Safety Management Plan (SMP)

for the Smart Columbus
Demonstration Program

REVISED REPORT | April 1, 2019

Produced by City of Columbus

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.

Acknowledgement of Support

This material is based upon work supported by the U.S. Department of Transportation under Agreement No. DTFH6116H00013.

Disclaimer

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

Abstract

This document presents the Safety Management Plan for the Smart Columbus demonstration program. The Smart Columbus demonstration program goal is to advance and enable safe, interoperable, networked wireless communications among vehicles, the infrastructure, and travelers' personal communications devices and to make surface transportation safer, smarter, and greener. The purpose of this document is to identify the major safety risks associated with the Smart Columbus demonstration program and lay out a plan to promote the safety of the participants and surrounding road users including drivers, pedestrians, bicyclists, and transit riders. The plan describes the potential safety risk scenarios related to the program and project applications proposed, assesses the level of risk for each safety scenario using the Automotive Safety Integrity Level (ASIL) process defined by international standard ISO 26262, provides mitigation strategies and puts forth a safety operational concept for the Smart Columbus demonstration program. This document also discusses coordination with other Smart Columbus demonstration program tasks.

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

1.1. SAFETY MANAGEMENT PLAN INTRODUCTION

The Safety Management Plan (SMP) for the Smart Columbus Demonstration Program is a companion document to the program and project-level systems engineering documents, including various Smart Columbus Project Concept of Operations (ConOps), System Requirements (SySR), Program Data Management Plan (DMP), Data Privacy Plan (DPP), a Human Use Approval Summary, and Performance Measurement Plan. It is the key document which outlines how each project ensures the safety of travelers and users of the various systems contained in the demonstration, and the security of the system data and communications.

This document follows the principles of assigning an Automotive Safety Integrity Level (ASIL) to the identified safety scenarios for each project, as the International Organization for Standardization (ISO) standard 26262 outlines. The authors also sought input from the eight Smart Columbus program project teams to identify and assess safety issues, their impacts and strategies to mitigate them. The result is a reference document for the eight Smart Columbus project teams to use to design their project deployments to avoid potential safety risks from the vehicles and infrastructure, and to protect the safety of travelers. This plan identifies the major safety issues associated with each project and lays out a preliminary plan to promote the safety of participants, motorists and other road users such as pedestrians, bicyclists, and transit riders.

The plan accomplishes these goals by describing the underlying needs of the demonstration with respect to participant and traveler safety. It also documents the impacts of various scenarios at program and project levels, for example power outages, communication failures, unintended or malicious attacks, severe crashes, and adverse weather conditions. It assesses each risk, provides and documents the guidance on designing a safety-critical system that is capable of either eliminating these risks from the design, reducing the risks by modifying the design to lower the probability of the occurrence of the hazard, or at minimum, mitigating the impact of the hazard if it does occur.

The Smart Columbus Program Management Office (PMO) and project teams recognize the importance of safety for users of the smart vehicles, applications, and infrastructure this program will deploy. Although the teams will design and implement the project systems to be as fail-safe as possible, they cannot eliminate all potential for hazard due to unforeseen events.

As a federal research project, an Institutional Review Board (IRB) must provide oversight for Smart Columbus projects. Formal informed-consent documents, which the IRB will approve, will add a level of safety by informing participants of their responsibilities and risks, and by implementing adequate training in the use of the connected devices. To further ensure safety, the Smart Columbus PMO and project teams will continue to evaluate additional enablers to improve participants interactions with the systems. For example, a help line will be considered to assist connected vehicle drivers and multimodal travelers using smartphone-based applications.

As a pilot for smart cities, the SMP needs to be built into the design rather than tacked as an afterthought. The development of the smart vehicles, applications and infrastructure follow fault-tolerant or fail-safe procedures to eliminate or minimize the risk of faults and failures. The success of this demonstration depends on the public's acceptance that the safety of both the users and non-users of these technologies is enhanced and, at the very least, not endangered.

1.2. DOCUMENT OVERVIEW

This document includes the following chapters, which detail the Smart Columbus program's safety-critical system that is designed to address various, potential risks from project demonstration:

- **Chapter 1. Introduction** introduces the SMP.
- **Chapter 2. Smart Columbus Program** describes the demonstration program, its goals and vision and introduces the program's eight projects.
- **Chapter 3. Safety Risk Process and Approach** explains the program's overall approach to safety risk management as ISO 26262 outlines.
- **Chapter 4. Safety Needs** provides analysis and assessment of the safety scenarios identified within the Smart Columbus projects.
- **Chapter 5. Safety Operational Concept** explains the program's safety operational concept including its functional requirements, SMP and systemwide fail-safe mode.
- **Chapter 6. Coordination with Other Tasks** describes how this SMP coordinates with related program tasks.
- **Chapter 7. Conclusions** summarizes this document's conclusions.

1.3. REFERENCES

Table 1 lists the documents and literature this document used to gather information.

Table 1: References

Doc. No.	Title	Rev.	Pub. Date
–	Integrating Intelligent Driver Warning Systems: Effects of Multiple Alarms and Distraction on Driver Performance http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E7907EDF6BF9081A68F3D9C0813658AE?doi=10.1.1.353.9940&rep=rep1&type=pdf	–	Nov. 15, 2005
–	Ohio Manual of Uniform Traffic Control Devices. Ohio Department of Transportation http://www.dot.state.oh.us/Divisions/Engineering/Roadway/DesignStandards/traffic/OhioMUTCD/Pages/OMUTCD2012_current_default.aspx	–	Jan. 13, 2012
	Preparing a Safety Management Plan for Connected Vehicle Deployments https://www.its.dot.gov/pilots/pdf/CVP-Tech-Assistance-Webinar-Safety-Management_Final.pdf	–	Dec. 7, 2015
–	Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan – ICF/Wyoming https://rosap.ntl.bts.gov/view/dot/30734	–	March 14, 2016

Doc. No.	Title	Rev.	Pub. Date
–	Central Ohio Transit Authority (COTA) – Long Range Transit Plan https://www.cota.com/wp-content/uploads/2016/04/LRTP.pdf	–	April 2016
–	Connected vehicle pilot deployment program phase 1, Safety Management Plan – Tampa (THEA) https://rosap.ntl.bts.gov/view/dot/30733	–	April 6, 2016
–	NYC CV Pilot Deployment: Safety Management Plan: New York City https://rosap.ntl.bts.gov/view/dot/31726	–	April 22, 2016
–	USDOT Guidance Summary for Connected Vehicle Pilot Site Deployers: Safety Management. Contract No. DTFH61-11-D-00018 https://rosap.ntl.bts.gov/view/dot/31556	–	July 1, 2016
–	Opportunities and Challenges of Smart Mobile Applications in Transportation https://www.sciencedirect.com/science/article/pii/S2095756416302690	–	Nov. 9, 2016
–	City of Columbus Americans with Disabilities Act (ADA) Rules and Regulations https://www.columbus.gov/publicservice/Design-and-Construction/document-library/Curb-Ramp-Construction/	–	April 1, 2018
–	Low-Speed Automated Shuttles: State of the Practice Final Report https://rosap.ntl.bts.gov/view/dot/37060	–	Sept. 9, 2018
	ISO 26262, Road Vehicle Functional Safety Standards		Nov, 2011
–	Traffic Signal Design Manual. City of Columbus, Department of Public Service https://www.columbus.gov/WorkArea/DownloadAsset.aspx?id=2147506380	–	Oct. 1, 2018

Source: City of Columbus

Chapter 2. Smart Columbus Program

2.1. INTRODUCTION

The U.S. Department of Transportation (USDOT) pledged $40 million to the City of Columbus (COC) as the winner of the Smart City Challenge (SCC). By challenging American cities to use emerging transportation technologies to address their most pressing problems, USDOT aimed to spread innovation through a mixture of competition, collaboration and experimentation. The SCC called on cities to do more than merely introduce new technologies onto city streets. It called on them to boldly envision new solutions that would change the face of transportation in our cities by closing the gap between rich and poor, capturing the needs of both young and old, and bridging the digital divide through smart design so that the future of transportation meets the needs of all city residents.

As the winner of the SCC, the Smart Columbus program will demonstrate how advanced technologies can be integrated into other operational areas within the COC, utilizing advancements in Intelligent Transportation Systems (ITS) and connected, and autonomous electric vehicle technologies to meet these challenges, while integrating data from various sectors and sources to simultaneously power these technologies while leveraging the new information they provide. Community and customer engagement will be present throughout the program, driving the requirements and outcomes for each project. This end-user engagement reinforces the idea that, ultimately, the residents of Columbus are the owners and co-creators of the Smart Columbus program.

2.2. PROJECT DESCRIPTION AND GOALS

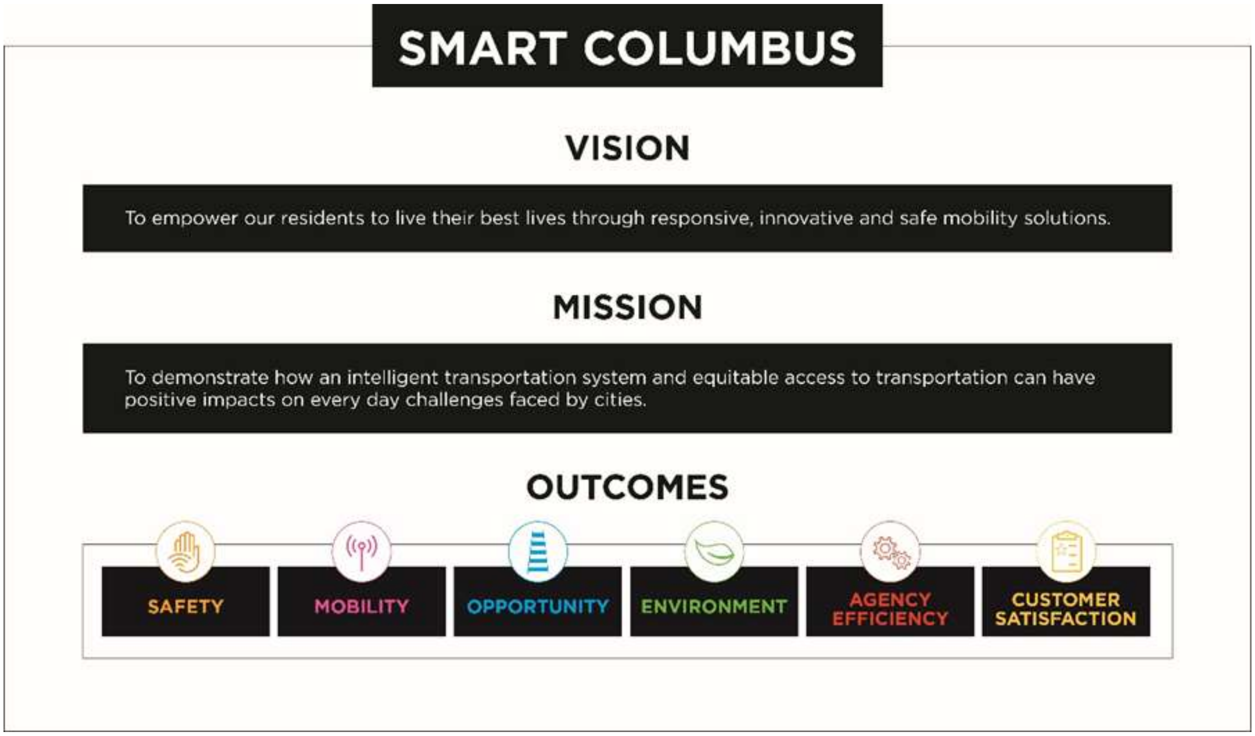
The COC established the following vision and mission for its strategic Smart Columbus program:

- **Smart Columbus Vision:** Empower residents to live their best lives through responsive, innovative, and safe mobility solutions.
- **Smart Columbus Mission:** Demonstrate how equitable access to transportation can have positive impacts of every day challenges faced by cities.

The Smart Columbus program includes the following outcomes:

- **Improve Safety:** Columbus wants to create safer streets where vehicles, cyclists and pedestrians are less likely to be involved in accidents.
- **Enhance Mobility:** Columbus wants to make traversing the city and parking as efficient and convenient as possible.
- **Enhance Access to Opportunities and Services:** Columbus wants to make multimodal transportation options and the ability to access them equitably available to all residents; especially those who need to access to opportunities related to health care, jobs, school, and training.
- **Reduce Environmental Impact:** Columbus wants to reduce the negative impact transportation has on the environment through becoming more efficient and embracing multimodal options.
- **Agency Efficiency:** Columbus wants to provide tools and access to the data generated by the projects to improve operations and efficiency of the city services.
- **Customer Satisfaction:** Columbus wants to provide resources and information to the citizens to increase their satisfaction with city services through the use and application of technology.

Figure 1 shows the Smart Columbus vision, mission, and outcomes.



SMART COLUMBUS

VISION

To empower our residents to live their best lives through responsive, innovative and safe mobility solutions.

MISSION

To demonstrate how an intelligent transportation system and equitable access to transportation can have positive impacts on every day challenges faced by cities.

OUTCOMES

SAFETY | MOBILITY | OPPORTUNITY | ENVIRONMENT | AGENCY EFFICIENCY | CUSTOMER SATISFACTION

Figure 1: Smart Columbus Vision

Source: City of Columbus

The Smart Columbus program organized these new capabilities into three focus areas addressing unique user needs: Enabling Technologies, Enhanced Human Services (EHS), and Emerging Technologies.

- **Enabling Technologies:** These advanced technologies use new and innovative ways to enhance safety and mobility of the transportation infrastructure. These technologies allow deployments that increase our capabilities with rich data streams and infrastructure that can respond on demand. The CV Environment (CVE) improves safety using cutting-edge technology that advances the sustainable movement of people and goods.
- **EHS:** These services encompass meeting human needs through technology applications that focus on preventing and remediating problems and improving users' overall quality of life with technology-based solutions. EHS projects create opportunity by improving access to jobs, health care, and events.
- **Emerging Technologies:** These are new and developing technologies that will substantially alter the business and social environments within the next five to 10 years. By focusing on key emerging technologies, the city can demonstrate potential future solutions to transportation and data-collection challenges.

2.3. PROJECT DESCRIPTIONS

Figure 2 summarizes the Smart Columbus Operating System (Operating System) and portfolio of USDOT projects. It depicts the criticality of the Operating System tying together these three themes, as well as the supporting projects. It also shows how the documentation and management of the overall program, anchored by the tools and documentation used in coordination and cooperation between the COC and USDOT.

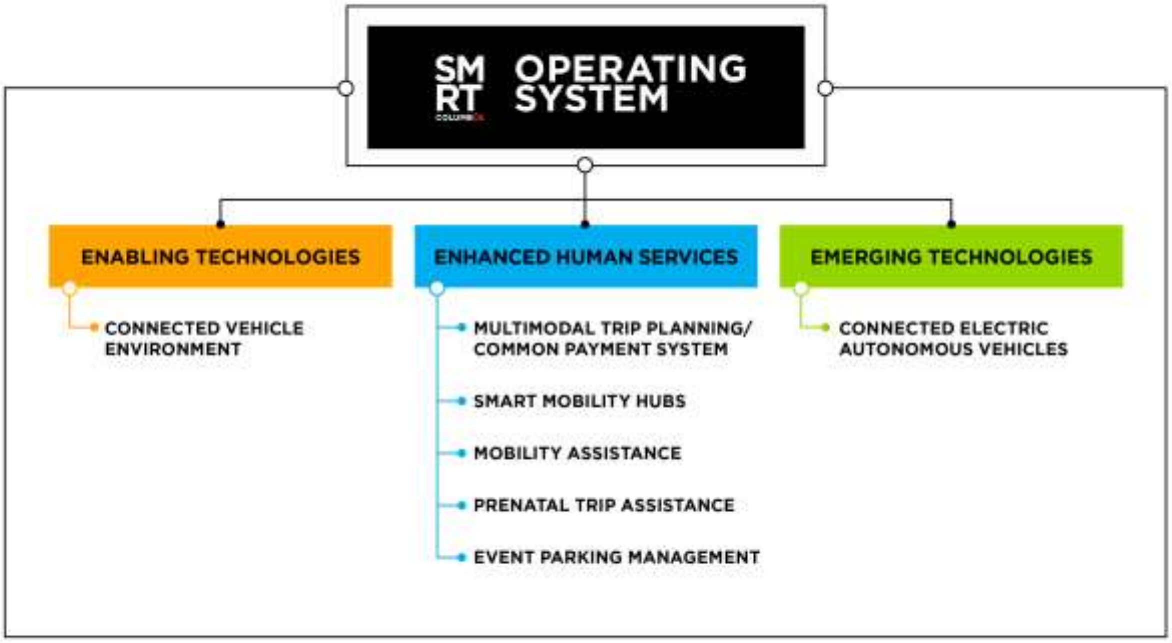


Figure 2: Smart Columbus Framework

Source: City of Columbus

2.3.1. Smart Columbus Operating System

The Operating System is envisioned as a web-based, dynamic, governed data delivery platform built on a federated architecture that is at the heart of the Smart Columbus system. It will ingest and disseminate data while providing access to data services from multiple sources and tenants, including the planned Smart Columbus technologies, traditional transportation data and data from other community partners, such as food pantries and medical services. The Operating System will embody open-data, best-of-breed technologies including open-source and commercial off-the-shelf concepts that enable better decision-making and problem solving for all users. It will support a replicable, extensible, sustainable data delivery platform. The Operating System will be the source for performance metrics for program monitoring and evaluation; serve the needs of public agencies, researchers and entrepreneurs; and assist health, human services organizations and other agencies in providing more effective services to their clients. The Operating System will be scalable and demonstrate the potential for serving city and private sector needs well beyond the life of the SCC award period.

2.3.2. Enabling Technologies

2.3.2.1. CONNECTED VEHICLE ENVIRONMENT

Columbus has corridors and intersections with high numbers of crashes involving vehicles, bicyclists, and pedestrians, and several congested corridors have poor mobility for emergency vehicles, freight, and transit buses. The project team selected the CVE corridors based on regional crash data, enhanced transit services, recent infrastructure investments, and their relationships to other Smart Columbus projects.

The CVE will connect up to1,800 vehicles and 113 smart intersections across the region. The project team plans to install safety applications for multiple vehicle types including transit buses, first responder vehicles, city and partner fleet vehicles, and private vehicles. Application deployments will ensure that emergency vehicles and the Central Ohio Transit Agency (COTA) bus rapid transit (BRT) fleet can utilize signal prioritization as needed to maximize safety and efficiency. The data created by the system will be aggregated by the Operating System, anonymized, de-identified and stored for historical analysis and visualization.

The CVE project will utilize CV technologies and applications with an emphasis on addressing congested and high-crash intersections and corridors. The project team anticipates the CVE project outcomes will include enhanced safety and mobility throughout the COC's transportation system.

2.3.3. Enhanced Human Services

2.3.3.1. MULTIMODAL TRIP PLANNING APPLICATION/COMMON PAYMENT SYSTEM

Columbus residents and visitors do not have access to a system that allows for the seamless planning of or paying for a trip involving multiple transportation service providers and parking providers. Moreover, some Columbus residents are unbanked and therefore cannot access alternative modes of transportation including car and bike sharing systems

The Multimodal Trip Planning Application (MMTPA) will make multimodal options easily accessible to all by providing a robust set of transit and alternative transportation options including routes, schedules, and dispatching possibilities. The application will allow travelers to request and view multiple trip itineraries and make reservations for shared-use transportation options such as bikeshare, transportation network companies (TNC) and carshare. Using the multimodal trip planning application, users will be able to compare travel options across modes, plan and pay for their travel based upon current traffic conditions and availability of services

A Common Payment System (CPS) will process payments for transportation service and parking providers. The city’s goal for the CPS application, which may be the first of its kind in the United States, is that the public will use it to access Columbus’ current and future transportation systems, maximizing these services to live their best lives.

This project is anticipated to provide an innovative solution to improve mobility and access to opportunity.

2.3.3.2. SMART MOBILITY HUBS

Currently, no enhanced mobility or multimodal transit features alleviate first-mile/last-mile (FMLM) challenges in the Linden area or along the Cleveland Avenue corridor. Columbus is working to make mobility a great equalizer in part by embracing multimodal transportation and making it as accessible and easy to use as possible. Our vision is to transform some COTA bus stops along the BRT CMAX corridor and transit centers into smart mobility hubs, where someone getting on or off the bus can easily access the next leg of his or her trip. Public Wi-Fi will be a key enabler for the hub and its points of connection (Wi-Fi is also present in COTA's stations, CMAX, and buses). The city plans to outfit the hubs with kiosks to assist in travel planning and expanded transportation options via other modes, such as bike and car-sharing. The smart mobility hubs will be linked with COTA systems to provide transit information with real-time arrival and departure times to the passengers waiting at the hubs. This project will also explore the utility of these hubs in the commercial district, which faces similar FMLM challenges in connecting travelers to their destinations.

This project provides an opportunity for residents and visitors to access multiple modes of travel to solve FMLM challenges.

2.3.3.3. MOBILITY ASSISTANCE FOR PEOPLE WITH COGNITIVE DISABILITIES

People with cognitive disabilities who wish to independently use public transit services in Columbus must either qualify for special paratransit services in accordance with federal law, or they must be able to safely use fixed-route bus service without assistance. The city's goal for the Mobility Assistance for People with Cognitive Disabilities (MAPCD) application is that it will allow people with cognitive disabilities to travel independently via COTA's fixed-route bus system. The mobile application will feature a highly accurate, turn-by-turn navigator designed to be sufficiently intuitive such that senior adults and people with cognitive disabilities and visual impairments can use it to travel independently.

This project provides an opportunity for users to empower themselves and gain mobility independence and not rely upon caregivers or the COTA paratransit system for transportation.

2.3.3.4. PRENATAL TRIP ASSISTANCE

The COC has one of the highest infant mortality rates in the country, which is partially caused by pregnant women not getting necessary prenatal healthcare. The existing Non-Emergency Medical Transportation (NEMT) system does not always provide reliable round-trip transportation. Linden residents have challenges accessing healthcare services due to the current NEMT model and technologies. The goal of the Prenatal Trip Assistance (PTA) project is to work with Franklin County and CelebrateOne to develop a means for bridging the gap among healthcare providers, expectant mothers and NEMT services that are paid for through the Medicaid system. A driving force for deployment of this project is the need to provide a more streamlined and efficient NEMT system to improve mobility and satisfaction for users.

2.3.3.5. EVENT PARKING MANAGEMENT

The COC lacks an integrated system for residents and visitors to view easily and efficiently the available parking spaces at parking garages, surface lots and parking meters; especially at large events. Indirect routing of travelers causes congestion and inefficiency in the transportation network.

This project will integrate parking information from multiple providers into a single availability and reservation services solution. This will allow travelers to plan and search for parking options at certain locations to reserve and book a parking space with the CPS. More direct routing of travelers during large events is expected to reduce congestion during those times.

2.3.4. Emerging Technologies

2.3.4.1. CONNECTED ELECTRIC AUTONOMOUS VEHICLES

The use of connected and autonomous shuttles has been widely proposed as a solution to the FMLM problem. Therefore, this project will address, investigate and develop solutions to the social and technical challenges associated with the use of Connected Electric Autonomous Vehicles (CEAV) technology for safer and more efficient access to jobs in a smart city.

This project will introduce and develop holistic modeling and simulation tools that will enable a priori determination and solution of connected and autonomous mobility technical challenges including the actual route and other vehicles and mobility improvements. This will be followed by proof-of-concept work and pilot deployments to demonstrate that connected and autonomous mobility can be used to improve the FMLM access to jobs in a smart city.

The team will conduct the CEAV project with partners from the Ohio Department of Transportation (ODOT), The Ohio State University (OSU) and The Columbus Partnership to plan, implement and evaluate the deployment of autonomous vehicles in the COC. Working with these partners allows for the generation of various use cases, which will result in the deployment of CEAVs in various settings including a university and corporate campuses.

This project provides an opportunity for residents and visitors to access cutting edge mobility technologies to solve FMLM challenges.

2.3.5. Deployment Area

While the COC will deploy some projects within specific areas, it will deploy many projects citywide, integrating them with the Operating System, which is the backbone and heart of all current and future Smart Columbus projects.

Figure 3 shows an overview of the deployment area.

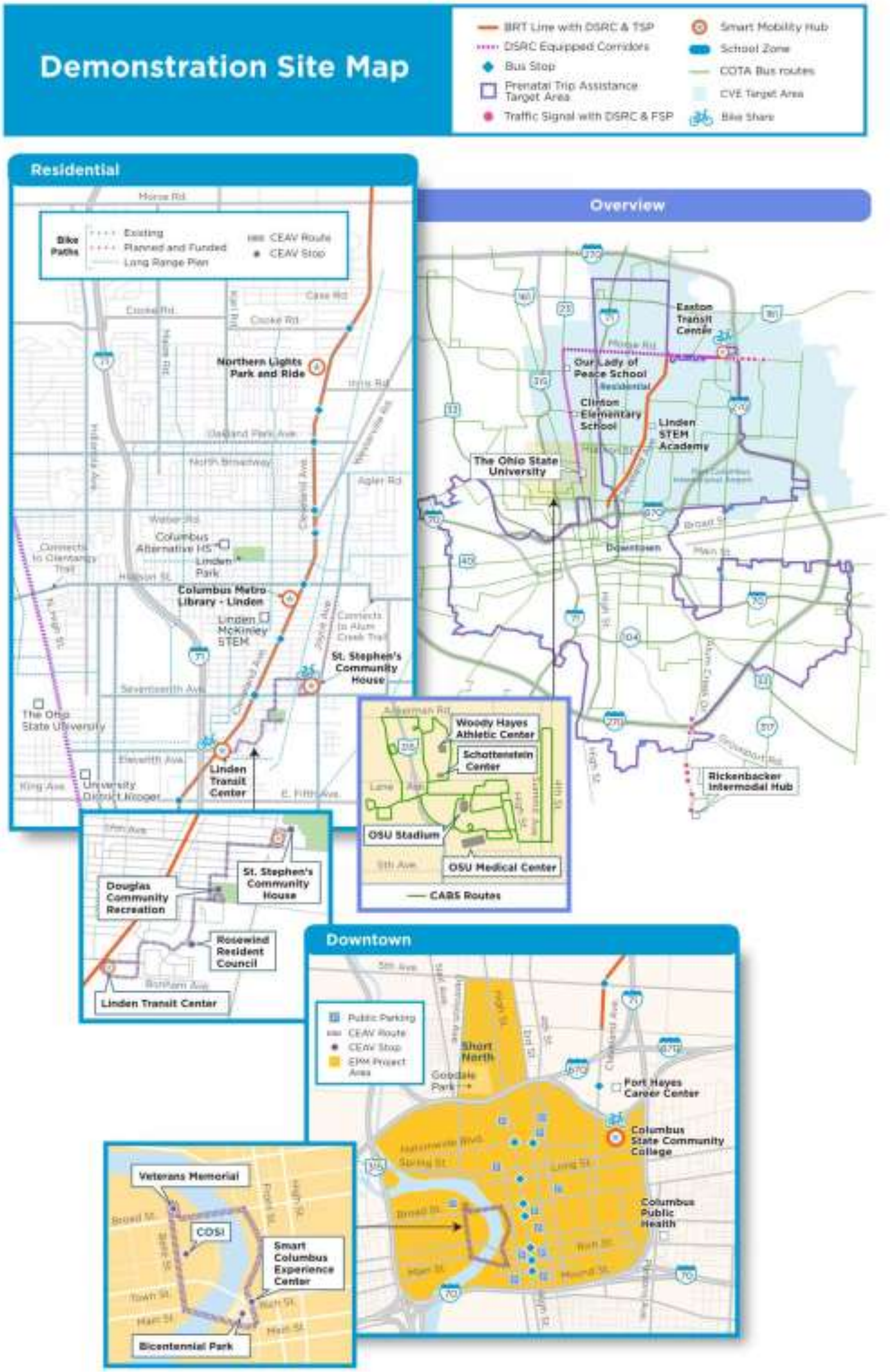


Figure 3: Smart Columbus Deployment Map

Source: City of Columbus

Table 2 identifies the relationships among the demonstration projects and their potential outcomes.

Table 2: Smart Columbus Project Outcomes

Smart Columbus Project	Safety Outcomes	Mobility Outcomes	Opportunity Outcomes	Environment Outcomes*	Agency Efficiency Outcomes	Customer Satisfaction Outcomes
1. Smart Columbus Operating System					X	X
2. Connected Vehicle Environment	X	X		X		
3. Multimodal Trip Planning Application/Common Payment System		X	X	X		X
4. Mobility Assistance for Cognitive Disabilities		X	X	X	X	X
5. Prenatal Trip Assistance		X	X	X		X
6. Smart Mobility Hubs		X		X		X
7. Event Parking Management		X		X		X
8. Connected Electric Autonomous Vehicles		X	X	X		X

**Indicates program level objectives*

Source: City of Columbus

Chapter 3. Safety Risk Process and Approach

3.1. INTRODUCTION

This section describes the safety risk process and approach for Smart Columbus project deployments and the procedures the Smart Columbus PMO and project teams will use to manage safety risks.

3.2. SAFETY RISK PROCESS AND APPROACH

Deployments will include a structured approach to identifying safety risks within the eight Smart Columbus projects, and the program will mitigate those risks to keep participants safe. As the program proceeds from planning to design and implementation, and then to operations and maintenance, the approach to managing safety risks will continue to evolve, identifying new risks, and either mitigating completely the currently identified risks or changing their statuses. The process that the team develops and utilizes will produce periodic updates to the risk assessment table (see **Table 11**) to reflect current and emerging mitigation efforts.

The approach adapts the steps in ISO 26262 for developing a safety plan in the concept phase. During the systems engineering phase, the Smart Columbus PMO and project teams worked to develop the safety-related requirements for each project. As the projects move into design and implementation, this plan will verify and implement these requirements. The development of this SMP followed the USDOT guidelines originally distributed to the CV Pilot Projects. The first two steps of the process shown in **Figure 4** are the focus, although initial documentation regarding the definition of the safety operational concept has started.

- Identify safety scenarios for the eight Smart Columbus projects based on the proposed applications defined in the ConOps of each project.
- Assess the level of risk for each safety scenario.
- Develop a safety operational concept for each scenario if it is identified as high/medium risk.

Figure 4 illustrates the development process for the safety scenarios.

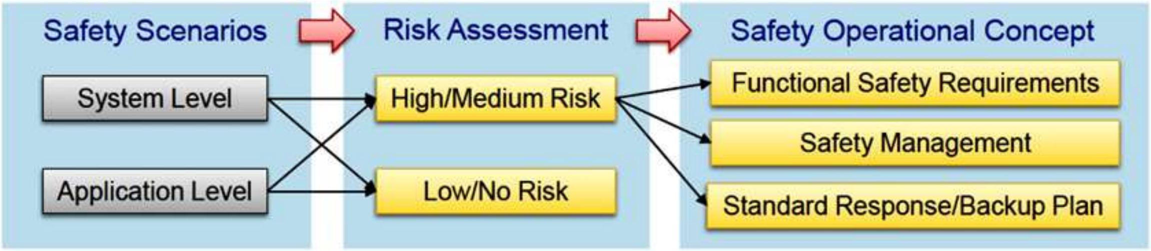


Figure 4: Safety Management Plan Development Process

Source: USDOT Guidance Summary for Connected Vehicle Deployments: Safety Management

3.3. SAFETY STAKEHOLDERS

Table 3 lists in no certain order the safety stakeholders for the eight Smart Columbus program projects. As travelers, participants fall into broad categories of drivers, pedestrians and transit users and are not treated here. Project participants will receive instruction through the individual projects according to the human use treatments, Informed Consent Documents and participant training programs. The project stakeholders listed in **Table 3** are supporting participants in their travel and extending their services to meet participant needs. **Table 3** summarizes the safety stakeholders who are providing services to the project participants and to identify multiple-project involvement, responsibility and safety management.

Table 3: Smart Columbus Safety Stakeholders by Project

Stakeholder	Smart Columbus Operating System	Connected Vehicle Environment	Multimodal Trip Planning Application/ Common Payment System	Mobility Assistance for Cognitive Disabilities	Prenatal Trip Assistance	Smart Mobility Hubs	Event Parking Management	Connected Electric Autonomous Vehicles
City of Columbus Police		✓		✓	✓	✓	✓	✓
City of Columbus Fire, Emergency Medical Services		✓		✓	✓	✓	✓	✓
City of Columbus Dept. of Public Service Traffic Managers	✓	✓	✓				✓	✓
City of Columbus Department of Technology	✓	✓	✓	✓	✓	✓	✓	✓
City of Columbus Light-Duty Vehicle Operators		✓						
City of Columbus Car-Share Vehicle Operators			✓		✓	✓		

Stakeholder	Smart Columbus Operating System	Connected Vehicle Environment	Multimodal Trip Planning Application/ Common Payment System	Mobility Assistance for Cognitive Disabilities	Prenatal Trip Assistance	Smart Mobility Hubs	Event Parking Management	Connected Electric Autonomous Vehicles
Logistics Providers		✓						
COTA (Fixed-Route Paratransit)		✓	✓	✓		✓		
COTA (Supervisor Vehicle)		✓						
Mobility Providers	✓		✓			✓		
Third-Party Users	✓		✓					
Certification and Accreditation Provider	✓		✓					
Metro Library – Linden Branch						✓		
St. Stephens Community House						✓		
Columbus State Community College						✓		
Third Party Developer or Application	✓			✓	✓	✓	✓	
Prenatal Travelers/Application Users					✓			
NEMT Providers – TNCs and COTA, Taxis/Limo					✓			

Stakeholder	Smart Columbus Operating System	Connected Vehicle Environment	Multimodal Trip Planning Application/ Common Payment System	Mobility Assistance for Cognitive Disabilities	Prenatal Trip Assistance	Smart Mobility Hubs	Event Parking Management	Connected Electric Autonomous Vehicles
Managed Care Organizations					✓			
Ohio State University (Safety Study)					✓			
Ohio Department of Medicaid					✓			
Medical Offices					✓			
Parking Facilities and Parking Operators							✓	
Clinton Township Police						✓		
Clinton Township Fire						✓		
Franklin County Sheriff		✓		✓	✓	✓	✓	✓
Franklin County Fire Rescue, Emergency Medical Services (EMS)		✓		✓	✓	✓	✓	✓

Source: City of Columbus

3.4. EMERGENCY RESPONDER COORDINATION

Agencies within the State of Ohio, Franklin County, COC and other associated localities have their own emergency response plans for various events, such as severe incidents, natural disasters, or planned events. The Smart Columbus PMO and project teams will coordinate with emergency responders on what actions are expected from both the agencies and the deployment program (e.g., safety manager(s)) in response to the emergency situations identified in this SMP.

Should a vehicle or pedestrian in the deployment be involved in a crash due to any cause, the response will follow existing emergency response procedures. As with any emergency involving a vehicle, multimodal traveler or pedestrian, an available person will call 911, and COC responders will perform according to their standard training. **Table 4** lists the emergency response agencies along with their operation timings.

Table 4: Emergency Response Stakeholders

Agency	Response Hours
COC Police	24 hours x 7 days
COC Fire Rescue	24 hours x 7 days
COC EMS	24 hours x 7 days
Franklin County Sheriff	24 hours x 7 days
Franklin County Fire Rescue	24 hours x 7 days
Franklin County EMS	24 hours x 7 days
Ohio Highway Patrol	24 hours x 7 days
COC Traffic Operations and Maintenance	24 hours x 7 days
COC Traffic Management Center	Mon-Fri 6:30am-6:30pm
Smart Columbus Demonstration Program Operations and Maintenance	Mon-Fri 5am-6:30pm
Clinton Township Police	24 hours x 7 days
Clinton Township Fire	24 hours x 7 days

Source: City of Columbus

Chapter 4. Safety Needs

The safety needs were considered from the perspective of the travelers (travelers for Smart Columbus includes CV and CEAV vehicle operators, multimodal travelers, prenatal travelers, and people with cognitive disabilities) using the solutions being developed and deployed as part of the Smart Columbus demonstration program. Each project will provide a system of hardware and/or software. Some projects, such as CVE and CEAV, contain applications that will have interfaces to other specialized equipment in the deployment, existing infrastructure, and people using the solutions (drivers or riders). Other projects will provide a strictly software solution which will have several types of traveler interfaces available (mobile, web, voice, etc.). Regarding the projects that contain both hardware and software elements, the solutions deployed for each of the projects could present a hazard due to an internal failure of one of its components, or because of failures in one of the external elements with which it interfaces. Software solutions can present a hazard with respect to protection of traveler data or availability of the application.

Each project's solutions must perform its functions in ways that do not introduce new risks. They must do so regardless of whether their functions are operating as intended or malfunctioning due to internal failures, external failures, or foreseeable misuse. This SMP identifies and assesses user safety needs and safety problems that may arise and offers safety mitigations that need to be decomposed into functional requirements and, then, design solutions. System requirements are written in the project SyRS document. This SMP does not offer design solutions but lays out the overarching strategies intended to bring about requirements that lead to designs that work and, when they do fail, fail safely. While is not possible to design entirely safe systems or ones with complete backup, redundancy and error-checking at every step, it is the intention of the SMP to make the use of the hardware and software systems it deploys helpful to users and safe to use.

Table 5 summarizes the software and hardware uses in the projects.

Table 5: Hardware and Software Uses

Project	Software	Hardware
Smart Columbus Operating System	Operating System	Data storage
Connected Vehicle Environment	CV Applications	OBU, RSU
Multimodal Trip Planning Application/Common Payment System	Smartphone Application	Smartphone
Mobility Assistance for Cognitive Disabilities	Smartphone Application	Smartphone
Prenatal Trip Assistance	Smartphone Application	Smartphone
Smart Mobility Hubs	SMH Software	Kiosk
Event Parking Management (EPM)	Smartphone Application	Smartphone
Connected Electric Autonomous Vehicles	CEAV Software	CEAV Lidar, etc.

Source: City of Columbus

4.1. IDENTIFY SAFETY SCENARIOS

The intent of the safety scenarios is to identify, and document potential safety risks associated with the Smart Columbus Demonstration Program and each project therein. This is accomplished through a systematic analysis process that includes system hardware, software, interfaces, human behavioral factors, intended applications, operational environment, weather events, external factors, data security, user abilities, and infrastructure. The scenarios consider the entire life of the program and the eight individual projects. The potential safety impacts of each scenario are then documented so mitigation measures may be developed.

4.1.1. Program Level

Safety scenarios identified at the program level apply to the entire Smart Columbus demonstration program. The Smart Columbus Operating System, which is one of the eight projects of the program, serves as the heart and integral backbone of all the Smart Columbus projects. The risks identified under the Operating System are considered program-level risks. The program-level risks include power outage, communication failure, data storage, and external, malicious impacts on the system.

The Operating System will process and store data from all program projects. It will have operators, curators, and administrators, but it will not have human participants, per se. As the program proceeds and standards change, if required, the team will coordinate with an independent IRB. If the Operating System requires IRB oversight, it would be only for Personally Identifiable Information (PII) and data security, not for physical safety. Program-level Operating System issues are treated in depth in the Operating System ConOps, the DPP and the DMP. Operating System-related safety issues to users are treated specifically in each project's ConOps and development documentation and in this SMP under each project.

4.1.2. Project Level

Safety scenarios identified at the project-level apply to the specific elements (hardware, software/applications) selected and deployed for each Smart Columbus project. In addition, human application of the project applications and hardware is an important factor. Smart Columbus does not expect to replace human judgement and responsibility in travel with electrical and electronic (E/E) devices. By aiding human judgement with the capabilities of machines and machine intelligence, the best of both human and computer systems will complement one another.

Table 6 lists the project-level IRB oversight and informed consent needs identified for each project. In those cases where an IRB will review the project's research protocol and associated participant materials, potential safety issues will be explained to participants and the Informed Consent Document will contain instructions about what to do in case of a safety problem. A separate Smart Columbus report on human use will give further details on IRB activities and results in each project.

The Informed Consent Document, where applicable, will state that the user (e.g., driver, pedestrian) is responsible for control of their vehicle or their movements crossing city streets or negotiating transit vehicles. The training will include user responsibilities and limitations of the equipment, as well as what to do in case of a difficulty with user applications, equipment or a crash. Operator control and training is an important mitigation strategy and is the fallback to any system difficulties that are not circumvented by E/E failsafe, warning and control systems.

Table 6: Institutional Review Board Oversight

Project	IRB Oversight and Informed Consent?
1. Smart Columbus Operating System	No – no participants associated directly with this project
2. Connected Vehicle Environment	Yes – as in the USDOT CV Pilots
3. Multimodal Trip Planning Application/Common Payment System	Yes – for CPS
4. Mobility Assistance for Cognitive Disabilities	Yes – users are from a protected class
5. Prenatal Trip Assistance	Yes – users are from a protected class
6. Smart Mobility Hubs	Unlikely – no PII collected, open use
7. Event Parking Management	Possibly – IRB oversight of PII and data security; Informed Consent from User Agreement with application download for terms of use to include data privacy, user surveys
8. Connected Electric Autonomous Vehicles	No

Source: City of Columbus

4.1.2.1. CONNECTED VEHICLE ENVIRONMENT

Cars, trucks, and buses will communicate with the infrastructure and to one another to reduce congestion and increase safety. The project team plans to install safety applications for multiple vehicle types including transit buses, first responder vehicles, city and partner fleet vehicles, and private vehicles.

Safety scenarios for the proposed applications stem from the use of these applications and the use or interpretation of the alerts they may provide, and the potential impact of communications failures and interruptions. The CVE deployment applications will include:

- Emergency electronic brake lights warnings
- Forward collisions warnings
- Lane change and blind spots warnings
- Transit and freight signal priority
- Emergency vehicle preemption
- Red-light violations and
- School zone speed reductions

Safety scenarios for the proposed applications may be caused by pedestrian detection driver distraction, incorrect or non-issuance of warnings, improper installation and miscommunication of devices, road conditions, device tampering, inadequate training, breach of device data protection, and public outreach.

The IRB will oversee human use in this project. The informed-consent document will explain potential safety issues to participants, and it will include instructions for actions in response to problems or an emergency.

For CV drivers, appointments to register, install or reinstall equipment, fix operational problems, and so forth will be included in the training and is also provided in the User manual. Smart Columbus wishes to proactively solve CV onboard unit (OBU) problems before they cause driver distraction and driving difficulty.

Safety issues may range in seriousness from a loose connection in the OBU to an actual crash. In the event of a crash, the participant will be instructed to call 911. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

4.1.2.2. MULTIMODAL TRIP PLANNING APPLICATION/COMMON PAYMENT SYSTEM

Travelers interact with the MMTPA/CPS using smartphones, web portal, kiosks at Smart Mobility Hubs, ticket vending machines, or the interactive voice response system.

The MMTPA is enabled by trip optimization services that connect with mobility providers such as transit agencies, TNCs, car- and bike-sharing companies and taxis to create customized trip itineraries for the Traveler. The CPS and COTA fare system are integrated, so travelers may fund a single account to pay for services, enabling them to simply “click to pay once” for multimodal trips.

Safety scenarios for the proposed application may be caused by impacts of maintenance modes, call failures, mobile device failure, mobile service provider network failure, multimodal transportation not available, special events, trip planning during traffic incidents, and driver distraction. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

The oversight of an IRB would pertain primarily to PII and data security issues and not much about the physical safety of travelers. The use of the CPS may require IRB oversight. For the MMTPA application, as the project proceeds and standards change, if required, the team will coordinate with an independent IRB.

4.1.2.3. MOBILITY ASSISTANCE FOR PEOPLE WITH COGNITIVE DISABILITIES

The MAPCD mobile application will include a highly accurate, turn-by-turn navigator designed to be sufficiently intuitive such that older adults and groups with disabilities including those with cognitive and visual disabilities can travel independently.

Safety scenarios for the proposed applications may be caused by connectivity issues, inaccurate route information, or issues with the pedestrian portion of the route (such as issues with Americans with Disabilities Act (ADA) compliance in a crosswalk). Safety scenarios include the potential impacts of maintenance modes, emergency call failures, mobile device failure, mobile service provider network failure, traveler distraction, and inaccurate instructions or route information. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

The IRB will oversee human use in this project. Persons with cognitive disabilities comprise a vulnerable population and deserve fair treatment according to their needs. The IRB will explain potential safety issues, such as getting lost, to participants and their caregivers. Informed-consent document will communicate risks to the participants and their caregivers and provide information around tools available to helped eliminate the risk or mitigate its impact.

4.1.2.4. PRENATAL TRIP ASSISTANCE

Pregnant women will interact with the PTA system to schedule rides through three flexible options: a website, a smartphone app, or the call center.

The PTA System is integrated with MCOs to verify Medicaid eligibility for each of the NEMT requests and to share usage data. Based on the eligibility of the prenatal traveler, PTA system will be connected to the NEMT Mobility Providers who will be responsible for providing the NEMT service to the Prenatal Traveler. The PTA System is also connected to the medical offices, so they can be notified if a patient is running late.

Safety scenarios for the proposed applications may be caused by impacts of maintenance modes, emergency call failures, mobile device failure, mobile service provider network failure, driver distraction, cancellations and late arrivals of the scheduled rides, vehicle crashes, and NEMT safety precautions. This unique project also considers the risks that may occur because of the traveler's condition and the effect of increased stress on pre-term labor, and related risks that can arise related to the installation of car seats to accommodate the traveler's children that may accompany her on a trip. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

The IRB will oversee human use in this project. Pregnant women comprise a population that is especially vulnerable to potential safety hazards and stresses in travel. The IRB will explain potential safety issues to participants and their caregivers. Informed-consent document will communicate risks to the participants and provide information around tools available to help eliminate the risk or mitigate its impact.

4.1.2.5. SMART MOBILITY HUBS

The purpose of the Smart Mobility Hubs project is to provide travelers with consolidated transportation amenities at physical facilities to solve FMLM challenges in the Linden area. Mobility hub services include interactive kiosks, Wi-Fi, and emergency call buttons. These services will enable access to real-time transportation information and comprehensive trip-planning tools, and they give residents and visitors the opportunity to access multiple travel modes to solve FMLM challenges.

Smart Mobility Hub facilities will feature designated bike-, car-, and scooter-sharing areas, pickup and drop-off zones for ride-sharing, park-and-ride lots, and access to COTA bus services.

Safety scenarios for the proposed applications may be caused by both software and connectivity issues such as cellular network failure, unavailability of the MMTPA, special events or incidents that impact traffic, kiosk Wi-Fi failures, and mobile service-provider network failures. Safety scenarios also consider the impact of infrastructure-related risks such as emergency call button failure, safety feature failures related to multimodal transportation options (e.g., not wearing helmets for bikes and scooters), obstruction of hub features due to weather hazards (snow not cleared), and potential accessibility issues. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

This project will not collect PII because it does not require formal participation. Although the project team does not anticipate IRB involvement at this time, as the project proceeds and standards change, if required, the team will coordinate with an independent IRB.

4.1.2.6. EVENT PARKING MANAGEMENT

The EPM project will be a one-stop shop for parking. Users will be able to identify available parking spaces from parking garages and surface lots to parking meters and loading zones. Through the EPM services users will be able to reserve and pay for the parking through the CPS application in advance.

Safety scenarios for the proposed applications may be caused by impacts of the application's maintenance modes, connectivity and data sharing for payment, and driver distraction from using the mobile application. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

It is expected that an IRB will oversee human use in this project to protect privacy with use of the CPS, though physical safety is not so much a focal point in this project.

4.1.2.7. CONNECTED ELECTRIC AUTONOMOUS VEHICLES

The project provides an accessible and easily expandable FMLM transportation solution to the region by deploying a fleet of multi-passenger CEAVs that will use the enhanced connectivity provided by the CVE and citywide travel-planning solution.

Safety scenarios for the proposed applications of the CEAV project may be caused by the use of connected vehicle hardware, communications interruptions and failures and applications failures. Safety scenarios include the vehicle's lane change and blind spot warning, transit and freight signal priority warnings, mobility emergency vehicle preemption warnings, reduced speed school zone warning, vehicle crashes, pedestrian detection, driver distraction, incorrect or non-issuance of warnings, improper installation, miscommunication of the devices. They also include operational risks related to automated vehicle technology, including the impact of vehicle speed limits, stopped operations of the vehicles, road conditions, tampering with the device, mixed traffic environment and inadequate training. Specific issues and mitigation strategies are detailed in the risk assessment matrix later in this document.

The IRB will oversee human use in this project. The informed-consent document will explain potential safety issues to participants, and it will include instructions for actions in response to problems or an emergency.

4.2. RISK ASSESSMENT

There is more to assessing risks than statistical measures of risk; risk assessment includes the following three steps:

1. An analysis identifying the risks.
2. Making judgements on the tolerability of the risks.
3. Mitigation of the risks.

For this risk assessment, data sources for risk analysis are in short supply as the projects are innovations new to the cityscape, making the risks also new to data collection and analysis. As these are new applications, informed engineering judgement is the tool of greatest efficacy. The analysis follows identification of risks, evaluation and mitigation, using the ISO 26262 Automotive Safety Integrity Level (ASIL) Standards for software development and design. ASIL is a risk classification scheme that uses Severity, Exposure and Controllability of the operating scenario for the risk analysis. Rating Rules were applied to determining the values of the Severity, Exposure and Controllability scores.

The ASIL analysis is extended from exclusively vehicular uses to include pedestrians and transit users who are travelers using E/E apps that interface especially with transit vehicle uses in the transportation network. This includes MMTPA/CPS, SMH, MAPCD and PTA. EPM is a vehicular application like CVE and CEAV. This extension of ASIL to MMTPA, SMH, MAPCD and PTA is justified since Severity, Controllability and Exposure are useful measures of E/E application capabilities in vehicular environments. ASIL risk assessment was also used in the CV applications in the USDOT CV Pilots, including vehicular, pedestrian and transit environments. The same kind of safety risks appear for MMTPA, SMH, MAPCD and PTA travelers as do CVE, CEAV and EPM users. The Operating System has obvious ASIL application, as it has E/E interfaces with all the projects and corresponds to Traffic Management Center (TMC) data collection, storage and management functions within CV and generic vehicular ITS projects.

Analysis of each of the identified safety scenarios and the level of severity, exposure and controllability was conducted following the ISO 26262 ASIL determination matrix shown in **Table 7**.

The project teams examined all safety scenarios related to the installation of the devices for both the vehicle fleets and infrastructure and mobile applications that are deployed as part of the Smart Columbus program. The ConOps, SyRS, DPP and DMP documents provide guidance regarding security and privacy, as well as mitigation plans for security breaches for confidentiality, integrity, and availability, along with the potential threats. There are four ASIL ratings identified: ASIL A, ASIL B, ASIL C, and ASIL D. Safety risks identified as QM, or “Quality Management,” do not require specific mitigation measures as the risk is handled by normal quality management practices. For all risks, quality management practices to be performed are described in **Chapter 5** and includes provisions for equipment procurement, device installation, a fail-safe system mode, quality training, safety manager responsibilities, safety reviews, and safety incident reporting.

Safety risks that are determined to be ASIL D have the highest safety risk and need the highest level of mitigation measures, while those that receive ratings of ASIL A have the lowest level of testing requirements per ISO 26262.

The following three classes of attributes determine an ASIL rating:

- **Classes of Severity**
  - S0: no injuries
  - S1: light and moderate injuries
  - S2: severe and life-threatening injuries (survival probable)
  - S3: life-threatening injuries (survival uncertain), fatal injuries
- **Classes of Probability**
  - E1: very low probability
  - E2: low probability
  - E3: medium probability
  - E4: high probability
- **Classes of Controllability**
  - C1: simply controllable
  - C2: normally controllable
  - C3: difficult to control or uncontrollable

In addition to these ASIL classes, the SCC team used classes of S0a and C0 for instances when the integrity level would be of inconsequential severity (S0a) or insignificant to control (C0).

Table 7: Automotive Safety Integrity Level Determinations

Severity	Probability of Exposure	C1 Controllability	C2 Controllability	C3 Controllability
S0	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	QM
	E4	QM	QM	QM
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C

Severity	Probability of Exposure	C1 Controllability	C2 Controllability	C3 Controllability
	E4	B	C	D

Source: ISO 26262

A multidisciplinary team including the Smart Columbus PMO, project teams, independent staff (Battelle and Michael Baker), partners and vendors (AbleLink, COTA, OSU, Mtech, Kaizen Health, Pillar technologies, May Mobility and CelebrateOne) assembled to identify and assess each safety scenario and develop the corresponding safety risk response plans for all the eight Smart Columbus projects.

Rating Rules were applied to the safety risks for Severity, Exposure and Controllability to help in the assessment of the values in the final score for each risk. The Severity, Exposure and Controllability Rule Ratings are shown in **Table 8**, **Table 9** and **Table 10**.

Table 8: Automotive Safety Integrity Level Severity Rule Ratings

Rule	Description	Rating	Score
S-A	Any incident where a vehicle strikes a pedestrian is severe.	S3	3
S-B	A malfunction that cannot lead to a vehicle striking a vehicle, a pedestrian, or a fixed object is at most an inconvenience. Pedestrians are assumed to be able to avoid fixed objects and one another. Missed messages do not themselves cause a crash.	S0a	0
S-C	A low speed crash is assumed to cause minor injuries	S1	1
S-D	Vehicle-to-vehicle or vehicle-to-fixed-object crashes where the speed limit is 25 mph or below	S2	2
S-E	Vehicle-to-vehicle or vehicle-to-fixed-object crashes where the speed limit is above 25 mph	S3	3
S-F	Fires in vehicles are S2	S2	2
S-G	Existing policy or tested equipment prevents a scenario and it can be argued that the deployment will not disrupt the existing protections.	S0	0
S-H	The severity of a missed message depends on the application or unknown misuse of the vehicle. A preliminary severity will be resolved later.	S3	3
S-I	Release of personal data is a concern but not a safety hazard	S0a	0
S-J	Traveler unable to complete the trip (or have a long wait) but is in a safe location	S0a	0
S-JA	Traveler unable to complete the trip and is subject to element	S1	1
S-K	Traveler unable to complete the trip (or have a long wait) and in a risky location	S2	2
S-L	Pedestrian slip, trip, or fall. Bicycle or scooter fall or collision with a fixed object.	S1	1
S-M	Minor non-traffic injury or disease	S1	1
S-N	Missed or ignored messages do not themselves cause a crash	S0	0
S-O	False warnings or inappropriate warnings	S1	1

Source: City of Columbus

Table 9: Automotive Safety Integrity Level Exposure Rule Ratings

Rule	Description	Rating	Score
E-A	Existing policy or tested equipment prevents a scenario and it can be argued that the deployment will not disrupt the existing protections.	E0	0
E-B	Extreme weather events, such as lightning strikes, hurricane landfall, and deep snow	E1	1
E-C	Storms, such as rain or ice are also rated E1, though they may actually occur more frequently. (E1.5 would be good for this.)	E1	1
E-D	Vandalism of protected equipment happens.	E1	1
E-E	All organizations will experience staff turnover. Scenarios related to new employees are E2, except those associated with management or key staff or other rationale may be E1.	E2	2
E-F	School begins and ends every year. Work zones are established, moved, and cleared.	E2	2
E-G	Periodic maintenance occurs occasionally.	E1	1
E-H	A designed-in fault that affects every trip or an application expected to activate on every or nearly every trip	E4	4
E-I	A designed-in fault that affects applications expected to activate only occasionally	E3	3
E-J	A designed-in fault that is manifested only when unusual circumstances occur is rated at the frequency of those circumstances.	E2	2
E-K	A designed-in fault that is manifested only when unusual circumstances occur is rated at the frequency of those circumstances.	E1	1
E-L	Difficulties in radio transmission, at least at a minor level, are expected daily, unless historical data shows a different frequency.	E2	2
E-M	Even with training, a few participants can be expected to misunderstand their role or forget a function used infrequently.	E1	1
E-N	Project equipment does not deliver permissive messages.	E0	0
E-O	Crashes involving fleet vehicles are expected a few times during the deployment.	E1	1
E-P	Delayed DSRC messages are rare but happen.	E0	0
E-Q	GPS vagaries occur regularly but not always	E2	2
E-R	Automated vehicle encounters a situation outside its operational design domain.	E2	2
E-S	The general public is untrained and will occasionally act unexpectedly.	E2	2
E-T	Malicious activity is assumed to succeed occasionally.	E1	1
E-U	Random fault in one of the components of the system	E2	2
E-V	A few participants can be expected to lose situational awareness and become distracted. Rate of occurrence is expected to be a few times a year	E2	2

Source: City of Columbus

Table 10: Automotive Safety Integrity Level Controllability Rule Ratings

Rule	Description	Rating	Score
C-A	UMTRI showed in RDCW and IVBSS that drivers can ignore spurious warnings. (We should check the SPMD results to confirm that is true in a connected vehicle environment)	C1	1
C-B	Ignoring or missing a message that calls for action is an incorrect response.	C1	1
C-C	Failure to present an advisory message when a message is warranted will not degrade the performance of a normal driver with all ordinary information (sights and sounds) available. Missed alerts are rated C1 to account for the case of a driver who has become accustomed to them and expects to be alerted to developing situations.	C1	1
C-D	Distractions other than frequent unwarranted messages, such as displays that are difficult to interpret or loose equipment, can cause the driver to miss important external information.	C2	2
C-E	A message with incorrect information, even if it be only an advisory, is rated as less controllable than a missing message or a spurious message. The incorrect message will, at a minimum, require cognitive effort to discount, and may yield an incorrect response.	C2	2
C-F	A driver who misinterprets a signal or misunderstands the desired response behave inappropriately.	C3	3
C-G	Traffic signals will be obeyed by drivers and pedestrians, so any improper operation by traffic signals cannot be overcome by travelers.	C3	3
C-H	System-wide malfunctions that can be recognized by staff at the Traffic Management Center can be controlled by those staff. Rank C1 instead of C0 because TMC staff will take time to respond and travelers will be affected until response is complete.	C1	1
C-I	A driver confronted with a fire can stop and exit the vehicle but must do so promptly.	C2	2
C-J	A traveler stranded by a disabled vehicle, or a vehicle not dispatched, or other equipment malfunction is wholly unable to use the vehicle to continue the trip.	C3	3
C-K	Equipment or wiring in the wrong place should not be moved by the driver while in motion and will slow emergency responders	C3	3
C-L	Any defect that exacerbates injury during a crash or impairs rescue following a crash is wholly uncontrollable by the driver	C3	3
C-M	Participant will notice nothing unusual, and normal movement is the proper course.	C0	0
C-N	Harm that occurs regardless of driver or traveler response is not controllable.	C3	3
C-O	Any system feature (static equipment or inappropriate message) that leads a driver to take harm-causing action is not controllable.	C3	3

Rule	Description	Rating	Score
C-P	Avoiding a crash requires skills beyond what is expected in most drivers. Professional drivers would be challenged beyond their ordinary skill to avoid a crash.	C3	3
C-Q	The response may be a more sudden steering or a harder braking.	C2	2
C-R	Failing to provide information from a driver or traveler is not controllable by the traveler.	C3	3
C-S	A person has little control immediately after person/ data is exposed.	C3	3
C-T	Drivers of surrounding vehicles can handle slightly erratic behavior of an AV.	C1	1
C-U	Drivers of surrounding vehicles cannot handle an AV with sudden odd behavior.	C3	3
C-V	Professional driver can intervene in moderate malfunctions.	C1	1
C-W	Traveler has probably encountered a similar situation before and handled it.	C1	1
C-X	Travelers who ignore safety equipment (like bicycle helmets) cannot be helped.	C3	3
C-Y	Vulnerable travelers are incapable of dealing with even minor mishaps.	C3	3
C-Z	System has no control over deliberate misuse of the system by the participants	C3	3
C-ZA	A trained operator on board will be capable of handling the situation	C0	0
C-ZB	Any system failure caused by the weather is not controllable by the driver	C3	3

Source: City of Columbus

Table 11 shows the results of the safety risk assessment process, detailing each safety scenario identified, the associated safety impacts anticipated, the safety risk response plan developed, the ASIL dimensions assigned, and the resulting ASIL rating.

The SCC risk assessment includes ratings of S0a and C0 that are not in the ASIL ratings table (**Table 7**). These scenarios that have a zero rating, as well as S0 which is in the ASIL matrix, can be excluded from further analysis. This applies if a scenario cannot happen, causes no harm or can be unquestionably handled by any participant. In these cases, that assessment is documented, and no safety requirements are needed. These items are scored as “-“ in **Table 11**.

Table 11: Summary of Safety Risk Assessment

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
PROGRAM-LEVEL RISKS										
Smart Columbus Operating System										
1	Unauthorized person has access to the data.	Safety issue to the users. An unauthorized person has access to the personal information and can be used to commit a crime. Unauthorized person collects the information from different application in the operating system and puts bits and pieces of data put together.	Diligent data security practices and regular patching and updates. Avoid collecting unnecessary or sensitive information from participants. Ensure adherence to wireless message standards. If hacking is discovered and access to PII is accessed, then users will be informed and about the breach and next steps that will be taken. Users will also be encouraged to use strong passwords for their mobile applications.	S-I	S0a	E-T	E1	C-S	C3	-
2	Malicious functionality: active monitoring of the traveler causes hacking of traveler account/activity.	Creates the potential for unauthorized account activity (related to payments, trip planning, personal data, etc.) while traveler is using the mobile applications. Also, app might store the user information when creating the user account.	Work with the developer and third-party developers to restrict the permissions requested by the app to only what is necessary for functionality. Development of the app along with vendor will provide visibility and customization allowing for more exposure of code base and how it functions.	S-I	S0a	E-T	E1	C-S	C3	-
3	Vulnerabilities of data transmission and storage.	Unauthorized access to PII (could be employees or hackers). Could release sensitive information regarding health, transportation patterns, credit card information. Increased potential for identify theft because of storage of the data collected from the app users.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality. Include lessons learned and best practices in the security measures. Perform routine information security audits. Avoid collecting unnecessary or sensitive information from participants.	S-I	S0a	E-T	E1	C-S	C3	-
4	Authorized user combines datasets to reidentify a person and commit crime.	Safety of the users. Authorized person collects and combines data stored under operating system for different applications of the project and has access to the personal information. Using this personal information, unauthorized person can use it commit a crime, which may result in a safety issue to the user.	Contractual terms will be in place on how someone shall not reidentify data. Assessment of safety risks introduced from new data sets, de-identification, potential exclusion of new data set, ethics policy will take place. Diligent data security practices and regular patching and updates will also be carried out.	S-I	S0a	E-T	E1	C-S	C3	-
PROJECT-LEVEL RISKS										
Connected Vehicle Environment										
5	The CVE system is hacked into and unauthorized personnel have access to traffic control system data.	Safety of the roadway users. Disrupt normal operations of the traffic control system and disconnect the CV that could result in issuing false warnings. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	The SCMS will protect RSUs, OBUs, CV and CEAV data transfers, and identify and block malicious actors. Diligent data security practices and regular patching and updates will be carried out per the DPP and DMP. Firewalls will be installed as part of the network security. Strong passwords will be used to increase the safety of CV connections. Signal controllers are physically secured with locks and accessible only to the TMC personnel.	S-N	S0	E-T	E1	C-H	C1	-
6	The CVE system is hacked into and unauthorized personnel have access to the data.	Unauthorized person may have access to the user's personal data and can be used to commit a crime, which may result in a safety issue to the user.	Diligent data security practices and regular patching and updates will be carried out. Strong passwords will be used to increase the safety of the PII information. If hacking is discovered, then the users will be informed.	S-I	S0a	E-T	E1	C-S	C3	-

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
7	OBU is hacked and provides false warnings to the driver	Device gives a warning that is not valid or accurate or fails to send a valid warning. Safety of the passengers and the roadway users is at issue. This may cause vehicle operator distraction and may result in a crash. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	The SCMS will protect RSUs, OBUs, CV and CEAV data transfers, identify and block malicious actors. Drivers will be instructed and will sign an Informed Consent Document that lays out operator control as primary. CV OBU warning systems are secondary to vehicle operator control. Operator is still to be in control of the vehicle and must assess the situation and react appropriately.	S-N	S1	E-T	E1	C-D	C2	-
8	Vehicle operator gets distracted by the device information or gets confused with the warnings given by the CV	Safety of the participant and nearby road users, including transit riders and pedestrians. This may cause driver distraction which could result in a crash. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Drivers will be instructed and will sign an Informed Consent Document that lays out operator control as primary. CV OBU warning systems are secondary to vehicle operator control. Operator is still to be in control of the vehicle and must assess the situation and react appropriately.	S-O	S1	E-M	E1	C-D	C2	QM
9	Miscommunication between the RSU and OBU because of radio interference issues, reduced power, capacity exceeded, occlusion, etc.	Safety issues because of the different warning systems. Primary concern is related to emergency signal priority and communications to automated vehicles. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Emergency vehicles are responsible for observing the actual traffic signal phase. CEAV will alert Operator if signal confirmation is not received. ConOps references applicability of normal rules of the road for intersection safety in lieu of notifications to vehicle operators of equipped vehicles.	S-B	S0a	E-L	E2	C-E	C2	-
10	Vehicle position not as accurate as needed for the successful operation of the application.	Safety of the roadway users and passengers in the vehicle. The CV application may not accurately provide alerts regarding potential Vehicle-to-Vehicle (V2V)/ Vehicle-to-Infrastructure (V2I) interactions. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Providing position correction capability (Radio Technical Commission for Maritime Services (RTCM)) improves accuracy and is a system requirement; also, alternate approaches can be considered to the extent feasible. Vehicle operator will be in full control of the vehicle and must assess the situation and revert back to normal driving. Drivers should understand vehicle position can be imprecise because of radio interference, occlusion, going out of system range, etc.	S-N	S0	E-Q	E2	C-E	C2	-
11	Incorrect information (MAP not updated) provided to the equipped vehicles concerning lane assignment and function.	Safety of the participant and nearby road users, including pedestrians and bicyclists. Incorrect warning information related about lane usage or false alarms may be given to the equipped vehicle. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	The user training will emphasize that CV is only a warning aid and is not at all intersections. Impact is not crash related. Vehicle operator will be in full control of the vehicle and must assess the situation and revert back to normal driving.	S-N	S0	E-H	E4	C-E	C2	-
12	Incorrect and/or misreported information provided to the equipped vehicle or RSU concerning vehicle position.	Safety of the participant and nearby road users, including pedestrians and bicyclists. Inaccurate vehicle position impacts operation/functionality of the CV applications, potentially creating a safety risk to the travelers. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Providing position correction capability (RTCM) improves accuracy and is a system requirement; also, alternate approaches can be considered to the extent feasible. Vehicle operator will be in full control of the vehicle and must assess the situation and revert back to normal driving. Drivers should understand vehicle position can be imprecise because of radio interference, occlusion, going out of system range, etc.	S-N	S0	E-L	E2	C-E	C2	-

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
13	Miscommunication of the device due to improper installation (for example, antenna position) causes incorrect /inaccurate warnings to the vehicle operator.	This may result in the distraction of the vehicle operator, increasing the potential for a crash. The risk may create a higher than normal number of false positives, which may desensitize the vehicle operator to the information being relayed. Vehicle operators may also disable their in-vehicle device due to the perceived annoyance with the number of alerts received.	Installer training to include sufficient checking of OBU installation. Driver to return vehicle for reinstallation/adjustment/repair as needed. The user training will emphasize that CV is only a warning aid and is not at all intersections. Impact is not crash related and the vehicle operator will be in full control of the vehicle and must assess the situation and revert to normal driving. Increased false alarms and missed warnings can reduce user reliance on the system but should not cause a safety concern.	S-N	S0	E-H	E4	C-E	C2	-
14	System power outage and RSU does not send or receive the necessary information to the operator.	Intersections equipped with this technology will not relay information as designed; they would revert back to pre-deployment state with no alerts being provided and vehicle operators needing to assess the situation to determine how to react. CV and AV will not be getting necessary messages. Not all intersections will have RSUs, but drivers may become accustomed to familiar CV signal operation.	Universal Power Supply at signal supplies backup power. Quick identification and repair of RSUs and power that is not working. Since these are warning systems and only available at some intersections, the vehicle operator is still in control of the vehicle and will need to assess the situation and determine how to react. Warnings are only intended as an additional way to draw attention to the situation.	S-N	S0	E-K	E1	C-C	C1	-
15	Device installed in the vehicle becomes in-operable (tampering, not installed properly etc.).	Safety of the vehicle operator, passengers, and other roadway users. Vehicle would not be able to send or receive communications from other vehicles or RSUs when the device does not operate as per the manual.	Training and ICD should refer user to help desk/installation resources for reinstallation/adjustment/repair as needed. Driver to be advised not to tamper with OBU equipment during training and to be stated in Informed Consent Document. Vehicle operator will be in full control of the vehicle and must assess the situation and revert back to normal driving.	S-N	S0	E-K	E1	C-C	C1	-
16	Vehicle operator lacks sufficient training to adequately understand and interpret alerts.	Driver is overconfident and ignores standard visual and auditory cues, causing a crash that compromises the safety of the vehicle operator, transit riders and to the nearby road users and pedestrians	CV is only a warning aid and is not at all intersections. Impact is not crash related – vehicle operator still makes the final decision. Increased false alarms and missed warnings can reduce user reliance on the system but should not cause a safety concern. Provide adequate training to the vehicle operators on how to react to different situations and understand that the CV system is a warning aid and vehicle operator will have full responsibility and control over the vehicle.	S-E	S3	E-I	E3	C-F	C3	C
17	Safety issue when the device is not operating how the user was trained or instructed for, when there is a malfunction.	This may result in the distraction and/or misinformation, which compromise the safety of the vehicle operator, transit riders, nearby road users and pedestrians.	Training and ICD should refer user to help desk/installation resources for reinstallation/adjustment/repair as needed. CV is only a warning aid and is not at all intersections. Impact is not crash related – vehicle operator still makes the final decision. Provide adequate training to the vehicle operators on how to react to different situations and understand that the CV system is a warning aid and vehicle operator will have full responsibility and control over the vehicle.	S-E	S3	E-K	E1	C-C	C1	QM
18	Important safety/warning messages given by the system ignored by the operator (due to number of alerts, etc.)	Vehicle operator does not acknowledge the alert or adjust his or her driving behavior to account for it, thereby compromising the safety of the vehicle operator, other vehicles, and nearby road users and pedestrians.	Reference studies/surveys that identify the appropriate number of alerts. The CV system will be configured based on the survey results for the warning messages.	S-H	S3	E-H	E4	C-A	C1	B

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
19	The operator not knowing how to react when the OBU disconnects.	Safety of the passengers and the roadway users. The OBU disconnects when the vehicle is in operation and the vehicle operator reacts inappropriately. Vehicle would not be able to send/or receive communications from other vehicles or RSUs.	Training and ICD should refer user to help desk/installation resources; vehicle operator is still in control of the vehicle and must assess the situation and continue/resume normal driving.	S-G	S0	E-E	E2	C-J	C3	-
20	Time of the school zone is wrong in the system and the device does not give necessary warnings.	Safety of the passengers, pedestrians, and the roadway users. The CV system does not give the vehicle operator appropriate warnings at the school zone and doesn't slow down during the active school zone, which may result in a crash. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	The roadside safety message to indicate school zone warning will be linked to the operation of the flashing school zone indicator signal; if light is flashing at the wrong time, the signal will be adjusted. However, the vehicle operator still maintains responsibility for the vehicle and the warning is only a reminder.	S-G	S0	E-H	E4	C-H	C1	-
21	Driver trained for the CV is assigned to a non-CV and comes to expect warnings that are not sent. Applies to personal vehicles as well.	Safety of the vehicle operator, passengers, and the roadway users. Vehicle operators become accustomed to alerts and/or priority and are desensitized to potential hazards, reducing their reaction to these situations.	Participant training includes vehicle operators switching from CV vehicle to a non-CV vehicle with safety precautions and how to react to different situations.	S-G	S0	E-E	E2	C-C	C1	-
22	A misconception by the participant results in the participant believing the system takes control of the vehicle in case of a hazard.	Safety of the participant and nearby road users, including transit riders and pedestrians, which may result in a crash when the vehicle operator is not in full understanding of the capabilities of the CV system and does not react to the situation as needed. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Incorporate into the Vehicle Operator Training and provide adequate training to all the participants to understand that the vehicle operator is in full control of the vehicle and ultimately responsible to obey the laws and CV is only a warning aid and is not at all intersections. Informed Consent Document covers that this is CV and not AV.	S-E	S3	E-M	E1	C-F	C3	A
23	A heavy snow storm or other weather-related issues result in the power outage and loss of communication to the CV system.	Safety of the participant and other road users, including transit riders and pedestrians. Loss of communication would result in the failure of warnings to be issued when appropriate. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Include lessons learned and best practices in the design. Perform design review of installation. Verify installation before deployment, including specific end-of-line testing and checklists. Provide adequate training to the vehicle operators on how to use the CV equipment and react in inclement weather.	S-B	S0a	E-B	E1	C-ZB	C3	-
Connected Electric Autonomous Vehicles										
24	AVs operating at low speed (slower than 35 mph) with vehicles at higher speeds (exceeding the posted speed limit).	The disparity in speed between an AV operating below 35 mph and other traffic exceeding the 35-mph limit might cause a crash.	Traffic calming measures, speed enforcement, AV information signage and route design on these sections of routes that AVs will be operating will help with the speed control. Also work with the vendor to have CEAVs travel as close to the speed limit as the technology allows for safe operation.	S-E	S3	E-S	E2	C-U	C3	B
25	Sudden stop of the AV because it encounters an unanticipated obstacle.	Safety to the passengers and the road users due to sudden stop. AV not recognizing the obstacle stops unexpectedly. This sudden stop of the AV can cause a safety issue to the passengers and to the road users behind the vehicle. This may also cause rear-end crashes.	Operator will be present in the vehicle all the time when the vehicle is in operation and must take control and maneuver around the obstacle. To improve passenger safety, the operator will instruct the passengers remain seated and belted, as available.	S-E	S3	E-I	E3	C-U	C3	C
26	Vulnerable road users (VRU) go into the path of an oncoming AV.	Safety risk to the VRUs and the passengers. VRU goes in front of the moving vehicle and the CEAV makes a sudden stop. The sudden stop may cause safety risk to the passengers in the AV and a safety issue to the pedestrian crossing the street.	Testing for reaction to VRUs of several types will be thoroughly vetted – at this time City has planned for bicycle, pedestrian and scooter. Operator should be aware of operating conditions. Ensuring pedestrian safety for interactions with AVs is accounted for in standard operating procedures. For example, increasing awareness and education of the operation of AVs on roadways for pedestrian and other road users will be included as part of the outreach and operating training procedures.	S-A	S3	E-S	E2	C-Q	C2	A

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
27	Passenger may not be fully boarded or alighted when AV begins to move.	Safety risk to the passenger. Passengers when trying to board the vehicle and the AV may depart not knowing that the passenger has not boarded the vehicle fully. The passenger then may try to catch the moving AV trying to board the vehicle.	Standard AV operations are to not move until the door is fully shut; door sensors should be aware of complete closure. (This is the biggest cause of failures in transit systems). Operator will always be present when the AV is in operation.	S-A	S3	E-S	E2	C-V	C1	QM
28	Passenger approaches the AV as it is departing a stop.	Safety risk to the passenger. Passenger in a hurry to reach the destination and try to board a moving AV. This may result in a safety issue to the passenger.	Operator training should include measures to handle operating the vehicle as potential passengers approach it (intervene and stop AV operation to manually open the door).	S-A	S3	E-S	E2	C-V	C1	QM
29	Passenger alighting may not accommodate an entire loading/unloading (for multi-passenger parties, ADA customers, etc.).	Safety risk to the passenger. Passengers are trying to board the vehicle and the AV may depart not knowing that all the passengers are not boarded yet. The passengers then may try to catch the moving AV trying to board the vehicle, which may result in an injury risk to the passengers.	Standard AV operations are to not move until the door is fully shut; door sensors should be aware of complete closure. (This is the biggest cause of failures in transit systems). Operator will always be present when the AV is in operation. Operator training should include measures to handle operating the vehicle as potential passengers approach it (intervene and stop AV operation to manually open the door).	S-A	S3	E-K	E1	C-ZA	C0	-
30	Slower speed and unpredictable operations of bike and scooter traffic, and any other shared mobility device along the AV route may cause dangerous interactions with the AV.	Safety risk to bicyclists, scooter operators and passengers. When there is an unpredictable interaction with the other roadway users, there might be a delayed response from the AV to stop and this may result in an injury risk to the bike and scooter passengers.	Scooter is a new mode that may interact with an AV – testing for reaction to VRUs of all types will be thoroughly vetted. Operator should be aware of operating conditions. Also include relevant standard operating procedures – for example, increase awareness and education of the operation of AVs on roadways for pedestrian and other road users. Operator will always be present when the AV is in operation. Operator training should include measures to handle operating the vehicle during these situations.	S-A	S3	E-S	E2	C-Q	C2	A
31	Stopped operation of an AV could create an impediment in the roadway.	Safety risk to the passengers and other roadway users. While on the roadway, there might be maintenance issues to the AV causing it to stop on the side of the roadway. This might result in the impediment in the roadway to the roadway users.	Standard operating procedures for first responders, protection for passengers, and operator training. Operator will always be present when the AV is in operation. Operator training should include measures to handle operating the vehicle as it makes a sudden stop for any maintenance reasons.	S-E	S3	E-R	E2	C-U	C3	B
32	An AV operating in manual mode and the operator may not notice VRUs (bikes, scooters and pedestrians) taking advantage of the AV.	Safety risk to bike and scooter operators and passengers. When there is an unpredictable interaction with the other roadway users, there might be a delayed response from the AV operator to make a sudden stop in the assumption the AV will be able handle the situation. This may result in an injury risk to the bike and scooter operators.	Operator training and operating procedures should account for potential vehicle operator distraction. AV is equipped with standard vehicle awareness equipment (mirrors, sensors, etc.) for the vehicle operator to rely on when operating manually.	S-A	S3	E-S	E2	C-U	C3	B
33	There is a danger of the public taking advantage of (or having a false sense of security around) AV safety protocols and slow down operations.	Safety of the passengers, pedestrians and the roadway users. With the increased interaction of pedestrians and other road users with AVs, there is an increased potential for risk. The roadway users might take advantage of AVs and have a false sense of the security around them.	Standard operating procedures, education and outreach, and increased enforcement will be implemented throughout the operational period of the AVs.	S-A	S3	E-S	E2	C-U	C3	B
34	Latency and high network traffic creating issues/problems in connectivity/communications with other road users and infrastructure.	Loss of connectivity impacts V2V and V2I communications, causing lack of alerts and interruption of data collection. This can cause a crash when the AV does not get the message of a red light or an emergency vehicle.	CV OBU warning systems are secondary to vehicle operator control. Operator is still to be in control of the vehicle and must assess the situation and react appropriately. Onboard Operator is a backup to the onboard systems – operator intervention would take over.	S-E	S3	E-L	E2	C-C	C1	QM

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
35	No certification, testing, and rating systems for safe pre-deployment evaluation methods for these shuttles currently exist.	Inconsistent approaches/solutions are available. No uniform/agreed upon process to ensure and measure public safety, so it is difficult to assess the 'safest' solution.	This project will be documenting lessons learned and the safety standards used for these specific deployments. System cannot to proceed from Level 4 to Level 5 until the standards are developed. Liability insurance has to account for lack of proven systems.	S-H	S3	E-S	E2	C-Y	C3	B
36	CEAV operator not trained to handle emergency or real-time situations.	Safety risk to passengers and other road users. In an emergency, operator not trained to handle the situation, which may result in delayed response and may increase severity of incident/impact.	Training and response; certification response for AV operator.	S-H	S3	E-M	E1	C-F	C3	A
37	CEAV operator is distracted and unable to handle emergency or real-time situations.	Safety risk to passengers and other road users. In an emergency, operator is distracted and unable to handle the situation which may result in delayed response, increased severity of incident/impact. Distraction of the driver (may be checking his phone) assuming he does not have to pay attention to the road 100% of the time since vehicle is an AV and might take advantage of that fact.	Operator training and operating procedures should account for potential vehicle operator distraction. Policies to remove distraction (e.g. no phones will be included as part of the training).	S-E	S3	E-J	E2	C-D	C2	A
38	Road conditions (lane closures, lane assignment) have changed and the CEAV mapping is not updated, impacting the AV's ability to understand current roadway assignment.	Safety risk to passengers and other road users. Reaction time of the AV will be impacted, increasing risk of unplanned or sudden stop, or potential interaction with obstacles.	Operator must take control and maneuver the route. Close coordination with construction projects to maintain current and accurate lane lines. Operating procedures include coordination between City and AV operator to assess road conditions, etc.	S-E	S3	E-R	E2	C-V	C1	QM
39	Passengers tamper with the controls of the CEAV if and when the AV will operate without a vehicle operator.	Safety of passengers and the roadway users. Without an operator on the AV, there is a possibility of passengers tampering with the controls of the vehicle, which may result in unexpected behavior of the vehicle.	As per the contract of the Smart Columbus program, all CEAVs will have an operator on board who would reactivate the AV or prevent passenger tampering. Surveillance cameras could monitor as well.	S-D	S2	E-S	E2	C-ZA	C0	-
40	Law enforcement and Emergency responders not trained to handle emergency situations with the AVs.	Safety risk to passengers or others involved in an emergency. Delayed response to passengers/other roadway users increases the potential severity of the risk when the emergency responders at the site are not trained to handle the situation involving AVs.	Outreach for emergency responders to train them on responding will also be part of the training agenda. Include tabletop exercise and standard operating procedures as part of the training.	S-A	S3	E-E	E2	C-N	C3	B
41	Flat tire or some kind of AV maintenance failure that a non-AV can experience.	Safety risk to the passengers. AV encounters a maintenance issue and delayed arrival to the stop. Passengers may end up waiting for the AV and get stranded for a long time, which may result in a safety issue for the user.	Operator should always be monitoring vehicle response to surroundings, and the training will include how to react to different situations.	S-JA	S1	E-J	E2	C-J	C3	-
42	ADA equipment could become dislodged during AV operations (some current operators are not ADA-accessible or -compliant; others are only accessible).	Safety of the traveler who needs access to the ADA equipment. The operator not familiar with the ADA equipment may not be able to safely board the passenger into the vehicle, which may encounter a safety situation to the passenger.	Operator should be monitoring vehicle response to surroundings at all times and assist passengers getting on and off of the AV. Operators will be trained to use the ADA equipment and assist the passengers that need ADA access.	S-M	S1	E-K	E1	C-L	C3	QM
Smart Mobility Hubs										
43	Passenger does not realize where the emergency call button is located at the hub location.	Safety of the traveler. Traveler could not locate the emergency call button located at the hub location and wait for long to find an alternate transportation option, which may result in a safety issue for the user.	Outreach at the location of the SMH sites about all the features provided by the kiosks will be provided. Information about the kiosks will also be available on the Smart Columbus website. In any emergency, the travelers are requested to call 911.	S-JA	S1	E-S	E2	C-J	C3	-
44	Over activation of call button (false alarms).	Safety of the traveler. Call button at the hub location is overactivated and is misused by the travelers. These false alarms can potentially result in longer response times, resulting in risk to the safety of the traveler.	Discussion with law enforcement will be held on how to handle these situations. Provide outreach at the SMH sites about all the features, including the use of the kiosk emergency button. Information about the kiosks will also be available in the Smart Columbus website. In any emergency the travelers are requested to call 911.	S-G	S0	E-S	E2	C-Z	C3	-

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
45	Responding late to the emergency calls from the hub location.	Emergency button for the police or officials to react when there is a theft or safety issue. Safety issue when the officials do not respond fast enough to the users.	Voice over IP channel is opened with the police during the time the passenger is waiting for help to arrive. Security manager information network – information put out through Capital Crossroads will be shared with stakeholders to notify passengers of safety concerns/trends affecting the area.	S-G	S0	E-M	E1	C-Z	C3	-
46	Emergency call button does not respond at the mobility hubs.	Safety of the traveler. In a situation where the traveler needs support, the emergency call button will not work, and the delayed response to the emergency need might increase the safety risk to the passenger.	Automatic monitoring of kiosk to notify maintenance if electronic heartbeat is not received. Routine testing of emergency call button will be implemented as part of the deployment process (determine timing of testing).	S-H	S3	E-K	E1	C-N	C3	A
47	Transit delay at the hub locations.	Safety of the passengers. Passengers get off the bus and wait for long to find another service. This may cause a safety issue to the traveler at the location.	Kiosk should be able to offer alternate transportation options for calling taxi or other transport. Camera and emergency call button available for passengers.	S-G	S0	E-K	E1	C-J	C3	-
48	Additional modes of transportation and increased passenger traffic may result in higher conflict interactions (motor vehicle to motor vehicle).	Safety of the drivers. With various transportation modes available at one location, there might be vehicle to vehicle crash at low speeds while navigating through the parking lot or through car share locations. This may also cause an impediment in the roadway for other roadway users.	SMH will have a designated area for specific modes to park to reduce the congestion. The travelers will be encouraged to use the designated areas. Additional signage, and pavement markings will be posted showing the parking locations for different modes of transportation for drop-off and pickup. Outreach will be conducted when the Hubs open to the public to educate them.	S-C	S1	E-I	E3	C-W	C1	QM
49	Additional modes of transportation and increased pedestrian traffic may result in higher conflict interactions (motor vehicle to VRU).	Safety of the driver and the VRU. With various transportation modes available at one location, there might be vehicle to VRUs crash at low speeds while navigating through the parking lot, car share locations, and bike and scooter docking stations. This may also cause an impediment in the roadway for other roadway users.	SMH will have a designated area for specific modes to park to reduce the congestion. The travelers will be encouraged to use the designated areas. Additional signage, pavement markings will be posted showing the parking locations for different modes of transportation for drop-off and pickup. Outreach will be conducted when the Hubs open to the public to educate them.	S-A	S3	E-S	E2	C-W	C1	QM
50	Additional modes of transportation and increased pedestrian traffic may result in higher conflict interactions (VRU to VRU).	Safety of the VRUs. With various transportation modes available at one location, there might be crash at low speeds involving VRUs while navigating through the parking lot, car share locations, and bike and scooter docking stations. This may also cause an impediment in the roadway for other roadway users.	SMH will have a designated area for specific modes to park to reduce the congestion. The travelers will be encouraged to use the designated areas. Additional signage, and pavement markings will be posted showing the parking locations for different modes of transportation for drop-off and pickup. Outreach will be conducted when the Hubs open to the public to educate them.	S-C	S1	E-S	E2	C-W	C1	QM
51	Unattended devices (like scooters, bikes) left on site blocking ramp and can pose tripping hazard.	Safety of the travelers. Additional modes and more travelers at the Hub locations might increase the possibility of having unattended devices which can increase the safety risks for the travelers at the locations.	Dockless device zones are designated at SMH to encourage these devices be left within areas that will not interfere with pedestrian traffic. There will also be signage and pavement markings designated for the dockless devices.	S-L	S1	E-S	E2	C-W	C1	QM
52	Planned maintenance mode occurs when the system is operating in Backup mode to restore, repair, or replace system components.	Safety of the travelers. Additional modes and more travelers at the Hub locations might increase the possibility of having unattended devices, which can increase the safety risks for the travelers at the locations.	These are planned events and should occur during off-peak hours to minimally impact users, and proper notification should be given to potential users in advance of the event when practical.	S-JA	S1	E-G	E1	C-H	C1	QM
53	Failure mode of the kiosk resulting in the complete systemic disruption of the user's ability to plan or complete the trip.	The kiosk is not working, and the users cannot access to plan or continue their journey and might be stranded there for long, which may result in a safety issue for the user.	MMTPA/ CPS should be able to offer alternate transportation options for calling taxi or other transport when not able to reach the central system. SMH Site will be able to offer alternate transportation options for calling taxi or other transport. Signage at the site will be able to provide contact information to other transportation modes.	S-JA	S1	E-U	E1	C-J	C3	QM

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
54	Unable to access kiosks because of the heavy snow fall or icy conditions.	Imminent severe weather expected in area. Ice/snow affects ability of passengers to safely move around SMH.	Weather warnings posted on kiosk. Stakeholders will be responsible for clearing snow and ice.	S-B	S0a	E-B	E1	C-J	C3	-
55	Passenger at St. Stephen's cannot access trip (off hours – lobby locked).	St. Stephen is closed, and the travelers cannot access the trip, as the kiosk is in the lobby of the building. Travelers end up waiting longer than anticipated and encounter an unsafe situation.	When installing the kiosks, stakeholders, along with the city, will look at different operating scenarios including how to deal with the scenarios when travelers are waiting for their ride or need to access the kiosk in off hours.	S-JA	S1	E-H	E4	C-J	C3	B
56	Planned travel modes are not readily available to users within a reasonable amount of time as shown by the kiosks.	Travelers plan the trip and the travel modes are not available as booked to continue their journey and might be stranded there for long which may result in a safety issue for the user.	Kiosk at the site will be able to offer alternate transportation options for calling taxi or other transport. Emergency call button available for passengers. Alert notifications sent out to site/social media/news media. Signage at the site will be able to provide contact information to other transportation modes.	S-JA	S1	E-C	E1	C-J	C3	QM
57	Passengers not utilizing safety features of bike shares, scooters, etc. when starting their ride from the mobility hubs.	Safety risk to the travelers. Travelers while using bikes, scooters etc., at the mobility hubs do not follow the safety standards (like wearing helmet) required while using these transportation modes and potentially create a safety risk.	The user agreements and local laws cover the safety standards before the traveler starts the ride with any transportation modes. Scooters and bikes will require the user to wear a helmet while riding. Mobility Providers can encourage the users of the scooters by giving out free helmets.	S-L	S1	E-S	E2	C-X	C3	QM
Multimodal Trip Planning Application/Common Payment System										
58	When the traveler cannot plan his or her entire trip origin-destination (including FM/LM options) due to system-unrelated event, such as a traffic incident or other emergency event.	Travelers unable to plan the trip as the travel modes are unavailable and traveler might be stranded at the location for long, which may result in a safety issue for the user.	App should be able to offer alternate transportation options for calling taxi or other transport. ConOps includes scenarios for changes in plans. Signage at the site will be able to provide contact information to other transportation modes.	S-JA	S1	E-K	E1	C-N	C3	QM
59	Planned travel modes are not readily available to users within a reasonable amount of time.	Travelers plan the trip and travel modes shown for the route are not available to continue their journey and might be stranded at the location for long, which may result in a safety issue for the user.	App should be able to offer alternate transportation options for calling taxi or other transport. ConOps includes scenarios for changes in plans. Kiosk at the site will be able to offer alternate transportation options for calling taxi or other transport. Emergency call button available for passengers. Signage at the site will be able to provide contact information to other transportation modes.	S-JA	S1	E-J	E2	C-J	C2	QM
60	Failure mode of the application results in the complete systemic disruption of the user's ability to access the transportation modes or complete the trip.	The MMTPA/CPS system is not working, and the users cannot access the system to continue their journey and might be stranded there for long, which may result in a safety issue for the user.	App should be able to offer alternate transportation options for calling taxi or other transport when not able to reach the central system.	S-JA	S1	E-I	E3	C-J	C3	A
61	Maintenance mode occurs when the system is operating in Backup mode to restore, repair, or replace system components.	Safety of the travelers. Travelers try to use the application and not able to connect because of the maintenance mode and wait to reserve other transportation modes. Safety issue when they wait long in an unsafe neighborhood.	These are planned events and should occur during off-peak hours to minimally impact users, and proper notification should be given to potential users in advance of the event when practical.	S-JA	S1	E-G	E1	C-J	C3	QM
62	Traveler is focused on the phone, not his or her surroundings (distraction). If headphones are in use, may not hear traffic or roadway noise as needed.	Safety of the traveler. Traveler pays attention to his or her phone trying to follow the instructions provided by the application and is distracted, not paying attention to the surroundings. The distraction of the traveler may result in a crash causing a safety issue to the traveler and the roadway users.	Road safety education and awareness programs are vital for discouraging the use of applications that stimulate unsafe driving/walking behaviors. Educating the traveling public about the dangers of unsafe driving/walking behavior could have significant safety benefits to all road users.	S-A	S3	E-V	E2	C-Y	C3	B

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
63	Malicious functionality: active monitoring of the traveler causes hacking of traveler account/activity.	Creates the potential for unauthorized account activity (related to payments, trip planning, personal data, etc.) while user trying to reserve a parking space using the mobile application. Also, app might store the user information when creating the user account.	Work with the developer to restrict the permissions requested by the app to only what is necessary for functionality. Development of the app along with vendor will provide visibility and customization allowing for more exposure of code base and how it functions. Make only services available to the user (availability of transportation modes, maps) that are related to the MMTPA/ CPS project.	S-I	S0a	E-T	E1	C-S	C3	-
64	Vulnerabilities for data transmission and storage.	Increased potential for identify theft because of storage of the data collected from the app users including credit card information, billing information that is used while booking a ride.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality. Include lessons learned and best practices in the security measures. Perform routine information security audits. Avoid collecting unnecessary or sensitive information from participants.	S-I	S0a	E-T	E1	C-S	C3	-
Mobility Assistance for People with Cognitive Disabilities										
65	Application provides inaccurate, incomplete, or incorrect walking instructions to the traveler with cognitive disabilities.	Safety of the traveler. The directions provided by the application are incorrect and traveler not realizing it, follows the instructions provided by the application and ends up at the wrong address, which might be an unsafe location.	Training that is customized to type of disability, instructions, etc. Coaching of pilot participants will be provided. For travelers with severe disabilities, coach may accompany the traveler on the trip (decided by multiple stakeholders in advance of the trip being planned).	S-K	S2	E-Q	E2	C-Y	C3	A
66	Application is not updated with current traffic/pedestrian information that will impact route provided to the traveler.	Safety of the traveler. The directions provided by the application are not up to date and the traveler may take a long route to reach the destination or might even end up in the wrong place.	Training recommends traveler to utilize “Help” feature within the application that will contact the traveler's caregiver. Training provided to the traveler will include all safety risk scenarios and how to react to these scenarios.	S-K	S2	E-J	E2	C-Y	C3	A
67	Application freezes or shuts down and the traveler cannot access it.	Safety of the traveler. MAPCD application malfunctions mid-trip, and the step-by-step navigation instructions are not provided to the traveler. The traveler may be stranded in an unsafe neighborhood with no further directions provided.	Assuming traveler is not with a coach; training indicates for the traveler to re-start the program and contact his or her ICE (in case of emergency contact). Training provided to the traveler will include all safety risk scenarios and how to react to these scenarios.	S-K	S2	E-K	E1	C-Y	C3	QM
68	Traveler selects incorrect route when departing his or her location.	Safety of the traveler. Traveler enters incorrect address in the MAPCD app. The app provides the directions for the address entered and traveler ends up in the wrong place.	Training recommends traveler to utilize “Help” feature within the application that will contact the traveler's caregiver. Training provided to the traveler will include all safety risk scenarios and how to react to these scenarios.	S-K	S2	E-M	E1	C-Y	C3	QM
69	Application malfunctions midtrip, and no instructions can be created.	Safety of the traveler. MAPCD application malfunctions mid-trip and the step-by-step navigation instructions are not provided to the traveler. The traveler may be stranded in an unsafe neighborhood with no further directions provided.	Assuming traveler is not with a coach; training indicates for the traveler to re-start the program and contact his or her ICE (in case of emergency contact). Training provided to the traveler will include all safety risk scenarios and how to react to these scenarios.	S-K	S2	E-K	E1	C-Y	C3	QM
70	Caregiver is not updated with the latest information of the traveler location.	Safety of the traveler. Missed communication between traveler and caregiver, and caregiver does not receive real-time feedback on traveler location, and in an emergency the caregiver is provided with inaccurate information about the location of the traveler.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality. Caregiver will be able to call the traveler at any time (voice call) to check in and provide their location information. City will be providing data plan to all the 30 participants to be able call the caregiver any time.	S-K	S2	E-K	E1	C-Y	C3	QM

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
71	Traveler is focused on the phone, not his or her surroundings (distraction). If headphones are in use, may not hear traffic or roadway noise as needed.	Safety of the traveler. Traveler pays attention to the phone trying to follow the instructions provided by the application and is distracted, not paying attention to the surroundings. The distraction of the traveler may result in a crash causing a safety issue to the traveler and the roadway users.	Visual and audio cues; travel training with the participants will be conducted before travelers can go out on the route (three levels of training: 1) group/lecture, 2) real-world simulation at COTA using Preview feature within WayFinder, 3) real-world training (on the route)). Goal of the training process is to have failures occur and be resolved prior to real-world use.	S-A	S3	E-V	E2	C-Y	C3	B
72	Traveler leaves the phone in the transit vehicle when he or she departs.	Safety of the traveler. Traveler forgets his or her phone in the transit vehicle and will not receive post-vehicle instructions. Traveler may be stranded in an unsafe neighborhood.	Current training will include travel training to guide travelers without a phone – identifying someone that can assist them (bus driver, police officer, etc.). For travelers with severe disabilities, coach may accompany the traveler on his or her trip (decided by multiple stakeholders in advance of the trip being planned).	S-K	S2	E-M	E1	C-Y	C3	QM
73	Application cannot accommodate changes to route/vehicle (if a vehicle breaks down mid route, and a traveler must change buses).	Safety of the traveler. Traveler transit vehicle breaks down and the application cannot provide route information to carry the trip. Traveler may be stranded in an unsafe neighborhood and may encounter an unsafe situation.	When traveler goes off route, a text is sent to the traveler's primary caregiver. These messages can continue at a prescribed time interval until the individual is back on route.	S-K	S2	E-I	E3	C-Y	C3	B
74	Traveler's phone does not have enough battery to provide instructions throughout the entire trip.	Safety of the traveler. Traveler's phone switches off and will not have instruction to continue the route. Traveler may be stranded in an unsafe neighborhood.	Current training will include travel training to guide travelers without a phone – identifying someone that can assist them (bus driver, police officer, etc.). Also, battery level can be checked when route is selected to alert traveler when battery level is low.	S-K	S2	E-M	E1	C-Y	C3	QM
75	Cell phone network goes down and the traveler cannot contact his or her caregiver if needed.	Safety of the traveler. Traveler may not be able to communicate with his or her caregiver due to the network loss, which might result in the safety issue to the traveler waiting for instructions.	Application only requires GPS (does not need Wi-Fi). City will also provide data plan to 30 participants in the plan. Also, the travelers will be trained to operate independently or depending on the disability level, a coach will accompany the traveler to guide throughout travel.	S-K	S2	E-K	E1	C-Y	C3	QM
76	Stop sign to cross the street instead of a walk sign.	Safety of the traveler. When following the step-by-step instructions provided by the app, there is a situation when there is stop sign at the street where the traveler needs to cross the street.	Stops can be personalized (if person creating the route includes this information). Participants will either be able to navigate independently as a pedestrian or will have a coach with them to assist on these types of stops. Training provided to the traveler will include all the safety scenarios and how to react to these scenarios.	S-A	S3	E-H	E4	C-Y	C3	D
77	Non-ADA-compliant crosswalks in the step by step navigation.	Safety issue for the traveler when the side walk ramps are not ADA-compliant and the traveler need to cross the street when following the instructions provided by the app.	A human creates routes, not an algorithm, and they be personalized. Caregiver (family, coach) has the responsibility for understanding and accounting for these requirements when creating the route.	S-L	S1	E-H	E4	C-Y	C3	B
78	The Help contact does not respond to the traveler's request.	Safety of the traveler. If lost, traveler cannot connect with their Help contact for additional guidance.	Training would also guide traveler to use phone capabilities on how and when to contact a secondary person when assistance is needed.	S-B	S0a	E-M	E1	C-Y	C3	-
Prenatal Trip Assistance										
79	Trip scheduled by the prenatal traveler is cancelled and the prenatal traveler is not informed about the cancellation of her ride.	Safety of the prenatal traveler. While waiting for her ride, she may encounter safety issues when at an unsafe location.	Passenger can contact call center for alternative. She can also contact the call center and get a last-minute pickup.	S-JA	S1	E-J	E2	C-R	C3	QM

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
80	Trip scheduled by the prenatal traveler for her doctor visit is late for the pickup.	Safety of the pregnant woman. Prenatal Traveler may encounter safety issues while waiting for her ride at an unsafe location.	Passenger can contact call center for alternative. She can also contact the call center and get a last-minute pickup. Notification to the medical office will be sent about the late arrival of the prenatal traveler. Check vendor responses.	S-JA	S1	E-J	E2	C-R	C3	QM
81	App is under maintenance and prenatal traveler cannot schedule a ride or obtain any updates about delayed or cancelled trips.	Safety of the pregnant woman. Waiting for her ride and encounter safety issues when at an unsafe location.	Passenger can contact call center for alternative. Training for the app use and how to react to different situations.	S-JA	S1	E-G	E1	C-J	C3	QM
82	Malicious functionality: Active monitoring of the traveler causes hacking of traveler account/activity.	Creates the potential for unauthorized account activity. Also, app might store the user information when creating the user account.	Work with the developer to restrict the permissions requested by the app to only what is necessary for functionality.	S-I	S0a	E-T	E1	C-S	C3	-
83	Vulnerabilities for data transmission and storage.	Increased potential for identity theft because of storage of the data collected from the app users.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality. Include lessons learned and best practices in the security measures. Perform routine information security audits. Avoid collecting unnecessary or sensitive information from participants.	S-I	S0a	E-T	E1	C-S	C3	-
84	When the prenatal traveler doesn’t have access to a mobile phone and won’t be updated when her ride back from the doctor visit is late or cancelled.	Safety of the prenatal traveler. Prenatal traveler does not have access to her phone and will miss updates about her ride being late or cancelled returning from her doctor’s visit. Prenatal Traveler may encounter safety issues while waiting for her ride at an unsafe location.	Traveler will be able to call the call center from the doctor’s office for her ride back. Training will be provided to the prenatal traveler how to react to different situations and how to contact call center when she does not have access to her mobile.	S-JA	S1	E-K	E1	C-N	C3	-
85	Pregnant woman feels more stressed while trying to use the app.	Prenatal traveler trying to use the app for the first time and feels more stressed.	Feedback from the focus groups about the application developed and design based on the feedback received. Pregnant woman can use web to schedule trips.	S-G	S0	E-S	E2	C-Y	C3	-
86	The ride arrived for the prenatal traveler pickup is less user friendly and doesn’t not follow the safety standards while driving the prenatal traveler.	Safety of the prenatal traveler. Ride provided to the prenatal traveler did not follow the safety standards and results in the injury of the prenatal traveler.	Car choice will be given to the prenatal traveler when scheduling the appointment based on her requirements.	S-E	S3	E-M	E1	C-X	C3	A
87	Car seats are provided by vendor upon request and the car seat is not installed properly and the child is injured.	Safety of the child traveling with the prenatal travel in her ride to the doctor office. The car seat provided by the vendor is not installed properly by the driver and the child may be injured due to the improper installation of the car seat.	Training will be provided to all the vendor drivers regarding all the safety features and driver will also be trained how to react in different situations.	S-E	S3	E-E	E2	C-J	C3	B
88	The car seats provided to the vendor might have bed bugs and lice.	Safety of the prenatal traveler and her kids. Both the traveler and her kids might get infected by bed bugs and lice while traveling with the car seat provided.	Disposable covers for the car seats that can be used; Lysol wipes will be provided for the safety of the child. Policies and procedures of the driver training will include the installation and protection procedures of the car seats.	S-M	S1	E-K	E1	C-N	C3	QM
89	Traveler enters incorrect destination when planning a trip.	Prenatal traveler is taken to the wrong location; misses her appointment; needs to contact provider to plan another trip.	Application design allows storage of frequent destination by name for selection by drop down. Training materials will also cover proper planning of a trip and reviewing information before booking. If wrong trip is executed, passenger can contact call center for assistance in planning an alternative.	S-J	S0a	E-M	E1	C-W	C1	-
Event Parking Management										
90	Driver distraction from paying attention to the app while driving to find the parking location.	Safety of the driver and other roadway users. Driver not paying attention while trying to find the parking spot that he reserved through the application and encounters a safety issue.	The app should not cause a risk to the drivers. The application developed shall have verbal navigation for the driver. All interaction should only be for stopped vehicles.	S-E	S3	E-S	E2	C-S	C3	B

ID	Safety Risk	Safety Impact	Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
91	Malicious functionality: active monitoring of the traveler causes hacking of traveler account/activity.	Creates the potential for unauthorized account activity (related to payments, trip planning, personal data, etc.), while traveler is trying to reserve a parking space using the mobile application. Also, app might store the user information when creating the user account.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality.	S-I	S0a	E-T	E1	C-S	C3	-
92	Vulnerabilities for data transmission and storage.	Increased potential for identify theft because of storage of the data collected from the app users.	Work with the developer to restrict the permissions requested by the application to only what is necessary for functionality. Include lessons learned and best practices in the security measures. Perform routine information security audits. Avoid collecting unnecessary or sensitive information from participants.	S-I	S0a	E-T	E1	C-S	C3	-

Source: City of Columbus

Chapter 5. Safety Operational Concept

5.1. FUNCTIONAL SAFETY REQUIREMENTS

This section defines the functional safety requirements for the projects within the Smart Columbus demonstration program. The program Safety Management Plan has been developed following the principles of assigning an ASIL risk assessment of the identified safety scenarios for each project, as outlined in ISO 26262. The safety activities will be included and considered in future systems engineering documents along with the activities that will eliminate or mitigate them such as the hazard analysis, security analysis and risk assessment. The systems requirements (for Vee model projects) and development backlogs (for Agile projects) developed for the eight projects will include appropriate functional safety requirements to mitigate the safety scenarios that **Table 11** identifies. These are requirements to ensure safe operation of the hardware and/or software and the actions to be taken within each project's deployment to reduce the likelihood and potential impact of the safety scenarios. Some of the requirements will be combined because they overlap between scenarios. Other requirements will be split because they apply differently, based on different applications deployed under each of the eight projects. All requirements (including safety functional requirements) will be subject to verification, for which testing plans and procedures will substantiate that the requirement has been implemented.

5.1.1. Equipment Procurement

The following three Smart Columbus program projects will be installing equipment:

- **CVE:** OBUs will be installed in transit private, emergency and freight vehicles. In addition, a Human Machine Interface (HMI) will also be deployed in private vehicles, although the specific type of HMI will be determined during the procurement process.
- **CEAV:** Autonomous vehicles will be deployed along specific routes within the COC, which the Smart Columbus PMO and the project teams will determine. The operational concept document will list the routes that the AVs would be operating along with connected infrastructure that will be installed as part of the project.
- **SMH:** Will install kiosks at locations in Columbus to fill FMLM service gaps.

These projects will utilize quality equipment by requiring all the suppliers to submit and follow a quality management process, approved by Smart Columbus project management, for designing, constructing, producing, and testing their devices, subsystems and interfaces. This will help to ensure the equipment provided is properly assembled to assist with safe operations. The supplier's quality management will verify that system requirements, listed in the project SyRS, have been met with the oversight of Smart Columbus project management.

For the CVE project, device certification will be sought. If certification is not available by one of the three USDOT contracted certification bodies (Omni Air, DanLaw, or Layer7), manufacturer self-certification may be utilized. In this scenario, the acceptable QM plan for these devices will include the submission and approval of test plans, test procedures and test results. The system equipment shall be interoperable with other vendor equipment at any interfaces. Interfaces shall be compatible according to the system requirements and their standards as defined in the SyRS.

A safety review of the proposed operator interface will be performed. Lessons learned, and best practices will be included in the design. Safety checks for all the installed equipment will comprise the equipment reset functions, redundancy, security, and actions upon power loss and restoration which will be discussed in each project's documentation of the installed equipment.

5.1.2. Device Installation

Precautions and measures will be taken to make sure the equipment is properly installed to minimize the risks associated with equipment installation. The project, thus, requires all the installers to provide and follow a quality management process in installing the equipment. Installer/maintainers will be comprised of manufacturer approved vendors or Smart Columbus demonstration program partner personnel who have been sufficiently trained by manufacturer approved vendors.

As **Table 5** shows, only the CVE, CEAV and SMH projects will require hardware installations by developers. The other projects require only participant smartphones.

- CVE RSUs and OBUs will be installed by trained and qualified manufacturer installers. The OBU installations will require the most planning as OBUs will need to be retrofitted to a variety of privately-owned vehicles and COTA buses. The OBU manufacturer will submit an installation plan that will meet the CVE user needs and system requirements. Installers will need to follow the installation safety requirements. Lessons learned in the USDOT CV Pilots will be applied as appropriate to the CVE installation process.
- CEAVs will come prepackaged and tested in the manufacturer's plant and any related equipment external to the vehicles will be installed according to the safety requirements of the CEAV quality management plan.
- SMHs will be kiosks openly available to the public and installed according to the system design requirements.

A design review of the device installation will be performed, and safety checks will be completed for the installation that consider the condition of the vehicle or smart mobility hub site, bypasses, manual shutdown, security, possible overload conditions and a safety review of the proposed location of the OBU and of the Smart Mobility Hubs. Installation will be verified before deployment, including specific end-of-line testing and checklists. The draft installation plan will include details on the quality management activities described in this document for CVE, CEAV, and Smart Mobility Hubs. The draft site map and installation schedule will be developed following the system requirements phase for these three projects.

Final project documentation, lessons learned, and best practices used in the installation procedures will be shared with other cities interested in pursuing similar efforts.

5.1.3. Fail-Safe System Mode

All eight projects within the Smart Columbus program will have a fail-safe system mode. The system will revert to a fail-safe mode upon failure of the system to meet necessary and essential operational capabilities as defined in each project's system requirement documentation. Failsafe mode intends to guarantee that, in the event of a system failure, the system, applications and devices will respond in a way that will not harm the system, devices, participants or other road users. It is a safeguard that prevents safety risks to people and property, if failure occurs. The design mitigates unsafe consequences of the system's failure.

The system default position may be the fail-safe mode in which the user does not receive safety or mobility feedback from the unit and must drive unassisted. Therefore, in the event of a failure, the system and devices return to default mode, about which the participant will be familiarized during training program. Each project's system requirements document presents additional detail about their respective fail-safe modes. Safety management will include the periodic testing of these conditions and following established procedures.

5.1.4. Quality Training

All system operators, system maintainers, installer/maintainers and owners of a response plan included referenced herein will receive adequate, approved training based on their point of interface with the system. This training will be documented as it occurs as part of the Smart Columbus demonstration program.

While systems and installer trainings are essential, the most critical aspect of safety training concerns the project participants who will be using the project devices in the street environment. Development and implementation of participant training for the projects will be evaluated as the teams move into the design phase. In several projects, an IRB will oversee safety, which will be further strengthened by an informed-consent document that explains safety and data privacy risks to participants.

For projects that an IRB oversees, the IRB may require participant trainers to be certified in protecting human research participants to work with the participants. Training may be required for project staff involved with project management, person-to-person recruitment of participants, explanation of the informed-consent document, training of participants, the Safety Manager, caregivers and others who may work with participants.

Each Smart Columbus project has a training plan based on the infrastructure and device installation that will installed. A training plan which will be discussed in detail in the QM process of each project.

5.2. SAFETY MANAGEMENT

Safety management is the oversight of the activities necessary to ensure the safe execution of the project's deployment, which includes preparing this document and ensuring the project teams follow through with the plans. As the deployment begins for each of the listed applications for each project, the project team will ensure that functional safety requirements in the project's SyRS are met. The systems engineering process supports and advances all the safety requirements that are identified in the SyRS or project backlog (for projects using the Agile software methodology) as the requirements are carried out through design, implementation, verification and validation. Requirements are systemically designed to flow down to the design and acquisition activities. Suitable verification of safety requirements will be performed and documented as part of the SyRS check list of requirements. Safety management also includes policies that need to be carried out during the deployment phase, such as ensuring equipment is calibrated and installed as per the safety requirements, speed limits are enforced strictly for the CVE and CEAV routes, end user agreements for applications that will be deployed in Columbus, user training for applications like MAPCD and PTA, and TMC operator and Operating System training is conducted. The policies for each project will be identified and developed as part of the engineering and IRB process for each project; the list presented in this paragraph is not intended to be exhaustive for all the projects.

All Smart Columbus projects will develop operations and maintenance plans or a standard operating procedures guide. These documents will include and address safety management procedures and practices to be followed during the demonstration period.

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

The Smart Columbus PMO has appointed a Safety Manager for the deployment phase of the program. At a high level, the safety manager's role will be to work with project leadership, suppliers, systems engineers and other stakeholders. Each project team will also identify certain staff to ensure that the elements of the risk response plan are implemented and documented.

5.2.1. Safety Manager Responsibilities

The Smart Columbus Safety Manager's role will be to work with the COC, project teams, suppliers/vendors, systems engineers and other stakeholders. The following are some of the key safety coordination areas that the safety manager will be responsible for:

- Leadership and direction in safety procedures
- Ensuring compliance with applicable regulations and the Safety Management Plan
- Ensuring Safety Management is represented in the informed-consent documents and participant training
- Incorporating safety into design, deployment, and operational phases
- Guidance for equipment procurement and acceptance
- Oversight for device certification, testing and installation
- Safety leadership for maintenance and updates
- Operational safety and monitoring
- Incident reporting, documentation, and investigation of the incident
- Maintaining and updating safety processes and the Safety Management Plan
- Safety coordination with other entities and task leads

5.2.2. Safety Reviews

Safety reviews support the Smart Columbus PMO focus on safety, ensure compliance with the Safety Management Plan, and identify opportunities to improve safety. Regular assessments help to identify any new safety risks and develop the appropriate control measures. The review panel will be identified/defined prior to the review and will likely include members of the PMO and project team (to include vendors and testers), although independent/third party staff may also be considered to offer an objective opinion on the review.

When safety reviews are conducted, the reviewers will ensure that:

- Appropriate technical experts and team members conduct review.
- Identify improvement opportunities.
- Communicate outcomes to team members.
- Implement actions that arise from reviews.
- Maintain ongoing operations monitoring for compliance with the Safety Management Plan.

Certain project milestones and events will prompt the following reviews:

- Each project deliverable will include a review to determine the potential impacts to the safety risk assessment and which measures the deliverable can include to mitigate risks.
- During design and before project installation.
- Safety and system security reviews before deployment.
- Equipment, software, and process checks before deployment.
- Periodic equipment, software, and process checks during operation.
- Regular safety communications and updates.
- After an incident.

- After a critical event or significant change that could affect safety.
- After a participant, team member or other individual submits a safety-related complaint.
- After a change to applicable standards and codes of practices.

Figure 5 illustrates the Safety Incident process described above.

5.2.3. Safety Incident Reporting

Reporting an incident helps identify improvements that can prevent the incident from reoccurring. The Smart Columbus PMO anticipates that a safety incident reporting policy will be developed before any Smart Columbus project goes live. The policy will accomplish the following actions:

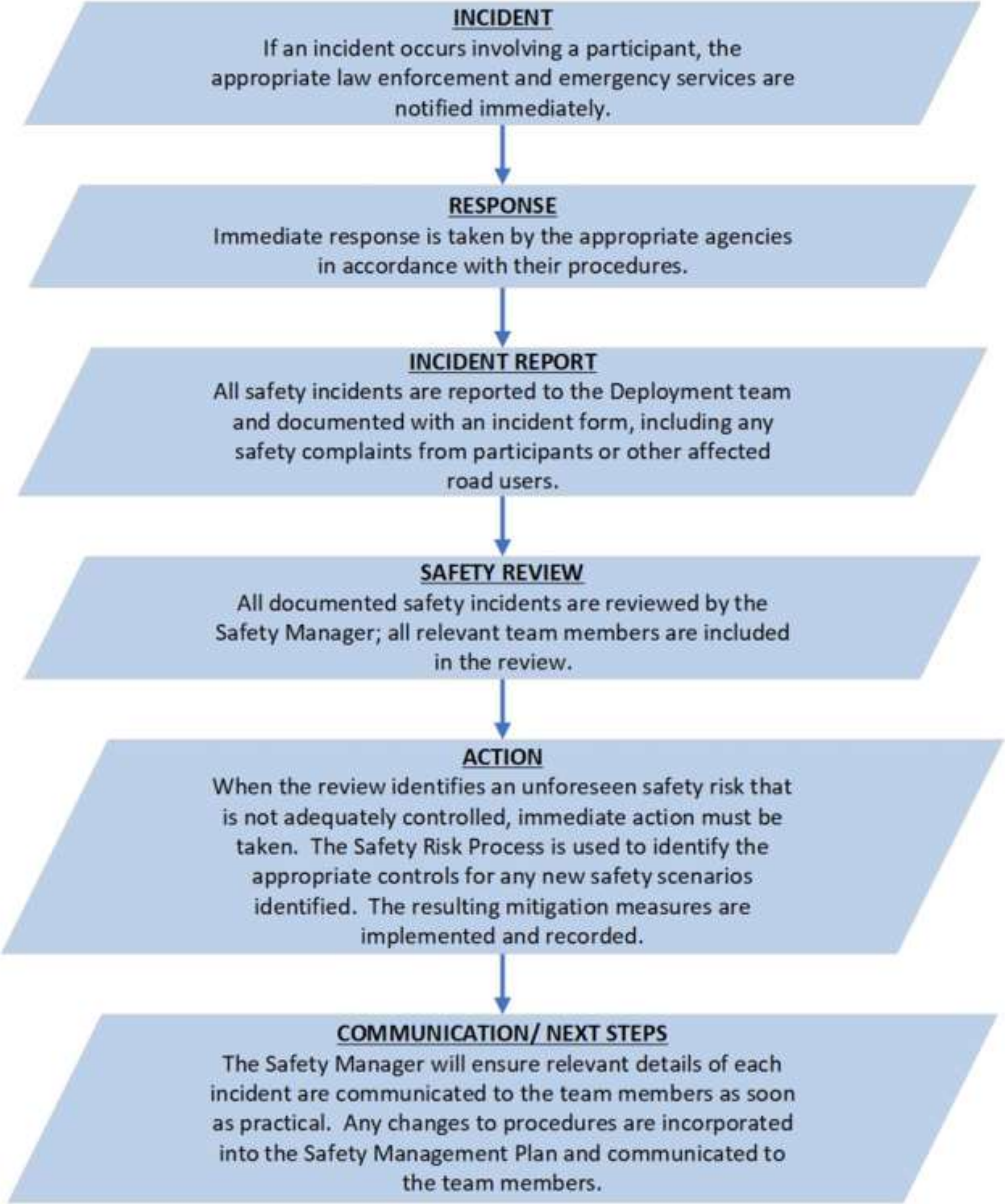
- Report and record all safety incidents.
- Safety Manager will use draft Incident Report Form, which the project teams have yet to develop.
- Participants will receive guidance about safety reporting during training and in the informed-consent document.
- Safety incidents will be investigated, and the underlying causes identified.
- Serious harm incidents will prompt a review of application performance.
- A regular review of all safety incidents occurs to identify any trends.
- System upgrades will be undertaken as needed for safety.
- Participants will be notified, as needed, of systemic safety problems that occur and/or of system upgrades to their applications.

Figure 5 illustrates the safety incident process.

5.2.3.1. PRIVACY INCIDENTS

While not causing physical harm to any one person, privacy incidents, such as breach of PII or Sensitive PII (SPII), may adversely affect persons whose employment, finances, healthcare or personal security could be compromised by data or identity theft.

Treatment of privacy incidents is described in the DPP. To summarize, data privacy has standard built-in protections that include filtering and de-anonymizing of PII before it would be stored for use. Per the Informed Consent Document that each participant signs, affected participants will be notified of a data breach and informed of what Smart Columbus data managers are doing about it. The IRB will be informed of the data breach and the IRB or the PMO will inform U. S. Department of Health and Human Services (HHS) of the breach, according to the provisions of HHS guidelines.



INCIDENT

If an incident occurs involving a participant, the appropriate law enforcement and emergency services are notified immediately.

RESPONSE

Immediate response is taken by the appropriate agencies in accordance with their procedures.

INCIDENT REPORT

All safety incidents are reported to the Deployment team and documented with an incident form, including any safety complaints from participants or other affected road users.

SAFETY REVIEW

All documented safety incidents are reviewed by the Safety Manager; all relevant team members are included in the review.

ACTION

When the review identifies an unforeseen safety risk that is not adequately controlled, immediate action must be taken. The Safety Risk Process is used to identify the appropriate controls for any new safety scenarios identified. The resulting mitigation measures are implemented and recorded.

COMMUNICATION/ NEXT STEPS

The Safety Manager will ensure relevant details of each incident are communicated to the team members as soon as practical. Any changes to procedures are incorporated into the Safety Management Plan and communicated to the team members.

Figure 5: Safety Incident Process

Source: City of Columbus

Chapter 6. Coordination with Other Tasks

Part of safety management is coordinating tasks in the deployment of the SCC Program so that safety needs are addressed throughout it. The safety needs and operational concepts discussed in this plan will be incorporated into the program portfolio by the project leads and team members who coordinate tasks during their monthly progress meetings. It is the intention of the Smart Columbus team to avoid "stove piping" tasks and projects and reduce isolation of systems development among the projects, except as necessary for system integrity protection. Agreement between project systems across artificial boundaries is a goal of project coordination and is an essential feature of the Operating System. The following subsections explain how the systems engineering process advances safety in the SCC Program. With the exception of the Operating System, individual projects oversee participant physical safety. The Operating System does not address participant physical safety, per se, but rather secures data collection and overall system integrity. The following subsections explain how the systems engineering process advances safety in the SCC Program.

6.1. TASK B: CONCEPT OF OPERATIONS

Safety scenarios in this Safety Management Plan follow the ConOps, operational concept or trade studies developed for the eight Smart Columbus projects based on the project type. These documents list the user needs, applications to be deployed and operational practices to be followed for each project. Chapter 5, Safety Operational Concept was developed in coordination with the proposed operational practices described in these conceptual documents for each project.

6.2. TASK B: SYSTEMS REQUIREMENTS SPECIFICATION

The System Requirements Specification Plans include functional requirements, interface requirements, data requirements, performance requirements, security requirements etc., for all the systems that will deployed as part of the Smart Columbus demonstration program. The Safety Management Plan lists all the requirements and the safety risks associated with those requirements. This Safety Management Plan will be incorporated into the respective SyRS documents developed for all the Smart Columbus projects. For projects following the Agile software development methodology (MMTPA/CPS, PTA, and CEAV), the development backlog will contain the traceability to requirements.

6.3. TASK B: SYSTEM ARCHITECTURE AND STANDARD PLAN

The Systems Architecture and Standards Plan (SASP) documents the architecture for systems associated with the Smart City program and associated standards that will be used. The architecture document captures enterprise, functional, physical and communications architecture of the system architecture. The SASP will follow this Safety Management Plan's assessments of risks, impacts and mitigations to the extent that they apply to and influence the architecture.

6.4. TASK B: INTERFACE CONTROL, SYSTEM DESIGN AND TEST PLAN DOCUMENTS

The Interface Control, System Design and Test Plan documents should refer to the Safety Management Plan to make sure all the safety risks listed in this plan in **Table 11** are addressed while designing and testing the system and applications developed in the Smart Columbus demonstration program.

6.5. TASK C: PERFORMANCE MANAGEMENT PLAN

The methods and processes detailed in the Performance Measurement and Evaluation Support Plan need to be consistent with the safety operational concept discussed in chapter 5 in this Safety Management Plan. Performance measurement will be done electronically and over the air, and so will not endanger safety of persons. The data security issues discussed in the DPP, and briefly summarized in **Section 5.2.3.1**, apply to performance measurement data and metadata which might be used to identify persons and compromise PII.

6.6. TASK D: DATA PRIVACY PLAN

The Safety Management Plan outlines the high-level mitigation for the risks identified for the privacy and security of the participants and the system. The Smart Columbus DPP provides detailed protections and mitigation for data risks identified to protect the privacy of the users and ensure secure operations. The DPP works with this Safety Management Plan to ensure that PII is secure and that SPII, particularly that of vulnerable populations such as users of the MAPCD and PTA, are protected. Any breach in data security with PII loss will be reported to participants along with the measures taken by the Smart Columbus program team to ensure safety of the participants. Also, the IRB will be notified and the HHS, as needed, per HHS Guidelines.

6.7. TASK E: DATA MANAGEMENT PLAN

While the Safety Management Plan outlines high-level mitigation strategies for the data storing risks identified, the Smart Columbus DMP describes how data will be collected, managed, integrated, and disseminated before, during, and after the Smart City program. The DMP also provides detailed protections and mitigation for data risks identified to protect the privacy of the users and ensure secure operations. The DPP and DMP work to ensure that data privacy and operations are secure.

6.8. TASK E: HUMAN USE APPROVAL SUMMARY

The Smart Columbus Human Use Approval Summary aims to document the efforts made to ensure the protection of personal information, which is the purview of the DPP, and human safety, which includes the mitigation strategies discussed in this Safety Management Plan. The Safety Management Plan, with safety scenarios and associated safety operational concepts, is necessary to obtain IRB approval to proceed for any project requiring IRB oversight (see **Table 5** for IRB oversight of projects). An IRB-approved Informed Consent Document will instruct participants that, in the event of a data breach of PII or SPII, they will be notified of the breach and what the Smart Columbus PMO is doing about it. Participants will be instructed in proper device use, that the devices in the projects are only aids to travel and that they, as travelers, are responsible for their travel behavior while using the devices. The Informed Consent Document will inform participants where to call and what to do if help is needed.

6.9. TASK G: COMMUNICATIONS AND OUTREACH

Communications and Outreach includes Participant Training and Stakeholder Education. These activities identify the roles that program staff will take during the deployment, their actions, responsibilities, and training requirements. Communications and Outreach will be consistent with the actions described in the Safety Management Plan to reduce the likelihood and potential impact of each safety scenario.

Chapter 7. Conclusions

The Safety Management Plan provides guidance material about the identification of safety scenarios and risk mitigation for the Smart Columbus demonstration program. The plan identifies the safety scenarios at both program-level and project-level, assesses the level of risk for each scenario, and provides a safety operational concept for high/medium risk scenarios. Safety stakeholders for each project were identified and coordination with emergency responders was incorporated in the Safety Management Plan.

At this time, the Smart Columbus PMO has determined that the risks to the demonstration program are manageable. For the CVE and CEAV projects, the conservative approach of delivering only alerts and not permissive messages means that many applications will naturally fail to a safe condition. Training of all participants, from mechanics to drivers will be necessary. For the projects deploying mobile applications, training will be provided to the users willing to use the application. Careful attention to details in design, software requirements, combined with diligent testing, will address many of the safety risks identified in **Table 11**. Ongoing safety management throughout the remainder of the project will ensure follow-through.

Additional conclusions and next steps regarding safety management for both the program and projects include:

- A named project manager will lead a safety team to continue to follow all the scenarios. The purpose will be to document verification of safety-related requirements and to coordinate safety-related activities of all stakeholders, under the direction of Smart Columbus PMO.
- For projects receiving IRB oversight, participant training and the Informed Consent Document will advise participants of the safety problems that might arise and how to get aid, if needed.
- While the ConOps and SyRS documents are finalized for the projects, refined analysis may lead to more safety scenarios being identified. They will be rated and tracked along with those already identified. Some of the safety scenarios will be addressed by writing safety requirements and verifying designs to those requirements. They will be tracked through design and development phases of the program. Other hazards will require ongoing safety management through the duration of the deployment phase.
- As the project proceeds to detailed design, safety requirements will be allocated to systems and subsystems, and to their interfaces. Evidence that requirements have been met will be collected, scrutinized, and documented. The level of documentation and independent review will be in accordance with the rating of each safety risk assigned.

Appendix A. Acronyms and Definitions

Table 12: Acronym List contains project specific acronyms used throughout this document.

Table 12: Acronym List

Abbreviation/Acronym	Definition
ADA	Americans with Disabilities Act
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicle
BRT	Bus Rapid Transit
CMAX	COTA's Bus Rapid Transit (BRT) Service
COC	City of Columbus
ConOps	Concept of Operations
COTA	Central Ohio Transit Authority
CPS	Common Payment System
CV	Connected Vehicle
CVE	Connected Vehicle Environment
DMP	*Data Management Plan for the Smart Columbus Demonstration Program*
DPP	*Data Privacy Plan for the Smart Columbus Demonstration Program*
DSRC	Dedicated Short Range Communications
E/E	Electrical and Electronic
EHS	Enhanced Human Services
EMS	Emergency Medical Services
EPM	Event Parking Management
FHWA	Federal Highway Administration
FMLM	First Mile/Last Mile
GPS	Global Positioning System
HHS	U. S. Department of Health and Human Services
HMI	Human Machine Interface
IRB	Institutional Review Board
ISO	International Organization for Standardization
ITS	Intelligent Transportation System
MAPCD	Mobility Assistance for People with Cognitive Disabilities
MMTPA	Multimodal Trip Planning Application

Abbreviation/Acronym	Definition
NEMT	Non-Emergency Medical Transportation
ODOT	Ohio Department of Transportation
OBU	Onboard Unit
Operating System	Smart Columbus Operating System
OSU	Ohio State University
PII	Personally Identifiable Information
PTA	Prenatal Trip Assistance
PMO	Program Management Office
QM	Quality Management
RCTM	Radio Technical Commission for Maritime Services
RSU	Roadside Unit
SASP	Systems Architecture and Standards Plan
SCC	Smart City Challenge
SMH	Smart Mobility Hub
SMP	Safety Management Plan
SPII	Sensitive Personally Identifiable Information
SyRS	System Requirements and Specifications
TMC	Traffic Management Center
TNC	Transportation Network Company
USDOT	U.S. Department of Transportation
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
VRU	Vulnerable Road User

Source: City of Columbus

SM
RT
COLUMBUS

THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR