Phase 1 Safety Management Plan (SMP)

University of Washington ITS4US Deployment Project

www.its.dot.gov/index.htm

Final Report – November 27, 2021
FHWA-JPO-21-874

COMPLETE TRIP
ITS4US

U.S. Department of Transportation

Produced by University of Washington ITS4US Deployment Program, Phase 1
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

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. **FHWA-JPO-21-874**	**2. Government Accession No.**	**3. Recipient's Catalog No.**

4. Title and Subtitle Phase 1 Safety Management Plan—University of Washington ITS4US Deployment Project	**5. Report Date** November 27, 2021
	6. Performing Organization Code N/A
7. Author(s) Mark Hallenbeck, Director of the Washington State Transportation Center at University of Washington; Anat Caspi, Director of the Taskar Center for Accessible Technology at University of Washington,	**8. Performing Organization Report No.**
9. Performing Organization Name and Address University of Washington 4333 Brooklyn Ave NE Box 359472 Seattle, WA 98195-9472	**10. Work Unit No. (TRAIS)**
	11. Contract or Grant No. 693JJ321C000004
12. Sponsoring Agency Name and Address U.S. Department of Transportation ITS Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	**13. Type of Report and Period Covered** N/A
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

Kate Hartman, COR

16. Abstract

This report is the initial Safety Management Plan for the Transportation Data Equity Initiative (TDEI) project, an effort funded by the Federal Highway Administration's ITS4US Program. The project, led by the University of Washington's (UW) Taskar Center for Accessible Technology and the Washington State Transportation Center, will develop a national pipeline to create, disseminate, and share standardized data about pedestrian environments, transportation environments, and on-demand transportation services to enable better use, discoverability, and data analytics of these assets and services. Specifically, the project will release nationally the OpenSidewalks data standard for digitizing pedestrian ways and will extend the national data standards for on-demand transit services (GTFS-Flex) and for mapping of multilevel transit stations (GTFS-Pathways). Additionally, the project will demonstrate the use of those data and standards in three applications: a multimodal, accessible travel planner (an extension of Access Map), an expansion of Microsoft's Soundscape application, which helps blind and low-vision people navigate and explore the environment, and a simulation tool to be built by Unity Technologies that allows travelers to explore the layout of transit stations prior to using those facilities.

The Safety Management Plan describes the underlying needs associated with the safety of all travelers, caregivers, service providers, and all other individuals potentially impacted by the planned deployment of the TDEI. The report assesses the safety needs and risks of travelers who will be interacting with the TDEI. It presents the strategies to be deployed by the team to minimize and mitigate those risks, as well as respond to potential incidents once the DEI is in operation. The report is intended to help inform end users, developers, agencies, organizations, and staff involved in the system of these risks and the planned responses of the project team.

17. Keywords ITS4US; Complete Trip; Deployment; ITS; Intelligent Transportation Systems; Safety Management, Accessibility; Sidewalks; Navigation software; Data Standards	**18. Distribution Statement** N/A

19. Security Classif. (of this report) N/A	**20. Security Classif. (of this page)** N/A	**21. No. of Pages** 62	**22. Price** N/A

Revision History

Update the revision history table upon each update to the Safety Management Plan.

Name	Date	Version	Summary of Changes	Approver
Mark Hallenbeck, University of Washington	30 July, 2021	1	Initial Draft	–
Mark Hallenbeck, University of Washington	23 August, 2021	1	Final Report	–
Mark Hallenbeck, University of Washington	27 November, 2021	1	Refined Final Report	–

Table of Contents

List of Tables

List of Figures

1 Introduction

This document presents the Safety Management Plan for the University of Washington's (UW) ITS4US Deployment Project, the Transportation Data Equity Initiative (TDEI), which is being performed as part of the U.S. Department of Transportation's (USDOT's) Complete Trip—ITS4US Deployment Program. It provides guidance regarding the identification of safety scenarios and risk mitigation to be used in planning for the project's design, construction, and deployment in phase 2 and 3 of this project. The document identifies safety scenarios at both the system and application levels, assesses the level of risk for each scenario, and provides a safety operational concept for high/ medium risk scenarios. Safety stakeholders are identified.

No usable system is completely secure or impenetrable. The goal of the Safety Management Program is to identify the risks, understand their likelihood and impacts on the ITS4US project, and then implement controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, the UW team will develop a robust risk management program through ongoing performance metrics, evaluation, and assessment of safety and security risks and controls throughout the life cycle of the software system.

All potential risks will be handled and mitigated by using the best practices of system engineering and project management in designing the system infrastructure. The Safety Management Plan will also be coordinated with other tasks.

1.1 Document Overview

The Safety Management Plan for the TDEI is a companion to the Concept of Operations (ConOps)[1] and is a key element for ensuring the safety of project participants and the security of system data and communications.

This document describes the underlying needs for safety for those who are expected to use the data, software, and systems being developed and deployed as part of the TDEI. It describes the project team's initial effort to identify various threat scenarios and understand how those threats should be addressed. These scenarios include events such as the publication of invalid data, power outages to both servers and end user devices running project applications, a variety of communication failures, unintended or malicious attacks on the service, and adverse weather conditions.

[1] Phase 1 Concept of Operations (ConOps)—University of Washington ITS4US Deployment Project, by the University of Washington and Cambridge Systematics, Inc., June 2021, Report Number FHWA-JPO-21-861.

The report documents the resulting guidance for designing safety-critical subsystems that are capable of eliminating hazards from the design of the over-arching TDEI system. This will reduce risks to users by lowering the probability of hazards occurring or, at minimum, mitigating the impacts of hazardous events should they occur.

1.2 Project Background

In late 2019, the United States Department of Transportation (U.S. DOT) launched a new department-wide initiative. This initiative, referred to as the Complete Trip initiative, aimed to expand access to transportation for people with disabilities, older adults, and individuals of low income. This initiative recognized that all Americans need access to high-quality, affordable, safe, frequent, and accessible transportation options to access employment opportunities, educational opportunities, healthcare services, and other activities, but that some groups do not receive the same quality of service. To support these underrepresented groups, U.S. DOT aimed to increase its investments in innovations that enhance access and mobility for all travelers, including, but not limited to, the following user groups: people with disabilities, older adults, low-income earners, rural residents, veterans, and those with limited English proficiency (LEP) (henceforth referred to as “underserved travelers”).

In support of this initiative, the Federal Highway Administration created a Broad Area Announcement opportunity, (BAA) #693JJ3-20-BAA-0004, “Complete Trip - ITS4US Deployment.” The University of Washington submitted one of five projects selected for funding under this BAA, “Complete Trips Empowered by Data Standards: Accessible Mapping Standards and Data Collaboration Drive Accessible Multimodal Mobility” (referred to as the “Transportation Data Equity Initiative, TDEI, or the UW ITS4US Project”).

The UW ITS4US Deployment Project aims to create the foundational data tools necessary for both public and private entities to collect, share, manage, and use transportation data that provide equitable outcomes to all travelers. At its core, the project is about creating the foundational requirements for interoperable transportation data sharing that fulfills the informational needs of all travelers, allowing them to discover and use diverse travel options that meet their specific needs. The UW ITS4US project itself consists of multiple parts.

- First, it includes work with three existing standards committees to extend and update existing, early-stage international data standards: OpenSidewalks, GTFS-Flex, and GTFS-Pathways. These three data standards enable the consistent collection and reporting of data that provide the underlying information needed by the currently underserved target populations— people with disabilities, older adults, and individuals with low income—to efficiently travel.
- Second, it is developing a series of tools that help agencies, jurisdictions, and other stakeholders collect the data that can be stored with these refined data standards. These tools are needed to lower the cost and improve the quality and consistency of those data collection efforts to increase the availability of the data.
- Third, it is developing tools, policies, and procedures that allow sharing and governance of the collected data. The tasks performed will enable effective and efficient vetting, aggregation, management, and fusion of the data that participating agencies, jurisdictions, and other stakeholders collect. This portion of the project will also include tasks required to enable and

manage the sharing of those data with application developers that write software to deliver requested travel information.

- Fourth, it is developing a data repository to contain the data to be shared within the six counties that represent the geographic boundaries for this ITS4US project. The data repository will be developed to illustrate how these data can be collected, stored, governed, updated, and maintained over time and then served upon request to application developers.
- Finally, the project is developing three example applications that use the collected data. The three applications are intended to demonstrate three very different uses of the data that are made available to application developers as a result of the other four aspects of this project. Those data can be used to fulfill a variety of information needs, and those needs can be met through an almost infinite number of applications. The three applications deployed as part of this project are meant to show other application developers how the newly available data can be obtained and delivered.

Figure 1 illustrates the overall “new mobility” ecosystem to which the UW’s ITS4US project is contributing. The outer circle consists of the variety of public transportation services that exist, such as fixed route transit services, micro-mobility services, and taxi services. Many of these services already generate data that can be readily obtained by applications via internet connections. The UW ITS4US project will help add the data sources that are particularly important to people with mobility disabilities, shown in purple at the bottom of the image. These are data that describe pedestrian pathways, transit station infrastructure. on-demand paratransit and community transit services, and other on-demand shared ride modes. The UW ITS4US project is also building the interoperable integrated transportation data sharing layer and application programming interfaces (APIs) shown in the green inner circle. This is the functionality needed to collect, fuse, and aggregate the data from disparate transportation services. Finally, the UW ITS4US project will demonstrate a small number of applications used by the travelers shown in the center of the diagram. The applications will take requests for information from the travelers, extract the required data from the data sharing layer (green circle), perform any required tasks (such as computing navigation directions) and deliver information to users in formats (audio, text, tactile displays) designed to meet their needs.

The project will achieve three primary goals:

1. **Coordinate Collaborative Releases of Data Standards**—Through community leadership, this project will co-create, improve, and extend data formats that describe currently under- or un-represented, detailed travel network information about the following:
   - The pedestrian-built environment (sidewalks and footpaths), through the OpenSidewalks data standard.
   - Transportation stations and hubs, through the General Transit Feed Specification Pathways (GTFS-Pathways) data standard.
   - Demand responsive travel services through the GTFS-Flex data standard (excluding real-time feeds).

   Phase 1 will include working with the various standards committees to ensure that changes made to those standards support the needs of travelers with disabilities and other mobility constraints, and specifically their need to identify paths and transit services that they can use. These changes will include the addition of new variables to the standards and the definitions for how those variables are coded.

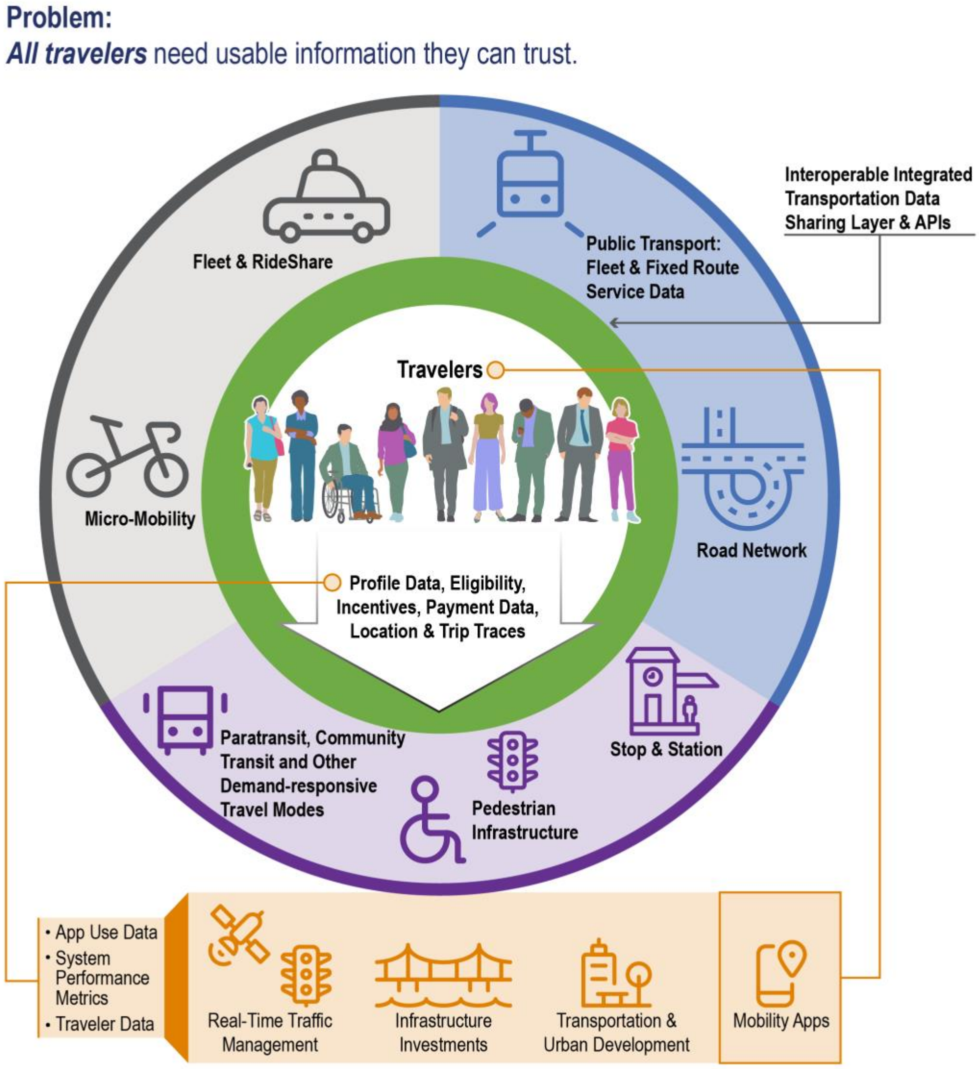
Problem:
All travelers need usable information they can trust.
Fleet & RideShare
Public Transport: Fleet & Fixed Route Service Data
Interoperable Integrated Transportation Data Sharing Layer & APIs
Travelers
Micro-Mobility
Road Network
Profile Data, Eligibility, Incentives, Payment Data, Location & Trip Traces
Stop & Station
Paratransit, Community Transit and Other Demand-responsive Travel Modes
Pedestrian Infrastructure
• App Use Data
• System Performance Metrics
• Traveler Data
Real-Time Traffic Management
Infrastructure Investments
Transportation & Urban Development
Mobility Apps

Figure 1: Diagram. UW ITS4US project's ecosystem

Source: University of Washington.

2. **Publish and Maintain Interoperable Data Infrastructure**—During Phase 2, the UW team will build, refine, and use data collection and data vetting techniques to generate data for all three data standards, as well as develop data provisioning services that distribute those data for use in a variety of applications. Much of the Concept of Operations will be devoted to the needs associated with these tasks. By the end of Phase 2, the UW team will publish collected data for the six U.S. counties that are part of this project. Those data will be maintained for five years after the conclusion of Phase 3 of this project, thereby supporting the interest of the team and any third-party applications in consuming the data. The six counties, as shown in **Figure 2**, are King and Snohomish

counties in Washington state, Multnomah and Columbia counties in Oregon, and Harford and Baltimore counties in Maryland.

Data availability will depend on the cooperation of multiple agencies in those counties. This will be part of the outreach effort of the UW ITS4US project, but the results of that outreach effort are unknown at this time. GTFS-Pathways data will be demonstrated at transit centers in the three states. The exact number and locations of the transit centers will be a function of the comfort level of the transit agencies that will ultimately be responsible for maintaining the data and the overall cost of the data collection process.

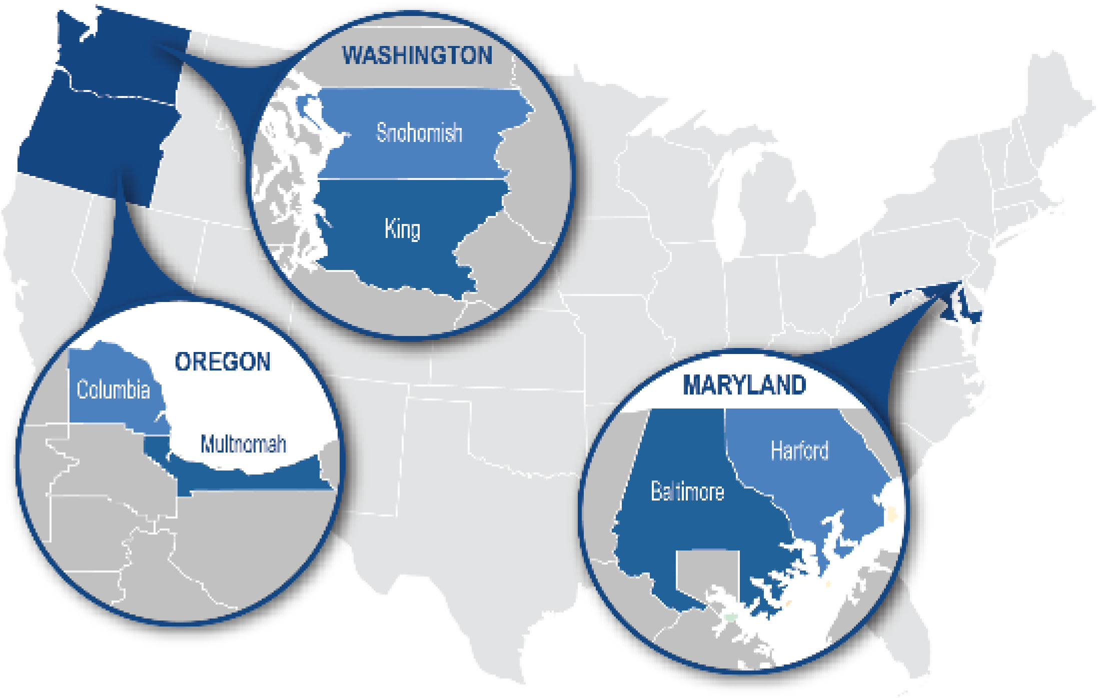

Figure 2. Map. Washington, Oregon, and Maryland counties.

Source: United States Department of Transportation, University of Washington, and Cambridge Systematics.

3. **Deploy and Sustain Three Accessible Mobility Applications**—This project will deploy three accessible mobility applications to evaluate and test the usability and efficacy of the data standards developed in Phase 1 and the supporting infrastructure developed in Phase 2. The mobility applications will close information gaps for three very different populations and will address demonstrably different travel goals:
    a. Multimodal AccessMap (by the Taskar Center for Accessible Technology)—a comprehensive, multimodal, personalized routing and trip planning Web and mobile application addressing the needs of people with mobility limitations, particularly supporting travel and exploration through new environments.
    b. Soundscape (by Microsoft)—a specialized orientation and exploration mobility iOS application enabling blind, vision disabled, or deafblind travelers to spontaneously travel and explore new pedestrian environments without having to specify a destination.

c. Digital Twin (by Unity Technologies) —a simulation tool that allows travelers (specifically sighted older adults and multilingual, multicultural travelers) to explore and visualize a trip path through a transit station that they need to use prior to taking a trip.

Figure 3 presents a conceptual framework for the project's vision. It illustrates the use of the data and data standards proposed for this project. It shows how data that need to be part of the transportation routing decision will come from multiple sources, including transit agencies, other governmental agencies, the private sector, and crowdsourcing. The data will be obtained in a consistent fashion by aggregators and supplied to applications that interact with end users. In this vision, the aggregators will collect non-personally identifiable information (PII), and the applications will maintain all the PII necessary to personalize the selection, presentation, and delivery of travel options. This framework represents the entire vision of a proposed system, including hardware, software, and services provided by both the UW team and the partnering application developers. In the context of the ITS4US Program, the framework can be subdivided into several different efforts, which are discussed in greater detail in Section 5 of the Concept of Operations report for the project.[2] These include the following:

- Components that the UW team will directly develop and test, which primarily include the data validation, storage, and services technologies that are the focal point of this project.
- Components that the UW team will assist in developing, which include tool sets to be used by data providers and data generators that support the collection and submission of data.
- Software demonstrations that use the data generated in (2) and made available in (1). These demonstrations will be designed to illustrate the success of the pipelines in (1) and will comprise three applications that will provide services needed by underserved end users.
- A co-Design effort with project stakeholders to develop and implement the policies and institutional relationships needed to scale and sustain the technology ecosystem being developed. The co-Design effort will apply to all technical components constructed directly or indirectly by the project team.

[2] Phase 1 Concept of Operations (ConOps), University of Washington ITS4US Deployment Project, Final Report—June 28, 2021, Report number FHWA-JPO-21-861.

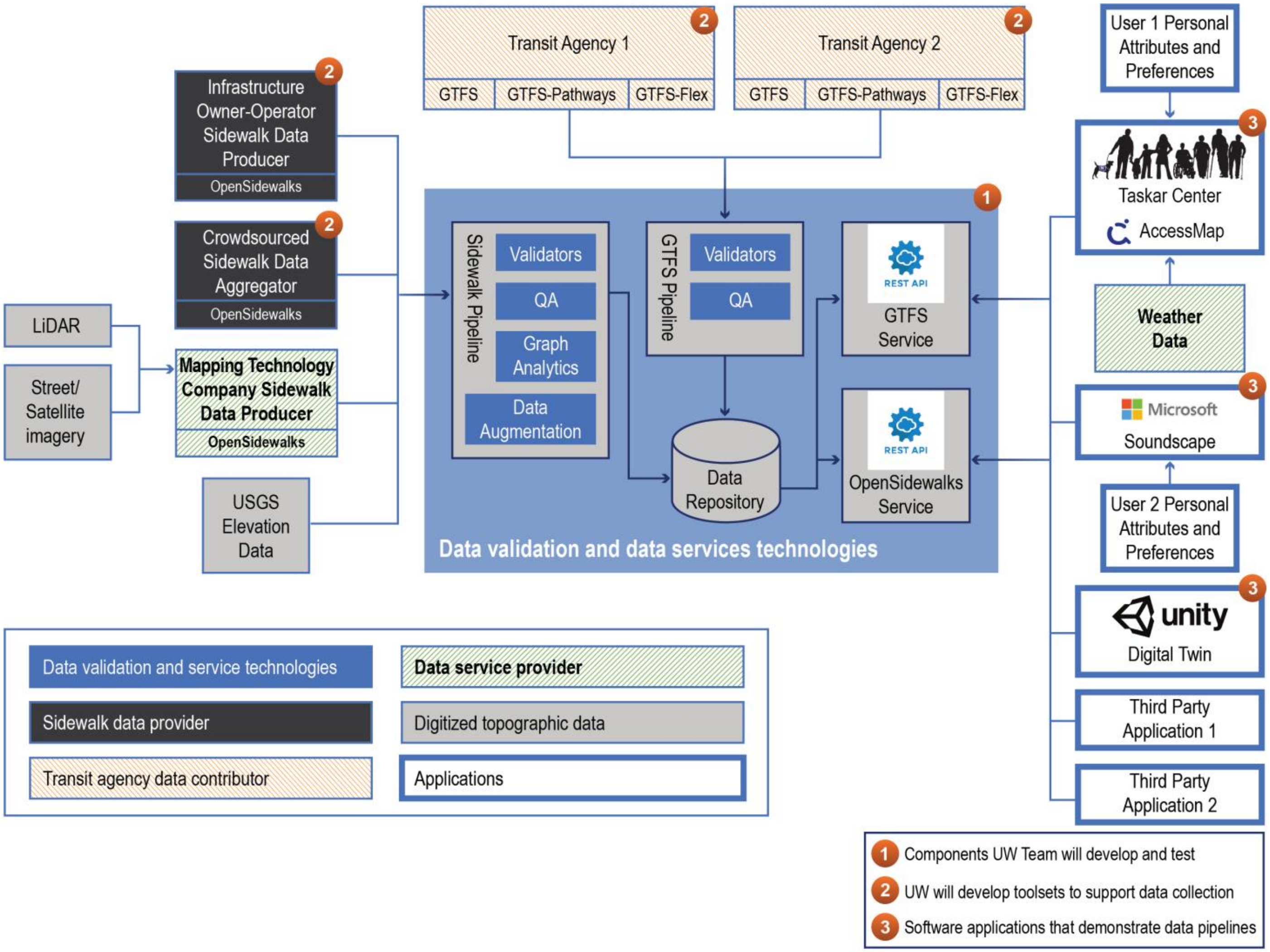
Transit Agency 1
2
GTFS
GTFS-Pathways
GTFS-Flex
Transit Agency 2
2
GTFS
GTFS-Pathways
GTFS-Flex
User 1 Personal Attributes and Preferences
Infrastructure Owner-Operator Sidewalk Data Producer
OpenSidewalks
2
Crowdsourced Sidewalk Data Aggregator
OpenSidewalks
2
LiDAR
Street/ Satellite imagery
Mapping Technology Company Sidewalk Data Producer
OpenSidewalks
USGS Elevation Data
1
Sidewalk Pipeline
Validators
QA
Graph Analytics
Data Augmentation
GTFS Pipeline
Validators
QA
REST API
GTFS Service
Data Repository
REST API
OpenSidewalks Service
Data validation and data services technologies
3
Taskar Center
AccessMap
Weather Data
3
Microsoft
Soundscape
User 2 Personal Attributes and Preferences
3
unity
Digital Twin
Third Party Application 1
Third Party Application 2
Data validation and service technologies
Data service provider
Sidewalk data provider
Digitized topographic data
Transit agency data contributor
Applications
1 Components UW Team will develop and test
2 UW will develop toolsets to support data collection
3 Software applications that demonstrate data pipelines

Figure 3. Diagram. Conceptual framework for the proposed data services.

Source: University of Washington and Cambridge Systematics.

The main stakeholders to be involved in the design, development, and operation of the proposed system include the UW, City of Bellevue, Unity Technologies, Google Inc., Microsoft Inc., Mapillary (now a subsidiary of Facebook Inc.), Washington State Department of Transportation (DOT), Oregon DOT, and Maryland DOT. The stakeholders' roles and responsibilities in the current system are described in more detail in the Concept of Operations report[3] for this project.

The main user groups that will interact with the proposed system include the following:

- Data generators (e.g., municipal infrastructure –owner/operators, private sector pedestrian-built-environment owner/operators, crowdsourced sidewalk reporters, elevation data providers).
- Transportation service providers (e.g., transit agencies and the companies that support the delivery of transit services operated by or for those transit agencies).
- Data service providers (e.g., mapping services, weather data providers).
- Application developers (e.g., AccessMap developers, Soundscape developers, Digital Twin developers, third-party application developers).
- Digital device end users (e.g., travelers with sidewalk preferences; blind, vision disabled, or deafblind travelers; sighted older adults; multilingual or multicultural travelers; low-income transit users; and rural transit users).

These main user groups are referenced in Chapter 2, which discusses how safety tasks are divided among different stakeholder groups participating in the project.

1.3 References

The following is a list of supporting documents used in the development of the plan and safety management.

- Accessible Transportation Technologies Research Initiative (ATTRI) Performance Metrics and Evaluation, Final Evaluation Framework Report, FHWA-JPO-20-784, https://rosap.ntl.bts.gov/view/dot/50748/.
- Bolten, Nicholas, Amirhossein Amini, Yun Hao, Vaishnavi Ravichandran, Andre Stephens, and Anat Caspi. "Urban sidewalks: visualization and routing for individuals with limited mobility." First International Workshop on Smart Cities and Urban Analytics (UrbanGIS). Seattle, WA: 2015.
- Bolten, Nicholas, Veronika Sipeeva, Sumit Mukherjee, Anissa Tanweer and Anat Caspi. A pedestrian-centered routing approach for equitable access to the built environment. 2017. IBM J. RES. & DEV. VOL. 61 NO. 6:10 [November/December 2017] 10.1147/JRD.2017.2736279.

[3] Ibid.

- Bolten, Nicholas and Anat Caspi. "Towards routine, city-scale accessibility metrics: Graph theoretic interpretations of pedestrian access using personalized pedestrian network analysis." PLoS one 16.3 (2021): e0248399.
- Caspi, Anat, et. al., Phase 1 Concept of Operations (ConOps), University of Washington ITS4US Deployment Project, Final Report—June 28, 2021, Report number FHWA-JPO-21-861.
- Caspi, Anat, et. al., Phase 1: Project Management Plan (PMP), University of Washington ITS4US Deployment Project, May 6, 2021.
- FHWA. University of Washington ITS4US Deployment Project—Phase 1 Needs Summary. Final Report—May 3, 2021.
- FHWA. Accessible Transportation Technologies Research Initiative (ATTRI)—User Needs Assessment: Stakeholder Engagement Report. Final Report—May 2016. FHWA-JPO-16-354.
- FHWA. Accessible Transportation Technologies Research Initiative (ATTRI) Policy and Impacts Assessment—Policy Assessment, Gaps & Needs. Final Report—July 2019. FHWA-JPO-17-506.
- GTFS-Flex document (ongoing), http://bit.ly/gtfs-flex-v2.
- GTFS-Flex GitHub site, https://github.com/MobilityData/gtfs-flex.
- GTFS-Pathways document (ongoing), http://bit.ly/gtfs-pathways.
- GTFS-Pathways GitHub site, https://github.com/google/transit/pulls?q=is%3Apr+pathways.
- (GTiO) Data Interoperability: A Practitioner's Guide to Joining Up Data in the Development Sector. https://www.data4sdgs.org/sites/default/files/services_files/Interoperability%20-%20A%20practitioner%E2%80%99s%20guide%20to%20joining-up%20data%20in%20the%20development%20sector.pdf, accessed 4/13/2021.
- National Academies of Sciences, Engineering, and Medicine 2020. *Development of Transactional Data Specifications for Demand-Responsive Transportation*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25800.
- Needs expressed by MVTransit: How data science is driving digital transformation at MV Transportation. https://www.dxc.technology/workplace_and_mobility/insights/148131-how_data_science_is_driving_digital_transformation_at_mv_transportation.
- OpenSidewalks website, https://tcat.cs.washington.edu/opensidewalks-2/.
- OpenSidewalks GitHub site, https://github.com/OpenSidewalks/OpenSidewalks-Schema.
- Tanweer, Anissa, Margaret Drouhard, Brittany Fiore-Gartland, Nicholas Bolten, Jess Hamilton, Kaicheng Tan, and Anat Caspi. Mapping for Accessibility: A case study of ethics in data science for social good. Bloomberg Data for Good Exchange Conference. 24-Sep-2017, New York City, NY, USA.
- Transportation Data Equity Initiative website, https://transitequity.cs.washington.edu/.
- Trapeze Group (2021). Esri and Trapeze collaborating on integrated data platform. Mass Transit Magazine (4/1/2021).

2 Safety Overview and Relationships

This Safety Management Plan was developed in accordance with guidance provided by the USDOT and follows five steps.

- Identify safety stakeholders and their relationships with the project.
- Identify safety scenarios at both the system and application levels as defined in the ConOps.
- Identify the safety needs derived from the ConOps scenarios.
- Assess the levels of safety risk associated with the deployment.
- Develop a safety operational concept for each scenario that identifies a potential medium or high-risk event.

The outcomes from these risk analyses will then be carried into multiple other project planning tasks, as illustrated in Figure 4.

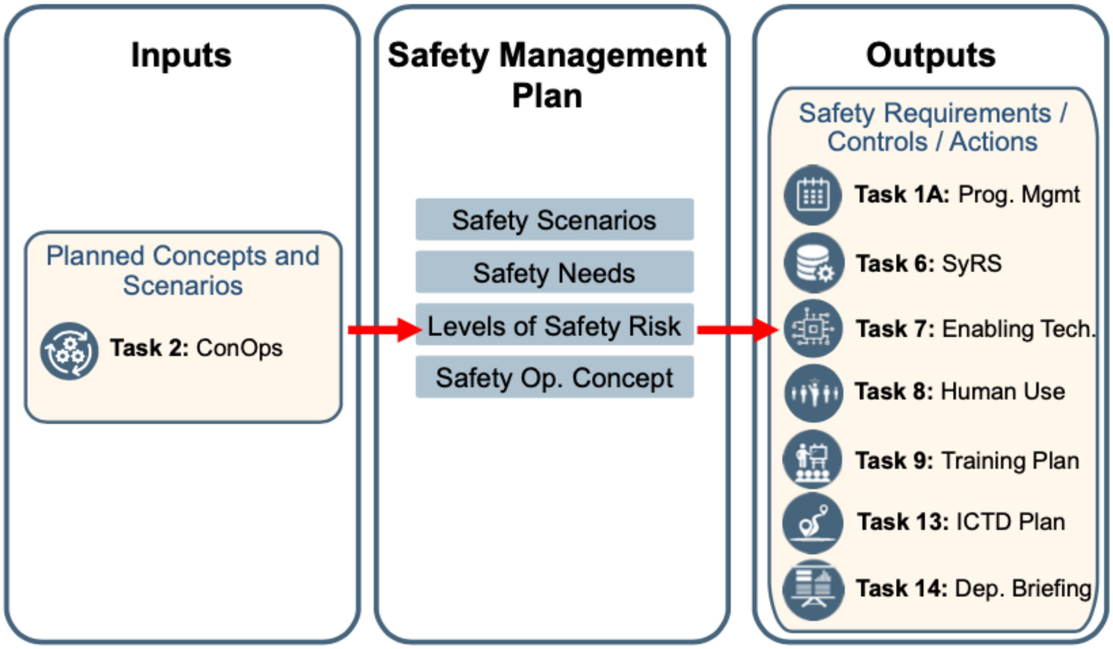

Figure 4: Safety Management Plan interdependencies

Within this project, safety responsibilities sit with all participants in the data and application supply chain. The project team has responsibility for designing the data standards to include the data needed for people to determine what paths are best for themselves (including incorporating in that route selection their own personal trade-offs between safety and efficiency.) This includes, to the extent possible, where hazards are located. Accurate data that informs user's information needs helps improve/ensure safety.

To accomplish this goal, the project team is involving stakeholders in a co-design process to identify what data are required. The project team must then determine whether those data can physically be collected, and how to collect those data which can be collected. When data needed by stakeholders are not available, the data service needs to clearly indicate when data are missing. This alerts data users to these data gaps and allows them to make travel decisions with full knowledge of the lack of data, again improving safety outcomes by removing uncertainty.

The project team is also responsible for maintaining the data services in a way that keeps the data collected secure and available to applications used by end users. Data generators have responsibility for collecting accurate data (because inaccurate data could cause a hazard), and for working with others to vet their data, improving the available data whenever errors are discovered by the vetting process. Finally, application developers are responsible for safe and reliable delivery of the data to users in ways that meet user needs.

Note that many of the tasks required to maintain traveler safety through the collection and provision of data needed to travel more safely are dealt with more directly in the data management plan, and are not discussed in detail in this Safety Management Plan. This document discusses the project's overall approach to safety, explains how risks are being identified, and how those risks are being addressed and mitigated.

2.1 Related Project Tasks

This Safety Management Plan is a key portion of the overall project planning for the TDEI. Its design is primarily influenced by the Concept of Operations document, and it in turn significantly influences the multiple other planning documents described below.

1. Task 1 – Project Management.

The Project Management Plan lays out the project's overall program structure; project partners and participants; deliverables; related management plans and procedures; and the methods used to plan, monitor, control, and improve the project development efforts. As a result, it lays out the basic approach to safety management. That approach is defined in detail in this document.

2. Task 2 – Concept of Operations

The Concept of Operations document provides an overview of the users and stakeholders of the planned system, the functional tasks associated with the system being developed and deployed, the support environment required for those functions, the modes of operation for the system, and the system's required operational policies and constraints. Much of the Concept of Operations is devoted to resolving the needs identified for the five groups of stakeholders described in Section 1.2.

The ConOps also describes a variety of different operational scenarios for the system and describes the functional tasks that need to occur for those scenarios to unfold as desired. These scenarios and the functionality of the system described in the ConOps serve as the basis for the Safety Management Plan. They allow the project team to identify the safety needs associated with the project for the identified system users, determine the level of risk associated with each need, and develop systems and processes that will mitigate those risks.

Outcomes from the safety management planning activities and the technical work that flows from the Safety Management Plan will be used to update the ConOps as the project continues and will flow into other tasks as noted below.

3. Task 3 – Data Management Plan

The Safety Management Plan includes the need to collect data that measure the occurrence of and response to safety events and the precursors to potential safety events. The Data Management Plan (DMP) defines the data collection, storage, and processing of those data which result in safer travel. The DMP ensures that the data being collected and published are handled in ways that ensure that the travel safety goals of the project are met to the highest degree possible, that errors in the data are identified and fixed, and that the data are stored in a secure manner and correctly retrieved and published in ways which maintain their integrity, thus ensuring both maximum possible traveler safety and ensuring that those data are available for use in system performance measurement and safety management activities.

4. Task 5 – Performance Management and Evaluation Plan

The Performance Management and Evaluation Plan (PMEP) includes discussions of the UW team's plans for measuring and reporting on both safety events, and the precursor events that can lead to hazardous outcomes for travelers. These events and the data collected to measure and report on them are discussed later in this document.

5. Task 6 – Deployment System Requirements

The safety needs, risks, and risk mitigation strategies identified in this Safety Management Plan will flow into the System Requirements Plan. They will add detail to the information included in the ConOps that needs to be addressed in the Systems Requirements document.

That information includes not only human factors safety needs (e.g., how to limit potential harmful events from happening to people who are using applications built as part of this project), but also maintenance of overall system security, maintenance of the quality of the data collected and stored within the project databases, to ensure that incorrect or invalid data do not cause harm, ensuring the privacy of the individuals who use the applications constructed as part of this project, and identification of how specific safety threats need to be identified and mitigated by the developed systems.

6. Task 7 – Enabling Technology Readiness Assessment

The Enabling Technology Readiness Assessment will use input from the Safety Management Plan to identify where potential safety issues can occur if enabling technologies do not perform at the level required. Understanding these safety areas will allow the project team to develop both performance tests and performance standards for those tests that can be used to determine the current level of readiness for enabling technologies needed by the project.

7. Task 8 – Human Use Approval

Similarly, the risks identified from this Safety Management Plan will serve as inputs to the documentation developed and submitted to obtain Human Use Approval (i.e., Institutional Review Board or IRB approval). The Safety Management Plan identifies the risks associated with the project and how the project team will address, mitigate, and avoid those risks. These will be key inputs to the IRB submittal. They include the procedures for protecting the privacy and confidentiality of the participants (e.g., how, where, and for how long the data will be stored; who will have access to the data; and other confidentiality issues).

8. Task 9 – Participant Training and Stakeholder Education Plan

Similarly, the outcomes from this Safety Management Plan will assist in the development of training and education materials to be used by 1) agency staff and consultants who collect data to be used by the system, 2) agencies and companies writing applications that use the data collected and shared as part of this project, and 3) users of the applications built as part of this project to demonstrate the use of the data. This plan will identify specific subject areas that need to be addressed in the training and educational materials to both minimize the occurrence of identified risks and maximize the quality of the responses to those risks.

9. Task 13 – Integrated Complete Trip Deployment Plan

The Integrated Complete Trip Deployment Plan (ICTDP) will build upon multiple Phase 1 tasks. From the Safety Management Plan, the ICTDP will gain insight into specific risks that are of concern as part of the deployment, as well as the actions that must be taken to avoid and mitigate those risks, as described in the risk response plan. These include understanding the risks associated with the publication of invalid data, failures in the developed software, failures in the technology used by the end users to access those data, and failures in communication with those users.

Incorporating the SMP into the ICTDP will result in deployment schedules and acceptance testing to ensure that when the system becomes active, safety risks are identified, minimized, and responded to and are mitigated to the degree possible. The ICTDP will also incorporate the data collection, data sharing, and performance measurement activities needed to measure and report on the occurrence of risk events, how they are responded to, and the outcomes within the testing and operational phases of the project.

10. Task 14 – Deployment Readiness Summary Briefing

Key safety concerns identified in this plan will be highlighted in the Deployment Readiness Briefing, along with the activities undertaken to prevent those risk events from occurring, how safety events will be identified and recorded if they do occur, and how the system will respond to mitigate the potential harms.

2.2 Safety Stakeholders

Numerous stakeholders in the project will be involved with safety-related planning and management. First, within the UW project team, roles will include safety management for the portion of the project for which they are responsible. We will define a data oversight role, a data infrastructure oversight role, a cybersecurity oversight role, and a role that continuously reviews and responds to the interests of data producers, consumers, and travelers as part of the co-design process. One individual will be tasked with interacting with 3rd party application developers to highlight best practices for improving safety when using TDEI data. This will occur each time new firms or agencies sign up to access the data. Note that because the data being published are publicly available, this project can only interact with 3rd party developers to instruct them on best practices in the use and delivery of data for ensuring the safety of their application’s users. We cannot place terms and conditions on the use of those data with respect to how those applications deliver that data to their users.

The individuals listed in the paragraph above have not yet been named. These roles will be assigned to individuals working on the UW Team during Phase 2 as the software system required to store and data is constructed and the operations plan for the system is developed, tested, refined, and finalized.

In addition to the direct UW project team roles, we will engage project participants in the safety management process. This will be accomplished by creating feedback mechanisms designed to 1) continuously improve the quality of the published data – lowering the potential risk from publication of invalid data, and 2) identify vulnerabilities in the system, so they can be addressed before they create hazards.

To accomplish this, we will request feedback from data producers and consumers, such as local DOT staff in the jurisdictions where deployment is planned, and from application developers with specific safety considerations.

As noted in Section 1.1, the project team has stratified stakeholders into five specific groups:

- Data generators (DG)
- Transportation service providers (TS)
- Data service providers (DS)
- Application developers (AD), and
- Digital device end users (DU).

For safety management, one additional group has been added to our list of stakeholders, **experts on accessibility**. These are individuals who have training and experience in the analysis of mobility for vulnerable travelers and can therefore help the project team identify threats to the safety of those users as they travel. This group of experts includes some digital device users and caregivers who have lived experience supporting vulnerable travelers and have been working with the UW Team already within the DU category of stakeholders. Table 1 describes the overall list of safety stakeholders. The majority of the five groups of stakeholders identified in the ConOps will fall in the category of providing data producer/consumer feedback. The safety management tasks they will perform are shown in Table 2. Experts on accessibility, along with individuals with lived experience, will perform the safety management tasks shown in Table 3. (Note that specific individuals are not currently named in Table 1, as this project is still in the planning stage.)

Table 1. Safety management stakeholders list

Role	Organization	Expertise	Safety Management Role
DG	Cities, counties, state highway agencies,	Sidewalk data generation	Sidewalk data vetting and data accuracy, Sidewalk data improvement
DG	Consultants hired by sidewalk owners	Sidewalk data generation	Sidewalk data vetting and data accuracy
DG	Pedestrian advocacy groups	Sidewalk data generation	Sidewalk data vetting and data accuracy
DG	Community / neighborhood groups	Sidewalk data generation	Sidewalk data vetting and data accuracy

Role	Organization	Expertise	Safety Management Role
DG	ADA transit service providers	Sidewalk data generation	Sidewalk data vetting and data accuracy, sidewalk data improvement
DG	Private sector pedestrian-built-environment owner/operators	Sidewalk data generation	Sidewalk data vetting and data accuracy, sidewalk data improvement
TS	Transit facility owners	Transit facility data generation	GTFS-pathways data vetting, GTFS-Pathways data improvement
TS	Consultants hired by transit facility owners	Transit facility data generation	GTFS-pathways data vetting
TS	Transit service providers	On-demand transit service data generation	GTFS-Flex and GOFS data vetting, and GTFS-Flex and GOFS data improvement
TS	Consultants hired by transit service providers	On-demand transit service data generation	GTFS-Flex and GOFS data vetting
DS	Private mapping service companies	Data aggregation, data vetting, data service provision	Data vetting, data service operational stability, data security, privacy protection
DS	University of Washington	Data aggregation, data vetting, data service provision	Data vetting, data service operational stability, data security, privacy protection
DS	OpenStreetMap Foundation	Data storage and data service provision	Data service operational stability, data security
DS	Federal data service providers (and their contractors)	External data sources (e.g., elevation data, weather data, etc.)	Data service operational stability, data security
AD	University of Washington	AccessMap	Application stability, failure planning, failure identification, failure recovery
AD	Microsoft	Soundscape	Application stability, failure planning, failure identification, failure recovery, assistance provision
AD	Unity Technologies	Digital Twin	Application stability, failure planning, failure identification, failure recovery, assistance provision
AD	Private sector application developers	Application development	Application stability, failure planning, failure identification, failure recovery, assistance provision operation
AD	Public sector organizations	Application development	Application stability, failure planning, failure identification, failure recovery, assistance provision
AD	Consulting firms hired by public sector organizations	Application development	Application stability, failure planning, failure identification, failure recovery, assistance provision

Role	Organization	Expertise	Safety Management Role
DU	Individual travelers	Lived experience	Failure identification, request for assistance, feedback to data service providers
DU	Caregivers	Lived experience assisting others with mobility needs	Support of travelers with mobility needs, failure identification, request for assistance, feedback to data service providers s
_	Accessibility experts	Experience assisting others with mobility needs	(See Table 3)

Table 2: Safety management tasks that will require data producer/consumer feedback

Identify and classify sensitive deployment assets
Identify and analyze electronic security entry points
Perform a system vulnerability assessment
Assess the risk of system breach and information
Consider producer/consumer missions, environments, culture, and budgets
Monitor and assess the effectiveness of the controls

Individuals with specific lived experience, expertise, and understanding of safety relating to underserved communities (e.g., understanding of accessibility needs and considerations) will be considered for supporting feedback and validation activities, including the safety management tasks shown in Table 3.

Table 3: Safety management and project operations that will require expert accessibility feedback

Clear system definition
Identify and analyze traveler safety model
Perform a traveler vulnerability assessment
Assess the risk of system breach and information
Monitor and assess the effectiveness of the controls

2.3 Safety Risk Process and Approach

A summary of the UW team's approach to limiting risks and improving the safety of the project's data and application users is presented below. The UW team has been performing many of these tasks for several years as part of its continuing co-design process, and will continue to work with the following:

- Individuals with lived experience are participating in the co-design process to identify hazards they experience when traveling on sidewalks, on pathways, through transit centers, and when using on-demand transit so these hazards can be addressed in the data collected and made available for navigation routing.
- Individuals with lived experience and agencies that own, maintain, and operate transportation infrastructure and on-demand services are participating in the co-design process to identify data that identify those hazards so that they can be avoided or mitigated.
- Agencies that own, maintain, and operate transportation infrastructure and on-demand services are participating in the co-design process to determine how data can be collected and codified in objectively measured units that can be stored, published, and shared with travelers in a variety of formats (e.g., audio, text, tactile.) This ensures that subjective descriptions of services or infrastructure are not published because many subjective assessments do not provide correct information to many users when those users have different requirements than assumed when making the subjective assessment.
- Public agencies, data service providers, and application developers are participating in the co-design process to suggest ways enhance existing data standards so they can incorporate those data, which ensures that all key data items needed for safe user travel are incorporated in the refined data schema.
- Agencies and developers are participating in the co-design process to develop tools and procedures to collect those data, so that the data identified above are readily collected and published, making them accessible to users, and thus improving their safety.
- Data service providers and application developers are participating in the co-design process to determine how to protect and secure the data pipelines used to collect and share those data.
- Application developers and individuals with lived experience are participating in the co-design process to develop, test, and deploy applications that obtain and deliver those data to end users through available digital device technologies, as these technologies are needed to deliver to travelers the currently missing information that is needed to ensure safe travel.

Table 4 summarizes the security and safety areas, best practices, and controls that this Safety Management Plan takes into consideration while the project team is performing the outlined activities. This table introduces the context for consideration and the tasks being performed as part of the UW team's approach to safety management. Later sections describe the planning and preparation that will be undertaken to offer continuous review and assessment for how consumers, producers and travelers interact with the system as those aspects of the TDEI come into place.

Table 4: Safety management tasks

Risk/Safety Area or Consideration	Rationale
1) Provide ongoing safety management	Active and visible support from a management position at each stage of planning, deployment, and monitoring of security efforts will be crucial to the success of this deployment project.
2) Assign responsibility for security risk management	Security risk mitigation is included in resource allocation decisions and an accountability matrix. Enforcement is the responsibility of a clearly defined project lead.
3) Devise clear system definitions	Careful system definition is essential to the accurate depiction and understanding of vulnerabilities and risks. Clear definition also leads to controls that provide adequate assurances of safety management.
4) Identify and classify sensitive deployment assets	It is important to understand the system assets and data that are being developed to understand the best protections for those assets, along with their classification (e.g., private traveler information, etc.). This is pertinent for making informed decisions about the appropriate controls needed to protect those assets, commensurate with risk severity and impact to data producers, consumers, and travelers.
5) Identify and analyze electronic security entry points	To build a system threat model, it is important to understand the potential entry points that an adversarial entity might use to interrupt any project asset or system functioning. The system threat model is an important component of safety management and assessment.
6) Identify and analyze traveler safety models	To build a traveler threat model, it is important to understand the potential travel failures that travelers may sustain at every link of the travel chain. The traveler threat models are important components of the data schema definition and management effort, but changes in the schema so that data exists to help protect users will not significantly change the hardware or software developed as part of the UW ITS4US project.

Risk/Safety Area or Consideration	Rationale
7) Perform system vulnerability assessments	Vulnerability checks performed as part of the Safety Management Plan provide a realistic assessment of the weaknesses in existing security controls.
8) Perform traveler vulnerability assessments	Vulnerability assessments provide for realistic periodic assessment of traveler threats to estimate the likelihood of failure and to prioritize remediation activities.
9) Assess risk to system breach and information	These risk assessments provide a information that combines the likelihood of a successful attack with its potential impact on the data producers' and consumers' mission and goals. This helps ensure that mitigation efforts developed by the team target the highest security risks and that the controls selected are appropriate and cost-effective for all the participating organizations.
10) Consider producer/consumer missions, environments, culture and budgets	This consideration provides for the appropriate management, operation, and technical controls across participating organizations that are needed to lower risk in the most cost-effective way possible. The team is identifying partnering organizations' missions, environments, culture and budgets to select and prioritize appropriate safety controls.
11) Monitor and assess the effectiveness of the controls	Effective testing and ongoing monitoring and evaluation provides a level of confidence that security controls adequately mitigate perceived risks.
12) Provide for data quality vetting and feedback, so that 3rd parties can contribute to data quality and accuracy	Data quality and accuracy are the primary method for improving safety in this project. Providing functional 3rd party vetting and data quality feedback procedures both improve data quality and decrease the cost of that process to data generators.
13) Provide information on data provenance and the confidence level associated with data points	Data provenance and confidence levels (e.g., the age of data describing infrastructure conditions) give travelers insight into the degree of trust they place on information they are being provided, improving their ability to travel with confidence and prepare for unexpected conditions, thus traveling safer.

2.4 Principles for Traveler Safety Management Implementation

The UW team will incorporate the four basic principles listed below to guide the design and implementation of all disability-inclusive safety management measures. These four principles are drawn from the principles outlined in the United Nations Convention on the Rights of Persons with Disabilities.[4]

2.4.1 Equality and non-discrimination

Emergency or safety management should be inclusive of all those in need, particularly those who are most vulnerable, such as people with disabilities. Discrimination on the basis of disability "means any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment or exercise, on an equal basis with others, of all human rights and fundamental freedoms. It includes all forms of discrimination, including denial of reasonable accommodation".

2.4.2 Accessibility

People with disabilities should have "access, on an equal basis as others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and rural areas." Having access to these data ensures that people with disabilities are able to travel safely because they understand the environment in which they are traveling and can select routes and paths that are safe for them.

2.4.3 Participation and dignity

People with disabilities have the right to participate in the assessment, design, implementation and monitoring of safety programs; make their own choices; and be recognized and respected as equal citizens and human beings with a contribution to make before, during and after an emergency.

2.4.4 Resourcefulness and capacity

Many people with disabilities have existing resources and capacities to make meaningful contributions to safety and risk management. They also have the right to receive support and assistance to develop the skills, knowledge, and capacities required to prepare and protect

[4] https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/guiding-principles-of-the-convention.html

themselves from hazards, and to maximize their ability for survival and recovery following an emergency or safety failure

3 Safety Needs and Scenarios

The ConOps for this project defines 14 operating scenarios. Those scenarios describe six basic functional components. Those components are summarized as follows for use in defining and describing the safety needs of the system:

- Collection of connected sidewalk infrastructure, on-demand transit services, and transit center pathways data.
- Transmission of the collected data to centralized data repositories.
- Quality assurance activities and feedback that supports those activities for all three data types.
- Operation of the centralized data repositories.
- Provision of those data by the central data repositories to applications that develop information for delivery by travelers.
- Use of that information by travelers.

The relationship between the operational scenarios defied in the Concept of Operations and these six functional areas which are used for safety analysis and management are shown in Appendix B.

3.1 Safety Needs and Response Activities by Project Component

The safety needs and response activities for each of the six functional categories are briefly presented in the following subsections, along with short descriptions of the types of management actions needed to reduce the risks of safety threats.

3.1.1 Data Collection

Two basic safety needs are associated with the data collection function. The first is the safety impact of inaccurate or incomplete data. That is, if the data reported to the central data repository are not accurate representations of the transportation infrastructure or transportation services, then the use of those invalid data could result in harm to those who use that invalid information. For example, an individual using a wheelchair might be sent down a steep sidewalk having been told that a curb ramp exists at the bottom of the slope. If that ramp description is not current, that individual might be trapped on that sidewalk at the base of a hill. The severity of that outcome is then a function to that individual's ability to summon help, or perhaps their ability to jump the curb. Similarly, if no data exists for that sidewalk, the wheelchair user has to make an uninformed decision about traveling on that sidewalk, risking that same outcome. However, if there is a curb ramp, and the alternative path is dangerous, the lack of information might also result in that user choosing the known danger over the unknown (but actually safer) option.

An important task for ensuring that the data are “complete” within this project will be the refinement and expansion of the three data standards (GTFS-Flex, GTFS-Pathways, and OpenSidewalks.) These data standards will need to incorporate the data necessary to safely route travelers with mobility disabilities. Therefore, one of the initial tasks of the project will be to work with stakeholders to expand the current standards to include data fields that will ensure that the collected data will help route individuals safely and successfully. These results will be documented as part of the data standards acceptance process. This is just part of the project’s continuing stakeholder involvement and co-design efforts. As a result, the core safety needs for the data collection activities will be the collection of complete and accurate data, as well as the ability to adequately describe when data are missing or when the level of confidence in the data’s provenance is low. These outcomes too will be documented in the meta data for the accepted data standards. If the co-design process identifies further changes in data standards are required, these revisions will also be documented as part of the revision process for data standards.

The second major safety need relates to the individuals generating the data. Many of the data will be generated in an office setting using software that derives data from previously collected datasets. In an office setting, there are no significant safety issues other than the data accuracy concerns mentioned above. However, in some cases, data collection will occur in the field, using tools and techniques developed and provided through this project. These field data collection techniques must be built and used in ways that ensure the safety of the collection staff, as well as the safety of the public interacting with those data collection activities. Therefore, the design and use of field data collection techniques for this project will need to account for the safety of staff performing those activities and the public traveling through areas where data are collected.

3.1.2 Data Transmission

Once data have been collected by an organization, they will need to be transmitted to the central databases that will vet, store, and serve them to multiple applications. The primary safety needs during this stage of the data collection process will reflect the accuracy, completeness, and security of the data.

The data being transmitted to the central database must come from approved sources and be vetted according to established rules and procedures. Developing the permissions, tasks, and procedures that ensure the safe and secure transmission of data and metadata will be the core management tasks required to secure the data for this component of the system and thereby contribute to the overall safety of system users.

3.1.3 Quality Assurance Activities

To further the data management task, data quality assurance activities will be required. For this safety management report, the quality assurance effort will be treated as a separate component of the system. In reality, quality assurance tasks will occur during both the data collection component and the data acceptance and vetting activities.

The safety need that drives these quality assurance activities is the same as mentioned earlier: the need for accurate, complete data. The UW team will develop a series of quality assurance activities capable of handling data quality changes over time. For example, transit services change, making previously vetted service descriptions invalid because they are out of date. Similarly, infrastructure condition both may degrade over time and may improve or change as a result of maintenance and construction activity. For example, during any given year, most cities add at least several new curb ramps. Sidewalk infrastructure descriptions need to be updated to account for these changes. Similarly, other roadway or land use changes may make some sidewalks unusable or relocated. Ideally these changes will be submitted by cities when the changes occur, but in many cases, these changes are identified by community groups tracking infrastructure conditions in their communities.

In this component, two major management activities will occur to improve and maintain the quality of the data and thus the safety of the data users. The first management activity will be the establishment of procedures for vetting data collected and submitted to the database. The vetting process will be designed to identify invalid data that have been reported. Vetting tools will include software that can identify invalid data entered into database fields (e.g., alpha characters entered into a text field, date and time entries that are not valid, or values that exceed allowable limits) and report data outliers, that will then be checked for accuracy. This project will also develop and deploy data vetting tools and procedures that will allow participating groups and organizations to compare submitted data with observations from the field, report observed discrepancies, and thus improve data quality over time.

The tools developed for vetting data and reporting errors in the database will be made available to organizations that have a recognized interest in improving the opportunity for active transportation in the U.S. These tools are also useful for providing feedback to the agencies when changes in infrastructure occur in the field but are not reported as changes within the database. Community vetting is an excellent way of maintaining data quality over time.

The second management activity will be the development and operation of two-directional communication channels between the central database and the organizations that “own” the facility or service being described with data. The two-directional communication will be designed to ensure that the “owners of the facility/service” are aware of changes in the data describing their services and either 1) agree with the change, or 2) can indicate why such a change is not correct. This two-directional data management feedback process was specifically requested by multiple stakeholders during the ConOps stakeholder meetings. While specific responsibilities for data quality are still being developed, in general, owners of specific infrastructure or services will have the primary responsibility for the quality of the data describing their systems and services. However, the OpenStreetMap model for community data provision allows trained, authorized volunteers to make map changes when facility owners are not able or willing to undertake such duties. This design of responsibilities is one of several models being considered to implementation and will be discussed as part of the co-design process with data generators and data providers as part of that process.

3.1.4 Central Database Operations

This component of the system involves the operation of the central database function used to provide the three types of data to appl ications that will interact with end users on their digital devices. <u>The safety needs for this component of the system are associated with the security of the central database and whether that database operates in a manner that meets the needs of the application developers that depend on it.</u>

Guarding the security of the database will start with the design and deployment of systems that ensure that the organizations that supply data are correctly identified, vetted, and interact with the database in a controlled and secure manner. These same tasks will be required for working with application developers that need to obtain data from the database. Those organizations will also need to be vetted, appropriately provided with permissions, and managed to ensure that their data requests occur in a controlled fashion.

The other major effort within this component will be to ensure that the overall safety, security, and performance of the central servers that ingest, store, and serve the data to external applications are not compromised. This aspect of the system will be associated with the overall health and security of the database system, the hardware on which it operates, and the software it uses. Management will assign key staff to routinely test and report on the ongoing performance of the central database system. These activities will include, for example, tests for memory usage, network latency, and runtime errors.

In addition, the UW team will run nightly checks for system intrusions and other cyber security issues, as well as ensure that the operating system and databases are kept up-to-date with the latest security patches.

Finally, the basic system design of the central database will include redundancy and encrypted data archiving to ensure the continued operation of the system if major failures of or attacks on the system occur. The UW team will assign responsibility to specific individuals to perform those tasks.

3.1.5 Application Interactions with the Central Database

The fifth category of components for the system includes the activities associated with serving data to applications that, in-turn, will interact directly with travelers and other end users. The safety needs for this functionality are similar to those described above for Data Transmission (Section 3.1.2) and Central Database Operations (3.1.4).

There are two basic safety needs. The first is to ensure that the process of requesting data results in the correct data being transmitted safely and securely to the requesting application. The second need is to ensure that the application developer understands the nuances of those data, so that the application will correctly interpret the data it receives and understand the limitations in those data.

Project management tasks similar to those described in Section 3.1.2 will meet the first of these needs, using the same organizational vetting and data security techniques previously discussed. These will be led by UW team members specifically tasked with these responsibilities.

To ensure that application developers understand the nuances of the data schema being used and thus use those data in ways that enhance traveler safety, the UW team will work with the national standards groups to ensure that appropriate meta data and strong examples are supplied along with the data standards themselves. This will also ensure that application developers are able to take advantage of the capabilities incorporated into the schema maximizing information delivery and thus traveler safety.

3.1.6 Traveler Use of Applications

The final component of the TDEI consists of the digital device-based, end user applications. Three of these will be demonstrated within this project. The primary goal of these applications is to demonstrate the wide range of uses of the data the TDEI project is generating. This section discusses potential risks – outside of the data quality discussed in 3.1.1 and 3.1.3 above, that application errors may generate. It also discusses the various ways those risks can be mitigated. Different applications will select different combinations of these mitigation approaches, depending on the specific target populations for those applications. The TDEI will promote these safety concepts but is not responsible for the design or operation of 3rd party applications.

One of those – Digital Twin – is intended only for use by individuals interested in previewing their trips through facilities. Because the application will be simply a digital simulation of station environments, little safety risk will be associated with that application. Any errors occurring within the application (e.g., communication failure, coding errors, or power failures during use of the Digital Twin), will not directly affect the safety of users, who will be preview that station pathway from a safe location, and application errors and failures, while annoying, will not create safety threats. The application will be tested in the lab to ensure that it is correctly routing users through the transit centers prior to release of the application.

However, both Microsoft's Soundscape and the UW's Multimodal Access Map are designed to be used while traveling. Therefore, errors or system failures that occur during such a trip will have the potential to place a user in a hazardous situation. While the data standards delivered for this project will not include "real-time" updates (e.g., the current operating status for elevators and escalators will not be reported), both applications are designed to provide information such as turn-by-turn directions that will require real-time knowledge of the traveler's current location.

For both of these applications, if the user expects location-specific navigation directions, and the central data system either fails to provide information (e.g., because of a power failure in the application or a communications failure between the application and the central data repository) or delivers incorrect information (e.g., because the application has an incorrect location for the traveler or delivers invalid data because the central database is inaccurate), then the user may be placed in a hazardous situation. Examples of this latter situation may include telling the traveler that a sidewalk or path has specific features, when that is not the case, or that an on-demand transit service will stop at a specific location at a given time when that is not the case, as the traveler may miss an appointment (because they miss their transit ride) or even become stranded because that transit ride was the only ride available. Steps for identifying and addressing data errors are discussed above in sections 3.1.1 and 3.1.3. Steps for addressing the safety implications of application errors are discussed below.

In the above examples, the traveler could be left without useful navigation directions and in need of assistance. Mitigation for these outcomes (in addition to the efforts already described above to improve the quality of the data contained in the central database) will take several forms in the demonstration applications, including the following:

- Helping the traveler identify when errors have occurred,
- Providing easily accessed "help" functions that allow users to quickly obtain information about how to safely navigate from their current location,
- Providing insight into transit service capabilities and training to help travelers avoid potential hazardous outcomes,
- Providing information about data provenance to help travelers pre-determine locations of potential hazards due to known data limitations so that travelers can avoid them or prepare for them.

These functions are currently present in many vehicle navigation applications. For example, the ubiquitous “recalculating” voice indicates both that a traveler is off-route and that the navigation application is updating its navigation plan. This is an excellent example of the application identifying that an “error” has occurred and then proactively providing assistance. This same basic functionality will be needed for hazard mitigation for travelers with mobility limitations. However, because the travel activities will be more complex, especially for on-demand transit services, the “help” function itself will be more complex.

Where possible, the “help function” may consist of providing the ability to easily make a phone call to someone who can provide assistance to the traveler. While this feature can be deployed in a variety of ways, for Multi-Modal AccessMap, the planned feature is to allow the user to enter their own “help phone number” into their profile, allowing each user to personalize this feature. Multi-Modal AccessMap will also have an option for recalculating navigation paths on demand, providing new routes when the initial route is determined to no be unacceptable. 3rd party applications will control their own approaches to “help functionality” and will not be tested as part of this project. Help functionality and recovery from failures of all kinds happening within the Multimodal AccessMap application will be tested in laboratory and limited field experiments performed in Phases 2 and 3 of this project, where the conditions can be controlled, in order to ensure that the demonstration application help functions work robustly and effectively. The lab tests will be designed to cover a variety of failure scenarios which will be identified from the lived experience of our co-design team as part of Phase 2 development and Phase 3 testing.

In addition, “proactive” notification is also being considered for the UW’s Multimodal AccessMap. By incorporating data provenance scores (e.g., Does the database have a little or a lot of confidence that the sidewalk is 6 feet wide, as stated? Is there high or low confidence that a curb ramp is at this location?) into the data standard, and then using those data to provide both confidence scores and alternative paths within the navigation instructions, the application can provide users with a warning when data are limited. This will allow travelers to select an alternative path that provides more confidence in the path’s accessibility and will provide a warning that specific segments of a path may be difficult to traverse, should they choose a path that includes links with limited data quality.

Determination of the best way to deliver information about travel segments for which data quality is questionable will be one of the topics that the UW application development team will work on closely with individuals with lived experience who are co-designers of the application during Phase 2 of this project.

Finally, the UW team has already been told by stakeholders that one situation of specific concern is when emergencies or major service disruptions affect transit operations at major transit centers. In these cases, many people with mobility disabilities will be unable to obtain information needed to safely respond to those events. Such information may include determining the path required to exit a station, or finding emergency equipment (e.g., a defibrillator). By working with both transit agencies and individuals with lived experience during Phase 2, the UW team will determine how emergency response information can be obtained, stored, and delivered to travelers when emergencies occur.

3.2 Summary of Safety Scenarios by Project Component

Table 5 provides a short summary of each of the safety risks and the management activities planned to help avoid, mitigate, and respond to those safety needs. Each of these risks is rated for controllability, severity, and exposure. Controllability is defined as the degree to which an involved individual will be able to withdraw from a hazardous situation, thereby avoiding injury or exposure to further hazardous conditions. Controllability is ranked from 0 (best or fully avoidable) to 3 (worst or outside of the traveler’s ability to avoid.) For example, the potential for a traveler to fall down a flight of stairs they were unaware of is relatively controllable. Stairs can be marked with tactile delineators, and accurately described in data being used to describe a path, significantly limiting the potential for the event from taking place. In contrast, lack of real-time information limits the ability to identify is an elevator is actually working. Thus, the status of an elevator, for this project is not a controllable factor for a traveler within this project, which does not include real-time status of infrastructure.

Severity is defined according to the likelihood and severity of injury occurring. Severity is ranked from 0 (no injuries) to 3 (life-threatening injuries are likely.) The severity of an event is correlated with the individual involved and the type of event. So, a fall down a flight of stairs would be fairly severe for anyone, but for an older adult, it could be life-threatening.

Exposure is defined as the probability that a specific type of hazardous condition will occur when a traveler is making a given trip. Exposure is rated from 0 (the scenario is very unlikely to happen) to 3 (the scenario is very likely to happen.) Thus, exposure to minor sidewalk imperfections that are not included in the sidewalk data is likely very high (sidewalk conditions vary constantly along a sidewalk, and are not easily summarized in data), while experiencing a car running a red light is very unlikely to happen, thus making risks of crossing with a green light

Additional material on these risks and how the rankings are computed are presented in Section 4 of this report.

Generating a generalized risk rating for these categories is difficult because the level of risk changes considerably depending on the disabilities each specific individual faces and the nature of the specific hazard occurring at a given location. The ratings shown in Table 5 typically report a mid-level response to rating each hazard assessment. Some individuals, in some situations, will be at a higher risk than noted in Table 5, while others will experience lower risk during the occurrence of the same basic event. Unfortunately, the extremes for almost all risks range from essentially zero risk (e.g., a normative person, traveling in a group, with multiple options for assistance needs to cross a busy street where the routing data do not correctly describe that street crossing), to extremely dangerous (a deaf-blind individual, traveling alone, at night, attempting to cross that same street without assistance.)

Table 5: Summary of Safety Scenarios

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
Sidewalk data collection (OpenSidewalks) ConOps #1, #2, #5, #7, #10, #11, #12, #13	1) Invalid sidewalk data are generated/collected to be shared with consumers. 2) The collected data do not include all attributes needed to safely route pedestrians. **Risk:** Travelers will be routed over paths not accessible to them, resulting in failed trips, and potential harm to the travelers.	Data standards will be revised to incorporate data items required for safe navigation Meta-data will be developed and incorporated with the data to describe the provenance of collected data, describing the confidence with which those data should be used (e.g., age of data reported, or confidence level associated with image recognition software, or status or vetting.) Data vetting by multiple available parties • Owner/hired consultant review • Community/organization reviews • Traveler feedback Data storage will contain a reported confidence score based on data collection technique, age, vetting status.	2 3	1 1	2 2

[5] Numbers shown in this column of Table 5 correspond to the Safety Risk Management Summary IDs shown in Table 7.

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
On-demand transit service data collection (GTFS-Flex) ConOps #4, #5, #6, #7, #13	3) Transit service provider generates invalid transit service schedule 4) The reported transit service schedule is out of date. 5) The collected data being do not include all attributes needed to safely route travelers **Risk:** Travelers will be routed to services that do not exist as described, resulting in failed trips, and potential harm to the travelers.	Data standards will be revised to incorporate data items required for safe navigation Meta-data will be developed and incorporated with the data to describe the provenance of the collected data, describing the confidence with which those data should be used (e.g., age of data reported, or confidence level associated with image recognition software, or status or vetting.) Data vetting by multiple available parties Owner/hired consultant review Automated data review (format / permissible data) Traveler feedback Date stamps will be present to ensure that the data are valid for specific dates and are not used past valid time periods.	0 1 2	2 1 1	1 2 2
GTFS-Pathways data generation ConOps #3, #8	6) Transit service provider generates invalid transit facility descriptions 7) The collected data being do not include all attributes needed to safely route pedestrians **Risk:** Travelers will be routed over paths not accessible to them, resulting in failed trips, and potential harm to the travelers.	Data standards will be revised to incorporate data items required for safe navigation Meta-data will be developed and incorporated with the data to describe the provenance of the collected data, describing the confidence with which those data should be used (e.g., age of data reported, or confidence level associated with image recognition software, or status or vetting). Data vetting by multiple available parties Automated data vetting Owner / hired consultant review Traveler feedback	0 2	1 1	1 2

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
Navigation application with transit and sidewalk data ConOps #5, #6, #7, #8, #9, #10, #11, #12, #13	8) User travel preferences are incorrectly applied when determining route identification **Risk:** Travelers will be routed over paths not accessible to them or routed using services that do not exist as described, resulting in failed trips, and potential harm to the travelers.	Application developer and traveler engagement with the process for establishing data standards to ensure that • The data standards incorporate the data fields required to effectively describe infrastructure and service attributes needed for routing of all members of society. • Applications developers understand how to use those standard data fields to correctly incorporate traveler preferences in their application outcomes.	1	1	1
Navigation application for non-English speaking users of transit and sidewalk data ConOps #8	9) Navigation directions are not understood due to an inability of the application to effectively communicate application outputs. **Risk:** Travelers will not correctly understand the navigation choices and instructions given to them.	Application developer and traveler engagement in the process for establishing data standards to ensure that • The data standards are designed so that infrastructure and services can be effectively described in all languages. • Applications developers are able to understand how to use those standard data fields in multiple languages or communications devices.	0	1	1
Navigation application with transit and sidewalk data for low-income user ConOps #9	10) Navigation directions are incorrectly computed because of an inability of the application to effectively communicate the financial costs for using specific modal or route choices. **Risk:** Travelers will not correctly understand the navigation outcomes presented to them.	Application developer and traveler engagement in the process for establishing data standards to ensure that • The data standards incorporate fields required to effectively describe infrastructure and service attributes. • Applications developers understand how to use those standard data fields to correctly incorporate traveler preferences in their application outcomes.	0	1	1

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
Data service provisioning All ConOps Scenarios	18) System security is breached **Risk:** System will become inoperable as a result of an attack (e.g., a denial-of-service attack) or other malicious activity	Clear assignment of responsibilities for system security and sufficient resource allocations to support that position. The individual responsible for security is in charge of: • Identifying and analyzing electronic security entry points • Vulnerability assessments • Security checks • Monitoring and assessing the effectiveness of the controls.	2	0	1
Data service provisioning All ConOps Scenarios	19) System or network latency is too slow 20) System hardware/software resources are overloaded. **Risk:** Travelers are unable to obtain data in a timely fashion, resulting in unsafe behavior due to a lack of information.	Clear assignment of responsibilities for system performance and sufficient resource allocations to support that position. The individual responsible for system performance oversees: • Measuring and analysis of runtime errors • Network latency checks • Memory use.	1 1	1 1	1 1

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
Demonstration applications ConOps Scenarios #5, #6, #7, #13	11) Staff of the transit service provider are inadequately trained, and that information is not passed along to travelers. 12) The suggested transit service does not have the attributes required by the traveler (e.g., no wheelchair tied downs are available). 13) Emergency response features are not accessible to all travelers (e.g., navigation applications do not have the ability to route users to emergency evacuation routes or to emergency response equipment, such as a defibrillator). **Risk:** Lacking information on service capability or availability, a rider is directed to use a service that is unsafe for that user. **Risk:** Lacking the ability to obtain information that other travelers also obtain (e.g., deaf individuals do not hear auditory emergency notifications and directions, or individuals with visual impairments do not identify signed evacuation routes), travelers with disabilities may be put at risk during emergencies.	Data on staff training levels are proposed for inclusion in the GTFS-Flex extension. Data on transit service attributes will be added to the GTFS-Flex data standard and will be populated to include in navigation software. Data on emergency equipment and routes are proposed for incorporation in the GTFS-pathways extension.	2 2 2	2 1 2	2 2 2
Demonstration applications ConOps Scenarios #6, #13	14) Assistance verifying trip eligibility is not available to staff operating transit services, resulting in denial of travel on those services. **Risk:** Travelers may be directed to use a service for which they are not eligible, potentially stranding them.	Extensions to the GTFS-Flex data standard have been requested to include better eligibility fields to ensure that service eligibility is correctly determined. Extensions to the GTFS-Flex data standard have been requested to include information on how to request help in real-time when disagreements over service provision occur.	2	2	1

Component	Scenario and Risk[5]	Control Mechanism / Mitigation	Controllability	Severity	Exposure
Navigation application with transit and sidewalk data ConOps #5, #6, #7, #8, #9, #10, #11, #12, #13	15) Application uses too much battery power, causing the end user's device to shut down during a trip. 16) Location reference within the application is wrong, causing the navigation instructions to be inaccurate. 17) Communication between the application and the data server is lost during a trip. **Risk:** Travelers will be left without routing instructions when they need them. **Risk:** Travelers will be routed over the wrong paths or services that do not actually exist as described, resulting in failed trips, and potential harm to the travelers.	Application developer and traveler engagement in the process for establishing data standards to ensure that • The data standards incorporate the data fields required to effectively describe infrastructure and service attributes needed to route all members of society. • Applications developers understand how to use those standard data fields to correctly incorporate traveler preferences in their application outcomes. • AccessMap and Soundscape incorporate low-power warnings in their applications. • AccessMap and Soundscape incorporate improved "call for assistance" functionality in their applications.	2 2 2	2 1 2	1 1 2

4 Assessment of Safety Risks

This section of the report describes in more detail the assessment of the risks listed in Section 3. These risks were assessed by summarizing the comments of stakeholders with lived experience as the risks were identified and discussed as part of the co-Design process. However, generalizing these risk assessments is difficult because the level of risk changes considerably depending on the disabilities of each specific individual and the nature of the specific hazard at a given location.

For example, people with a hearing disability may face considerably more danger than individuals who have normative hearing abilities during an emergency because people with a disability cannot hear an emergency announcement or any audio instructions to keep them safe. In such a situation, both types of individuals are in a hazardous situation, but those with a hearing disability are at greater risk because they are less able to gain information about either the hazardous situation or how to respond.

Similarly, an individual who requires use of on-demand transit for mobility may be in a much more hazardous situation if, while that individual is traveling, the trip by an on-demand vehicle is cancelled, in comparison to a user of a low headway, fixed-route transit system when a fixed-route vehicle trip is cancelled. This is because the on-demand rider may be stranded for a longer period than the rider of the fixed route system, who may only have to wait a short time for the next vehicle to come along. Thus, a similar event—a missed vehicle trip—may result in very different hazard levels, both because the riders have different capabilities and because the service levels differ.

Therefore, this section takes a middle of the road approach to rating each hazard assessment. Some individuals, in some situations, will be at a higher risk than noted in Table 5, whereas others will experience relatively little risk during the same basic event. The outcomes of the risk assessments are shown in the Table 5.

In general, the project team takes the following approach to risk mitigation. The team is working with individuals with lived-experience and experts in the field of mobility for people with disabilities to identify the information gaps which caused risks to travelers with disabilities and the data needed to resolve those information gaps. The team is working with infrastructure owners, transportation service providers and technology firms to identify ways to collect that data, describe the quality and limitations of that data, and lower the cost of that data collection effort to increase the ability of those infrastructure owners and transportation service providers to generate, collect, maintain, share, and verify those data. The team is working with those same owners and service providers along with community and advocacy groups to develop efficient and functional data vetting functions to ensure that those data are as accurate as possible. The team is working with data service providers to develop secure data services which protect the data and data services from malicious individuals and organizations, so that the accurate data collected are not changed or deleted as a result of malicious intent. Finally, the team is working with both individuals with lived-experience and application developers to determine how to best deliver those data in ways which both remove information gaps, and which produce applications which are robust and fault tolerant, so as to reduce risk to users when failures in the technology being used occur. The risk identification and mitigation efforts which occur within these various activities take place primarily in Phase 1 and Phase 2 of the ITS4US project. Specific risks identified to data are described in the remainder of this chapter.

4.1 Traveler Safety Risk Assessment

This subsection of the Safety Management Plan focuses on the risks that travelers will face when using the system that this project is developing. It briefly describes the management approach for lowering the frequency with which those hazardous situations occur and the severity of those events when they do occur.

The risks summarized below, identified by UW team and its stakeholders, result from a combination of limitations in infrastructure or transit service provision and the lack of communication about those limitations to travelers. The goal for the project’s avoidance/mitigation effort is to identify and publish data that will describe those infrastructure/service limitations in order to highlight potential hazards to travelers who use the applications developed both in this project and by third party developers in the future. Because the data being developed are open to the public, the UW team does not have control over how those data are used, nor how applications built by 3rd party developers design safety into their applications. It is therefore not part of this project to test those applications for their deployment of safety features. The team will provide references for best practices for the development of applications designed to increase mobility for people with disabilities. Testing of safety features as part of the ITS4US deployment will be limited to the UW demonstration applications.

4.1.1 Risk #1 Poor Resource Allocation

The first set of identified hazards results from the fact that many transit service providers have limited resources for planning and implementing services that include attributes required by people with disabilities. For example, on-demand vehicles serving healthcare facilities may have a limited number of wheelchair tie-downs and can thus become “full” more quickly than their ridership indicates. Similarly, transit stations without functioning elevators are “accessible” for people with some disabilities but not for travelers with other disabilities. The risk identified here is for a trip in which the attributes for all trip segments are not accessible by a specific user. This may result in that user’s inability to complete the trip and can place that individual in a hazardous situation where that trip path fails. The severity of that failure will vary considerably depending on when, where, and to whom it occurs.

The UW team is working with both individuals with lived experience and agency personnel throughout Phases 1 and 2 of the ITS4US project to determine what data are required to describe the features and feature attributes that allow specific infrastructure to be “accessible” for a broad set of mobility abilities. They will also determine how data on these features and attributes can be collected and described in electronic formats that can be readily delivered in multiple ways (e.g., audio, text, tactile). This includes the ability to describe the following:

- The wide range of assistive travel devices used by people with disabilities,
- The features present on vehicles that transport people with disabilities to health facilities and other life preserving services,

- The level of training and sensitization provided to staff, volunteers, and community workers who are likely to interact with travelers during a trip (e.g., At a fare gate to a subway station, can an individual in a wheelchair expect to find a trained individual who will help in navigating that faregate?).

The result will be data collected and stored in ways that meet the GTFS-Flex, GTFS-Pathways, and OpenSidewalks data standards. These data will describe to potential travelers how “welcoming” specific trip segments are to an individual with their mobility characteristics and the degree to which they can expect specific barriers that they will need to overcome on those segments.

Discussions with application developers and the co-Design participants with lived experience will then work through how best to deliver this information to digital device users.

4.1.2 Risk #2 Human Resource Sensitivity Training for Data Producers/Consumers

The second set of risks for those traveling within the transit environment results from the facts that information that is readily available to travelers with normative abilities is often not readily accessible to travelers with disabilities, and agency staff may not be sufficiently trained for interacting with those travelers.

Lack of awareness about the needs of people with disabilities and uncertainty about effective actions are common among staff and volunteers from all sectors. At the same time, people accustomed to working with individuals with disabilities may lack experience in safety risk management, and safety teams may lack knowledge about the rights of persons with disabilities, staff who have the expertise to provide appropriate services for people with disabilities, or information about local specialist disability services. Because of this general lack of knowledge across important subject areas, the disability awareness of staff and volunteers across different sectors will be best increased during routine vulnerability reduction and data production preparedness programs.

Consequently, the UW team will work with stakeholders to capture data that describe whether specific agencies or facilities that are described in our project’s data streams can demonstrate the ability (outside of the applications being developed in this project) to accomplish the following:

- Broadly disseminate data about potential safety hazards and emergency situations faced by people with disabilities, specifically having to do with real-time conditions,
- Deliver that information across a wide range of communication formats to ensure it is obtained by people with range of disabilities,
- Demonstrate non-discriminatory attitudes and practices toward people with disabilities,
- Deliver data and information services using appropriate reasonable accommodations where required for people with disabilities,
- Demonstrate awareness of the resources available for people with disabilities.

Describing these service capabilities will help people with disabilities gain insight into the capabilities and operating environments of community transit services. That insight will help individuals select between alternative routes and services on the basis of the differences in risk inherent in using a service that is well prepared to serve people with disabilities and a service that is basically unprepared to work with such people.

4.1.3 Risk #3 Information and Knowledge Management

The third set of traveler risks pertains to the primary work area associated with this project. It involves the availability of data needed to accurately describe the transportation infrastructure and services available to travelers, and the level of confidence users should have in the data presented to them as part of one or more routing plans. The risks to users of the services developed by the UW ITS4US project come from three basic sources:

- Information that describes an attribute of interest for a trip segment (e.g., infrastructure link or transit service) is missing.
- Information that describes an attribute of interest for a trip is present, but the validity of that information is uncertain because of
    - The age of the data (e.g., the data were collected long enough ago that conditions may have changed),
    - Limitations in the technique used to collect the data (e.g., data on sidewalk width were collected via video image analysis, but a combination of image quality and the technique used decreased the precision of that sidewalk width estimate), or
    - The lack of vetting of a reported statistic by a secondary source.
- The available data cannot be readily displayed to a traveler in a usable format (e.g., information on a path with a significant side-slope may be difficult to deliver to a traveler who relies on tactile feedback).

The risk associated with any of these three outcomes will be a function of the individual traveler, the nature of the missing or imprecise data, and the travel link (trip segment) being traversed. For example, a lack of definitive sidewalk width is more important for a narrow sidewalk (e.g., less than 6 feet) than for a wide sidewalk. Whereas even a 20 percent error in the reported width of a wider sidewalk will have little impact on whether most people are able to use it, a narrow sidewalk may not be usable by individuals with wide mobility devices, and the difference between a 3.5-foot and 5-foot width could easily matter to those using a wide wheelchair.

Similarly, stakeholders would like the system to provide real-time information on elevator and escalator operating status, as well as other real-time information such as whether snow has been removed from sidewalks after a winter storm. Unfortunately, real-time status information is not currently reliably available, and therefore it will not be included in this project. But basic infrastructure characteristics also change over time as a result of age, environmental conditions (e.g., growth of tree roots, the impacts of freeze-thaw cycles on joint smoothness), and construction and maintenance activity. Therefore, even data that were perfectly accurate five years ago may no longer be correct.

Risks to travelers occur when reported data are not accurate. Again, the severity of that risk varies with the significance of the data error, the characteristics of the traveler, and the location of that error. While an assessment of all aspects of risk (controllability, severity, and exposure) can be easily made for any specific combination of data error, location, data use, and traveler, summarizing the vast array of outcomes is almost impossible. The co-design process used to both finalize the data schema and develop data delivery techniques during phases 1 and 2 of the project will used to identify the most significant safety risks to our stakeholders, and the most effective ways of both identifying and then mitigating those risks through data collection, provision of meta-data about the collected data and delivery of that data in ways which delivers the needed information to travelers. This will be documented as part of the project's design documentation.

As a consequence of the variety of environmental conditions, information gaps, and physical outcomes that travelers with mobility disabilities face as a result of those various information gaps, the risks assessed for these errors are typically an average of multiple possible outcomes. The project team and its stakeholders expect that there will be some ability to control the occurrence of that risk through careful data curation, but the lack of expected resource availability strongly suggests that there will always be some risk. As a result, the management of that risk will be based on informing users about the level of confidence they should have in each data item. When presented effectively through an end user-oriented application, these will allow users to foreshadow different hazards and take mitigating steps appropriate for them.

Therefore, to manage risks associated with imperfect data, the UW team's management approach will be to use multiple approaches to risk mitigation. These include the following:

- Improving the data collection techniques,
- Involving multiple techniques and groups to help vet the data, to further improve their reliability and accuracy,
- Defining and maintaining the data provenance associated with the collected and published data to provide insight to travelers about the level of trust they should give to specific data of importance to them, where "data provenance" can include the following:
    - The statistical confidence associated with a variable computed automatically (e.g., from an AI based analysis of imagery),
    - The age of that data point from when it was collected or last vetted,
    - The vetting status of the data,
    - The method used to develop the data value (e.g., crowdsourced, AI, city asset database, etc.).

The specific data provenance variables will be developed with input from the project stakeholders as part of the enhancement of the three data standards that are part of this project. Guidance on the use of the data provenance values will be developed as part of the co-Design process associated with the application development effort for this project.

4.1.4 Risk #4 Service Delivery Assistance

Another identified traveler risk occurs when assistance is required by a traveler during a trip. Travelers with disabilities are more likely to require assistance and requesting that assistance can be difficult. Hazards can result if that assistance is not readily available. The delivery of assistance can range from correctly securing a wheelchair on a transit vehicle, to successfully navigating a fare gate, to identifying the location of emergency equipment (e.g., an eyewash station or a defibrillator).

As with the previous three risk categories, the agencies providing services (or infrastructure) are responsible for providing those services and facilities. This project is responsible for describing the availability – or lack of availability – of those services. To do that, the UW Team will use the co-design process to identify the assistance services that need to be reported on, identify how to describe those services, design the data standard extensions (GTFS-Flex, GTFS-Pathways) to contain those data, build tools that make it easy for transit agencies to report on the services they do or do not provide, and then determine how to deliver that information in an understandable manner.

For this risk, the UW team's management approach will be to work with our stakeholders to determine the types of assistance required and codify how the availability (or lack) of that assistance can be captured in objective parameters. These parameters will then be included in the data standards that describe available transit services, facilities, and infrastructure.

The risks posed by lack of assistance can range from moderate (e.g., fare gate navigation can be accomplished without assistance with some trial and error) to severe (the inability to secure a wheelchair on a moving transit vehicle could result in severe injury or death).

The risk mitigation approach taken by the UW team will be to report on the availability of specific services and infrastructure. As in previous cases, delivery of this type of information will determine whether the availability (or lack) of specific types of assistance will result in travelers' willingness or unwillingness to use specific travel choices. The key to our approach is that an informed user will be able to make good choices on the basis of their individual capabilities and comfort levels, thus effectively managing their risks better than a one-size-fits-all approach.

This risk is related to risks 2 and 3, which describe the types of training provided and the overall data available for distribution. This risk category differs in that it focuses on the specific delivery of assistance, as opposed to the types of training provided.

4.1.5 Risk #5 Application Failure

The final category of identified risks is associated with failures that occur during the use of applications and the digital devices on which they run. In some cases, for example, when a trip route is planned at home on a desktop computer, a failure of either the application software, the computer it runs on, or the communications between that computer and the central database will pose almost no safety risk. The user might be unhappy, but little risk will be associated with that failure. On the other hand, if that failure occurs in the middle of a trip, when the user is relying on turn-by-turn navigation features, this error could place the traveler at risk. Even in this situation, the severity of that risk will be a function of the type of error (a total loss of power? A momentary loss of communication?), the location of the traveler, the importance of that information at that point in time, and the characteristics of the traveler.

If a user's digital device does not have an accurate location reference because of limitations in the device and how it computes its location, those errors will be far more significant for travelers who do not have other location references available. Thus, individuals who are blind or have low vision will face a more hazardous situation when poor location determination results in false navigation instructions than travelers with normative vision who have more ability to confirm their location and request additional assistance or provide feedback to their digital device asking for information appropriate for their actual location.

As before, the UW Team has chosen to take a middle ground on these types of errors. We treat them as not being totally preventable, but where actions taken by the project team can both reduce their occurrence and provide for mitigation of the outcomes if they occur.

From a risk management perspective, the UW team will perform failure assessments for all components of the systems built for this project. Where possible, warnings of impending errors (e.g., low battery or off-route navigation warnings) will be given to travelers to allow them to take actions that limit the severity (or occurrence) of an event. In addition, software design can also limit the impacts of some errors. One example of this would be to download all navigation directions to the user's device at the start of a trip to limit the impact of a loss of communications mid-trip. Another example would be to set up visual or auditory warnings to users of the AccessMap application when their smartphone's location has become uncertain due to the factors such as an inability to see a sufficient number of GPS satellites.

In addition, the team will look to include recovery and assistance functions into the applications it develops. These may include call numbers for assistance (e.g., to on-demand service providers) or the ability to replan navigation paths from the current location if the user goes off-route.

The result of these collective actions should reduce both the occurrence of hazards and the severity of those risk hazards when they occur.

4.2 System Safety Risk Assessment

The second source of risk the project will need to address are the risks associated with the operation of a major database system on which multiple application developers and information providers rely. The approaches to managing these risks are discussed in in Chapter 5. The safety risks associated with the operation of the system can be summarized into four areas:

- The security of the data sharing infrastructure,
- The ability to maintain the integrity of the central data sharing system given cyber security concerns and attacks of various kinds,
- The performance of the data sharing services under load,
- The ability to manage the relationships with both organizations submitting data to the system and application developers extracting data from the system to keep the system operating without disruption.

Regardless of where the risk occurs, it will be important to apply risk mitigation strategies at each stage in the life cycle of both system components and protocols. Questions such as the following will help guide strategy choices:

- Is the risk a compliance, privacy, technical, or some other issue?
- Does the mitigation deal primarily with people, process, or technology?
- Is the assessed risk acceptable to the organization and the data cooperative as a whole?
- Is the cost of fully remediating the risk reasonable?

The UW team will use NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, for guidance as it includes an extensive catalog of management, operational, and technical security controls. Table 6 lists the controls and maps them to risk categories.

Table 6: Security control families

Control Family	NIST Class	Risk Category
Access control	Technical	Process
Awareness and training	Operational	People/Policy
Audit and accountability	Technical	Technology
Security assessment and authorization	Management	Process
Configuration management	Operational	Process
Contingency planning	Operational	Process
Identification and authentication	Technical	Technology
Incident response	Operational	Process
Maintenance	Operational	Process
Media protection	Operational	Process
Physical and environmental protection	Operational	Process
Planning	Management	Process
Personnel security	Operational	People/Policy
Risk assessment	Management	Process
System and services acquisition	Management	Process
System and communications protection	Technical	Technology
System and information integrity	Operational	Process
Program management	Management	Process

Effective access controls will help limit risks associated with both intrusion from bad actors and inadvertent changes made by untrained staff. Staff training in both workflows and permissions will support management of access control, as well as raise the overall awareness, knowledge, and execution of safety protocols and procedures. Access controls are effective only when security assessments are completed, proper authorizations are granted, and appropriate identification and authentication techniques are established and rigorously followed.

Effective audit and accountability procedures will both ensure that procedures are followed and identify potential security threats and intrusions quickly. This will allow for fast incident detection and response, for which effective and flexible contingency plans will be required. These tasks will need to be part of a complete program management effort that has a strong focus on risk assessment and safety planning.

Programmatic risk management will also include risk assessments and analysis as part of system development, with system security and integrity built into system and services acquisitions, the communication protocols selected and implemented, the maintenance activities performed, the management of the overall system configuration as the system evolves over time, and the physical and environmental protections provided to the systems developed and used.

The overall result of this programmatic approach to safety will be a system that is designed from the start

- for safe and secure operations,
- with careful attention to the implementation of procedures that maintain that safety and security,
- with effective staff training, and
- with an audit/reporting system that routinely scans for security risks.

With this system, planning for incidents will allow for fast and effective responses that minimize risks and limit system downtime.

Each of those risks is discussed in more detail in Chapter 5.

5 Safety Operational Concept

The key outcome from this ITS4US project is to fill three specific information gaps that currently limit the ability of many individuals with mobility disabilities to travel freely. These information gaps not only limit the mobility of these individuals – who decline to make trips when they are unsure of their ability to safely complete those trips – but those information gaps can present risks to those individuals while they are traveling. Thus, the entire project's primary goal – the collection and effective publication of data which fill those information gaps, is the key operational safety concept for the project. Because infrastructure conditions and transportation services are constantly changing (in some case, such as infrastructure, slowly, in other cases, such as the operational performance of a transit vehicle on any given day, sometimes quickly) the quality and quantity of the data being collected and published are the primary mechanism for improving safety.

As part of collecting and delivering that data, this project relies heavily on the participation of our co-design teams. These teams, listed earlier in Table 1 include individuals with lived-experience, infrastructure owners, transportation service providers, and community and advocacy groups with vested interests in the collection and delivery of accurate data. The tasks required to collect data, vet that data, assign both data confidence and data province metrics to those data (helping users understand the level of trust they should place in data they are using, and raise awareness of limits in the available data), are discussed more extensively in other documentation for this project. In particular, the reader should examine the ConOps, Systems Requirements, Data Management and Performance Management reports.

However, the efforts placed on the collection, vetting, and publication of these data are not sufficient if the data system which performs those tasks is not secure. As a result, this chapter, discusses the tasks required to protect the data system collecting, storing, and serving those data to end-user applications, keeping the data being collected secure from malicious individuals and organizations.

Consequently, the remainder of this chapter provides practical operational safety best practices and controls designed to help the UW ITS4US project improve safe outcomes by protecting the data systems being built for this project. The UW team has reviewed a volume of guidance from organizations such as the National Institute of Standards (NIST) and others (referenced later in this document). The goal of this document is not to supplant or replace other extensive work on this topic but rather to condense safety operations into a number of coherent tasks that the project can adopt. Condensing best practices into such a set required the UW team to make trade-offs and use their experience to focus on the most important "do first" types of activities. The operational practices and controls presented here are those that the project can begin to adopt to mitigate some of the greatest safety risks. This document attempts to make projections about the highest safety risks based on the current technology road map, available resources, and other factors, but as Phase II begins and the group implements its plan, changes to the safety management plan may be required. Additionally, at present the technology plan does not include lower-level detail, and those details may include additional implementation tasks that will require mitigation not described in this plan. It is also important to note that adding or modifying existing safety controls should be done with care and sufficient planning.

Our project environment will require testing to ensure that changes to controls do not break important functionality or introduce new risks. The operational guidance in this document should be used as a description of what needs to be done and changes will be introduced in a careful and thoughtful manner. Safety improvement is a gradual process.

This document describes security risks and recommends security controls in each of the following categories:

- People and policy security risks
- Operational security risks
- Insecure software development life cycle (SDLC) risks
- Physical security risks
- Third-party relationship risks
- Network security risks
- Platform security risks
- Application security risks

Data sharing technologies introduce some new risks into transportation cooperative environments. Data sharing and publishing, by design, make extensive use of remote network connectivity, communication protocols, hardware that is difficult to configure, and complex software. This added complexity and connectivity introduce additional security and data safety risk. Some significant steps will be taken in the context of the current demonstration project to help transportation data cooperatives mitigate some of these risks. One example is the introduction of redundancy into communications protocols to help preserve the confidentiality and integrity of communications between data producers and the data repository. An important aspect of future data cooperatives will be to make safe decisions and take actions based on real-time data arriving from field devices. This is outside the scope of this demonstration project, but our group intends to plan for the extension of our system to accommodate real-time data in the future.

While the benefits to interoperable transportation data sharing are numerous, so are the safety implications. These technological changes make it increasingly important that data producers ensure the bar is set high enough to preserve the confidentiality, integrity, and availability of networked data assets. The most pressing safety concerns are to ensure that attempts to tamper with any field-devices, software, or hardware do not disrupt the overall operations of the interoperable data sharing infrastructure on a large scale and do not result in incorrect actions being taken at the data producer level and synchronized up to the data sharing environment.

The safety risks in our system can be categorized in many ways, but we will put them into three categories: people, process, and technology. Raising the security posture of a data cooperative will require raising the bar in all of these categories. Adversaries will go after the weakest link, so it is important to approach any security and safety program comprehensively using risk management practices as a guide. It will also be important to comply with design principles such as compartmentalization, least privilege, and fault isolation. Failure will happen, so it will be important to plan for it, isolate it, contain its damage, and recover from it gracefully. An organization’s security policy and controls must be adaptable to emerging threats in a constantly evolving world. Large transportation data producers are already instituting practices such as proper network segmentation, regular security patching, up-to-date antivirus software that runs regularly, security-aware software development and acquisition processes, proper vendor risk management, remote attestation of firmware running on field equipment, and personnel security training. These go a long way toward mitigating risk. But not all the agencies included in this data sharing cooperative will be at the same level of risk mitigation or will even have the resources to deploy such mitigation measures. The ongoing assessment of security threats, balanced against the existence and adequacy of security controls at the interoperable data sharing infrastructure level, will be needed to ensure that security controls and countermeasures in place are commensurate with potential risks. The operational steps described below are intended to provide the data sharing cooperative with an adequate security posture as it acquires, integrates, deploys, and maintains data sharing infrastructure technologies, and to assist and provide guidance to each participating organization in managing its own internal risks.

5.1 Safety Design Elements

This section of the Safety Management Plan describes the design elements that will be used to avoid or prevent safety impacts in each of the categories identified above.

5.1.1 People and Policy Security Risks

5.1.1.1 Train project staff in incident-handling and contingency plans.

The UW team's safety management approach will ensure that personnel responsible for responding to cyber incidents or major disruptions have a firm grasp of response plans and can execute them under stress. **Well-designed training** can go a long way in preparing people to adopt security conscious behaviors and in establishing policies. The goal of both that training and the policies will be to maintain a secure environment toward improving the data cooperative's overall security posture.

5.1.1.2 Assign to a senior manager responsibility for developing, implementing, and enforcing security policy

The UW team's safety management approach will ensure that the senior manager has the requisite authority across departments to enforce safety-related policies. The development and implementation of effective security policies, plans, and procedures will require the collaborative input and efforts of stakeholders in many third-party partners of the data cooperative. Assigning a senior manager to organize and drive the efforts, with the authority to make and enforce decisions at each stage, will raise the likelihood of success.

5.1.2 Insecure Software Development Life Cycle (SDLC) Risk

Listed here are several design techniques intended to improve software development that have traditionally been used to avoid failures created through inconsistent software procedures, and processes and unstable system and network configurations.

5.1.2.1 Improve runtime validation

A large class of flaws results from inadequate runtime validation. Careful attention to techniques such as argument validation and bounds checks (especially, to prevent insertion of Trojan horses such as executables added to arguments, causing buffer overflows), divide-by-zero checks, and strong typing of arguments can provide enormous benefits. Brian Randell[6] long ago suggested the benefits of moving checking closer to the operations being performed (whether in space, in time, or in layer of abstraction) to reduce the amount of intervening infrastructure that must be trustworthy. This is also applicable to end-to-end checks and end-to-end security.

5.1.2.2 Make naming consistent

Aliases, pointers, links, caches, and dynamic changes without relinking, and various redundant representations all represent common sources of security vulnerabilities. Symmetric treatment of aliases, symbolic naming and dynamic linking, strong type checking, use of globally unique names, and recognition of stale caches and cache invalidation are examples of beneficial techniques the UW team will implement.

5.1.2.3 Ensure proper encapsulation

Exposure of procedure and process internals may allow leakage of supposedly protected information or externally induced interference. Proper encapsulation requires a combination of system architecture, programming language design, software engineering, static checking, and dynamic checking.

5.1.2.4 Ensure synchronization consistency

Many vulnerabilities arise as a result of timing and sequencing issues, such as dependence on relative ordering, race conditions, synchronization, and deadlocks—in both synchronous and asynchronous contexts. Note that many of these problems arise because of the sharing of state information (particularly in real time or in sequential ordering) across abstractions that otherwise appear disjointed. Atomic transactions, multiphase commits, and hierarchical locking strategies are examples of constructive design techniques the UW team will implement. A classical kind of vulnerability is a time-of-check to time-of-use (TOCTTOU) flaw, which results from a lack of atomicity to which inadequate encapsulation can also be a contributing factor.

5.1.2.5 Reduce adverse dependencies

Dependence on untrustworthy programs or subsystems is another source of vulnerabilities. They can emerge as a result of flawed compilers and flawed runtime library programs, as well as program bugs—including those resulting from improper program changes and upgrades, but also from Trojan horses.

[6] Brian Randell (born 1936) is a British computer scientist, and Emeritus Professor at the School of Computing, Newcastle University, United Kingdom. He specializes in research into software fault tolerance and dependability. https://en.wikipedia.org/wiki/Brian_Randell

5.1.2.6 Conduct logic error checking

There are many common logic errors (such as off-by-one counting and omitted negations) that need to be avoided. Many of these arise in the design process, but some involve bad implementation. Three examples of logic error checking that pertain to our interoperable data system include consistency checking on data entry, determination of the suitable availability of appropriate resources, and deletion of old artifacts and residues when appropriate.

5.1.3 Physical Security Risks

Some safety design mechanisms involve designing adversarial tests designed to exploit and compromise the security system. Some examples include the following adversarial tests:

- Exploit the physical access of authorized staff to enter organizational facilities. Example process: Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities and circumventing physical security checks.
- Exploit poorly configured or unauthorized information systems exposed to the Internet. Example process: Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
- Exploit split tunneling. Example process: Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.
- Exploit multi-tenancy in a cloud environment. Example process: Adversary, with processes running in an organizationally used cloud environment, takes advantage of multi-tenancy to observe the behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
- Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). Example process: Adversary takes advantage of the fact that transportable information systems are outside the physical protection of organizations and the logical protection of corporate firewalls and compromises the systems on the basis of known vulnerabilities to gather information from those systems.
- Exploit recently discovered vulnerabilities. Example process: Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

5.1.4 Third-party Relationship Risks

5.1.4.1 Develop context-sensitive authorization

Context-sensitive authorization will be designed into the system. Monolithic access controls tend to grant all-or-nothing or extremely coarse permissions. The development and consistent use of finer-grained authorization techniques are very helpful in enforcing the separation of privilege and least privilege. This is analogous, in the classified world, to the difference between gross levels (e.g., Top Secret, Secret, Confidential, and Unclassified) and finer-grained authorizations.

5.1.4.2 Develop robust identification and authentication

With the goal of avoiding spoofable identities and inter-subsystem authentication within user systems and network infrastructures, our system will ensure the robust networking of systems. Good authentication practices will secure the system against denial-of-service attacks and penetrations. It will also enable traceback abilities to identify the source of misuse, assuming that the misuse can be detected. However, we will still use fixed/reusable passwords (which leaves a certain level of exposure), which will be managed by avoiding dictionary words and other similar practices. Greater security design can be achieved by using one-time authenticators such as cryptographic tokens, and—in certain constrained user environments—biometrics, at least within supposedly trustworthy subsystems and subnetworks, but this is well outside the scope of this project. We will not allow unauthenticated IP addresses that could be easily spoofed. We will ensure remote sites and remote users are properly identified and authenticated. Meaningful authentication helps restrict many kinds of misuse.

5.1.5 Platform Security Risks

5.1.5.1 Implement, save, and archive logs of all platform access and platform manipulation

The UW team will document and implement mechanisms to control access at all electronic access points to the data sharing infrastructure. These will include technical and procedural controls (e.g., logs, user account reviews, account management, restricted use of shared accounts, passwords) that enforce the authentication and accountability of all user activity. The team will use an access control model whose default setting is to deny access, thereby requiring explicit permission changes to enable access. Similarly, for all access points, we will enable only the ports and services required for approved operations and monitoring. Remote interactive access to a point within the platform will typically have to be accompanied by strong procedural or technical controls to enforce authentication. Electronic or manual processes for monitoring and logging the usage of electronic perimeter access points will be documented and operational at all times. Where technically feasible, these processes will have to detect unauthorized access attempts and alert specified personnel. If no alerting capability exists, the UW team will review the access logs at least every 90 days. The UW team will ensure that only the most limited access privileges are granted to fulfill the business need.

5.1.5.2 Build and conduct vulnerability assessments

To identify areas where potentially hazardous situations could arise, the UW team will conduct a vulnerability assessment of the platform access points to each component of the system at least once a year. That assessment will include the following at a minimum:

- A description of the vulnerability assessment process,
- A discovery analysis of all access points to the data sharing infrastructure,
- A review of ports and services configurations to verify that only the ports and services required for operation of the cyber assets within the perimeter are enabled,
- A review of network and asset accounts, focusing on controls for default accounts.

The findings of these tasks will be documented, a remediation plan will be developed for all discovered weaknesses and faults, and the execution status of that plan will then be reported monthly to the program manager.

5.1.6 Application Security Risks

5.1.6.1 Define and enforce secure change control and configuration management processes.

The UW team will ensure that secure change control and configuration management processes are very clearly defined and followed to ensure that any system changes in the interoperable data sharing environment do not “break” security controls established to protect downstream applications that consume and use the data sharing endpoint.

The team will ensure that new data assets and significant changes to existing data assets do not adversely affect existing security controls or the overall security posture of the system, particularly as they impact downstream consuming applications. The UW team will document and implement processes that help ensure ongoing system security design elements, such as the following:

- Ensuring that all ports and services not required for normal and emergency operations are disabled,
- Tracking, evaluating, testing, and installing applicable infrastructure security patches for all data assets within the platform,
- Testing after the installation of security patches, cumulative service packs, and version upgrades (which are all considered significant changes),
- Using antivirus and malicious software prevention tools, where technically feasible, and
- Defining and enforcing restrictions on who can perform maintenance and repair, emergency procedures, and remote configuration and maintenance.

5.1.6.2 Design configuration unit tests and run them periodically.

Managing change is essential to maintaining a robust ongoing security posture. The UW team will establish and promulgate a change management process that includes unit tests that are consistent with backward compatibility and compliance requirements. At a minimum, this process will test changes in the data sharing system that include adding, modifying, replacing, or removing critical components of the system or the asset hardware, software, or related documentation. The process will also address any vendor- or data producer-related changes to critical data collection mechanisms or data assets. The change management process will also ensure that all documents produced as part of security and safety documentation, assessment, and remediation are kept up to date with current physical and logical configurations. All such documentation will be updated within 90 days of the physical or logical changes.

5.2 Safety Operational Processes, Including Assessment, Mitigation, and Fail-Safe Processes

Operational process gaps leave the door open to an adversary. For instance, failure to conduct a vulnerability assessment of a system when new functionality is introduced may allow a security weakness to go undetected. To provide another example, lack of periodic review of system logs may let a breach go undetected. Therefore, the UW team will institute and follow these proper security processes that are vital to the security of an organization.

This section describes how the project will develop and execute operational processes to control safety risks. This description includes the design of different assessments, mitigation efforts, and fail-safe procedures. Where appropriate, mitigation measures will help control the severity of safety impacts if/when they occur. These may include both design elements that revert to a safe condition (fail-safe) or other types of controls and responses.

Implementation and enforcement of such safety controls and procedures will require defined processes to disseminate them effectively, ensure that they are understood and available at all times, and enforce compliance (e.g., through audits and actions for noncompliance). Over time, organization or environmental changes will require changes to these policies. Defined and documented processes for requesting, evaluating, and approving changes will ensure that the policy remains current and relevant.

5.2.1 People and Policy Security Risks

This subsection discusses how the UW team will use operational processes to manage risks associated with individuals working on the project team and its aligned developers and organizations.

5.2.1.1 Document a brief, clear, high-level policy statement for each issue identified

The UW team will develop and follow high-level policy statements that express three things:

- The data cooperative management’s commitment to the program,
- The high-level direction and requirements for plans and procedures addressing each area, and
- A framework to organize lower-level documents.

5.2.1.2 Define the implementation plan and enforcement mechanisms for all partnering organizations

The UW team will perform a careful rollout of the safety management program, with well-documented policies that are accessible to the data sharing partner organizations and personnel they affect and that clearly communicate the consequences of violating policies to help ensure compliance with those policies.

5.2.2 Insecure Software Development Life Cycle (SDLC) Risks

5.2.2.1 Improve initialization and allocation.

Failures in the initialization of procedures, processes, and indeed stable system and network configuration management represent a large class of system flaws. As a result, the UW team will emphasize consistency checking on entry, determination of suitable availability of appropriate resources, and deletion of possible residues, which are examples of techniques that can improve initialization and allocation.

5.2.2.2 Attend to finalization

A lack of graceful termination and complete deallocation is recognized as a source of flaws. For example, deletion of leftover residues from previous executions is often ignored or relegated to an initialization problem, rather than treated systematically on termination (perhaps on the grounds that it might be avoided altogether in some circumstances). In general, finalization should be symmetrically matched with initialization. Whatever is done in initialization may need to be explicitly undone or at least checked for consistent status at finalization. Programming languages that incorporate garbage collection (GC) attempt to do this implicitly, although not always perfectly. For example, note that Java's finalizers based on pointer unreachability are inherently imprecise. Various other GC-based languages have subtle finalization problems, as do non-GC-based programming languages. Overall, the need for secure and robust finalization remains a research topic, but it will be specifically examined during testing of the software developed for this project.

5.2.2.3 Conduct periodic software risk assessment

To provide insight into the project as new software, capabilities and partners are brought into the project, the UW team will perform periodic risk assessments of the software being developed. Assessments will be performed of each new functional improvement of code both as part of the initial design of the code and then as part of the testing of that code prior to its acceptance. Mitigation will then be performed to account for any vulnerabilities identified in that threat analysis.

5.2.3 Physical Security Risks

5.2.3.1 Perform periodic travel risk assessment through application deployments

The UW team will perform periodic risk assessment and risk mitigation, including traveler threat analysis and vulnerability assessments, to assess the quality and viable interpretation of the data shared by the collaborative through traveler-facing applications. Doing such periodic assessments will help maintain a fresh picture of the effectiveness of the deployment project's data versus travel threats facing the intended population.

5.2.3.2 Redeploy or dispose of protected assets securely.

The UW team will ensure that the redeployment or disposal of physical assets does not inadvertently expose sensitive information to unauthorized entities. For example, if automated imagery collection is done onboard a wheelchair-mounted camera, we will ensure that the redeployment or disposal of the camera and associated storage hardware does not inadvertently expose the imagery information that was previously collected.

5.2.4 Third-party Relationship Risks

The UW ITS4US project will involve a large number of contributing partners. These will include data generators, data vetting organizations and individuals, data service providers, and application developers. The UW team will thoroughly vet these groups and will provide them with safety management training prior to accepting their participation in the project. Assessments of third-party organizational performance will then be performed over the course of the project to ensure that work by individual organizations does not create risks over the course of the system deployment and operation.

5.2.5 Platform Security Risks

5.2.5.1 Log access to system

The UW team will control, monitor, and log all access to protected data assets. Logging helps prevent and understand any unauthorized access to assets and increases the ability to detect unauthorized access to assets. Logging also further enhances the ability to enforce accountability.

5.2.5.2 Document incident-handling policies

The UW team will create and document incident-handling policies, plans, and procedures. This will ensure that the organization is prepared to act quickly and correctly to avert or contain damage after a security incident.

5.2.5.3 Develop contingency plans and procedures

The UW team will create and document contingency plans and procedures. This will ensure that the organization is prepared to act quickly and correctly to recover critical assets and continue operations after a major disruption, should one occur.

5.2.6 Application Security Risks

The UW team will perform threat analysis assessments for each application proposed as part of this project. That assessment will examine identification and authorization tasks, communications protocols, data transfer risks, configuration management, security controls, and where applicable, travel risk assessments for end users of that application.

5.3 Safety Responses

The purpose of the safety response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by doing the following:

- Developing alternative courses of action for responding to risk,
- Evaluating alternative courses of action,

- Determining appropriate courses of action consistent with organizational risk tolerance, and
- Implementing risk responses based on selected courses of action.

While the UW ITS4US deployment project will institute safety response procedures, we also plan to design real-time responses into the data sharing infrastructure. Given the results of some of the designed real-time system analyses described above, it will be possible to trigger automated or semiautomated rapid responses. These will include dynamic alterations of system and network configurations, carefully controlled automated software upgrades in response to detected flaws, and enforced alterations in certain user processes, based on evaluations of the perceived real-time events. (Note that alternative-computation architectures and alternative-routing schemes have a similar objective and outcomes.)

5.4 Safety Reporting

The sections above describe numerous safety assessment and monitoring techniques that this deployment project intends to employ. The safety reporting component is intended to document the assessments and tests in order to accomplish the following:

- Determine the ongoing effectiveness of safety mitigation and responses (consistent with the organizational risk frame),
- Identify safety-impacting changes to organizational information systems and the environments in which the systems operate, and
- Verify that planned safety responses are implemented, and information security requirements derived from, and traceable to, organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

For each safety assessment or test above, the UW team will emphasize communicating and sharing Information, including

- Determining the appropriate method (e.g., executive briefing, risk assessment report, or dashboard) to communicate risk assessment results,
- Communicating risk assessment results to designated organizational stakeholders, and
- Sharing the risk assessment results and supporting evidence in accordance with organizational policies and guidance, including reporting these outcomes to USDOT at an interval to be determined as part of Phase 2 for this project.

6 Safety Management Summary

6.1 Safety Risk Summary

Table 7 provides a summary of the overall areas of risk, their significance to this project, and the operational concept strategies that apply to them. The assessed level of risk is based on the total scores of the controllability, severity, and exposure rankings from Table 5. A combined score for controllability, severity, and exposure of 3 or less is considered a “low hazard”, a 4 is a moderately low hazard, a 5 or 6 is moderately hazardous, and anything above a 6 is very hazardous. The risks identified in Table 7 will be discussed as part of the overall co-design process. The co-design effort includes stakeholders from all five groups (e.g., end users, data collector/generators/providers, and application developers), who will work together to prioritize the design, testing, and implementation of the activities needed to mitigate these risks, based on the importance of the activity and data required to mitigate that risk to the end users, and the technical and financial ability to obtain and publish that data.

Table 7. Safety risk management summary

ID	Safety Risk	Safety Assessment	Safety Operational Concept Strategies	Factors to Monitor	Overall Status
1	Invalid sidewalk data are generated/collected to be shared with consumers	5 (moderate)	Data standard design, Tools for data generation, Operational processes for vetting, Feedback to agencies	Volume of changes produced by vetting activities	Identified
2	Collected sidewalk data do not include all attributes needed to safely route pedestrians	6 (moderate)	Data standard design, Applications designed to account for missing data	Percent of missing values in key fields	Identified
3	Transit service provider generates an invalid transit service schedule	3 (low)	Data standard design, Tools for data generation, Operational processes for vetting, Feedback to agencies	Percent of transit agency submissions returned for errors	Identified

ID	Safety Risk	Safety Assessment	Safety Operational Concept Strategies	Factors to Monitor	Overall Status
4	The transit service schedule reported is out of date	4 (moderately low)	Data standard design, Operational processes for vetting, Feedback to agencies	Number of transit agency submissions listed as out of date	Identified
5	Collected on-demand transit service data do not include all attributes needed to safely route travelers	5 (moderate)	Data standard design, Applications designed to account for missing data	Percent of missing values in key fields	Identified
6	The transit service provider generates invalid transit facility descriptions	2 (low)	Data standard design, Tools for data generation, Operational processes for vetting, Feedback to agencies	Percent of transit agency submissions returned for errors	Identified
7	Collected transit center data do not include all attributes needed to safely route pedestrians	5 (moderate)	Data standard design, Applications designed to account for missing data	Percent of missing values in key fields	Identified
8	User travel preferences are incorrectly applied when determining route identification	3 (low)	Data standard design, Applications designed to account for missing data	Lab tests of Multi-Modal AccessMap	Identified
9	Navigation directions are not understood due to an inability of the application to effectively communicate application outputs.	2 (low)	Data standard design, Applications designed to include easy access to assistance/help	Lab tests of Multi-Modal AccessMap	Identified
10	Navigation directions are incorrectly computed due to an inability of the application to effectively communicate that individual's financial costs for using specific modal or route choices	2 (low)	Data standard design, Applications designed to include easy access to assistance/help, 3rd-party communications with agencies to correctly determine rider eligibility criteria and rider status	Lab tests of Multi-Modal AccessMap	Identified
11	Staff of the transit service provider are inadequately trained, and that information is not passed along to travelers	6 (moderate)	Data standard design, Feedback to transit agencies, Applications designed to include easy access to assistance/help	Percent of missing values in key fields	Identified

ID	Safety Risk	Safety Assessment	Safety Operational Concept Strategies	Factors to Monitor	Overall Status
12	Attributes required by the traveler are not present on a recommended transit service (e.g., no wheelchair tie-downs are available)	5 (moderate)	Data standard design, Applications designed to account for missing data, Applications designed to include easy access to assistance/help.	Percent of missing values in key fields	Identified
13	Emergency response features are not accessible to all travelers (e.g., navigation applications do not have the ability to route users to emergency evacuation routes or to where emergency response equipment, such as a defibrillator, is located.)	6 (moderate)	Data standard design, Feedback to transit agencies, Applications designed to account for missing data, Applications designed to include easy access to assistance/help.	Percent of missing values in key fields Lab tests of Digital Twin	Identified
14	Assistance verifying trip eligibility is not available to staff operating transit services, resulting in denial of travel on those services.	5 (moderate)	Data standard design, Feedback to transit agencies, Applications designed to include easy access to assistance/help.	Percent of missing values in key fields Lab tests of Multi-Modal AccessMap	Identified
15	Application uses too much battery power, causing the end user's device to shut down during a trip.	5 (moderate)	Software design, Applications designed to include easy access to assistance/help.	Lab tests of Multi-Modal AccessMap	Identified
16	Location reference within the application is wrong, causing the navigation instructions to be inaccurate.	4 (moderately low)	Software design, Applications designed to include easy access to assistance/help	Lab tests of Multi-Modal AccessMap	Identified
17	Communications between the application and the data server is lost during a trip	6 (moderate)	Software design, Software/hardware performance tracking and reporting, Applications designed to include easy access to assistance/help.	Field tests of Multi-Modal AccessMap	Identified
18	System security is breached	3 (low)	Software design, Software/hardware performance tracking and reporting	Routine security assessment	Identified
19	System or network latency is too slow	3 (low)	Software design, Software/hardware performance tracking and reporting	System performance assessment	Identified

ID	Safety Risk	Safety Assessment	Safety Operational Concept Strategies	Factors to Monitor	Overall Status
20	System hardware/software resources are overloaded.	3 (low)	Software design, Software/hardware performance tracking and reporting	System performance assessment	Identified

6.2 Continuing Safety Planning

The primary process for continuous safety analysis and planning will come from the co-Design process that is at the core of the systems engineering approach the UW team is applying to this project. The UW team will work with stakeholders throughout the design and development of the system. We will share with those stakeholders the outcome of design work as it occurs. This will allow those stakeholders to continue to provide their insights to the project team throughout the project. Thus, when any of those participating groups or individuals identifies a risk, that risk or hazard will be immediately highlighted to the project team and will be incorporated into both the design and testing work and this Safety Management Plan

Appendix A. Acronyms and Glossary

This appendix includes a list of acronyms and a glossary of key terms used in the document.

Acronym	Definition
AD	Application developer
ADA	Americans with Disabilities Act
AI	Artificial intelligence
API	Application program interface
ATTRI	Accessible Transportation Technologies Research Initiative
BAA	Broad Area announcement
ConOps	Concept of Operations
COVID	Coronavirus disease
DG	Data generator
DMP	Data Management Plan
DOT	Department of transportation
DRSB	Deployment Readiness Summary Briefing
DS	Data service provider
DU	Digital device end user experiencing travel barriers
ETRA	Enabling Technology Readiness Assessment
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
GIS	Geographic information systems
GOFS	General On-Demand Transit Feed Specification
GTFS	General Transit Feed Specification
GTFS-Flex	The Flex route extension to the General Transit Feed Specification, designed to describe demand-responsive or paratransit service
GTFS-Pathways	The Pathways extension to the General Transit Feed Specification which defines pathways linking together locations within stations
HUA	Human Use Approval
ICTDP	Integrated Complete Trip Deployment Plan
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IRB	Internal Review Board
ISO	International Organization for Standardization
IT	Information technology
ITS	Intelligent transportation system
ITS JPO	Intelligent Transportation Systems Joint Programs Office
ITS4US	The name of a USDOT program to enable communities to showcase innovative business partnerships, technologies, and practices that

Acronym	Definition
	promote independent mobility for all that is led by the Intelligent Transportation Systems Joint Program Office with support from the Office of the Secretary of Transportation, Federal Transit Administration, and Federal Highway Administration.
LEP	Limited English proficiency
LiDAR	Light detection and ranging
MARC	Mid-Atlantic Regional Council
MOOVEL	A software services provider to transit agencies
MVP	Minimum viable product
OGC	Open Geospatial Consortium
OST	Office of the Secretary
PII	Personally Identifiable Information
PMESP	Performance Measurement and Evaluation Support Plan
PMP	Project Management Plan
PPNA	Personalized pedestrian network analysis
PTSEP	Participant Training and Stakeholder Education Plan
REST API	Representational State Transfer Application Program Interface
ROI	Return on investment
SEMP	Systems Engineering Management Plan
SMP	Safety Management Plan
SyRS	System Requirements Plan
Taskar Center or TCAT	Taskar Center for Accessible Technology at the University of Washington
TCRP	Transportation Cooperative Research Program
TDEI	Transportation Data Equity Initiative
TRAC	Washington State Transportation Center at the University of Washington
TSP	Transportation service provider
U.S.	United States
U.S. DOT	United State Department of Transportation
USGS	United States Geological Survey
UW	University of Washington
VA	Veterans Affairs
W3C	World Wide Web Consortium
AD	Application developer

Appendix B. Crosswalk Between Operational Scenarios and Functional Components

This appendix shows a crosswalk between the operational scenarios presented in the Concept of Operations document and the basic functional tasks that are used in Chapter 3 to organize the safety management activities for the TDEI.

Scenario	Data Collection	Transmission of Data to Central Repositories	Quality Assurance Activities	Operation of the Central Repository	Provision of Data By Central Repository	Use of Information By Travelers
1) Sidewalk data generation, collection, and vetting.	X	X	X	X	N/A	N/A
2) Vetting of sidewalk data and street crossing identification.	X	X	X	X	N/A	N/A
3) Generation and vetting of GTFS-Pathways data.	X	X	X	X	N/A	N/A
4) Generation and vetting of GTFS-Flex data.	X	X	X	X	N/A	N/A

Scenario	Data Collection	Transmission of Data to Central Repositories	Quality Assurance Activities	Operation of the Central Repository	Provision of Data By Central Repository	Use of Information By Travelers
5) Individual with mobility disability uses verified sidewalk and transit data to navigate through several cities.	N/A	X	X	X	X	X
6) Veteran with mobility disability traveling from a rural home to the Veterans Affairs (VA) hospital for a medical appointment.	N/A	X	X	X	X	X
7) Blind, vision disabled, or deafblind individual uses verified sidewalk and transit data.	N/A	X	X	X	X	X
8) Multilingual tourist tries to conduct pre-trip planning for a multilevel transit station.	N/A	X	X	X	X	X
9) Low-income traveler utilizes a third-party application (One-Call/One-Click Service) to reach a destination.	N/A	X	X	X	X	X
10) Travelers with sidewalk preferences utilize data generated by a city government.	X	X	X	X	X	X
11) Travelers with sidewalk preferences utilize data generated by civic organization.	X	X	X	X	X	X
12) Travelers with sidewalk preferences utilize data generated by an aerial mapping company’s analytics engine for aerial images.	X	X	X	X	X	X
13) Transit users utilize GTFS-Flex and GTFS-Pathway extensions through a navigation application.	N/A	X	X	X	X	X

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-21-874

U.S. Department of Transportation