SMRT COLUMBUS

Annual Safety Review

for the Smart Columbus Demonstration Program

April 9, 2021

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

The safety reviews ensure compliance with the Safety Management Plan and identify opportunities to improve safety. The review panel include members of the Smart Columbus Project Management Office and project team (including vendors and testers), and independent/third party staff was also considered to offer an objective opinion on the review. Safety reviews will be conducted either annually, prior to a project's launch, or when an incident occurs. This document compiles the Annual Review completed March-April 2021.

Table of Contents

List of Tables

Chapter 1. Safety Review for Smart Columbus Projects

1.1. INTRODUCTION

Safety reviews are conducted either annually, prior to a project's launch, or when an incident occurs. When safety reviews are conducted, the reviewers will ensure that:

- Appropriate technical experts and team members are present
- Improvement opportunities are discussed and/or identified
- Review outcomes are communicated to the Smart Columbus Project Management Office (PMO) and project team members
- Follow up is completed with project team regarding actions that arise from reviews
- Ongoing operations are monitored for compliance with the Safety Management Plan (SMP)

As identified in **Table 1**, for 2021 annual safety review, all Smart Columbus projects were considered to be in the project completion phase. Review meeting agenda that was used for this review is included in **Appendix B**. The revised Risk Assessment reflecting up-to-date risks, safety impacts and mitigation strategies can be found in **Appendix A, Table 14**.

Table 1: Smart Columbus Projects' Status

Smart Columbus Project	Project Status
Smart Columbus Operating System (Operating System)	Project Complete
Connected Vehicle Environment (CVE)	Project Complete
Connected Electric Autonomous Vehicles (CEAV)	Project Complete
Smart Mobility Hubs (SMH)	Project Complete
Multimodal Trip Planning Application (MMTPA)	Project Complete
Mobility Assistance for People with Cognitive Disabilities (MAPCD)	Project Complete
Prenatal Trip Assistance (PTA)	Project Complete
Event Parking Management (EPM)	Project Complete

Source: City of Columbus

1.1.1. Project Completion Review

Project competition review is conducted when the demonstration period for a Smart Columbus project has ended. As defined in the cooperative agreement with USDOT, all projects will be in demonstration for at least 12 months or until March 31, 2021.

1.1.1.1. SMART COLUMBUS OPERATING SYSTEM

Table 2: Smart Columbus Operating System

Smart Columbus Operating System - Annual Safety Review	
Name of Reviewer: Andy Wolpert	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021
Version of the Risk Assessment that reflect the below changes: **Revision:** 2021 Annual Safety Review	**Date:** 4-7-2021
Review Notes: **Were there any new safety issues identified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Review Notes: **Were there any safety issues identified as obsolete?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Review Notes: During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below. **Were there any mitigation strategies listed for identified safety issues modified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Andy Wolpert		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.2. CONNECTED VEHICLE ENVIRONMENT

Table 3: Connected Vehicle Environment

Connected Vehicle Environment - Annual Safety Review	
Name of Reviewer: Ryan Bollo	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021
Version of the Risk Assessment that reflect the below changes: **Revision:** 2021 Annual Safety Review	**Date:** 4-7-2021
Review Notes: **Were there any new safety issues identified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	

Review Notes:

Were there any safety issues identified as obsolete? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended risk and mitigation action: N/A

Review Notes:

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Ryan Bollo, P.E.		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.3. CONNECTED ELECTRIC AUTONOMOUS VEHICLES

Table 4: Connected Electric Autonomous Vehicles

Connected Electric Autonomous Vehicles - Annual Safety Review	
Name of Reviewer: Jeff Kupko	**Date of Review:** 3-26-2021 to 4-2-2021

What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.)

Project Completion

Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.)

Annual Safety Review

Version of the Risk Assessment that was used during the review:

Revision: 2020 Annual Safety Review **Date:** 12-23-2021

Version of the Risk Assessment that reflect the below changes:

Revision: 2021 Annual Safety Review **Date:** 4-7-2021

Review Notes:

Were there any new safety issues identified? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Review Notes:

Were there any safety issues identified as obsolete? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Review Notes:

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.4. SMART MOBILITY HUBS

Table 5: Smart Mobility Hubs

Smart Mobility Hubs - Annual Safety Review	
Name of Reviewer: Jeff Kupko	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021
Version of the Risk Assessment that reflect the below changes: **Revision:** 2021 Annual Safety Review	**Date:** 4-7-2021
Review Notes: **Were there any new safety issues identified?** (please select one) ☐ YES ☒ NO If **YES** – Describe the issue: If **YES** – Describe recommended mitigation action: N/A	
Review Notes: **Were there any safety issues identified as obsolete?** (please select one) ☐ YES ☒ NO If **YES** – Describe the issue: N/A If **YES** – Describe the issue and mitigation action: N/A	
Review Notes:	

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.5. MULTIMODAL TRIP PLANNING APPLICATION

Table 6: Multimodal Trip Planning Application

Multimodal Trip Planning Application - Annual Safety Review	
Name of Reviewer: Andy Wolpert	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021

Version of the Risk Assessment that reflect the below changes:

Revision: 2021 Annual Safety Review **Date:** 4-7-2021

Review Notes:

Were there any new safety issues identified? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Review Notes:

Were there any safety issues identified as obsolete? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Review Notes:

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Andrew Wolpert, P.E.	Andrew Wolpert	4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.6. MOBILITY ASSISTANCE FOR PEOPLE WITH COGNITIVE DISABILITIES

Table 7: Mobility Assistance for People with Cognitive Disabilities

Mobility Assistance for People with Cognitive Disabilities - Annual Safety Review	
Name of Reviewer: Andy Wolpert	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021
Version of the Risk Assessment that reflect the below changes: **Revision:** 2021 Annual Safety Review	**Date:** 4-7-2021
Review Notes: **Were there any new safety issues identified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Review Notes: **Were there any safety issues identified as obsolete?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Review Notes: During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below. **Were there any mitigation strategies listed for identified safety issues modified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO	

If **YES** – What was the issue identified? N/A		
If **YES** – Has the Safety Manager been contacted to include the risk? N/A		
(please select one) ☐YES ☐NO		
Andrew Wolpert, P.E.		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.7. PRENATAL TRIP ASSISTANCE

Table 8: Prenatal Trip Assistance

Prenatal Trip Assistance - Annual Safety Review	
Name of Reviewer: Andy Wolpert	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	
Version of the Risk Assessment that was used during the review: **Revision:** 2020 Annual Safety Review	**Date:** 12-23-2021
Version of the Risk Assessment that reflect the below changes: **Revision:** 2021 Annual Safety Review	**Date:** 4-7-2021
Review Notes: **Were there any new safety issues identified?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A If **YES** – Describe recommended mitigation action: N/A	
Review Notes: **Were there any safety issues identified as obsolete?** (please select one) ☐YES ☒NO If **YES** – Describe the issue: N/A	

If **YES** – Describe recommended mitigation action: N/A

Review Notes:

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

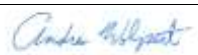
If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Andrew Wolpert, P.E.		4/7/2021
Project Manager's Name	Signature	Date
Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

1.1.1.8. EVENT PARKING MANAGEMENT

Table 9: Event Parking Management

Event Parking Management - Annual Safety Review	
Name of Reviewer: Ryan Bollo	**Date of Review:** 3-26-2021 to 4-2-2021
What type of review was it? (Project Completion, Deployment Review, Pre-Installation Review, Pre-Deployment Review, Design Review, etc.) Project Completion	
Purpose of the review: (Annual Safety Review, Periodic/Random Check, Post-Incident Review etc.) Annual Safety Review	

Version of the Risk Assessment that was used during the review:

Revision: 2020 Annual Safety Review **Date:** 12-23-2021

Version of the Risk Assessment that reflect the below changes:

Revision: 2021 Annual Safety Review **Date:** 4-7-2021

Review Notes:

Were there any new safety issues identified? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If YES – Describe recommended mitigation action: N/A

Review Notes:

Were there any safety issues identified as obsolete? (please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If YES – Describe recommended mitigation action: N/A

Review Notes:

During the safety review, each risk was reviewed for occurrence with the project team. If the risk has occurred, mitigation strategies were revised based on the strategy that was implemented in real-time. Only the risks, mitigation strategies, and ASIL scores that were modified during the safety review meeting are listed below.

Were there any mitigation strategies listed for identified safety issues modified?

(please select one) ☐YES ☒NO

If **YES** – Describe the issue: N/A

If **YES** – Describe recommended mitigation action: N/A

Were any new safety issues identified that should be included on the risk register for future reviews? (please select one) ☐YES ☒NO

If **YES** – What was the issue identified? N/A

If **YES** – Has the Safety Manager been contacted to include the risk? N/A

(please select one) ☐YES ☐NO

Ryan Bollo, P.E.		4/7/2021
Project Manager's Name	Signature	Date

Jeffrey J. Kupko, P.E., PTOE		4/7/2021
Safety Manager's Name	Signature	Date

Source: City of Columbus

Appendix A. Risk Assessment

A.1 RISK ASSESSMENT

The project teams examined all safety scenarios related to the installation of the devices for both the vehicle fleets, infrastructure and mobile applications that are deployed as part of the Smart Columbus program. The Concept of Operations (ConOps), System Requirements and Specifications (SyRS), Operations and Maintenance Plan, Data Privacy Plan (DPP), and Data Management Plan (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 Automotive Safety Integrity Level (ASIL) ratings identified which will necessitate additional planning around the safety operational concept: 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 of SMP[1] and includes provisions for equipment procurement, device installation, inclusion of 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 Smart Columbus team used classes of S0a and C0 for instances when the integrity level would be of inconsequential severity (S0a) or insignificant to control (C0). It is a combination of these attributes that results in the ASIL scores. Analysis of each of the identified safety

[1] https://d2rfd3nxvhnf29.cloudfront.net/2020-03/SCC-F-Safety%20Management%20Plan_12-05-2019_FINAL.PDF

scenarios and the level of severity, exposure and controllability was conducted using the ISO 26262 ASIL determination matrix shown in **Table 10,** which illustrates how the attributes are considered collectively to develop the integrity level.

Table 10: 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
	E4	B	C	D

Source: ISO 26262

As mentioned above, the Smart Columbus risk assessment includes ratings of S0a and C0 that are not in the ASIL ratings table (**Table 10**). These scenarios 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 14**.

The ASIL attributes are generally very broad. In their application of the ASIL methodology, the NYC CV Pilot developed more specific rating rules which they used to better classify their project risks according to the ASIL attributes. Likewise, Smart Columbus started with the rating rules developed by the NYC CV Pilot and updated them with input and feedback from the PMO, project teams and an independent reviewer from Battelle. These rules provide granular description of the various severity, exposure and controllability attributes that the Smart Columbus projects may encounter and rolls them up to the higher level ASIL ratings for better application to the Smart Columbus projects. These rating rules provide justification to the ASIL scoring of the safety risks and helps the project team to better interpret and apply the ASIL scoring methodology. The Severity, Exposure, and Controllability Rule Ratings shown in **Table 11**, **Table 12** and **Table 13** were applied to the safety risks identified in **Table 14** to help in the assessment of the values in the final score of each risk. Each safety risk is rated with a rating rule and ASIL Severity scoring.

Table 11: 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 elements.	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
S-P	Delayed emergency response to the CEAV emergency increase the severity of the situation and uninformed response presents hazards to responders.	S2	2
S-Q	Safety concern when encountered in an assault related situation.	S2	2
S-R	Safety concern when appropriate training was not provided	S2	2

Source: City of Columbus

Table 12: 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	Rare, extreme weather events, such as lightning strikes, hurricane landfall, and deep snow	E1	1
E-C	More common storms, such as rain or ice.	E1	1

Rule	Description	Rating	Score
E-D	Vandalism of protected equipment happens.	E1	1
E-E	All organizations will experience staff turnover which can lead to untrained employees.	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 an unexpected situation.	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
E-W	A designed-in fault that is manifested to occur rare or never.	E0	0

Source: City of Columbus

Table 13: 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.	C1	1
C-B	Ignoring or missing a message that calls for action is an incorrect response.	C1	1

Rule	Description	Rating	Score
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 is 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 and behaves 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 TMC can be controlled by those staff. It could 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 that is stranded by a disabled vehicle, a vehicle is not dispatched, or other equipment malfunction causes the vehicle to be unusable 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
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	Provider cancelling the trip or being late is not controllable by the traveler.	C3	3
C-S	A person has little control immediately after personal data is exposed.	C3	3
C-T	Drivers of surrounding vehicles can handle slightly unexpected behavior of an AV.	C1	1

Rule	Description	Rating	Score
C-U	Drivers of surrounding vehicles cannot handle an AV with sudden or unexpected 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, seat belts) 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 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
C-ZC	Harm that occurs due to distracted driving	C3	3

Source: City of Columbus

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

Table 14 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 Smart Columbus risk assessment includes ratings of S0a and C0 that are not in the ASIL ratings table (**Table 10**). These scenarios 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 14.**

Table 14: Summary of Safety Risk Assessment

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
Operating System										
1	Unauthorized person has access to restricted data.	An unauthorized person has access to the restricted data that can be used to commit a crime. Unauthorized person collects the restricted information from different applications in the Operating System combines them to reidentify.	Data will be anonymized prior to transmission to the Operating System. Diligent data security practices and regular patching and updates take place (penetration testing has been conducted twice (Nov 2019 and April 2020) to validate security practices and patching). The Operating System avoids collecting unnecessary or sensitive information from users. The Operating System ensures adherence to wireless message standards. Users will also be encouraged to use strong passwords for their mobile applications. The Deidentification Policy and the Data Curation process outlines how data ingested into the Operating System is stored and protected. Risk re-identification testing is conducted biannually starting in May 2020 to validate deidentification policies.	S-I	S0a	E-T	E1	C-S	C3	-
2	Person has access to PII stored in the Operating System.	Person has access to the PII and can be used to commit a crime.	No PII is provided to the Operating System and this makes a rare/never risk of occurrence. Data received is de-identified by the data provider prior to transmission to the Operating System. The Deidentification Policy and the Data Curation process outlines how data ingested into the Operating System is stored and protected.	S-I	S0a	E-W	E0	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.	No PII, PHI, or Payment Card Industry (PCI) data is provided to the Operating System and this makes a rare/never risk of occurrence. Data received by the Operating System is deidentified by the data provider prior to transmission. Data curation process includes a review of sample data for PII prior to ingestion into the publicly accessible area. Smart Columbus DPP Chapter 5: Security Controls describes in detail how data collected will be stored and protected and the steps that will be taken if there is a data breach. These security controls are updated annually and reflect current best practices.	S-I	S0a	E-T	E1	C-S	C3	-
4	Any user combines datasets to reidentify a person and commit crime.	A user collects and combines data stored in the Operating System and can use this data to locate personal information from other sources. This personal information can be used to commit a crime, which may result in a safety issue.	The Operating System Terms of Use contains language regarding how users shall not reidentify data. The data curation process includes an assessment of safety risks introduced from new data sets, de-identification process, potential exclusion of new data set, and when the ethics policy takes place. Diligent data security practices and regular patching and updates is also be carried out. Penetration testing has been conducted twice (Nov 2019 and April 2020) to validate security practices and patching. Risk re-identification testing is conducted biannually starting in May 2020 to validate deidentification policies.	S-I	S0a	E-W	E0	C-S	C3	-
CVE										
5	The CVE system is hacked into and unauthorized personnel have access to traffic control system.	Disruption to normal operations of the traffic control system and disconnecting the CV 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 Security Credential Management System (SCMS) protects RSUs, OBUs, CVE and CEAV data transfers. Diligent data security practices and regular patching and updates are carried out per the DPP and DMP. Multiple firewalls were installed as part of the network security. Strong passwords increase the safety of CVE connections. Signal controllers are physically secured with locks and accessible only to the TMC personnel. RSUs also have access control. CVE network resides outside of traffic signal system.	S-N	S0	E-T	E1	C-H	C1	-

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
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 and vehicle identification data that is collected 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 are carried out. Strong passwords increase the safety of the participant registration and vehicle identification information that is collected. If data is exposed, users will be informed about the unauthorized access of the data. Smart Columbus DPP Chapter 5: Security Controls describes in detail how PII collected will be stored and protected and the steps that will be taken when there is a data breach.	S-I	S0a	E-T	E1	C-S	C3	-
7	OBU is hacked and provides false warnings to the driver.	Device gives a warning that is not valid or accurate. Safety of the passengers and the roadway users is at risk. 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 protect RSUs, OBUs, CVE and CEAV data transfers. Drivers are trained and sign an Informed Consent Document that lays out OBU warnings are secondary to vehicle operator control. Operator will still 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 is a risk. 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 are instructed and sign an Informed Consent Document that lays out CV OBU warning systems are secondary to vehicle operator control. Operator is still in control of the vehicle and must assess the situation and react appropriately. Siemens and Brandmotion worked with the COC with the frequency and type of alerts that will be received by the driver and continue coordination if needed after launch. HMI for private vehicles is a HUD which is designed to keep eyes on the road. Project team logs issues when noted and determines the root cause of the issue. Based on number of occurrences, the issues are analyzed to understand the reason of occurrence.	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, or occlusion.	Safety issues because of the different warning systems that could be impacted by these issues. No communication or warnings are provided to the user for the upcoming traffic events. However, these are warning systems and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	Participant training emphasizes that CVE is only a warning aid and is not at all intersections. Impact is not crash related. Vehicle operator is in full control of the vehicle and must assess the situation.	S-B	S0a	E-L	E2	C-E	C2	-
10	Vehicle position not as accurate as needed for the successful operation of the application.	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.	Device has its own proprietary position correction system and is designed to not convey improper messages if position accuracy exceeds the threshold of one meter. Vehicle operator is in full control of the vehicle and must assess the situation. Drivers should understand vehicle position can be imprecise because of radio interference, occlusion, or going out of system range.	S-N	S0	E-Q	E2	C-E	C2	-
11	Incorrect information (for example: 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 is a risk. 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.	Participant training emphasizes that CVE is only a warning aid and is not at all intersections. Impact is not crash related. Vehicle operator is in full control of the vehicle and must assess the situation. MAP update policies will be included in the O&M plan. Project team logs all issues when identified and determines the root cause of the issue. The issues are analyzed to understand the reason of occurrence. When an issue with a message is identified, updates (that correct these issues) will be incorporated into the message. The message previously broadcast from a given RSU(s) will be replaced with the updated message in a time-sensitive manner. The corrected information will be relayed to the vehicle when it next enters coverage of the affected RSU.	S-O	S1	E-I	E3	C-E	C2	QM

Risk ID	Safety Risk	Revised Safety Impact	Revised 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 includes sufficient checking of OBU installation. Driver to return vehicle for reinstallation/adjustment/repair as needed. Participant training emphasizes that CVE 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. Increased false alarms and missed warnings can reduce user reliance on the system but should not cause a safety concern. Device and installation checklists are completed before the vehicle is operated in real-time. Installation manager verifies the completion of checklist and completed checklist is archived.	S-N	S0	E-J	E2	C-E	C2	QM
14	Nonfunctioning RSU does not send or receive the necessary information to the vehicle operator.	Intersections equipped with this technology will not relay information as designed. CV will not be getting necessary messages. Not all intersections will have RSUs. V2I apps are no longer providing necessary warnings to the vehicle operators.	Quick identification and repair of RSUs and power that is not working using the RSU health monitoring system (CMCC from Kapsch and the TMC). 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. Health monitoring system will be available as noted above. RSUs communicate with one other and can identify if there is a disconnect loss of connection with other RSUs	S-N	S0	E-J	E2	C-C	C1	QM
15	Device installed in the vehicle becomes in-operable (e.g. tampering, not installed properly).	Safety of the vehicle operator, passengers, and other roadway users is at risk. 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.	Participant training and Informed Consent Document refers user to customer care line/installation resources for reinstallation/adjustment/repair as needed. Driver is advised during training not to tamper with OBU equipment and to be stated in Informed Consent Document. Vehicle operator will be in full control of the vehicle and must assess the situation. Device calibration and installation checklist is completed before the vehicle is operated in real-time. Installation managers verifies the completion of checklist and completed checklist is archived.	S-N	S0	E-J	E2	C-C	C1	QM
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 nearby road users and pedestrians.	CVE is only a warning aid and is not at all intersections. Informed consent and equipment training is provided at the time of installation to the vehicle operators on how to react to different situations and understand that the CV system is a warning aid. Vehicle operator will have full responsibility and control over the vehicle. Vehicle Operators receive training both in person and through videos based on the vehicle types. Siemens and Brandmotion coordinated with COC with the frequency and type of alerts that will be received by the drivers and can be adjusted if needed.	S-R	S2	E-K	E1	C-F	C3	QM
17	Safety issue when the device is not operating how the user was trained or instructed 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 Informed Consent Document refer user to customer care line/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. Training is provided to the vehicle operators (participants) at the time of installation on how to react to different situations and understand that the CVE system is a warning aid. 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 vehicle 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. Siemens and Brandmotion will coordinate with COC with the frequency and type of alerts that will be received by the drivers. The project team will have training videos for all drivers and the videos will be provided to the fleet operators through the training gateway. FAQs are listed on the website which is accessible to all users of the system. https://smart.columbus.gov/get-involved/connected-vehicle-environment	S-H	S3	E-H	E4	C-A	C1	B

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
20	Time of the school zone is wrong in the system and the device does not give accurate warnings.	Safety of the passengers, pedestrians, and the roadway users is at risk. The CVE system does not give the vehicle operator appropriate warnings at the school zone and operator doesn't slow down during the active school zone, which may result in a crash.	School Zone warning is a cloud hosted system. The timing of the school zone is connected directly to the CVE system. The roadside safety message to indicate school zone warning is linked to the operation of the flashing school zone indicator signal. The data of the school zone timings is live and automatically provides current signal timings to the CVE system. However, these are warning systems only and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately.	S-G	S0	E-K	E1	C-H	C1	QM
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 is a risk. 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-CVE 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 is a risk. A participant's misconception may result in a crash when the vehicle operator is not in full understanding of the capabilities of the CVE 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 Participant 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 a CV warning and not automated vehicle functions. Marketing and recruiting materials include this information and is conveyed to the participant during the recruiting, consent and training processes.	S-E	S3	E-M	E1	C-F	C3	A
23	A heavy snowstorm 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 is a risk. 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.	Lessons learned and best practices have been accounted for in the system design. Project team has performed a design review of installation. Project team verified installation before deployment, including specific end-of-line testing and checklists. Adequate training was provided to the vehicle operators on how to use the CVE equipment and react in inclement weather.	S-B	S0a	E-B	E1	C-ZB	C3	-
24	Signal changed to flash mode either manually or due to cabinet error and is not communicated to RSUs.	When the cabinet is flashing, the RSUs do not receive this information and still communicate the usual signal phase timings to the OBUs. Due to this situation the driver will be given alerts that are not applicable at that time and may cause driver confusion. This may result in a crash creating a safety issue to the driver, passengers and roadway users.	Participant training includes awareness to these unusual situations. However, these are warning systems only and the vehicle operator is still in control of the vehicle and must assess the situation and react appropriately. This scenario will be tested to understand the behavior of the RSU and OBU communications.	S-O	S1	E-M	E1	C-D	C2	QM
CEAV										
25	AVs operating at low speed (slower than 15 mph) with vehicles at higher speeds (exceeding the posted speed limit).	The disparity in speed between an AV operating below 15 mph and other traffic exceeding the posted speed limit might cause a crash.	Traffic calming measures, speed enforcement, AV informational signage, and route design on the sections of roads that AVs will be operating help with the speed control. City has worked with the vendor to have CEAVs travel as close to the speed limit as the technology allows for safe operation.	S-D	S2	E-S	E2	C-U	C3	A

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
26	Sudden stop of the AV because it encounters an unanticipated obstacle.	Safety to the passengers and the road users is at risk due to sudden stop. AV not anticipating 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 is present in the vehicle at all times when the vehicle is in operation and must take control and maneuver around the obstacle. To improve passenger safety, the operator instructs the passengers to remain seated and belted, as available. Passengers are instructed to hold onto rails. Signage was installed on the route to provide information about the AV operations. City and vendor have also added seat belts, non-stick coverings to the seats, and signage inside the vehicle encouraging passengers to remain seated, keep both feet on the floor and use handrails. The vehicle capacity is also limited so that all passengers can be seated. Please note, as of 11/30/20, passenger service will not resume. These mitigations were put into place in early summer when passenger service was still under consideration.	S-D	S2	E-I	E3	C-U	C3	B
27	Pedestrians go into the path of an oncoming AV.	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.	CEAV's were tested for reaction to several types of VRUs and were thoroughly vetted before launching. CEAV Test Plan and Report covers all the test cases and results related to testing for reaction to VRUs. Testing also included objects that are below knee height. Operator is trained to be aware of all operating conditions. Ensuring pedestrian safety for interactions with AVs is accounted for in SOP. For example, increasing awareness of pedestrians and other road users were included as part of operating training procedures and educating the public about the operation of AVs on roadways was also included as part of the outreach. Signage at the AV stops and also along the AV route is installed to inform other road users about the AV operation.	S-A	S3	E-S	E2	C-Q	C2	A
28	Passenger may not be fully boarded or alighted when AV begins to move.	Passengers may be 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.	EasyMile User Guide ensures that the vehicle does not move until the door is fully shut and vehicle operator training also emphasizes to make sure the door is fully closed before initiating the stop departure; door sensors should be aware of complete closure. Operator is always present when the AV is in operation and permits the vehicle to leave the station when passengers are fulling boarded or alighted.	S-A	S3	E-S	E2	C-V	C1	QM
29	Passenger approaches the AV as it is departing a stop.	Passenger in a hurry to reach the destination and tries to board a moving AV. This may result in a safety issue to the passenger.	Operator training includes 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
30	Passenger alighting may not accommodate an entire loading/unloading (for multi-passenger parties, ADA customers, etc.).	Passengers are trying to alight the vehicle and the AV may depart not knowing that all the passengers are not alighted yet, creating a safety risk to those passengers still boarding.	EasyMile User Guide ensures that the vehicle does not move until the door is fully shut and vehicle operator training also emphasizes to make sure the door is fully closed before initiating the stop departure; door sensors should be aware of complete closure. Operator is always present when the AV is in operation and permits the vehicle to leave the station when passengers are fulling boarded or alighted.	S-A	S3	E-K	E1	C-ZA	C0	-
31	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 is increased. 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 was conducted prior to launch and thoroughly vetted these interactions. CEAV Test Plan and Report covers all of the test cases and results related to testing for reaction to VRUs. Testing also included interactions with objects that are below knee height. Operator is present at all times when the AV is in operations and operator training includes measures to handle operating the vehicle during these situations.	S-A	S3	E-S	E2	C-Q	C2	A

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
32	Stopped operation of an AV could create an impediment in the roadway.	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, creating a safety risk to the passengers and other roadway users due to either a sudden stop, maneuver or collision.	CEAV Test Plan and Report and EasyMile User Guide covers training for first responders and CEAV operators on how to handle emergency situations. Operator is always present when the AV is in operation. Operator training includes measures to handle operating the vehicle as it makes a sudden stop for any maintenance reasons. Testing for this risk was performed under closed course conditions to minimize interaction with public. Hazard lights initiated for programmed stops before stopping. Outreach was conducted to communities with route information and vehicle operations.	S-D	S2	E-R	E2	C-U	C3	A
33	An AV operating in manual mode and the operator may not notice VRUs (bikes, scooters and pedestrians) taking advantage of the AV.	When there is an unpredictable interaction with the other roadway users, there might be a delayed response from the AV operator to 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, and possibly the passengers on the AV.	Operator training and operating procedures account for potential vehicle operator distraction. AV is equipped with standard vehicle awareness equipment (sensors) for the vehicle operator to rely on when operating manually and the safety chain will be active even when the vehicle is in manual mode. This information is contained in the EasyMile User Guide. CEAV Test Plan and Report covers all of the test cases and results related to testing for reaction to VRUs. Testing also included interactions with objects that are below knee height.	S-A	S3	E-S	E2	C-U	C3	B
34	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 is increased. 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.	Education and outreach has been implemented throughout the operational period of the AVs. CEAV Test Plan and Report and EasyMile User Guide also cover this aspect for the operators of the shuttles.	S-A	S3	E-S	E2	C-U	C3	B
35	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 signal phase and timing information.	CV OBU warning systems are secondary to vehicle operator control. Operator is still in control of the vehicle and must assess the situation and react appropriately. Onboard Operator is a backup to the onboard systems. Operator training includes situations to intervene in vehicle operations as necessary. Shuttle route does not cross any signalized intersections, so the vehicle only receives SPaT messages, and does not use them for navigational purposes. Vehicle is not reliant on CV warnings and messaging for navigation.	S-E	S3	E-L	E2	C-C	C1	QM
36	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 is documenting lessons learned and safety standards used for these specific deployments. System cannot proceed from Level 4 to Level 5 until the standards are developed. CEAV test results also identify other recommended tests that should be performed for other AV/passenger related mobility options. OSU performed a pre-deployment simulation to evaluate the safety of AV operations on the Linden LEAP route; the results of this study were published in Nov 2019. The CEAV Test plan for the Scioto Mile deployed in Columbus, OH and MnDOT Autonomous Bus Pilot Project deployments were referenced when developing the Test Plan prior to deploying CEAVs in the Linden area.	S-H	S3	E-S	E2	C-N	C3	B
37	CEAV operator not trained to handle emergency or real-time situations.	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 certification for AV operator is included in the EasyMile User Guide. CEAV Test Plan and Results also include different test cases for AV operator reaction in real-time situation. Training includes how to handle emergency situations. Training was thorough and precise to handle the situations. Operators were trained before they start operating CEAV. Tabletop exercise was conducted in January 2020 before the launch.	S-A	S3	E-M	E1	C-F	C3	A

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
38	CEAV operator is distracted and unable to handle emergency or real-time situations.	Safety risk to passengers and other road users is increased. 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 phone) under assumption of not having to pay attention 100% of the time since vehicle is an AV and might take advantage of that fact.	Operator training and operating procedures account for potential vehicle operator distraction. These guidelines were also addressed in the CEAV Test Plan and Report and EasyMile User Guide. Training includes proper operation of the vehicle which leaves no free handles to use a cell phone. Tabletop exercise was conducted in January 2020 before the launch of CEAV passenger service.	S-E	S3	E-J	E2	C-D	C2	A
39	Road conditions and construction projects (lane closures, lane assignment, detours) may affect the CEAV route impacting the AVs ability to understand current roadway assignment.	Safety risk to passengers, construction workers and other road users is increased. Reaction time of the AV will be impacted, increasing risk of unplanned or sudden stop, or potential interaction with obstacles.	Operator takes control and maneuvers the route. Close coordination with construction projects is conducted by the City to maintain current and accurate lane lines. EasyMile User Guide provides guidance on CEAV operations on route with road closures and detours. Operating procedures include coordination between City and AV operator to assess road conditions. Manual operating speed is much slower than programmed speed of roads. If a roadway construction is in progress along the AV route, the AV will not operate along that route and take alternate route.	S-E	S3	E-R	E2	C-V	C1	QM
40	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 is a risk. 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 Easy Mile contract of the Smart Columbus program, all CEAVs have an operator on board who would reactivate the AV or prevent passenger tampering. Surveillance cameras also monitor activity inside the CEAV.	S-D	S2	E-S	E2	C-ZA	C0	-
41	Law enforcement and emergency responders not trained to handle emergency situations with the AVs.	Safety risk to passengers, emergency responders and others involved in an emergency is increased. 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. Safety of the responders when not knowing how to interact with the CEAV.	Training plan and activities for CEAV included outreach and information for emergency responders regarding responding to an incident involving the CEAV. Tabletop exercise was conducted in January 2020 and was documented in the CEAV Test Plan and Report. CEAV communications and outreach plan included training of emergency responders before deploying CEAVs in the Linden area.	S-P	S2	E-E	E2	C-N	C3	A
42	Flat tire or other AV maintenance failure that a non-AV can experience.	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 monitors vehicle response to surroundings, and the operator training includes how to react to different situations. Operators were also trained to intervene in vehicle operations as necessary. Daily maintenance checks also occur.	S-JA	S1	E-J	E2	C-J	C3	-
43	ADA equipment could become dislodged during AV operations.	Safety of the traveler who needs access to the ADA equipment is a risk. 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 monitors vehicle response to surroundings at all times and assist passengers getting on and off the AV. Operators were also trained to use the ADA equipment and assist the passengers that need ADA access.	S-M	S1	E-K	E1	C-L	C3	QM
43A	Food pantry patrons exposed to severe weather while waiting for shuttle	Safety to the patrons. AV not operating due to severe weather conditions. Patrons waiting for the AV not aware of the delayed service of the AV.	The operator and food pantry staff use flip down signage and sandwich boards during weather events to report service delays or cancellations. Notifications of AV operations and timings are updated and available on Linden LEAP website.	S-J	S0a	E-C	E1	C-ZD	C3	-
SMH										
44	Traveler does not realize where the emergency call button is located at the hub location.	Traveler could not locate the emergency call button located at the hub location and emergency situation intensifies, which may result in a safety issue for the user.	Information about the kiosks is available on the Smart Columbus website https://smart.columbus.gov/projects/smart-mobility-hubs. Google Maps also lists amenities offered at each SMH location. In any emergency, the travelers are requested to call 911.	S-JA	S1	E-S	E2	C-J	C3	-

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
45	Over activation of call button (false alarms).	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.	Coordination and response planning were conducted with law enforcement prior to launch on how to handle these situations. Outreach about amenities provided at each SMH location was also conducted. Information about the SMH amenities is also available on the Smart Columbus website https://smart.columbus.gov/projects/smart-mobility-hubs. In any emergency, the travelers are requested to call 911.	S-G	S0	E-S	E2	C-Z	C3	-
46	Responding late to the emergency calls from the hub location.	Safety issue arises when the officials do not respond fast enough to the users.	Coordination and response planning were conducted with law enforcement prior to launch. Voice over internet protocol (VOIP) channel is opened with the emergency dispatch during the time the traveler is waiting for help to arrive. As with any law enforcement emergency request, the response will be handled based on the standard operating procedures of that department.	S-G	S0	E-M	E1	C-Z	C3	-
47	Emergency call button does not respond at the mobility hubs.	In a situation where the traveler needs support, the emergency call button does not work, and the delayed and/or lack of response to the emergency need might increase the safety risk to the traveler.	Automatic monitoring of kiosks occurs to notify maintenance if electronic heartbeat is not received. Testing of emergency call button was implemented as part of the deployment process. Timing and parameters of the test are discussed in the O&M plan, which is posted on the Smart Columbus website. Travelers can also call 911 through their phone in an emergency situation.	S-H	S3	E-K	E1	C-N	C3	A
48	Transit delay at the hub locations.	Travelers get off the bus and wait for a long time to find another service. This may cause a safety issue to the traveler at the location.	Kiosk offers information on alternate transportation options. Camera and emergency call button available for passengers to alert officials in an emergency situation when waiting for the ride. Travelers can also call 911 through their phone.	S-G	S0	E-K	E1	C-J	C3	-
49	Additional modes of transportation and increased passenger traffic may result in higher conflict interactions (motor vehicle to motor vehicle).	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 have a designated area for specific modes to park to reduce the congestion. Travelers are encouraged to use the designated areas. Additional signage and pavement markings are posted showing the parking locations for different modes of transportation for drop-off and pickup. Outreach was conducted when the SMH were launched to educate the public on the services provided at the hub locations.	S-C	S1	E-I	E3	C-W	C1	QM
50	Additional modes of transportation and increased pedestrian traffic may result in higher conflict interactions (motor vehicle to 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 parking locations. This may also cause an impediment in the roadway for other roadway users.	SMH have a designated area for specific modes to park to reduce the congestion. Travelers are encouraged to use the designated areas. Additional signage and pavement markings are constructed showing the parking locations for different modes of transportation for drop-off and pickup. Outreach was conducted when the SMH were launched to educate the public on the services provided at the hub locations.	S-A	S3	E-S	E2	C-W	C1	QM
51	Additional modes of transportation and increased pedestrian traffic may result in higher conflict interactions (VRU to VRU).	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 parking locations. This may also cause an impediment in the roadway for other roadway users.	SMH 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 were constructed showing the parking locations for different modes of transportation for drop-off and pickup. Outreach was conducted when the SMH were launched to educate the public on the services provided at the hub locations.	S-C	S1	E-S	E2	C-W	C1	QM

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
52	Unattended devices (like scooters, bikes) left on site blocking ramp and can pose tripping hazard or block pedestrian accessible routes.	Additional modes and more travelers at the SMH 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 is also signage and pavement markings designated for the dockless devices. Traditional bike racks and CoGo bike racks are also accessible at the hub sites. The agreements between the property owners and mobility providers outline asset management responsibilities.	S-L	S1	E-S	E2	C-W	C1	QM
53	Planned maintenance mode occurs when the system is operating in Backup mode to restore, repair, or replace system components.	Travelers try to use the kiosk and not able to connect to some of the services provided because of the maintenance mode and cannot plan their trip. Safety issues may arise when they wait long in an unsafe situation.	These are planned events. Architecture is a no-fail system and updates occur during off-peak hours to minimally impact users. Regular updates occur with minimal interruption. Travelers may still be able to use Pivot (MMTPA Application) or other applications through their smart phone, in addition to having the ability to call 911 if an emergency arises.	S-JA	S1	E-G	E1	C-H	C1	QM
54	Failure mode of the kiosk resulting in the complete systemic disruption of the user's ability to plan the trip.	The kiosk is not working, and the users cannot access to plan their journey or use any other services available on the kiosk including ECB and camera and might be stranded for a long time, which may result in a safety issue for the user.	MMTPA and SMH offer alternate transportation options for calling taxi or other transportation when not able to reach the central system. Travelers may still be able to use Pivot or other applications through their smart phone, in addition to having the ability to call 911 if an emergency arises.	S-JA	S1	E-U	E1	C-J	C3	QM
55	Unable to access amenities at the SMH because of heavy snowfall or icy conditions.	Imminent severe weather expected in area. Ice/snow affects ability of passengers to safely move around SMH.	Stakeholders will be responsible for clearing snow and ice at the installed designated zones for modes of transportation.	S-B	S0a	E-B	E1	C-J	C3	-
56	Traveler at St. Stephens cannot access kiosk (off hours – lobby locked).	St. Stephens is closed, and the travelers cannot access the kiosk, 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, looked 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. Outreach plan includes the lobby hours that can be posted by the building. Google Maps also list amenities offered and hours at each SMH location. Hours of the building is posted for St. Stephens in Google. Travelers may still be able to use Pivot or other applications through their smart phone, in addition to having the ability to call 911 if an emergency arises. Transportation modes at St. Stephens are located outside the building and are accessible 24x7.	S-JA	S1	E-I	E3	C-J	C3	A
58	Travelers not utilizing safety features of bike share or scooters when starting their ride from the mobility hubs.	Travelers using bikes and scooters at the mobility hubs do not follow the safety standards (like wearing helmet) required and potentially create a safety risk.	Notification of local laws covers the safety standards before the traveler starts the ride with any transportation modes. Scooters and bikes require the user to wear a helmet while riding. Mobility providers also encourage the safety of travelers (specifically, scooters) by giving out free helmets. The third-party mobility applications inform users of local laws before the use of their mobility options.	S-L	S1	E-S	E2	C-X	C3	QM
MMTPA										
59	A 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.	Traveler unable to plan the trip as the travel modes are unavailable and traveler might be stranded at the location for a long time, which may result in a safety issue for the user.	Traveler can end the current trip and reset the trip. App offers alternate transportation route and mode options. App notifies traveler when a mode becomes unavailable and provides traveler an alternative trip option to select.	S-JA	S1	E-K	E1	C-N	C3	QM
60	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 a long time, which may result in a safety issue for the user.	App offers alternate transportation route and mode options. App reroutes when the traveler goes off the trip route. App alerts the traveler about service disruptions and modal unavailability and is able to select other modes and routes options to continue the trip. When scheduling the trip, traveler is not be able to select a mode of transportation when not readily available.	S-JA	S1	E-J	E2	C-J	C3	QM

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
61	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 is not working, and the users cannot access the system to continue their journey and might be stranded for a long time, which may result in a safety issue for the user.	Travelers can use the third-party mobility apps to continue/complete their trip.	S-JA	S1	E-K	E1	C-J	C3	QM
62	Maintenance mode occurs when the system is operating in Backup mode to restore, repair, or replace system components.	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 for a long time in an unsafe situation.	These are planned events. Architecture is a no-fail system and updates occur during off-peak hours to minimally impact users. Proper notification will be given to potential users in advance of the event when the system is offline.	S-JA	S1	E-G	E1	C-M	C0	-
63	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.	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.	App provides audio and visual cues while navigating. A one-time notice is provided, and affirmative consent is required from the traveler to agree to the terms of use of the app. When planning a trip with scooters and bikes, a pop-up is presented to the traveler to follow the codes and policies of third-party mobility providers. Travelers can adjust the volume level within the app to be able to hear navigation and not block outside noise.	S-A	S3	E-V	E2	C-ZC	C3	B
64	Security flaw in the app causes exposure of sensitive information.	Creates the potential for unauthorized account activity (related to trip planning, personal data, etc.), identity theft while traveler plans or executes a multimodal trip. Also, the app stores user information when creating the user account.	The application collects limited PII which is necessary for the functionality of the application and does not collect higher risk data such as financial information. Users are notified of data collection through the vendor's privacy policy and terms of use. Vendor has an information security policy which lists security measures and controls taken to protect user data. Vendor is using AWS for storage and all data is encrypted in transit and at rest. Contractually, the vendor has to comply with the Smart Columbus Data Management (DMP) and Data Privacy Plans (DPP). Per the DPP, the vendor went through the Smart Columbus Governance Process which included a privacy impact assessment in June 2019.	S-I	S0a	E-T	E1	C-S	C3	-
65	Vulnerabilities for data transmission and storage.	Increased potential for identity theft because of storage of the data collected from the users when using the app.	Application design restricts the permissions and information requested from users to only what is necessary for functionality, including avoiding the collection of financial or sensitive data. Vendor has an information security policy which lists security measures and controls taken to protect user data. Vendor is using AWS for storage and all data is encrypted in transit and at rest. Data that is transferred to the Smart Columbus Operating System has been de-identified using the SharedStreets methodology. Contractually, the vendor has to comply with the DMP and DPP. Per the DPP, the vendor went through the Smart Columbus Governance Process which included a privacy impact assessment in June 2019. Smart Columbus DPP Section 5.3: Security Controls describes the standards that will be taken to protect and secure the confidentiality of PII collected.	S-I	S0a	E-T	E1	C-S	C3	-
67	Traveler/driver assault when booked through the MMTPA.	Driver or traveler may encounter an assault and is a safety concern.	In an emergency situation, traveler/driver can call 911. Traveler/driver can also leave the location and shout for help to get attention from surroundings.	S-Q	S2	E-T	E2	C-S	C3	A
MAPCD										

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
68	Application provides inaccurate, incomplete, or incorrect walking instructions to the traveler with cognitive disabilities.	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.	Traveler can contact his/her caregiver using the "Contact" feature within the application when assistance is needed. For travelers with severe disabilities, coach accompanies the traveler on the trip (decided by multiple stakeholders in advance of the trip being planned) until the traveler is able to travel independently. Safety training and COTA Transportation Training includes who and what to ask for help when lost getting to the destination (Store worker, manager, police officer, COTA bus driver). Goal of the training process was to identify potential failures and resolve them prior to real-world use.	S-K	S2	E-Q	E2	C-Y	C3	A
69	Application is not updated with current pedestrian and traffic information that will impact route provided to the traveler.	The directions provided by the application are not up to date and no alert is provided for the road closures and the traveler may take a wrong route to reach the destination or might even end up in the wrong place.	Training recommends that the traveler utilize the "Contact" feature within the application, which allows the traveler to contact their caregiver. Safety training includes who and what to ask for help if a traveler gets lost on the way to the destination (Store worker, manager, police officer, COTA bus driver). Goal of the training process is to identify potential failures and resolve them prior to real-world use. For travelers with severe disabilities, coach accompanies the traveler on the trip (need for a coach is decided by multiple stakeholders in advance of the trip being planned) until the traveler is able to travel independently.	S-K	S2	E-J	E2	C-Y	C3	A
70	Application freezes or shuts down and the traveler cannot access it.	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 situation with no further directions provided.	This risk assumes the 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). Safety training includes who and what to ask for help when lost getting to the destination (Store worker, manager, police officer, COTA bus driver). Goal of the training process is to identify potential failures and resolve them prior to real-world use.	S-K	S2	E-J	E2	C-Y	C3	A
71	Traveler selects incorrect route when departing his or her location.	Traveler selects wrong destination/route in the MAPCD app. The app provides the directions for the destination selected, and traveler ends up in the wrong place.	Training recommends traveler to utilize "Contact" feature within the application that will contact the traveler's caregiver. Safety training provided to the traveler includes all safety risk scenarios and how to react to these scenarios. Goal of the training process is to identify potential failures and resolve them prior to real-world use. Destinations in the app are preprogrammed and should be safe so while the traveler may be at the wrong one, it should be familiar and friendly to the user. For travelers with severe disabilities, coach may accompany the traveler on the trip (need for a coach is decided by multiple stakeholders in advance of the trip being planned) until the traveler is able to travel independently.	S-K	S2	E-M	E1	C-Y	C3	QM
72	Application malfunctions mid-trip, and no instructions can be created.	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 through the smart phone). Safety training and smartphone training provided to the traveler includes all safety risk scenarios and how to react to these scenarios. When the application is restarted, the application picks up the route from where the app crashed.	S-K	S2	E-J	E2	C-Y	C3	A
73	Traveler is lost and caregiver is not updated with the latest information of the traveler location.	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. Traveler may be stranded in an unsafe situation.	Traveler is able to call his/her caregiver using the "Contact" feature within the application or using his or her smartphone and provide location information to the caregiver. City provided data/phone plan to all the participants to be able call the caregiver any time.	S-K	S2	E-K	E1	C-Y	C3	QM

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
74	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.	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.	Application includes visual and audio cues; Safety training, COTA transportation training, smartphone training and application training were conducted with the participants before travelers were able to go on the route. These trainings discuss distraction caused by their mobile phone. Travelers are also required to take multiple quizzes through the training process until they achieve 80% proficiency.	S-A	S3	E-M	E1	C-Y	C3	A
75	Traveler leaves the phone in the transit vehicle when he or she departs.	Traveler forgets his or her phone in the transit vehicle and will not receive post-vehicle instructions. Traveler may be stranded in an unsafe situation.	Safety training and COTA transportation training includes who to ask for help and what to ask when lost getting to the destination (store worker, manager, police officer, COTA bus driver). For travelers with severe disabilities, coach accompanies the traveler on his or her trip until the traveler was able to travel independently.	S-K	S2	E-M	E1	C-Y	C3	QM
76	Application cannot accommodate changes to route/vehicle (if a vehicle breaks down mid route, and a traveler must change buses).	Traveler's transit vehicle breaks down and the application cannot provide route information to carry the trip. Traveler may be stranded and may encounter an unsafe situation.	When traveler goes off route, a text or email is sent to the traveler's primary caregiver. These messages continue at a prescribed time interval until the individual is back on route. Traveler can contact the caregiver with any unfamiliar situations using "Contact" button within the app. Safety training and COTA transportation training includes what and who to ask for help when lost getting to the destination (store worker, manager, police officer, COTA bus driver). A travel coach was accompanied with the traveler until the traveler was able to travel independently.	S-JA	S1	E-J	E2	C-Y	C3	QM
77	Traveler's phone does not have enough battery to provide instructions throughout the entire trip.	Traveler's phone switches off and will not have instructions to continue the route. Traveler may be stranded in an unsafe neighborhood.	Safety training provided to the traveler includes all the safety scenarios when leaving the house including checking the battery level and charging the phone overnight. Training also includes what and who to ask for help when lost getting to the destination (store worker, manager, police officer).	S-K	S2	E-M	E1	C-Y	C3	QM
78	Cell phone network goes down and the traveler cannot contact his or her caregiver if needed.	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 also provided data plan to participants in the plan. Also, the travelers were trained to operate independently. Depending on the disability level, a coach accompanied the traveler to guide throughout travel until the traveler was able to travel independently.	S-K	S2	E-K	E1	C-Y	C3	QM
79	Stop sign to cross the street instead of a walk sign.	When following the step-by-step instructions provided by the app, there is a situation when there is stop sign at an intersection where the traveler needs to cross the street.	Routes can be personalized based on the traveler's ability to complete the route. Participants either navigate independently or will have a travel coach with them to assist on these types of crossings until the traveler is able to travel independently. Safety training provided to the traveler includes all the safety scenarios and how to react to these scenarios.	S-A	S3	E-J	E2	C-Y	C3	B
80	Non-ADA compliant crosswalks or curb ramps, or no sidewalks in the step by step navigation.	Safety issue for the traveler when the sidewalk ramps are not ADA-compliant, and the traveler needs to cross the street when following the instructions provided by the app.	Routes and stops can be customized based on the traveler's ability to complete the route. Caregiver (family, coach) is also trained along with the traveler when creating the route for the traveler. A travel coach accompanies the traveler until the traveler can travel independently. Safety training provided to the traveler includes all the safety scenarios and how to react to these scenarios.	S-L	S1	E-H	E4	C-Y	C3	B
81	The ICE contact does not respond to the traveler's request.	If lost, traveler cannot connect with their ICE contact for additional guidance. Traveler may be stranded and may encounter an unsafe situation.	Training guides the traveler to use phone capabilities on how and when to contact a secondary person when assistance is needed. Traveler can also call the coach to get assistance.	S-B	S0a	E-M	E1	C-Y	C3	-
PTA										

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
82	Trip scheduled by the prenatal traveler is cancelled and the prenatal traveler is not informed about the cancellation of her ride.	While waiting for her ride, the prenatal traveler may encounter an unsafe situation.	The system will automatically request another ride for the traveler. The traveler will receive a text or phone call about the new ride scheduled. The traveler can also schedule a ride through the call center or through the app and get a last-minute pickup. Traveler can contact rides4baby hotline and schedule a new trip.	S-JA	S1	E-J	E2	C-R	C3	QM
83	Trip scheduled by the prenatal traveler for her doctor visit is late for the pickup.	Prenatal Traveler may encounter safety issues while waiting for her ride.	Traveler can contact the call center for alternatives and check the status of her ride through the app. Traveler can contact rides4baby hotline and schedule a new trip.	S-JA	S1	E-J	E2	C-R	C3	QM
84	App not working as intended and prenatal traveler cannot schedule a ride or obtain any updates about delayed or cancelled trips.	While waiting for her ride, the prenatal traveler may encounter an unsafe situation.	Prenatal traveler can contact call center for alternative. Training provides instructions for the app use and how to react to different situations. During training, all prenatal travelers were provided with a customer care number to call when in any unexpected situation.	S-JA	S1	E-G	E1	C-J	C3	QM
85	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.	Application design restricts the permissions requested from traveler to only what is necessary for functionality. Development of the app along with the vendor provided visibility and customization, allowing for more exposure of code base and how it functions. Only services related to this project are made available to travelers. Vendor security documents lists the security measures for the data collected through this application. Smart Columbus DPP Section 5.3: Security Controls describes the standards that protect and secure the confidentiality of PII collected.	S-I	S0a	E-T	E1	C-S	C3	-
86	Vulnerabilities for data transmission and storage.	Increased potential for identity theft because of storage of the data collected from the app users.	Application design restricts the permissions requested to only what is necessary for functionality. Lessons learned and best practices are included in the security measures. Routine information security audits are conducted. Only necessary information is collected from the participants. All parties to collect, transmit and store PTA data have received the DMP and DPP. Data is also governed in the IRB research study and Informed Consent Document.	S-I	S0a	E-T	E1	C-S	C3	-
87	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.	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 an unsafe situation while waiting for her ride.	Prenatal traveler can contact the call center from the doctor's office for alternative (ask for the status of her ride or schedule another ride). Traveler can contact rides4baby hotline and schedule a new trip.	S-JA	S1	E-K	E1	C-N	C3	-
88	Pregnant woman feels more stressed while trying to use the app.	Prenatal traveler trying to use the app for the first time feels more stressed.	Feedback from the focus groups about the application were incorporated into the application design and development. Pregnant woman can use web or call center to schedule trips. User guide and training are provided for each participant. User guide is provided in paper form and is also available in app and on the web. Retraining is available for travelers.	S-G	S0	E-S	E2	C-Y	C3	-
89	The ride arrived for the prenatal traveler pickup is less user friendly and doesn't follow safety standards while driving the prenatal traveler.	Ride provided to the prenatal traveler did not follow safety standards and results in the injury of the prenatal traveler.	Car choice is given to the prenatal traveler when scheduling the appointment based on her requirements. Prenatal traveler can cancel the ride at any point of time she feels unsafe and schedule a new ride. Prenatal traveler is able to provide feedback for the ride. Mobility providers provide defensive driving course to the drivers.	S-E	S3	E-M	E1	C-X	C3	A
90	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 is a risk. 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 is provided to all the vendor drivers regarding all the safety features and driver is also trained with different installation procedures for three different car seats that are provided as per the program. Car Seat User Guides, which includes installation procedure and troubleshooting, are also provided to the drivers as part of the training.	S-E	S3	E-E	E2	C-J	C3	B

Risk ID	Safety Risk	Revised Safety Impact	Revised Mitigation Strategy	S-Rule	S	E-Rule	E	C-Rule	C	ASIL
91	The car seats provided to the vendor might have bed bugs and lice.	Safety of the prenatal traveler and her kids is at risk. Both the traveler and her kids might get infected by bed bugs and lice while traveling with the car seat provided.	Kaizen Interior Sanitation Policy is in place to ensure each stakeholder understands the service standards. Carriers (drivers) ensure their vehicle(s), and any needed additional equipment, have been properly cleaned and sanitized prior to provided services. Appropriate cleaning solution and supplies are provided to clean any unsanitary object(s), seat(s) or piece(s) of equipment.	S-M	S1	E-K	E1	C-N	C3	QM
92	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 restricts destinations to preapproved locations for selection. Training materials 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 and get a last-minute pickup.	S-J	S0a	E-M	E1	C-W	C1	-
EPM										
93	Driver distraction from paying attention to the app while driving to find the parking location.	Driver not paying attention while trying to find the parking spot and encounters a safety issue.	All interactions should only be for stopped vehicles. The predictive availability feature enables the user to look in advance to see where parking is available. The predictive availability feature user interface contains color coded zones for quick comprehension of available locations.	S-E	S3	E-S	E2	C-ZC	C3	B
94	Driver distraction when navigating to the parking spot through the app.	Driver not paying attention while trying to find the parking spot reserved through the app and encounters a safety issue.	The application doesn't create any added risk. The EPM application sends the destination to the driver's preferred navigation app [external to the EPM application]. All interactions should only be for stopped vehicles.	S-E	S3	E-S	E2	C-ZC	C3	B
95	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.	Application design restricts the permissions requested to only what is necessary for functionality. Development of the app along with vendor provides visibility and customization to Columbus requirements, allowing for more exposure of code base and how it functions. Only services related to this project are made available to users. Vendor privacy policy and terms of use lists the data collected through this application. Vendor data protection policy and information security policy lists security measures and controls taken to protect user data. These policies are referenced in the EPM Operations and Maintenance Plan. Smart Columbus DPP Section 5.3: Security Controls describes the standards that will be taken to protect and secure the confidentiality of PII collected. ParkMobile is also a PCI Level 1 vendor.	S-I	S0a	E-T	E1	C-S	C3	-
96	Vulnerabilities for data transmission and storage.	Increased potential for identify theft because of storage of the data collected from the app users.	Application design restricts the permissions requested to only what is necessary for functionality. Lessons learned and best practices are included in the vendor's security measures. Application avoids collecting unnecessary or sensitive information from participants. Smart Columbus DPP Section 5.3: Security Controls describes the standards that will be taken to protect and secure the confidentiality of PII collected. ParkMobile is also a PCI Level 1 vendor.	S-I	S0a	E-T	E1	C-S	C3	-
97	Driver not able to access his/her car when parked in a garage after garage operation hours.	Traveler not able to access the car parked in a garage reserved through the app. Traveler may be stranded in an unsafe situation.	Traveler is presented with the terms of service before he or she starts using the app. Traveler is responsible for any actions related to parking his or her car. Traveler is responsible to check the hours and other information about the parking facility/space. ParkMobile has information about the parking operators and their facilities in the app. Towing information is also posted at the parking facility. In instances for timed reservations, traveler can request notifications (email and text) in advance for expiration of reservation.	S-JA	S1	E-M	E1	C-J	C3	QM

Source: City of Columbus

Appendix B. Safety Review Agendas

B.1 AGENDA FOR PROJECTS IN COMPLETION PHASE

For 2021 annual safety reviews, the agenda below was used for the safety review meeting.

- Walkthrough of each risk and mitigation strategy listed in the SMP (prioritize the risks with higher ASIL scores)
    1. Identify if any of the listed occurred.
        - If yes, update mitigation strategy based on the strategy that was implemented when the risk occurred.
        - Review ASIL scoring.
    2. Identify risks and mitigation strategies that are obsolete (closed or resolved).
    3. Identify changes to the mitigation strategies (additional strategies planned/implemented, changes and/or additions to policies, procedures, training etc., strategies removed or classified as obsolete).
    4. Identify new risks and mitigation strategies.
    5. Identifying/referencing where policies are documented.

Appendix C. Acronyms

Table 15 contains project specific acronyms used throughout this document.

Table 15: Acronym List

Abbreviation/Acronym	Definition
ADA	Americans with Disabilities Act
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicle
CEAV	Connected Electric Autonomous Vehicles
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
EPM	Event Parking Management
FMLM	First Mile/Last Mile
GPS	Global Positioning System
HMI	Human Machine Interface
HUD	Heads Up Display
ICD	Interface Control Document
ICE	In Case of Emergency
IRB	Institutional Review Board
LDV	Light Duty Vehicles
MAPCD	Mobility Assistance for People with Cognitive Disabilities
MMTPA	Multimodal Trip Planning Application
OBU	On-board Unit
Operating System	Smart Columbus Operating System
O&M	Operations and Maintenance
PCI	Payment Card Industry
PHI	Protected Health Information

Abbreviation/Acronym	Definition
PII	Personally Identifiable Information
PTA	Prenatal Trip Assistance
PMO	Program Management Office
RTCM	Radio Technical Commission for Maritime Services
RSU	Roadside Unit
SCMS	Security Credential Management System
SDD	System Design Document
SMH	Smart Mobility Hub
SMP	Safety Management Plan
SOP	Standard Operating Procedures
SyRS	System Requirements and Specifications
TMC	Traffic Management Center
VRU	Vulnerable Road User

Source: City of Columbus

THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR