describe each one of those safety operational concepts or approaches. We also list the safety scenarios to which the concept will be applied, and provide some of our initial thinking of the specific actions that would be taken to reduce the risk of the hazard and effectively manage the safety of that aspect of the Buffalo ITS4US project. It is to be noted that a few safety scenarios and hazards required the application of more than one of the four safety concepts. Those hazards will then appear more than once in the sections that describe each of the four concepts or approaches.

5.1 Safety Design Elements

To address several of the safety scenarios and hazards identified in this document, functional safety requirements will be added, specifically to address the identified hazards. Table 59 lists the safety scenarios from Section 4 which received a modified ASIL rating higher than "QM", and which will be addressed by Safety Design Elements. The table also describes some of our initial thinking about those added elements

Table 59. Safety Scenarios that will be addressed by Adding Safety Design Elements

Scenario	Scenario Tile	Modified ASIL	Operational Concept	Strategy
SF-U-5	Traveler Trips	Modified ASIL A	Safety Design Elements	Put a rail for shuttle entry/exit.
SF-S-4	Delayed vehicles	Modified ASIL A	Safety Design Elements	Consider adding design elements to provide protection from elements at pick-up locations.
SF-S-8	Inaccurate Directions	Modified ASIL C	Safety Design Elements	Add design elements to Improve accuracy; Add the ability to announce and identify landmarks en-route to serve as benchmarks.
SF-S-9	Orientation inaccuracy	Modified ASIL A	Safety Design Elements	Add the ability to calculate the positional displacement in a very short period to help identify the walking direction of the traveler. Additionally, the navigation could provide additional information about landmarks along the way.
SF-S-11	Inaccurate sidewalk data	Modified ASIL A	Safety Design Elements	Ensure integrity and accuracy of data
SF-S-21	SDS/HDS Sudden Stops	Modified ASIL A	Safety Design Elements	Appropriate securement; ensure acceleration/ deceleration profiles are within comfortable and safe ranges.
SF-S-32	Failing linking traveler's mobile device with Ped request signal	Modified ASIL A	Safety Design Elements	When the linking fails, the app should be designed to notify the user that the linking request had failed, and that the app would be incapable of requesting the phase.

In addition to the above, it should be noted that the Agile development process, which we plan to follow in Phase 2 when developing the CTP component of the Buffalo ITS4US project. This approach will further help us in addressing any additional safety concerns that are revealed, based upon the input from end users and system owners. Moreover, it should be noted that because the proposed Buffalo ITS4US system will integrate software, hardware, sensors, and equipment from several sources and vendors, the interfaces among all those elements will need to be carefully specified to ensure proper integration and interoperability through bench testing,

field testing and system integration testing prior to system deployment and release. These measures however are part of the “QM” and not directed toward safety per se.

5.2 Safety Operational Processes

Safety operational processes refer to the activities that are in place which are intended to ensure the safe operations of the ITS4US deployment. The process starts with the development of the SMP (this document) and of considering the various safety scenarios or hazards identified, through developing appropriate mitigation strategies. Additional processes may include:

(1) Procedures for ensuring that all equipment is well-maintained and inspected for safety regularly.

(2) Procedures for ensuring the accuracy and integrity of information used within the ITS4US system and that all information is up to date.

(3) Training programs.

(4) Monitoring any safety anomalies and near-misses.

(5) Examining incident reports to understand how such incidents may be avoided in the future.

(6) Ensuring information is updated in a timely fashion to with the most current information on driving or traveling events are delivered with minimal delay or latency.

Table 60 lists the safety scenarios from section 4 which received a modified ASIL rating higher than “QM”, and which will be addressed by safety operational processes. The table also describes some of our initial thinking about those added elements.

Table 60. Safety Scenarios that will be addressed by Safety Operational Processes

Scenario	*Scenario Tile*	*Modified ASIL*	*Operational Concept*	*Strategy*
SF-S-2	No return trip booking available	Modified ASIL A	Safety Operational Processes	Safety Shuttle to pick-up stranded passenger
SF-S-4	Delayed vehicles	Modified ASIL A	Safety Operational Processes	Safety Shuttle to pick up stranded passengers
SF-S-5	No show vehicle	Modified ASIL A	Safety Operational Processes	Safety Shuttle to pick-up stranded passenger
SF-S-8	Inaccurate Directions	Modified ASIL C	Safety Operational Processes	Processes to ensure integrity of information
SF-S-15	Insufficient Shuttle availability	Modified ASIL A	Safety Operational Processes	Safety Shuttle to pick-up stranded passenger

Scenario	Scenario Tile	Modified ASIL	Operational Concept	Strategy
SF-S-19	Pick-up, Drop-off Location occupied	Modified ASIL C	Safety Operational Processes	Ensure clearing pick-up and drop-off locations is a priority
SF-S-22	SDS Driving Environment beyond ODD	Modified ASIL B	Safety Operational Processes	Proper training stewards
SF-S-34	Incorrect PED-X signal direction	Modified ASIL A	Safety Operational Processes	Include frequent tests to ensure the accuracy and performance of PED-X signal
SF-S-35	Inaccurate PED-X signal timing	Modified ASIL A	Safety Operational Processes	Include frequent tests to ensure the accuracy and performance of PED-X signal
SF-S-36	Delayed PED-X signal alert	Modified ASIL A	Safety Operational Processes	Include frequent tests to ensure the accuracy and performance of PED-X signal

5.3 Mitigations and Fail-Safes

As a part of the system design requirement process, we will include specific requirements that vehicle systems revert to a fail-safe mode when it is unable to perform its function as intended. For example, in cases when the driving environment exceeds the safe ODD for the SDS, the human steward onboard would be expected to take over control of the vehicle and bring it to a safe parking spot for example (in some AV designs, the self-driving system would attempt to get the vehicle to a safe parking spot itself and park there until problem is resolved). Also, in the cases when a sensor onboard the SDS malfunctions, the shuttle will revert immediately to the manual driving mode (in that regard, it is worth noting that manual take over by a human steward is not trivial; however, we anticipate that the ODD for the SDS would not be very complex, and that properly trained stewards should be able to take over in a safe manner). Similarly, if the connectivity between a pedestrian's CTP app and the signal controller fails, the controller would revert to the basic mode of operations where a pedestrian would need to press the pedestrian crossing button manually to call for the crossing phase.

Table 61 lists the safety scenarios from section 4 which received a modified ASIL rating higher than "QM", and which will be addressed by mitigation and/or fail-safe strategies.

Table 61. Safety Scenarios that will be addressed by Mitigation and/or Fail-Safe Strategies

Scenario	*Scenario Tile*	*Modified ASIL*	*Operational Concept*	*Strategy*
SF-S-22	SDS Driving Environment beyond ODD	Modified ASIL B	Mitigation or Fail-Safe	Backup HDS when ODD exceeded.
SF-S-32	Failing linking traveler's mobile device with Ped request signal	Modified ASIL A	Mitigation or Fail-Safe	Fall back to using the manual pedestrian crossing button.
SF-S-34	Incorrect PED-X signal direction	Modified ASIL A	Mitigation or Fail-Safe	Revert to manual pedestrian push-button operations
SF-S-35	Inaccurate PED-X signal timing	Modified ASIL A	Mitigation or Fail-Safe	Revert to manual pedestrian push-button operations
SF-S-36	Delayed PED-X signal alert	Modified ASIL A	Mitigation or Fail-Safe	Revert to manual pedestrian push-button operations

During extreme weather scenarios, and based on input from weather forecasting systems, the Buffalo ITS4US will follow the existing procedures in place (many of which are documented in NFTA most recent Safety Management Plan), which may include suspending some of the system services until the extreme weather event ends.

Implementing many of the mitigation strategies will require working closely with several local agencies. For example, to address safety issues related to the safe operations of the SDS, coordination with NYS Department of Motor Vehicles (DMV), NYS Department of Transportation (NYSDOT), and the City of Buffalo will be needed. Similarly, with respect to safety improvements related to smart infrastructure, coordination with the City of Buffalo and NYSDOT are critical. For coordination, the Buffalo ITS4US Safety Management Committee will hold regular meetings with the pertinent agencies and organizations, keep them informed of the safety concerns and issues identified, and work with them to implement the appropriate response and mitigation strategies. The Operations of the SDS will require the development of a law enforcement interaction plan that details how the project will work with the DMV and the police to ensure the safety of operations.

5.4 Safety Responses

In the case of a serious vehicle crash, an accident involving a vehicle and a pedestrian, or a health emergency onboard the community shuttle, the existing emergency response plans of the City of Buffalo, Erie County and NYSDOT in place will be followed. This will include an available user and/or operator calling 911, and emergency responders responding to the emergency following their standard procedures. In case of accidents involving a malfunction of a technology

component (e.g., the PedX or SDS), the system would revert to the fail-safe mode of operations (i.e., using the signal push button or manually driving the shuttle) until the cause of the accident is determined. Table 62 lists the safety scenarios from Section 4 that received a modified ASIL rating higher than “QM”, and which will be addressed by mitigation and/or fail-safe strategies.

Table 62. Safety Scenarios that will be addressed by Safety or Emergency Response Plans

Scenario	*Scenario Tile*	*Modified ASIL*	*Operational Concept*	*Strategy*
SF-U-8	Traveler Health Emergency	Modified ASIL B	Safety Responses	Incident Management Plan
SF-U-9	HDS Driver Health Emergency	Modified ASIL A	Safety Responses	Incident Management Plan
SF-U-10	SDS Steward Health Emergency	Modified ASIL A	Safety Responses	Incident Management Plan

Additional response strategies will include restoring power after a black-out, re-booting the system after a software glitch, and repairing and/or replacing failing system components. Finally, a failure diagnosis and analysis will be conducted to uncover the root cause of the problem and to develop strategies in place to avoid similar incidents in the future.

5.5 Safety Reporting

All safety issues and incidents that occur during the deployment, evaluation, and operations phases of the Buffalo ITS4US project will be carefully recorded and reviewed by the Safety Management Committee of the project on a regular basis. The reported incidents will be carefully analyzed to identify the root cause of the problem, and appropriate safety operations processes and mitigation strategies will be implemented to avoid such hazards in the future. In addition, safety performance measures (or metrics) will be developed as part of the project’s Performance Management Plan and regularly monitored to assess the safety of the deployment and suggest any needed corrective measures. Information will be regularly shared with the USDOT and added to the repository of “lessons learned” from the Buffalo ITS4US Deployment.

6 Safety Management Summary

6.1 Safety Risk Summary

Table 63 summarizes the safety risks listed in this document. For each safety risk, the table also provides their assessment, safety strategy, factors to monitor, and overall status.

Table 63. Safety Risk Management Summary

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-U-1	Contradictory preferences	QM	Quality Measures - Include a preference selection system that will inform users when the selected preferences conflict.	The error messages automatically sent through the CTP app.	Planning
SF-U-2	Preference / notification selection mismatch with end user's device	QM	Quality Measures - Include a warning system that checks the device compatibility and sends warnings when a mismatch is detected.	The error messages automatically sent and the user reporting (feedback) through the CTP app.	Planning
SF-U-3	No trip plan generated	QM	Quality Measures - Include a system that would provide recommendations on the possible itineraries.	The error messages automatically sent through the CTP app. If some itineraries appear at very high frequencies, it might mean that such trips are in high demand.	Planning
SF-U-4	Unintended festination	QM	Quality Measures - Include additional destination confirmation step before starting the trip.	The frequency at which travelers are navigated to unintended destinations. If this occurs at an unacceptable rate, there may be an issue with the CTP app.	Planning
SF-U-5	Traveler trips	Modified ASIL A	Design requirements - Include designs (visual and voice) warning travelers about tripping at all shuttle exit/entrance doors and where there are stairs. Consider adding a rail for shuttle entry/exit	The frequency and reason of travelers tripping from CTP app users and drivers/stewards reporting (feedback).	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-U-6	Traveler early exit	QM	Quality Measures - Include a notification system that pushes an arrival notification to users' right after passing the prior-to-destination stop. Introduce this function to users before starting trips.	The frequency at which travelers using the system take early exits. If this occurs at an unacceptable rate, there may be an issue with the CTP app.	Planning
SF-U-7	Traveler misses exit	QM	Quality Measures - Include a notification system that pushes an arrival notification to users right after passing the prior-to-destination stop. Introduce this function to users before starting trips.	The frequency at which travelers using the system miss the correct stop. If this occurs at an unacceptable rate, there may be an issue with the CTP app.	Planning
SF-U-8	Traveler health emergency	Modified ASIL B	Safety or Emergency response - Available user or driver/steward calls 911 instantly when traveler health emergency occurs. Driver/steward takes first-aid actions (e.g., Cardiopulmonary resuscitation, CPR) as needed.	The frequency of traveler health emergencies in the shuttle and the consequences.	Planning
SF-U-9	HDS driver health emergency	Modified ASIL A	Safety or Emergency response - HDS driver safely stops the shuttle as best as he/she can. Available user calls 911 instantly when a driver's health emergency occurs.	The frequency of HDS health emergencies and the consequences.	Planning
SF-U-10	SDS steward health emergency	Modified ASIL A	Safety or Emergency response - SDS steward safely stops the shuttle as best as he/she can if driving manually. Available user calls 911 instantly when a steward health emergency occurs.	The frequency of SDS steward health emergencies and the consequences.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-U-11	Emergency stop button misusage	QM	Quality Measures - Include a warning sign of proper instructions about when and how to use the emergency button near the button.	The number of times emergency stop button is misused and the resulting consequences.	Planning
SF-S-1	No trip booking available	QM	Quality Measures - Include connectivity check between the app system and reservation service.	The error messages automatically sent through the CTP app. If some itineraries appear at very high frequencies, it might mean that such trips are in high demand.	Planning
SF-S-2	No return trip booking available	Modified ASIL A	Safety operational processes – Designate a safety shuttle service to pick-up stranded travelers, if needed. Include actively monitoring of travel demand and optimize shuttle distribution as needed.	The error messages automatically sent through the CTP app. If some itineraries appear at very high frequencies, it might mean that such trips are in high demand.	Planning
SF-S-3	Mismatched vehicle to traveler needs	QM	Safety operational processes - Include validation for vehicle equipment occupancy status and user preference.	The frequency of mismatched vehicle to traveler needs occur through user reporting (feedback) in the CTP app. If this happens at an unacceptable rate, there may be issues in the CTP app or in the shuttle distribution model.	Planning
SF-S-4	Delayed vehicles	Modified ASIL A	Design Requirements and Safety Operational Processes - develop verification and notification mechanisms to ensure users aware of the delays; Consider adding design elements to provide protection from elements at pick-up locations; Add Safety Shuttle service to pick-up stranded passengers	The frequency of vehicle delaying with respect to delaying reasons.	Planning
SF-S-5	No-show vehicles	Modified ASIL A	Design Requirements and Safety Operational Processes - develop verification and notification mechanisms	The frequency of vehicles is not showing up with respect to no-show reasons.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
			to ensure users are aware of the no-show situation; Add Safety Shuttle service to pick-up stranded passengers.		
SF-S-6	Delayed notifications about late shuttles / PAL	QM	Quality Measures - Include connectivity and notification checks that ensure any notifications about schedule changing can be received by users.	The frequency of delayed notifications with respect to various reasons for the delay.	Planning
SF-S-7	Inaccessible directions	QM	Quality Measures - Include additional input validation for location data relating to areas where certain user groups have difficulty traveling through.	The user reporting (feedback) on inaccessible locations with the choice of preferences through the CTP app to update the road information.	Planning
SF-S-8	Inaccurate directions	Modified ASIL C	Design Requirements and Safety operational processes Add design elements to Improve accuracy; Add the ability to announce and identify landmarks en-route to serve as benchmarks; Include additional input validation for location data used in navigation; Develop processes to ensure integrity of information	The user reporting (feedback) on inaccurate directions and the resulting consequences through the CTP app.	Planning
SF-S-9	Orientation inaccuracy	Modified ASIL A	Design Requirements - Add the ability to calculate the positional displacement in a very short period to help identify the walking direction of the traveler. Additionally, the navigation could provide additional information about landmarks along the way.	The user reporting (feedback) on orientation inaccuracy and the resulting consequences through the CTP app.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-S-10	Positional inaccuracy	QM	Quality Measures - Include an option that allows users to reposition themselves manually before navigation starts.	The user reporting (feedback) on positional inaccuracy and the resulting consequences through the CTP app.	Planning
SF-S-11	Inaccurate sidewalk data	Modified ASIL A	Safety operational processes - Include additional input validation for sidewalk data; actively monitoring user feedback about inaccurate sidewalk information.	The user reporting (feedback) on inaccurate sidewalk data through the CTP app to update the sidewalk data.	Planning
SF-S-12	Inaccurate indoor facility data	QM	Quality Measures - Include additional input validation for indoor facility data.	The user reporting (feedback) on inaccurate indoor facility data through the CTP app to update the indoor facility data.	Planning
SF-S-13	Traveler mobile device not linking with indoor/outdoor Smart Signs	QM	Quality Measures - Include a warning system that notifies users about connection error and be aware of the surroundings.	The error messages about not linking with the Smart Signs sent automatically through the CTP app.	Planning
SF-S-14	Inaccurate or delayed dynamic information about work zone and obstructions	QM	Quality Measures - Include additional input validation for dynamic work zone and obstruction data.	The frequency of inaccurate or delayed work zone and obstruction information. If the frequency is at an acceptable rate, this may indicate that there are issues regarding communication between the construction authorities (e.g., COB/NFTA) and the CTP data management center.	Planning
SF-S-15	Insufficient shuttle availability	Modified ASIL A	Safety operational processes - Safety Shuttle to pick-up stranded passenger; include actively monitoring on travel demand and optimize shuttle distribution as needed.	The error messages automatically sent through the CTP app. If some itineraries appear at very high frequencies, it might mean that such trips are in high demand.	Planning
SF-S-16	Unavailable special equipment's occupancy information	QM	Quality Measures – Ensure that information about special equipment’s occupancy is available.	The frequency of occupancy information is not updated in the system, and the corresponding reasons.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-S-17	Inaccurate pick-up or drop-off information	QM	Quality Measures - Include confirmation notification system that verifies the addresses with users.	The frequency of occurrence of wrong pick-up/drop-off location and the corresponding reasons to help improve the future performance.	Planning
SF-S-18	SDS/HDS accessibility equipment malfunction	QM	Safety operational processes - Include regular maintenance and timely repairs for shuttle accessibility equipment.	The frequency of such malfunction and the resulting consequences; shuttle maintenance reports.	Planning
SF-S-19	Pick-up, Drop-off location occupied	Modified ASIL C	Safety operational processes - Ensure plowing and clearing pick-up and drop-off locations is a priority; include plans for back-up loading/unloading locations; notify snow plowing authorities about pick-up and drop-off locations.	The frequency of pick-up/drop-off location being occupied and the resulting consequences (e.g., if the shuttle finds a spot to stop at the current station; how far it is from the designed location; is any traveler injured, etc.).	Planning
SF-S-20	SDS/HDS moves before traveler is secured	QM	Safety operational processes - Include driver/steward training on checking securements before vehicle moving. (steward may need to pause the autonomous mode to check).	The frequency at which the shuttle moves before necessary securement is completed.	Planning
SF-S-21	SDS/HDS sudden stops	Modified ASIL A	Design requirements - Include designs (visual and voice) that remind passengers to take proper safety procedure during the ride; ensure acceleration/ deceleration profiles are within comfortable and safe ranges.	The user reporting/complaining through the CTP app about the sudden stops and the consequences. It is also necessary to record the frequency of SDS sudden stops with recordings of the surrounding environment information to determine if the SDS driving behaviors can be improved.	Planning
SF-S-22	SDS driving environment beyond the ODD	Modified ASIL B	Safety Operational Processes and Mitigation/Fail-Safe – Proper training of stewards on how to take over; Revert to humanly controlling the shuttles.	The frequency of such an environment occurring, and the resulting consequences.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-S-23	Traveler misses connection trip	QM	Quality Measures - Include real-time shuttle location sharing or estimated arrival time at each stop, so that the traveler could take early actions (e.g., looking for alternative transportation mode) if the current mode would be delayed.	The frequency of travelers misses connection trip due to delays or scheduling problem.	Planning
SF-S-24	Delay or missed stop caused by re-route	QM	Quality Measures - develop verification and notification mechanisms to ensure users are aware of the delay or miss.	The frequency of re-route, and the probability of delay/miss any stops.	Planning
SF-S-25	V2X connection lost	QM	Quality Measures - Develop notification mechanism to inform the driver/steward about current situation (what V2X is lost and how it may affect driving).	The frequency at which the V2X communication is lost due to several reasons and the resulting consequences.	Planning
SF-S-26	SDS hardware/physical element malfunction	QM	Quality Measures - Include regular maintenance and timely repairs for SDS hardware/physical element equipment.	The frequency of the malfunction and resulting consequences; SDS maintenance reports.	Planning
SF-S-27	SDS/HDS accessibility/ securement mechanisms malfunction	QM	Quality Measures - Include regular maintenance and timely repairs for HDS accessibility/securement mechanisms.	The frequency of the malfunction and the resulting consequences; HDS maintenance reports.	Planning
SF-S-28	Driver / steward abandonment	QM	Quality Measures - Include driving/steward training on the correct procedure (never abandon the shuttle; if emergency and has to leave, contact the SOC, and wait until replacement arrives).	The frequency of driver/steward abandonment and the consequences.	Planning
SF-S-29	SDS/HDS rear-ended collision	QM	Quality Measures/ Emergency response - Driver/steward and available users call 911 immediately.	The frequency of near crashes to determine the likelihood of an incident being at the fault of the surrounding traffic.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
			Driver/steward takes first-aid actions to passengers (e.g., CPR) as needed.		
SF-S-30	SDS-pedestrian collision	QM	Quality Measures/ Emergency response - Driver/steward and available users call 911 immediately. Driver/steward takes first-aid actions to pedestrian and/or passengers (e.g., CPR) as needed.	The frequency of near vehicle-pedestrian crashes to determine the likelihood of such incident being at the fault of the SDS.	Planning
SF-S-31	SDS frontal collision	QM	Quality Measures/ Emergency response - Driver/steward and available users call 911 immediately. Driver/steward takes first-aid actions to passengers (e.g., CPR) as needed.	The frequency of near vehicle crashes to determine the likelihood of such incident being at the fault of the SDS.	Planning
SF-S-32	Failing linking traveler's mobile device with Ped request signal	Modified ASIL A	Design Requirements and Mitigation and fail-safes - When the linking fails, the app should be designed to notify the user that the linking request had failed, and that the app would be incapable of requesting the phase; Fall back to using the manual pedestrian crossing button.	The frequency at which traveler's mobile device fails to link with Ped request signal and the resulting consequences. Also, it is important to monitor and analyze the error messages of such hazard sent automatically through the CTP app.	Planning
SF-S-33	Dropped request at intersection	QM	Quality Measures - Develop verification and notification mechanisms to ensure users are notified of the dropped request, and guide users to take proper actions.	The frequency at which signal request is dropped and the resulting consequences. Also, it is important to monitor and analyze the error messages of such hazard sent automatically through the CTP app.	Planning

ID	Safety Risk	Safety Assessment	Safety Op. Concept Strategies	Factors to Monitor	Overall Status
SF-S-34	Incorrect PED-X signal direction	Modified ASIL A	Safety operational processes and Mitigation and fail safe - Include frequent tests to ensure the accuracy and performance of PED-X signal; Revert to manual pedestrian push button operations.	The frequency of incorrect PED-X signal direction and the resulting consequences. Also, it is important to monitor and analyze the error messages of such hazard sent automatically through the CTP app.	Planning
SF-S-35	Inaccurate PED-X signal timing	Modified ASIL A	Safety operational processes and Mitigation and fail-safe - Include frequent tests to ensure the accuracy and performance of PED-X signal; Revert to manual pedestrian push-button operations.	The frequency of PED-X signal timing and the resulting consequences. Also, it is important to monitor and analyze the error messages of such hazard sent automatically through the CTP app.	Planning
SF-S-36	Delayed PED-X signal alert	Modified ASIL A	Safety operational processes and Mitigation and fail-safe - Include frequent tests to ensure the accuracy and performance of PED-X signal; Revert to manual pedestrian push-button operations.	The frequency of delayed PED-X signal alert and the resulting consequences. Also, it is important to monitor and analyze the error messages of such hazard sent automatically through the CTP app.	Planning

6.2 Continuing Safety Planning

Like many other documents of the Buffalo ITS4US project, the SMP should be viewed as a living document. It is expected that additional risks and hazards would be identified as the project progresses through the design and deployment phases. In addition, as mentioned above, during the deployment and evaluation phases of the project, the factors to monitor in the table above should correspond, in part, to these system operations that are monitored. Safety incidents will be documented and analyzed, and safety metrics will be recorded and reported. A systematic procedure will be put in a place to allow for adding any additional identified risks to the SMP, along with the appropriate mitigation strategies.

Appendix A. Acronyms and Glossary

Table 64 list the acronyms used in the document.

Table 64. Acronyms used in the SMP

Acronym	Description
ASIL	Automotive Safety Integrity Level
AV	Autonomous Vehicle
AWS	Amazon Web Services
BHSC	Buffalo Hearing and Speech Center
BNMC	Buffalo Niagara Medical Campus
BO	Business Operation
BT	Bluetooth
CAV	Connected and Automated Vehicles
ConOps	Concept of Operations
COTS	Commercial-off-the-Shelf
CPR	Cardiopulmonary resuscitation
CTP	Complete Trip Platform
DMV	Department of Motor Vehicles
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
JPO	Joint Program Office
HDS	Human-Driven Shuttle
HTTPS	Hypertext Transfer Protocol Secure
ITS	Intelligent Transportation System
NITTEC	Niagara International Transportation Technology Coalition
NFTA	Niagara Frontier Transportation Authority
NY	New York
NYSDOT	New York State Department of Transportation
ODD	Operational Design Domain
OST	Office of the Secretary
PAL	Paratransit Access Line
PedX	Pedestrian Crossing
PRG	Priority Request Generator
PROW	Public Right of Way
PWD	Persons with Disability
QM	Quality Management
ROW	Right of way
SDS	Self-Driving Shuttle
SMP	Safety Management Plan
SOC	Shuttle Operations Center
UB	University at Buffalo

Acronym	Description
UC	Use Case
U.S.	United States
USDOT	United States Department of Transportation
V2X	Vehicle to Everything
VIA	Visually Impaired Advancement

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-21-873

U.S. Department of Transportation