Phase 2 Comprehensive Maintenance and Operations Plan

Georgia Department of Transportation: Safe Trips in a Connected Transportation Network ITS4US Deployment Project

www.its.dot.gov/its4us.htm

Revised Draft Report – June 27, 2025
FHWA-JPO-23-108

ITS4US
IT'S TRANSPORTATION FOR ALL OF US

U.S. Department of Transportation

Produced by Georgia Department of Transportation (GDOT)
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems (ITS) Joint Program Office (JPO)
Office of the Secretary of Transportation (OST)
Federal Highway Administration (FHWA)
Federal Transit Administration (FTA)

Notice

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

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

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-23-108		

4. Title and Subtitle	5. Report Date
Phase 2 Comprehensive Maintenance and Operations Plan (CMOP) Safe Trips in a Connected Transportation Network ITS4US Deployment Project	06/27/2025
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Polly Okunieff (GO Systems and Solutions), Natalie Smusz-Mengelkoch (ICF), Whitney Shavers (Arcadis), Binh Dam (Arcadis), Jon Campbell (Arcadis), Randall L. Guensler (Georgia Institute of Technology), Angshuman Guin (Georgia Institute of Technology), Alan Davis (GDOT), Kofi Wakhisi (ARC), Joseph Hacker (ARC)	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Georgia Department of Transportation – One Georgia Center 600 West Peachtree NW, Atlanta, GA 30308	**11. Contract or Grant No.** 693JJ32250011

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Intelligent Transportation System Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	Revised Draft Report
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

The following USDOT partners are supporting this document development: Elina Zlotchenko (Program Manager), Sarah Tarpgaard (Agreement Officer), and Norah Ocel (Agreement Officer Representative)

16. Abstract

The Georgia Department of Transportation ITS4US Deployment project, Safe Trips in a Connected Transportation Network (ST-CTN), is leveraging innovative solutions, existing deployments, and collaboration to make a positive impact using transportation technology to support safety, mobility, and reliability. The ST-CTN concept is comprised of an integrated set of advanced transportation technology solutions (connected vehicle, transit signal priority, machine learning, predictive analytics) to support safe and complete trips, with a focus on efficient and cost-effective transportation options for all.

The Comprehensive Maintenance and Operations Plan (CMOP) outlines Phase 3 policies and procedures for the operations and maintenance (O&M) of the Safe Trips in a Connected Transportation Network (ST-CTN) system. The CMOP defines roles, responsibilities, and processes for subsystem maintenance and system operations, including software and data maintenance, defect management, and preventive and corrective maintenance.

17. Keywords	18. Distribution Statement
ITS4US; deployment; ITS; Intelligent Transportation Systems; comprehensive maintenance; operations plan	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	(81)	N/A

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

Revision History

Name	Date	Version	Summary of Changes	Approver
ST-CTN Project Team	28 April 2025	0.1	Initial Draft	Polly Okunieff
ST-CTN Project Team	27 June 2025	0.2	Revised Draft	Polly Okunieff

This page intentionally left blank.

Table of Contents

1. Introduction 1

1.1. Scope 1

1.2. Audience 1

1.3. Document Organization 2

2. System Overview 3

2.1. High Level System Overview 3

2.2. Subsystems and Data Covered 5

2.3. Subsystems and Data Not Covered 6

3. Change and Issues Management Processes 9

3.1. Issues and Software Change Scope 9

3.2. Issues Management 11

3.3. Change Control Management 13

4. G-MAP Operations and Maintenance 17

4.1. Configurable Items / Operational Software 17

4.1.1. Open-Source Software (OSS) / Software Developed Under Contract 17

4.1.2. Procured Software Services 19

4.1.3. Operational Configuration Management 23

4.2. Security and Privacy 24

4.3. G-MAP Operations and Maintenance Roles and Responsibilities 25

4.4. Operational Modes 25

4.5. Operational Processes 27

4.5.1. System Monitoring 27

4.5.2. Operational Performance Reporting 27

4.5.3. Operational Processes 28

4.6. Operational Issue Handling Procedures 29

4.7. Operations Backup, Shutdown, Restart/Recovery 29

4.7.1. Operations Backup 29

4.7.2. Operations Shutdown 29

4.7.3. Operations Restart/Recovery 30

4.8. Software Maintenance Updates and Upgrades 30

4.8.1. Infrastructure software and security updates 30

4.8.2. OSS updates and upgrades 31

4.8.3. Data and Other Software Updates 32

4.9. G-MAP Operations and Maintenance Risks and Contingencies 32
5. STM Operations and Maintenance 34
5.1. Configurable Items / Operational Software 34
5.1.1. OSS / Software Developed Under Contract 34
5.1.2. Procured Software Services 34
5.1.3. Operational Configuration Management 37
5.2. Security and Privacy 37
5.3. STM Operations and Maintenance Roles and Responsibilities 38
5.4. Operational Modes 38
5.5. Operational Processes 39
5.5.1. System Monitoring 39
5.5.2. Operational Performance Reporting 40
5.5.3. Operational Processes 41
5.6. Operational Issue Handling Procedures 41
5.7. Operations Backup, Shutdown, Restart/Recovery 41
5.7.1. Operations Backup 41
5.7.2. Operations Shutdown 42
5.7.3. Operations Restart/Recovery 42
5.8. Software Maintenance Updates and Upgrades 43
5.8.1. Infrastructure Software and Security Updates 43
5.8.2. OSS Updates and Upgrades 43
5.8.3. Data and Other Software Updates 44
5.9. STM Operations and Maintenance Risks and Contingencies 44
6. Sidewalk Data Collection and Update Process 45
6.1. Configurable items 45
6.2. Maintenance Roles and Responsibilities 45
6.3. Maintenance Processes 46
7. Integration Elements and Service Level Agreements 49
7.1. Introduction 49
7.1.1. Integration-Element Governance 49
7.1.2. Integration Element Modes of Operation 51
7.2. CV Platform 52
7.2.1. Enhanced TSP 52
7.2.2. RSU 53
7.2.3. CV Data Feeds 54
7.3. PED-X 55
7.3.1. Proxy Server OSS 56
7.3.2. Other Systems Undergoing Transition 56

7.4. Public PMD 57
7.4.1. Roles and Responsibilities 57
7.4.2. Public PMD Security and Privacy 58
7.4.3. Public PMD Operations and Maintenance Contract 59
7.5. Ride Request 59
7.6. INS 60
7.6.1. Beacon Operations and Maintenance and Facility Pathway Management 61
7.6.2. CXApp SDK and Back Office Software 62
8. Operations and Maintenance Risks and Contingencies 63
9. Related References 65
10. Acronyms and Abbreviations 67
11. Appendix 69
11.1. RSU Site Locations 69
11.2. PED-X Site Locations 70

List of Tables

Table 1. Subsystems and Data Covered by CMOP 5
Table 2. Systems and Data Not Covered by CMOP 6
Table 3. Change and Issues Management Priority Levels 9
Table 4. Issues Management Timeline 13
Table 5. Description of Software Change Control Process 14
Table 6. OTP Elements and OSS Repositories 17
Table 7. AWS EC2 resources and cost estimates for G-MAP 20
Table 8. Procured Software Configurable Items 22
Table 9. Operational and Maintenance Roles and Responsibilities 25
Table 10. Operational and Maintenance Risks 32
Table 11. Procured Software Configurable Items 36
Table 12. STM Operational and Maintenance Roles and Responsibilities 38
Table 13. Operational and Maintenance Risks 44
Table 14. Maintenance Roles and Responsibilities 45
Table 15. Integration-Element Governance 50
Table 16. Enhanced TSP Roles and Responsibilities 52
Table 17. RSU Roles and Responsibilities 54
Table 18. PED-X Roles and Responsibilities 55
Table 19. PED-X Proxy Server Update Process and Responsibilities 55
Table 20. Public PMD Roles and Responsibilities 58
Table 21. Ride Request Roles and Responsibilities 60
Table 22. Indoor Navigation System Roles and Responsibilities 60
Table 23. Operational and Maintenance Risks and Mitigation 63
Table 24. References 65
Table 25. Acronym List 67
Table 26. RSU Site Locations 69
Table 27. PED-X Site Locations 70

List of Figures

Figure 1. Coded Legend of the Functional View for the ST-CTN System 3
Figure 2. High-Level Functional Architecture ..... **Error! Bookmark not defined.**
Figure 3. Issues Management Process 11
Figure 4. Software Change Control Process 14
Figure 5. Diagram of Data Import and Export Mode and Frequencies 28

1. Introduction

The Georgia Department of Transportation (GDOT) and Atlanta Regional Commission's (ARC) Safe Trips in a Connected Transportation Network (ST-CTN) project was selected by the U.S. Department of Transportation (USDOT) as a part of the ITS4US Deployment Program. The project seeks to enhance the traveler's complete trip travel experience by enhancing mobility, reliability, and safety for system users. This is done by leveraging innovative solutions, existing deployments and team collaboration such as integrating connected vehicle (CV) data with an open-source software-based trip planner that is used to provision web-based and mobile application user access. The trip planner will provide users with the ability to create a personalized trip plan with information regarding the navigation of physical infrastructure, the ability to resolve unexpected obstacles, and ensure users' visibility throughout the trip. The proposed deployment will provide users with the ability to dynamically plan and navigate trips.

1.1. Scope

The Comprehensive Maintenance and Operations Plan (CMOP) documents the Phase 3 operations and maintenance (O&M) policies and procedures that will be implemented following the go live of the ST-CTN system. This includes the necessary information to successfully operate and maintain the ST-CTN system. The CMOP describes policies and procedures for fully deployed subsystems including the Georgia Mobility and Accessible Planner (G-MAP) and Space Time Memory (STM) Platform and leverages the existing infrastructure owner/operator (IOO) policies and procedures for systems, subsystems and data sources that are already deployed.

The CMOP will define the roles and responsibilities for subsystem maintenance, document the tools and activities to monitor system operations, and explain the process for software and data maintenance. The operations of the system include the processes that will be used to track normal operations communications, security, and safety for both planned and unplanned activities. The maintenance of the system includes details regarding defect management, preventive and corrective maintenance, software enhancements, data curation, beacon maintenance, and data storage planning.

1.2. Audience

The ST-CTN project is being led by the GDOT. The intended audience for this CMOP is the USDOT and the ST-CTN project team, which includes GDOT and the following partners:

- ARC
- Gwinnett County
- Statewide Independent Living Council of Georgia (SILCGA)
- GO Systems and Solutions (GOSystems)
- Georgia Institute of Technology (GA Tech)

- Arcadis IBI Group (Arcadis)
- ICF International, Inc. (ICF)
- Kimley-Horn and Associates, Inc. (KHA)
- Georgia Tech Research Institute (GTRI)
- Avail Technologies (Avail)

This document provides details regarding the operations and maintenance procedures and technologies of the ST-CTN deployment and is intended to be utilized as a reference by agencies and industry professionals that are interested in deploying a system similar to the ITS4US ST-CTN Deployment.

1.3. Document Organization

The document is organized into eight major sections. The overall change control and incident management process will cover all subsystems, and external and leveraged systems. Each subsystem developed and operated by Team members will be described in separate sections. Leveraged systems include inter-agency agreements and external systems include service level agreements or warranty agreements. The scope of each section is described below.

- **Section 1**

- Introduction provides a brief description of the project scope, the intended audience for this document, and an outline of the document organization.
- **Section 1**

- **System** Overview provides an overview of the system with a focus on operations and maintenance.
- **Section 3 Change and Issues Management Processes** provides an overview of the processes for managing software issues and changes as well as the issues management process and software change control management process.
- **Section 0**
-
-

- **G-MAP Operations** and Maintenance discusses the operations and maintenance processes for the G-MAP subsystem.
- **Section 1**

- **STM Operations and** Maintenance discusses the operations and maintenance processes for the STM subsystem.
- **Section 1**

- **Sidewalk Data Collection and Update** Process describes the operational and maintenance activities concerning the sidewalk data collection process.
- **Section 1**

- **Integration Elements and Service Level** Agreements outlines the operations and maintenance of the major external systems by existing vendors or infrastructure owners, ensuring consistent service levels for end-user convenience and confidence.
- **Section 0**

- **Operations and Maintenance Risks and** Contingencies provides a list of any operational or maintenance risks and their associated contingencies.
- **Section 9 Related References** lists the documents that were used to support and contribute to this document.
- **Section 10 Acronyms and Abbreviations** provides a list of acronyms used throughout this document.
- **Appendix** provides a list of RSU and PED-X site locations.

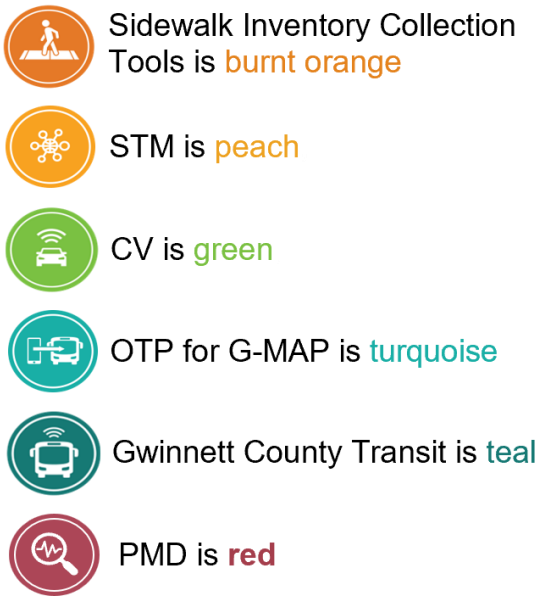
2. System Overview

This section presents a high-level description of the system in relation to Operations and Maintenance.

2.1. High Level System Overview

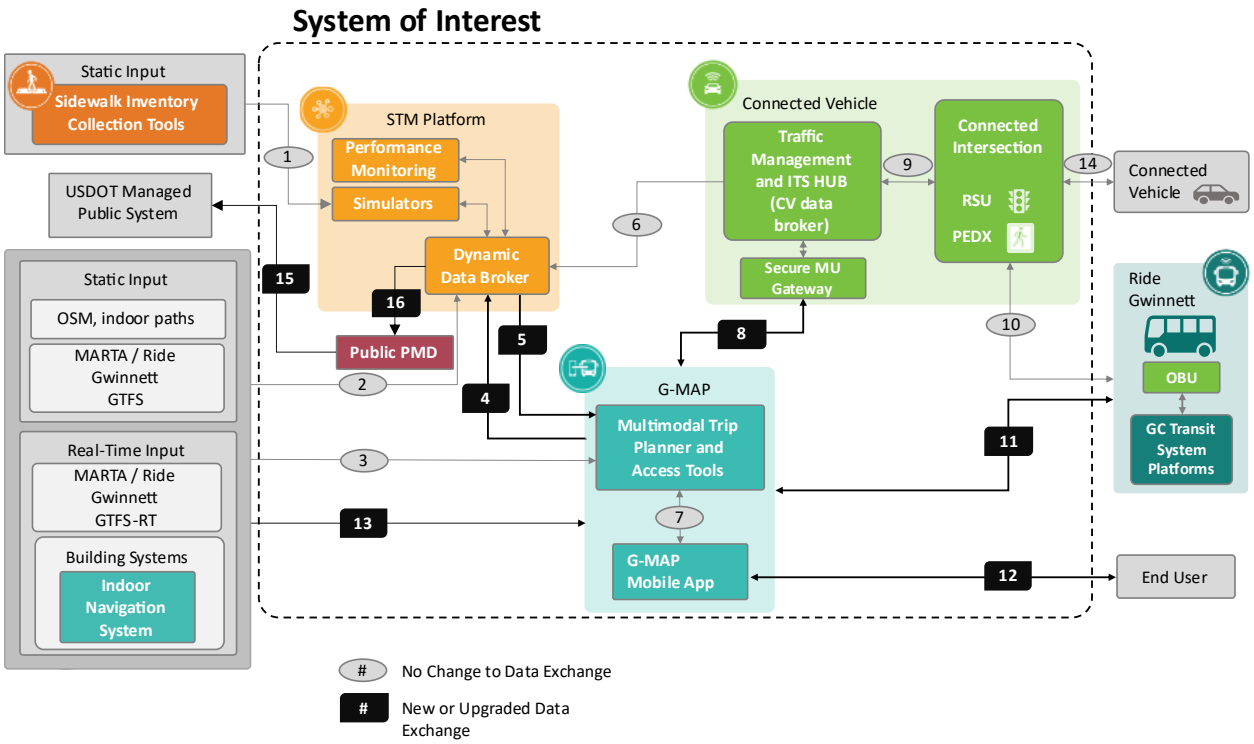
The high-level systems and subsystems are described by the functional architecture (System Architecture Document (SAD), 2025). The Functional View for the ST-CTN System and each subsystem within the system follow a coded legend, listed below.

- Bold dashed boxes outline the system/subsystem of interest,
- Major subsystem components presented by the ST-CTN project are depicted by rectangular boxes with black bold outlines,
- Major subsystem components that exist are depicted by rectangular boxes with transparent outlines,
- External system components are depicted by light grey rectangular boxes,
- People are designated with a silhouette inside of a rectangular box,
- Each subsystem is indicated by color and icon (**Figure 1**).



Source: GDOT, 2024

Figure 1. Coded Legend of the Functional View for the ST-CTN System



Source: GDOT, 2024

Figure 2. High-Level Functional Architecture

Error! Reference source not found. shows existing systems and project subsystems (i.e., boxes outside or inside the system of interest frame respectively).

Existing systems and data feeds will continue to be operated and maintained by existing entities while those within the system of interest frame will be operated and maintained by project resources throughout Phase 3. The specific communications, security, software and hardware operations and maintenance roles and responsibilities for each component are listed in **Sections 0** and **2.3** below. Detailed subsystem design level information about each subsystem is included in the System Design Document (SDD) [SDD]. External systems are also described in the SDD, albeit, at a functional level.

2.2. Subsystems and Data Covered

Table 1 lists the subsystems covered by this CMOP for Phase 3 operations and maintenance.

Table 1. Subsystems and Data Covered by CMOP

Item	Organization	Role	Responsibilities
G-MAP Platform	Arcadis	Operations and maintenance	• Monitor usage and operations (including reliability, security, etc.). • Incorporate Impedance Application Programming Interface (API) (every 15 minutes). • Manage user feedback. • Provide daily usage and deviation feeds to STM. • Update software (SW) platforms and interfaces for operating systems and security patches (mobile – iPhone Operating System (iOS)/Android and web). • Upgrade SW based on infrastructure upgrades for platforms. • G-MAP call center software operations and maintenance. • Secure registration and account information.
STM Platform	GTRI (managed by GA Tech)	Operations and maintenance	• Manage platform and reliability. • Manage data updates and ingestion processes. • Update impedance calculations (GA Tech & GTRI).
Sidewalk data collection and update of OpenStreetMap (OSM)	GA Tech	Data collection and maintenance	• Update changes to sidewalk infrastructure within the project area upon request by project manager.
Public Performance Measurement Dashboard (PMD)	ARC	Operations	• Daily review of operations (uptime and reliability). • Manage commercial off the shelf software, including configuration and license. • Monitor usage and user experience.

Item	Organization	Role	Responsibilities
Public PMD	ICF	Software Maintenance	• Recommend configuration updates if needed. • Support to migrate the Public PMD site to the ARC Power Bi platform.
Private PMD	GA Tech	Data and PM Evaluation and Maintenance	• Daily metric retrieval. • Weekly metric collation and distribution. • Annual metric collection, review and distribution. • Distribute and collect survey data (quarterly). • Secure and manage privacy and security of private data and servers.
Beacons and Indoor Pathway Status	Gwinnett Facilities	Beacon Maintenance Pathway Status Reporting	• Monitor beacon operations. • Update Indoor Pathway Status in CXApp.

2.3. Subsystems and Data Not Covered

Table 2 lists the systems and data feeds that currently exist and thereby have existing operations and maintenance procedures governed by other projects and programs. Additionally, any commercially procured systems operating as a Service as a System (SaaS) or contracted system are subject upon Service Level Agreements (SLA) when anomalies are detected, but are not covered by project operations and maintenance procedures. A description of these systems are discussed in more detail in **Section 1**.

Table 2. Systems and Data Not Covered by CMOP

Item	Organization	Role	O&M Responsibilities
CV Platform	GDOT and Gwinnett DOT (GCDOT)	Hardware, software, communications operations and maintenance	• Manage CV infrastructure (roadside units (RSU), onboard unit (OBU), Data Hub, etc.). • Manage (O&M) NaviGAtor. • Collect and share Pedestrian Presence Alert (PPA) data. • O&M Transit Signal Priority (TSP) (enhanced service). • Procure external traffic operations data sharing program.

Item	Organization	Role	O&M Responsibilities
Gwinnett General Transit Feed Specification (GTFS) and GTFS-realtime	Ride Gwinnett	Data maintenance	• Update and publish GTFS data feeds when revenue service changes (approximately 4 times per year). • Publish and maintain GTFS-real time streaming feeds for the public when buses are in revenue service.
Ride Gwinnett Bus Operations	Ride Gwinnett	Operations	• Governed by existing Standard Operating Procedures (SOPs) on hardware and resources. • Avail Computer-Aided Dispatch (CAD) software operations and maintenance.
Gwinnett signal and pedestrian systems	GCDOT	Hardware operations and maintenance Software / data maintenance	• Manage signal operations (MaxTime). • Operate and maintain pedestrian signal systems. • Share signal operations changes with proxy server maintenance team (GDOT and ST-CTN team).
Ride Request	Ride Gwinnett / Avail	Hardware operations and maintenance Software / data maintenance	• Manage CAD/AVL software and operations. • Coordinate Ride Request API format with GDOT Team. • Publish GTFS and GTFS-realtime per Ride Gwinnett direction.
Pedestrian Crossing (PED-X) Proxy Server	GCDOT	Server operations and maintenance (proxy server)	• Support update process when changes occur to existing PED-X sites or new locations are added to the proxy service. • Secure and operate proxy server.

Item	Organization	Role	O&M Responsibilities
PED-X Proxy Server Software	GDOT	Proxy server software maintenance and configuration	• Support update process when changes occur to existing PED-X sites or new locations are added to the proxy service. • Support update process when signal timing is changed. Request information from GCDOT (see Gwinnett signa and pedestrian system above). • Maintain proxy server software and interface needs.
Indoor Navigation	CXApp / Operations and SW Maintenance	Software Development Kit (SDK) / inventory operations and maintenance	• Maintain SDK by platform to ensure compliance with mobile platform stores. • Alert GDOT about changes to their SDK. • Provide access to Jibestream site functions (e.g., mapping) and training materials. • Provide SDK operations for mobile platforms to perform indoor navigation.

3. Change and Issues Management Processes

This section defines the scope of software anomalies, defects, and external impacts; explains how they are identified, prioritized, and addressed; and describes the oversight applied to managing these changes.

3.1. Issues and Software Change Scope

The issues and software changes cover any anomalies, issues, defects and external impacts on the software covered as described in **Section 0**. Although the processes flow through different stages, the Issues Management Process feeds into and is governed by the Software Change Control Process. The relationship is described in **Section 3.3**.

Each change and issue that is discovered is associated with a priority and severity level. The severity levels are consistent with those defined in the System Testing Plan (STP, 2023) with some additional impacts from operational concerns. The defined severity level drives the definition of the priority level to ensure that the changes or issues with the greatest potential impact to G-MAP are addressed first. The priority level and their corresponding severity levels are listed in **Table 3**.

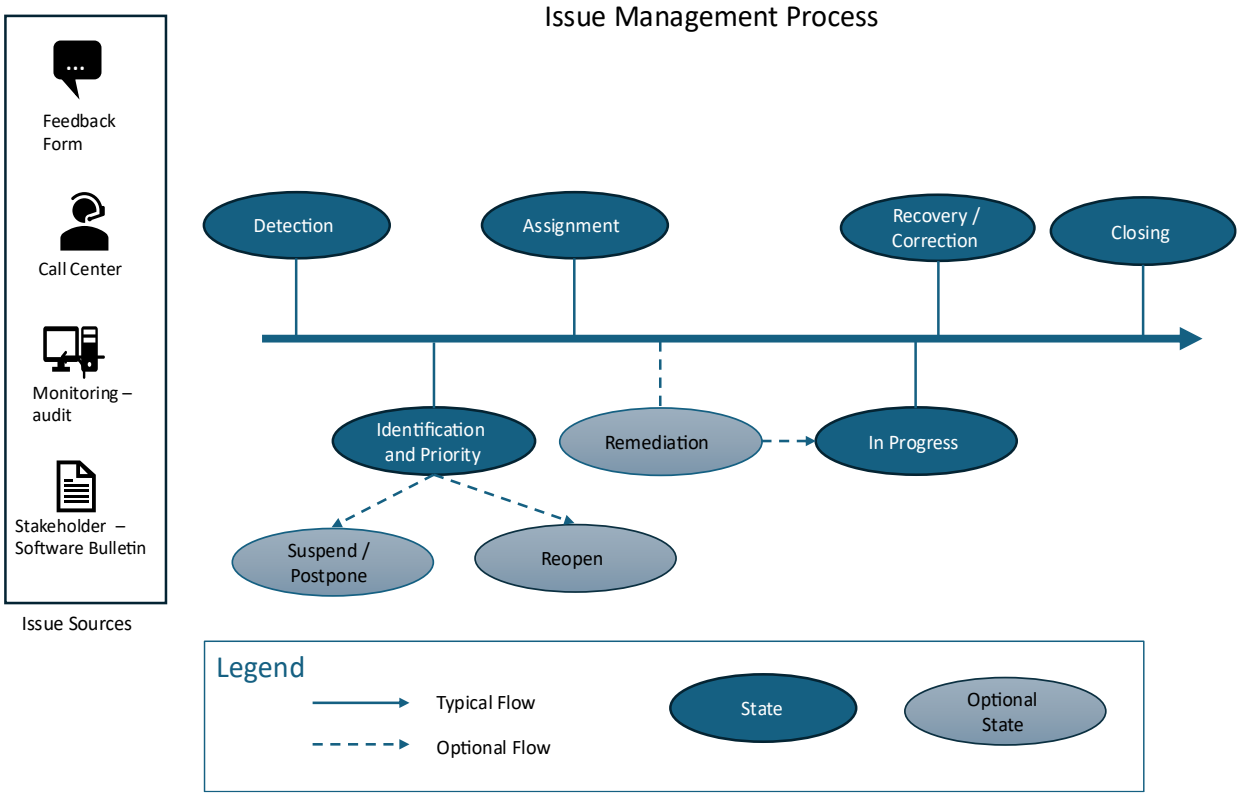
Table 3. Change and Issues Management Priority Levels

Priority Levels	Severity Levels (STP)	Description (Adapted from STP)
Critical	Critical	• Impacts that disrupt or shut down system operations. • Cybersecurity issue that impacts Personally Identifiable Information (PII).
High	High	• Impacts to participant safety or system security that is localized (e.g., at a specific intersection). • Persistent defect or anomaly occurring in system.

Priority Levels	Severity Levels (STP)	Description (Adapted from STP)
Non-critical	Medium and Low	• Impacts on user experience and usability, e.g., feedback from users on user interface (UI), notifications, turn-by-turn directions. • Incorrect information due to data input (e.g., GTFS, OSM triggered by incorrect directions). • Minor failure identified during Controlled Field Testing (CFT) procedure (e.g., missing flow in user process). • Impacts to operations or integrated operations that do not impact safety, privacy, or security. • Impacts on user accessibility when challenges arise in UI/user experience (UX). • Changes from external interface specifications. • Updates to infrastructure software due to vendor issued bulletins, patches and/or operating system version updates.

3.2. Issues Management

The issues management process governs disruptions, failures, and defects within the subsystems and data covered by this CMOP (see **Section 0**). The subsystems are governed by the ST-CTN executive management team (EMT) and issue management process. However, each subsystem provider will implement the process based on vendor internal processes, contract provisions, and service level agreements. The issues management process is shown in **Figure 3**. The timing of the process stages is dependent on the issue priority and criticality (as described above) and listed in **Table 4**.



Source: GDOT, 2025

Figure 3. Issues Management Process

The process flows through various states in which milestones are met prior to progressing to the next state. In some cases, a state may be skipped, for example when a non-critical issue is relegated to a sprint ticket where there is no interim fix or remediation, rather a correction and recovery plan.

Issue Sources. Issues, failures and defects may emerge from multiple sources. Sources that include internal business processes may be reported by:

- **G-MAP Feedback Form (the Trip "Report Issue" Link)**. Lists of these issues will be reported to the EMT at least once a week unless the issue is flagged for high priority or critical.
- **G-MAP Call Center.** The call center has a list of key project personnel to report issues.

- **Monitoring (Auditing)**. The software products include monitoring and auditing functions to detect anomalies and issues with the software. These range from operations to security alerts.

- **Stakeholder Reports or Infrastructure Software Bulletins**. These are delivered to the owner / operator of the software products. These may also include defects or failures that are detected in the integrated products such as the GCDOT signal system or indoor facility.

Detection and Logging. When an issue is detected, it is logged in an issues log. The issues log identifies the source including date and time recorded, software version number and other pertinent information needed to recreate the issue. In addition, the potential impact on the system is also logged. The issues log template is included in the Google Form and linked to a Google Sheet. Some subsystem issues will be documented in JIRA. If the Google form issues are related to software (versus business) issues, they will be transferred to the JIRA board and handled similar to the Agile process described in the SEMP.

Identification and Priority. Following detection, the issue is reviewed and diagnosed. The analysis identifies the cause of the issue, and the team(s) that need to work on resolving the issue. At this point the issue and proposed remediation/correction plan is presented to the Software Review Board (SRB) to review, assign and rank the severity category and priority. For critical issues, a formal SRB review may be bypassed in lieu of a discussion with the SRB chair or project manager. The results of the diagnosis and priority are documented in the issues log.

Assignment. Once the issue is identified, a task ticket is scheduled in the Sprint backlog process. If the issue is critical, an owner is assigned to it and then it is moved to the active or in-progress status and tracked through the sprint. A critical issue may include a short-term remediation strategy to ensure the system operates as completely as possible. To that end, a critical issue may include both a remediation and recovery plan. High priority tickets will be handled on a daily basis, while non-critical tickets will be assigned and scheduled for an appropriate sprint and release. The assignment may include outreach to the public when elements of the system are non-operational or degraded. If that is the case, an assignment to the community outreach and marketing teams will be included to alert the public.

Remediation. Remediation is a short-term fix to mitigate a critical issue. This may include changing an interface or hardcoding a parameter that is causing a problem. It may also include reducing the functionality of a service until the issue is resolved.

In-Progress. The in-progress state will default to the Agile process where the design, code, unit and integration testing occur. The result will correct the issue.

Recovery (Correction). The recovery state is when system testing is conducted to ensure that the software operates as expected. The system testing will follow the system test procedures described in the System Test Plan [STP].

Closing. Prior to deployment in the production platform, the closing state is subject to approval by the SRB as described in **Section 3.3**.

In addition, the optional states are as follows:

Suspend / Postpone. An issue may be initially identified by a source as a defect or anomaly just to be identified as a user error. Additionally, an issue may be detected, and not enough information is gathered

to reproduce the issue and identify a remedy. These issues will be noted in the issues log, however, they will be suspended or postponed until they can be diagnosed or addressed as a software update or upgrade.

Reopen. There are instances when the remediation or recovery did not solve an anomaly or defect. If the issue reappears, the original issue will be reopened (rather than opened as a new issue) so that the history of the change can be tracked throughout the diagnostic and progress states.

Table 4. Issues Management Timeline

Issue Priority	Detection	Identification	Assignment	In-Progress	Remediation	Recovery / Correction	Closing
Critical	Dependent on Source	Within 2-3 business hours	Within 6 business hours	Within 24-48 business hours	Within 48 business hours	Within 2 weeks	Within 3 weeks
High	Dependent on Source	Within 24 business hours	Within 24 business hours	Within 3-5 business days	Within 3-5 business days	By end of sprint cycles	By end of 2nd sprint cycle
Non-Critical	Dependent on Source	Within a sprint cycle	Next sprint cycle	1-2 sprint cycles	---	2 sprint cycles	3 sprint cycles

3.3. Change Control Management

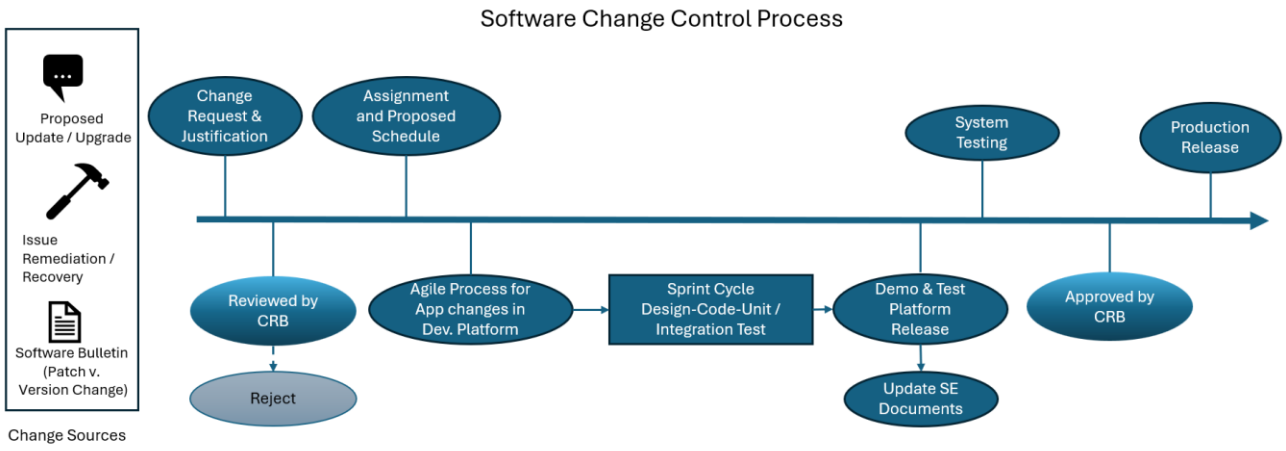
The Software Change Control Management process is governed by a software change review board (CRB) whose role is to manage changes to the software items covered by the this CMOP. The CRB will be composed of the ST-CTN EMT. Vendors, development teams and other infrastructure owner / operators will be invited as needed to these meetings.

The role of the CRB is to review operational performance (service level reporting), proposals to update or upgrade the covered software, review and approve remediation plans, as well as approve the verification and validation of updated software. During CRB meetings, the team will identify potential impacts to software changes whether these are from external sources (e.g., operating systems updates, data, operations or interface changes) or internally.

Initially, the CRB will meet weekly to review issue remediation plans, any proposals for change, and complaints / commendations from the feedback forms and call center agents. Software development teams will be provided waivers to address critical and high priority items as long as they inform the CRB of the issue and remediation actions that they plan to take. They will then report more fully on those issues during the next CRB during these meetings.

On a monthly basis, the software development teams will be asked to present their operational performance service levels to the CRB for their review.

The software change control process is illustrated in **Figure 4.**



Source: GDOT, 2025

Figure 4. Software Change Control Process

Descriptions of each stage in the software change control process are listed in **Table 5**.

Note: An optional state (Reject) includes rejecting or postponing the request for change.

Table 5. Description of Software Change Control Process

Order	Process	Description
0	Change Sources	The three major sources of a software change include: • **Proposed update or upgrade** to the covered software based on many factors including but not limited to expansion, extensions or improved usability. • **Issues** (mostly non-critical) that are instigated by an issue. • **Operating Software or Integration Interface Change Bulletin** necessitates updating or retesting the software to ensure compatibility with the app platform or integration element. A change may be identified by an IOO or representative who is knowledgeable about changes that impact the ST-CTN operations such as changing a Pedestrian Signal System or construction on pedestrian pathways or bus stops.

Order	Process	Description
1	Change Request and Justification	All change sources will require the submission of a change request, justification and proposed solution. The Issues will be detailed as Jira tickets even if the issue is associated with an external source. The updates due to a proposal or software bulletin will be documented in a short narrative addressing the request, justification and proposed solution. The request will be distributed to the CRB at least 24 hours in advance of the meeting.
2	SW CRB	The SW CRB will meet weekly during the first few months of Phase 3 to address any issues that might arise during the rollout of the system. During that time, an agenda with the SW change items will be drafted and presented. Minutes and action items will be taken and posted for the Team to review. The changes agreed to will be documented in the Jira board. The Jira ticket will include the party assigned and the sprint cycles(s) to completion. Tracking of the issue or change will fall to the Agile process and will not be reviewed by the CRB until the demo and then until after system testing is completed.
3	Assignment and Proposed Schedule	The Assignment and proposed schedule will be documented in a Jira ticket and in the Phase 3 schedule. The Jira ticket will serve as the tracking mechanism on a weekly basis.
4	Agile process for App changes in Dev. Platform	The Agile process will follow the process followed in Phase 2. The methodology is documented in the Phase 1 System Engineering Management Plan (SEMP) [SEMP].
5	Demo and test Platform Release & Update SE Documents	The solution is complete when it is demonstrated to the CRB, and all the system engineering (SE) documents have been edited to include the updates.
6	System Testing	The system testing will verify that the design elements have been included in the software and verified the end-to-end testing of the component and a set of regression tests that may be impacted by the change.
7	Approval by SW Review Board	Once the system testing is completed, the testing team will report its results to the SW CRB for the updates to be published to the public version. The Board may ask for additional tests if the results do not meet their expectations.
8	Production Release	The Development Team responsible for the updates will issue the updates to the production version of the subsystem software.

4. G-MAP Operations and Maintenance

This section describes the configurable items, procured services, operational processes, maintenance activities, and security measures that support G-MAP functionality (e.g., software components, cloud services, version control, operational modes, and procedures for updates, backups, and issue handling).

4.1. Configurable Items / Operational Software

The G-MAP configurable items include custom and open-source software, procured infrastructure and external application software used in the G-MAP web and mobile interface, and back-office components are described in this section.

4.1.1. Open-Source Software (OSS) / Software Developed Under Contract

The OpenTripPlanner (OTP) software is divided into the six open-source software elements as listed in **Table 6**.

Table 6. OTP Elements and OSS Repositories

OTP Elements	OSS Repository	Description
OTP (multi-modal routing engine)	(https://github.com/opentripplanner/OpenTripPlanner)	G-MAP uses a custom fork of OTP that contains custom code for ingesting mobility profile impedance data provided by STM and performing itinerary searches based on a given mobility profile.
OTP-React-Redux (Web user interface)	https://github.com/opentripplanner/otp-react-redux)	The web user interface for G-MAP is based on the active development branch of OTP-React-Redux with some minor configurations applied. This includes the reusable OTP-UI library of web front-end components (https://github.com/opentripplanner/otp-ui).

OTP Elements	OSS Repository	Description
OTP-personas (OTP-middleware)	https://github.com/ibi-group/otp-middleware)	OTP-personas is the main G-MAP backend component that handles trip monitoring and live tracking, including sending notifications, orchestrating Ride Request, Enhanced Transit Signal Priority requests, and PED-X crosswalk requests when someone with special needs travels along a monitored itinerary. G-MAP is based on the active development branch of OTP-personas.
Push notifications middleware	***Part of the OTP Middleware code base***	A push notifications middleware server component is enhanced for G-MAP to support push notifications such as trip reminders and notifications with tracking links to the post-travel survey. Push notifications are sent to iOS and Android devices. The source code for the push notifications middleware will be made available to the public.
OTP Native Mobile Apps	TBD (after deployment and testing is completed)	Native OTP mobile apps provide realtime, multimodal trip planning through an interface built specifically for iOS and Android devices. Leveraging the OTP routing engine to support transit, walking, and biking, offering detailed itineraries, live updates, and accessibility features to enhance in trip support

OTP Elements	OSS Repository	Description
Indoor Navigation Development	Due to proprietary APIs from CXApp, this code will not be posted in a repository.	In addition to the embedded CXApp SDK, G-MAP includes custom functionality to supplement the SDK. These features include: • Draws the path and waypoints on the indoor map, plots labels and text for units on the map, implementing route deviation logic based on the CXApp API and adding optimization logic, near-entrance detection logic, floor-switching logic, turn-by-turn navigation with alerts, location trigger feature to detect when users reach the building area/geofence: ○ Custom simulator to test turn-by-turn navigation, compensating for the inability to test indoor navigation directly from CXApp. Adjustment logic to optimize the CXApp extended library.

4.1.2. Procured Software Services

Procured software services include components of the cloud and other services (e.g., database, authentication). Each component is described below, and their unit costs and estimated usage are described in this section.

4.1.2.1. Cloud Services

This section details the cloud services utilized in G-MAP. Note: Pricing estimates use assumptions indicated, do not constitute a budget, will likely change over time with usage and other factors outside of the control of the CMOP.

Amazon Web Services (AWS) consists of multiple packages:

AWS S3

- **Type of Cloud Service.** Object storage service for storing and retrieving data.
- **Cloud Service Licensing.** Pay-as-you-go based on storage used, requests made, and data transferred.
- **Resource Usage as of Writing.**
  - Bucket for web application (~200 MB, includes snapshots of OpenStreetMap data)
  - Bucket for call center application (~10 MB)

- Bucket for usage data, trip histories (for PMD) (~50 M, increases at ~5 MB per month)
- Bucket for deviation surveys (~15 kB at time of writing, increases at ~5 kB per month)
- Total AWS S3 storage: less than 1GB @ $0.023/GB/month
- Price: $0.023/month (negligible)

AWS EC2

- **Type of Cloud Service.** Provides resizable compute capacity in the cloud.
- **Cloud Service Licensing.** Pay-as-you-go based on the compute capacity on an hourly basis.
- **Resource Usage as of Writing.** AWS EC2 resources are listed in **Table 7**Table 7 below**.**

Table 7. AWS EC2 resources and cost estimates for G-MAP

Component	Compute Units	Hourly Rate	Monthly (Always On)	Load Balancer? (+$22/Month)	Estimated Monthly Cost
OTP	1x r5d.xlarge	$0.288	$208	Yes	$230
OTP-personas	1x t2.medium	$0.0464	$34	No	$34
Push notifications middleware	1x t2.xlarge 1x db.m6gd.large for database	$0.1856 $0.0904	$134 $66	Yes	$222
App survey	1x t4g.small	$0.0168	$13	Yes	$35
Geocoder	1x c5.xlarge	$0.17	$123	No	$123

AWS API Gateway (OTP-Personas, PMD, Trip Surveys – No Caching)

- **Type of Cloud Service.** Fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs.
- **Cloud Service Licensing.** Pay-as-you-go based on the number of API calls received and data transferred.
- **Current Resource Usage.** The following estimates are provided but will need to be revisited during Phase 3 based on actual application usage.
  - $3.50 per million requests per month.
  - Assuming about 100 users at launch, each 60 minutes (3600s) of live tracking (1200 location updates at one every three seconds).

- There are currently no throttling restrictions.
- Total 120 million requests per month or $420/month.

AWS Route 53

- **Type of Cloud Service.** Internet domain and subdomain management.
- **Cloud Service Licensing.** Pay-as-you-go based on the number of (sub)domains managed.
- **Resource Usage as of Writing.** One hosted zone cost ($0.50/month) is shared across multiple deployments, G-MAP share is negligible.

AWS CloudFront

- **Type of Cloud Service.** Fully managed content distribution network to optimize data transfers from S3 buckets.
- **Cloud Service Licensing.** Pay-as-you-go based on the data transferred.
- **Resource Usage as of Writing.** Assuming 1TB traffic per month (free tier).

AWS SNS

- **Type of Cloud Service.** Fully managed service to send easily send push notifications to Android and iOS devices.
- C**loud Service Licensing.** Pay-as-you-go based on the number of requests.
- **Resource Usage as of Writing.** Assuming 1 million calls per month (free tier).

4.1.2.2. Other Cloud Services

Other cloud services include database and troubleshooting services. These include MongoDB and Google Firebase.

MongoDB Atlas (Database)

- **Type of Cloud Service.** Fully managed hosting of MongoDB, a no-schema database.
- **Cloud Service Licensing.** Pay-as-you-go based on the data stored and usage, with monthly price cap.
- **Resource Usage as of Writing.** Using Flex plan (pricing listed in Table 8). Total data size is less than 100MB but increases with number of users and number of recorded trips.

Google Firebase: Crashlytics and Performance Monitoring

- **Type of Cloud Service.** Fully managed service for application troubleshooting and performance analysis.
- **Cloud Service Licensing.** No cost.
- **Resource Usage as of Writing.** Only Crashlytics and Performance monitoring services are used for mobile app development. No other Google Firebase services are used.

4.1.2.3. Software Configurable Items

Other software services supported on an annual basis include those listed in **Table 8.** The table includes the software name, description, cost per unit, number of units per year, and annual costs for the service.

Table 8. Procured Software Configurable Items

Item	Description	Cost per unit	# Units	Annual Cost
Sparkpost	Email provider	$20/month	12	$240
Twilio	SMS provider Cost shared across multiple implementations	$71/month	12	$852
MongoDB	No-schema database	$30/month (Flex tier)	12	$360
MapTiler	Map (for web UI) $60/month shared across multiple implementations	$10/month	12	$120
MapBox	Map (for mobile apps)	Currently on free tier (less than 25,000 users per month)	N/A	N/A
Auth0	User authentication	Currently on free tier	N/A	N/A

Item	Description	Cost per unit	# Units	Annual Cost
Geocode Earth	Geocoder Cost shared across multiple implementations “Basic" plan equivalent usage	$200/month	12	$2400
TypeForm	Trip Survey	$64/month	12	$768
AWS Combined	G-MAP web UI and backend	$1064/month (rough estimate)	12	$12768
Google Firebase	Crashlytics and Performance Monitoring only	Currently on free tier	N/A	N/A

4.1.3. Operational Configuration Management

G-MAP software configuration management includes version control and deployment mechanisms for all software components.

G-MAP Version Control with GitHub. All source code and deployment scripts are managed using GitHub (see URLs provided in **Section 4.1.1).** Configuration files that include secrets (e.g., API tokens) and certain G-MAP-specific customizations are version-controlled and stored in an Arcadis private GitHub repository.

Software Deployment. G-MAP follows an automated deployment process tied to the G-MAP code branch of OTP-personas. The OTP routing engine is deployed on demand to AWS EC2 using the Arcadis TRANSIT-data-tools GTFS management software. The G-MAP web interface is deployed on-demand using the Arcadis private code repository mentioned in **Section 4.1.1**. Code changes for G-MAP, OTP routing engine, and the G-MAP web interface become available for deployment upon the passing of unit and integration tests.

Synchronization with the Physical Environment. Physical attributes that affect G-MAP functionality and behavior are indicated and managed as follows:

- **Points of Interest (POI).** Points of interest may occasionally be updated. See **Section 4.8.1**.
- **Transit Stops.** Location updates are handled with GTFS updates. See **Section 4.8.3**
- **Road Network and Features.** These are deemed fixed. See **Section 4.8.3**
- **Intersections.** PED-X activation is based on the physical location of intersections within the scope of this phase. Specifically, the vertices (starting and ending points) of each signal-

controlled crossing for the PED-X intersections are derived from OSM and entered as configuration for G-MAP. The number and coordinates of the crossings at each intersection are deemed fixed, however occasional corrections may be accommodated after stakeholder discussion.

4.2. Security and Privacy

This section describes high level security and privacy handling issues. The section describes data security at rest and in transit. It also describes high level data privacy provisions.

Data Security

- **Data in Transit.** All communications between G-MAP and other systems, including STM, AWS-S3, PED-X, Ride Request, and the TSP policy server are secured using HTTPS with TLS encryption. Internal transfers between G-MAP and MongoDB Atlas for storage are also end-to-end encrypted. *An API key and authenticated email address can only be used to retrieve the user information associated with the email address via authentication tokens issued by Auth0.*

- **Data at Rest**

    - **OTP Routing Engine**. Only authorized Arcadis administrators can access graph and log data from an AWS VPN, from the AWS console, or from Arcadis TRANSIT-data-tools.

    - **OTP-Personas (OTP-Middleware).** User ids, emails and phone numbers are written to log files to troubleshoot/debug notifications, and itineraries (including origins-destinations pairs) are dumped to log files to troubleshoot/debug trip monitoring. Emails, phone numbers, and itineraries are not linked in the logs. Log file access can only be done by authorized Arcadis administrators from an AWS VPN.

    - **MongoDB Atlas**. PII is stored in MongoDB's Atlas service, according to MongoDB's server tier limitations at https://www.mongodb.com/docs/atlas/reference/limitations/. All data on MongoDB's Atlas service is encrypted by default at rest per https://www.mongodb.com/docs/atlas/setup-cluster-security/. Access to the cluster is also restricted. Besides the G-MAP application, only authorized Arcadis administrators can login or access the database via the MongoDB Atlas site or remotely from approved VPNs.Besides the G-MAP application, only authorized Arcadis administrators can login or access the database via the MongoDB Atlas site or remotely from approved VPNs.

    - **AWS S3**. Data exchanged to the public PMD are compiled into ZIP files and stored on AWS S3 daily. Data are encrypted by default using server-side encryption with Amazon S3 managed keys (SSE-S3). Access to the AWS S3 bucket that holds the PMD data, including user PII, is restricted. Only authorized Arcadis administrators or the public PMD can retrieve data from the bucket, from the AWS console or using a PMD-specific API key, respectively.

- **API Security.** Requests to the protected G-MAP API and the PMD API are authenticated using secure keys available to the G-MAP application and the public PMD server respectively.

Privacy

- **Isolation of PII.** PII appear in three locations: MongoDB (full user account data resides there), OTP-personas logs (unlinked emails, IDs, and phone numbers), and the S3 bucket for PMD usage. Access to OTP-personas logs, MongoDB, and the PMD S3 bucket is restricted as described above.

- **Data Retention.** PII data will be retained in accordance with the IRB protocol.

4.3. G-MAP Operations and Maintenance Roles and Responsibilities

G-MAP Roles and Responsibilities for operations and maintenance are described in **Table 9**.

Table 9. Operational and Maintenance Roles and Responsibilities

Role	Organization	Responsibilities
Mobile App Operations and Maintenance Lead	Arcadis	Regular maintenance, bug fixes to iOS and Android, system monitoring, and regular security audits.
Web App Operations and Maintenance Lead	Arcadis	Regular maintenance, AWS monitoring, bug fixes to web app, system monitoring, and regular security audits.
Data & Deployment Manager	Arcadis	New deployments, coordinating with agencies on GTFS issues.
OTP Routing & OTP Personas Maintenance Lead	Arcadis	Maintaining the routing engine and OTP Personas module, system monitoring, and regular security audits.
Quality Assurance Lead	Arcadis	Regression/Acceptance testing for new releases.

4.4. Operational Modes

This section describes the different operational modes of the ST-CTN and how the G-MAP adjusts or mitigates the impact of degraded mode. The operational modes have been adapted from the Concept of Operations (ConOps) (2024).

Normal Operation. During normal operations, the full system,Error! Reference source not found. is functional and available to front facing and backend stakeholders. All objects in the environment are functioning normally and are being monitored by specified personnel.

Degraded Modes. In degraded mode, some or all of the subsystems are not functioning as intended. As the proposed system is a “system of systems,” several degraded modes are explained below.

- If the GCDOT and/or GDOT communications network experience a loss of communications, the ST-CTN system will function with limited functionality depending on where the communications

loss occurs. Degraded functionality could include the lack of STM real-time routing updates and enhanced TSP functionality.

- If the STM experiences a loss of functionality or there is a degradation of the STM/G-MAP API connection, real-time updated impedance values will not be provided to the G-MAP subsystem. The G-MAP subsystem, including the G-MAP Mobile App will be able to function in a degraded mode by providing routing information to the end user, but will not be able to provide accurate impedance values.

- If communication between the Sidewalk Inventory and the STM Platform is interrupted, accurate, real-time, impedance values for travel will not be provided to the G-MAP subsystem. The G-MAP subsystem, including the G-MAP Mobile App will be able to function in a degraded mode by providing routing information and historical impedance values for travel to the end user.

- If transit agency static GTFS schedule or GTFS-realtime data is temporarily unavailable or out of date, G-MAP functionality will continue to be available without that agency's unavailable information.

- If the Dynamic Data Broker experiences a loss of functionality, impedance values for travel and CV functionality will not be available for the G-MAP subsystem. The G-MAP subsystem, including the G-MAP Mobile App will be able to function in a degraded mode by providing routing information to the end user, but will not be able to provide accurate impedance values for travel. Additionally, connection to the CV subsystem will be severed if the Dynamic Data Broker experiences a loss of functionality. GCT will still be able to issue TSP commands, but pedestrian safety messages or pedestrian signal requests will not be available.

- If the Traffic Management or Intelligent Transportation System (ITS) Hub experiences a loss of functionality, CV functionality will not be available to the G-MAP subsystem or the GCT subsystem. The G-MAP subsystem, including the G-MAP Mobile App will be able to function in a degraded mode by providing routing information and impedance values for travel to the end user, but pedestrian safety messages, pedestrian signal requests, and TSP will not function. When communication loss to the CV subsystem is detected, the STM subsystem will be able to add a penalty to the impedance value for travel.

- If the connected intersection portion of the CV subsystem experiences a loss of functionality, through device failure or communication loss, CV functionality will not be available for all or part of the G-MAP subsystem or GCT subsystem. Communication or device malfunction can impact the performance of isolated parts of the CV subsystem or can be widespread throughout the entire project area. Regardless of the scale, the G-MAP subsystem, including the G-MAP Mobile App will be able to function in a degraded mode by providing routing information and impedance value for travel to the end user, but pedestrian safety messages, pedestrian signal requests, and TSP will not function for all or part of the network. When communication loss to the CV subsystem is detected, the STM subsystem will be able to add a penalty to the impedance value for travel.

Failure Mode. In failure mode, the ST-CTN application is not available to the end user in an operational or degraded mode. There are several scenarios that could cause the system to operate in failure mode, these include:

- If the G-MAP Mobile App experiences a loss of functionality, end users will not have functional access to the ST-CTN application. Trip feedback will not be provided to the STM Platform during this time, but all other system functions may remain operational.

- If the G-MAP Multimodal Trip Planner and Access Tools experiences a loss in functionality, the ST-CTN application will not function. Subsystems that push information to G-MAP Multimodal Trip Planner and Access Tools may still be able to communicate and provide data without any loss.

4.5. Operational Processes

This section describes the high-level operational processes that are applied to the G-MAP subsystem. The processes include system monitoring, performance management reporting, and standard operational processes that occur periodically during operations.

4.5.1. System Monitoring

Security, operations reliability and performance processes are listed below.

- **Security (Audits and Daily Review).** G-MAP OTP-personas and OTP-React-Redux use AWS and GitHub's built-in security monitoring and alerts.

- **Detecting and Identifying Issues and Anomalies.** Automated AWS email alerts are set up to detect instance health issues and server storage usage exceeding 92%.

- **Operational Performance (Uptime, Degraded Operations, etc.).** An uptime dashboard has been set up for G-MAP components.

4.5.2. Operational Performance Reporting

Arcadis will provide monthly SLA reporting on the following items:

- Reliability – uptime

- Storage usage

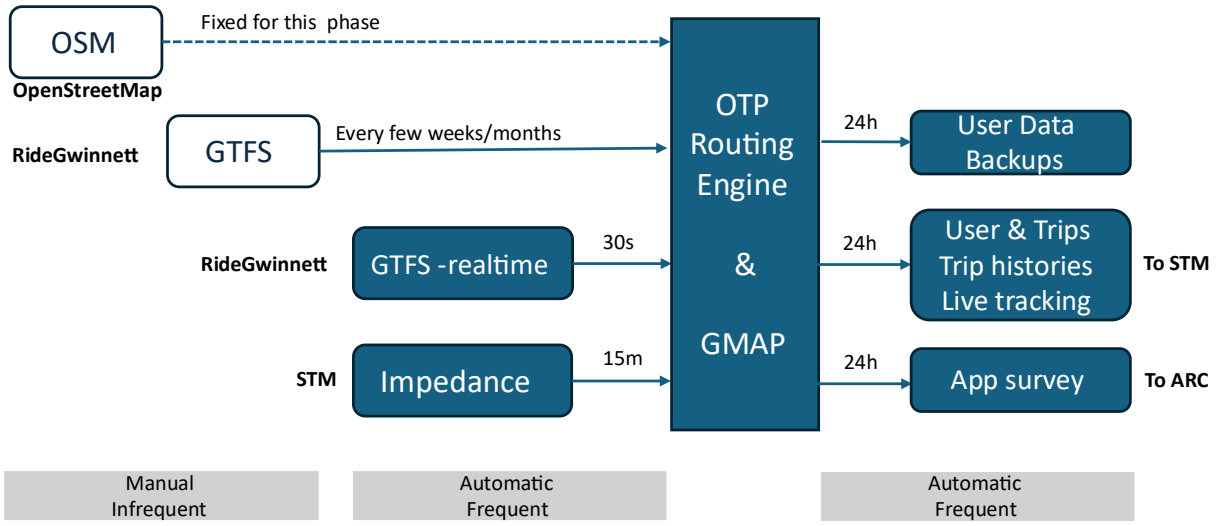
- Interface uptime/reliability

- Backup schedule

- Security Audit

4.5.3. Operational Processes

This section describes the periodic procedures for data exchange between G-MAP and other systems (see **Figure 5).**



Source: GDOT, 2025

Figure 5. Diagram of Data Import and Export Mode and Frequencies

GTFS Static Feeds. Arcadis will periodically monitor new GTFS feed versions published by MARTA and Gwinnett County (or their respective contractors) and deploy those updated feeds to the G-MAP OTP server.

GTFS-realtime Feeds. Ingestion of GTFS-realtime feeds as published by Gwinnett County or its contractors occurs automatically by the G-MAP OTP server. No additional action is required for real-time transit data to be available in G-MAP.

OpenStreetMap (OSM) Basemap Graph. The OSM graph is fixed due to limitations from frequently updating the street and impedance model in STM. Exceptions will be dealt on an individual basis and coordinated with GA Tech.

Impedances (Impedance API). Ingestion of travel time impedances published by STM occurs automatically by the G-MAP OTP server. No additional action is required for real-time impedances to be available in G-MAP.

Users, Trip Histories, and Trip Surveys. An export of users and trip histories and trip surveys is performed automatically, daily, as compressed archives, to G-MAPs AWS S3 bucket for use by the PMD. A list of exported entities can be found in the PMESP, (2025). Trip survey responses are deleted from TypeForm after being transferred to S3.

General G-MAP Feedback Surveys. Trip surveys are compressed automatically, daily, to G-MAPs AWS S3 application survey bucket for post-usage analysis.

Deleted Accounts. User account data are deleted immediately upon their request on the web UI or mobile app. Any preferences, saved monitored trips, trip search history, push notification devices are deleted. Companion/dependent/observer relationships to that user in other user accounts are marked invalid. Tracked journeys are preserved for subsequent post-travel analysis in STM.

Backups. G-MAP OTP-personas data on MongoDB Atlas are backed up automatically once per day. Snapshots are retained for 7 days.

4.6. Operational Issue Handling Procedures

The G-MAP issues handling procedures start at the Detection state described in the Change Management Process in **Section 3.3**. The process includes the following:

- **Identification.** Regular monitoring and prompt reporting of issues using a standardized form/email distribution to the Arcadis team.
- **Assessment.** Evaluate severity and impact, classify the issue.
- **Notification.** Alert relevant teams and stakeholders, develop a communication plan to coordinate resolution.
- **Investigation.** Conduct root cause analysis, document findings and steps taken.

Following review, prioritization and assignment during the Change Management Process, Arcadis will proceed with the following steps (that correspond to the in-progress and recovery states):

- **Resolution.** Create and implement a detailed action plan, monitor progress.
- **Verification.** Confirm resolution, continue post-resolution monitoring.

4.7. Operations Backup, Shutdown, Restart/Recovery

This section describes the approach to operations backups, shutdown, and restarts/recoveries.

4.7.1. Operations Backup

G-MAP OTP-personas data on MongoDB Atlas are backed up automatically once per day. Snapshots (full backups) are retained seven days.

The graph for OTP routing engine does not require backups, the source data for the OSM snapshot and impedances that create the graph and GTFS static feeds are maintained in STM, by RideGwinnett or its contractors. G-MAP specific configurations are managed by Arcadis private configurations repository on GitHub.

4.7.2. Operations Shutdown

The G-MAP system is intended to remain always up and running, except under the following conditions:

- Cloud service providers deem it necessary to temporarily shut down instances (e.g., due to hardware failures).

- The ST-CTN project team decides to shut G-MAP down temporarily or permanently, including to address failure modes from **Section 4.4**.

Stakeholders will be notified of a system shutdown via email notification, with as much lead time as possible. These notifications will include a well-defined reason for the shutdown, as well as the expected duration that the G-MAP application is expected to be unavailable.

The system shutdown follows the vendor process for each component as identified in **Section 4.1.2**.

4.7.3. Operations Restart/Recovery

The G-MAP system may be restarted at the discretion of Arcadis system administrators for the following reasons:

- G-MAP or OTP Software update described in **Section 4.8**, in coordination with stakeholders.

- Cloud service providers deem it necessary to restart G-MAP servers (e.g. due to hardware failures). Stakeholders will be notified in a timely fashion.

- Degraded and failure modes identified in **Section 4.4**.

- Shutdown as described above.

- Critical software failure (e.g. memory exhausted).

System recovery consists of the restarting of the G-MAP backend server and will rely on the last known snapshot of the database if data is corrupted/lost.

4.8. Software Maintenance Updates and Upgrades

This section describes the approach to infrastructure updates, OSS improvements, data management, and procedures for addressing security, compatibility, and functionality enhancements.

4.8.1. Infrastructure software and security updates

When infrastructure software such as Android, iOS, AWS, or web browsers are updated, changes may impact or degrade operations of the G-MAP app. The impacts are grouped by severity.

- **Web, Middleware, iOS and Android Updates for High Severity Issues.** Updates for iOS and Android platforms will be prioritized and released immediately if high severity issues are identified, including security bulletins from software vendors used in the OSS. These issues include bugs or technical failures that prevent users from accessing or using critical features within the app. This ensures that core functionality is restored as quickly as possible to minimize user disruption and maintain reliability across platforms.

- **Bundling Minor and Medium Priority Tickets.** Minor and medium priority tickets will be grouped together into a single update cycle to optimize development resources and streamline the release process. By bundling these issues, we can address multiple smaller fixes or enhancements in one release, reducing the frequency of updates while maintaining steady improvements to the app's performance and user experience.

- **Upgrades Requiring Refactoring or New Functionality.** Any upgrades that involve refactoring existing functionality or adding new features will be subject to the formal change order process to ensure proper planning, alignment, and accountability. These upgrades must be reviewed and approved by the Arcadis product owner and the G-MAP project's product owner according to **Section 3.3** to confirm their necessity, scope, and impact on the product roadmap. This process ensures that upgrades are strategically prioritized and executed in line with business objectives and stakeholder expectations.

- **Web, Middleware, OS and Android apps will target preventative maintenance deployments quarterly.** The development roadmap includes quarterly updates for iOS and Android apps to focus on preventative maintenance, addressing minor bugs, optimizing performance, and ensuring compatibility with new OS features or changes. These regular deployments aim stabilize app performance, improve user experience, and prevent urgent fixes or outages, while offering a predictable and manageable update cycle.

- **Web browsers, iOS and Android OS will officially support the current OS version minus one major version**. The apps will provide official support for the latest OS version and the version immediately preceding it (e.g., iOS 17 and iOS 16, or Android 14 and Android 13). This ensures users running recent OS versions have a reliable experience while encouraging upgrades to benefit from enhanced security and features. Devices running older OS versions beyond the supported range may face limited functionality or compatibility challenges.

- **NOTE: Mobile App updates may be dependent on upstream dependencies, which may affect the timing of releases.** App update schedules may occasionally be impacted by upstream dependencies, such as external libraries, APIs, or OS-level features that the app relies on. Delays or changes in these dependencies can affect development timelines, but teams will monitor them closely and implement contingency plans to minimize disruptions and ensure app functionality remains secure and reliable.

Software security alerts are reviewed periodically, and security patches are applied accordingly, typically during off-peak times to minimize disruption to the users.

4.8.2. OSS updates and upgrades

- **OSS Update (to 3+ backoffice software)**
    - **OTP Routing Engine**. The G-MAP fork of OTP will only receive select major bug fixes after operational launch.
    - **OTP-Personas and OTP-React-Redux**. Behind-the-scenes improvements may be periodically made available after launch.

- **OSS Upgrades (to 3+ backoffice software)**

- **OTP Routing Engine**. Because support of the STM impedance model and mobility profiles is not part of the OTP roadmap, the G-MAP fork of OTP will not be reconciled with the main OTP development branch and will not receive new features or improvements after launch.
- **OTP-Personas and OTP-React-Redux**. No new features will be added/activated to these components after launch.

- **Integration Changes that Impact OSS**
  - **Integration Changes**. No integration changes are anticipated that would impact G-MAP software components.

4.8.3. Data and Other Software Updates

Data updates are typically from external sources, like GTFS or the OSM snapshot. Additionally, POIs or names not contained in the OSM snapshot are added to a POI update process.

- **GTFS Changes**
  - **GTFS Static Feeds**. Arcadis will periodically monitor new GTFS feed versions published by MARTA and Gwinnett County (or their respective contractors) and deploy those updated feeds to the G-MAP OTP server.

- **OSM Changes to Coordinate with STM**
  - **G-MAP and STM Share an OSM Snapshot.** The OSM snapshot is fixed to correspond to field measurements the GA Tech team collected around the time of the OSM snapshot. This OSM snapshot is used to generate the STM travel and impedance model. G-MAP and STM will coordinate updates as described in **Section 1.**

- **POI Updates or User Lookup Requests**
  - **Changes to POI**. May be updated as reported when issues are identified and submitted to Arcadis.

4.9. G-MAP Operations and Maintenance Risks and Contingencies

Table 10 lists G-MAP operational and maintenance risks as well as their corresponding approach to mitigation.

Table 10. Operational and Maintenance Risks

Risk #	Risk	Mitigation Measures
1	G-MAP or OTP software update introduces a regression or critical bug	Arcadis reverts code changes made to the corresponding branches and deploys those reversals in order to restore service or functionality.

2	Changes in the physical street environment result in suboptimal or incorrect routing	Arcadis will coordinate an update to the OSM extract, GA Tech or other stakeholders to resolve the issue.
3	GTFS transit data is not provided/updated	Arcadis will coordinate with Gwinnett County or their respective contractors to resolve the issue.

5. STM Operations and Maintenance

This section outlines the STM operational software, procured services, configuration management, security, operational processes, maintenance activities, and associated risks, including procedures for monitoring, backups, updates, degraded operations, and recovery.

5.1. Configurable Items / Operational Software

The STM operational software elements that have specific operations and maintenance policies associated with are listed in this section. All custom, OSS, and SaaS that play a critical role within STM and Private PMD are listed as a configurable item.

5.1.1. OSS / Software Developed Under Contract

Software elements developed in support of STM generally fall under three groups: AWS Lambda functions, API endpoints created within AWS Api Gateway, and the STM graph database, leveraging AWS Neptune.

STM Lambda Functions. A collection of AWS Lambda functions was developed to address STM functionality falling under several categories. Importing data into the STM database, including OSM data, default impedance values, sidewalk data, and event data from Waze and Georgia NaviGAtor are all managed via AWS Lambda functions triggered by private API calls. Additional details related to STM Lambda functions can be found in the SDD.

STM API. The API developed in support of STM can be divided into the authorized API available to the G-MAP client, and a private API accessible only within the STM AWS environment. The G-MAP API contains endpoints solely for returning dynamic impedance data to the G-MAP client. Additional details related to the G-MAP API can be found in the SDD.

The private API internal to the STM AWS environment contains endpoints related to triggering several types of data imports, ingesting alerts/events data, and dynamically calculating impedance values. Additional details related to STM API endpoints can be found in the SDD.

STM Graph Database. The STM graph database is implemented in AWS Neptune and contains mapping data from OSM as well as measured sidewalk asset and defect data, and multiple types of dynamic traffic alert/event nodes.

5.1.2. Procured Software Services

This section provides an overview of the cloud services and software resources supporting STM operations, detailing the various uses and associated licensing and costs.

Cloud Services. This section details the cloud services utilized in STM. All these services are provided by Amazon Web Services (AWS).

- **AWS Lambda**
    - **Type of Cloud Service.** Serverless compute service that executes code in response to events.
    - **Cloud Services Resources.** The STM utilizes a collection of AWS Lambda functions executing Python 3 scripts. In the STM these functions are generally allocated 512MB of working memory, though simpler functions are limited to as low as 128MB, and more complex functions can be configured to use as much as 2048MB. Compute resources allocated to Lambda function execution are generally limited to one AWS vCPU, but compute allocation scales linearly with each function's memory usage and can increase as needed on demand.
    - **Cloud Service Licensing.** Pay-as-you-go based on the number of requests and compute time consumed.
- **AWS Simple Storage Service (S3)**
    - **Type of Cloud Service.** Object storage service for storing and retrieving data.
    - **Cloud Services Resources.** STM utilizes a collection of seven S3 buckets, each utilizing Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). These buckets utilize shared capacity within the STM AWS environment using the Standard storage class.
    - **Cloud Service Licensing.** Pay-as-you-go based on storage used, requests made, and data transferred.
- **AWS API Gateway**
    - **Type of Cloud Service.** Fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs.
    - **Cloud Services Resources.** The STM API Gateway is configured with a single ITS4US API, consisting of 15 available resource URLs. The STM API is configured to support a throttling rate of 10,000 requests per second, with bursts of 5,000 requests.
    - **Cloud Service Licensing.** Pay-as-you-go based on the number of API calls received and data transferred.
- **AWS Neptune**
    - **Type of Cloud Service.** Fully managed graph database service.
    - **Cloud Services Resources.** The STM Neptune database uses a serverless configuration with scaling storage allocation. The database cluster is configured to allocate a maximum of 128 Neptune Capacity Units (NCUs).
    - **Cloud Service Licensing.** We operate under a pay-as-you-go model, where we are charged based on the NCUs and storage consumed by the STM Neptune database.

- **AWS Amazon EventBridge**
    - **Type of Cloud Service.** Serverless event bus that makes it easy to connect applications together using data from your own applications, SaaS applications, and AWS services.
    - **Cloud Services Resources.** STM utilizes AWS EventBridge with five different Rules within a single Event Bus.
    - **Cloud Service Licensing.** Pay-as-you-go based on the number of events processed.
- **AWS EC2**
    - **Type of Cloud Service.** Provides resizable compute capacity in the cloud.
    - **Cloud Services Resources.** STM uses EC2 instances within the VPC primarily for dedicating resources to the Neptune database. EC2 instances are configured using the “t2.micro” instance type, with 1 vCPU and 1 GiB of memory.
    - **Cloud Service Licensing.** Pay-as-you-go based on the compute capacity on an hourly basis.
- **AWS CodePipeline**
    - **Type of Cloud Service.** Continuous integration and continuous delivery (CI/CD) service for fast and reliable application updates.
    - **Cloud Services Resources.** STM leverages two sets of three-stage pipelines in support of building and deploying code changes and executing unit tests.
    - **Cloud Service Licensing.** Pay-as-you-go based on the resources used in the pipeline, such as build time and storage.

Software Configurable Items. Table 11 describes the software that is procured, licensed or used and its cost for this subsystem.

Table 11. Procured Software Configurable Items

Item	Description	Cost per unit	# units	Annual Cost
AWS Neptune	AWS Neptune monthly expenses	~$2,875	12	$34,500
AWS EC2	AWS EC2 monthly cloud expenses	~$85	12	$1,020
AWS VPC	AWS VPC monthly cloud expenses	~$25	12	$300
AWS CloudTrail	AWS CloudTrail monthly cloud expenses	~$15	12	$180
AWS Lambda	AWS Lambda monthly cloud expenses	~$11	12	$132

AWS S3	AWS S3 monthly cloud expenses	~$20	12	$240
AWS CloudWatch	AWS CloudWatch monthly cloud expenses	~$15	12	$300
AWS Cloud Total Expenses	**N/A**	**~$3,056**	**12**	**~$36,672**

5.1.3. Operational Configuration Management

The STM utilizes version control, CI/CD pipelines, and infrastructure-as-code principles to manage the configuration of operational software.

Version Control with Git. All source code, configuration files, and deployment scripts are managed using Git.

CI/CD with AWS CodePipeline. AWS CodePipeline automates the build, test, and deployment processes for the STM software. This ensures that code changes are thoroughly tested and deployed consistently across different environments.

Infrastructure as Code with AWS EC2. The STM application is deployed on Amazon EC2 instances. This utilizes infrastructure-as-code principles to manage the configuration of these instances, using tools like AWS CloudFormation stacks to define and provision infrastructure resources in a repeatable and consistent manner.

Configuration Backups with AWS Backup. AWS Backup is used to create regular backups of the STM graph database and the EC2 instances, including the application files and configuration settings. This ensures a quick recovery in the event of an outage or disaster, minimizing system downtime and ensuring application continuity. AWS Backup contributes to our system's high availability by providing durable and secure storage for backups, with guarantees on data durability and availability. These backups are stored in S3, which offers 99.999999999% durability and is designed for high availability with data replicated across multiple Availability Zones.

5.2. Security and Privacy

This section outlines data security, privacy, and compliance measures for STM, including encryption, access controls, PII handling, and ongoing monitoring through audits and vulnerability scans.

Data Security

- **Data in Transit.** All communication between STM system components, including the G-MAP application client and the API, is secured using HTTPS with TLS encryption.
- **Data at Rest.** The STM graph database is secured inside an AWS Virtual Private Cloud (VPC), which logically isolates the database. Requests sent to the VPC are routed to the AWS Lambda functions that are responsible for querying the database and processing a response. Only requests from the AWS API Gateway and AWS EventBridge are authorized by the VPC.

- **API Security.** Requests to the protected G-MAP API and the PMD API are authenticated using secure keys available to the G-MAP application and the public PMD server respectively. The G-MAP API key also authorizes G-MAP access to the STM S3 bucket for retrieving data too large to be sent via Lambda responses.

Privacy

- **Isolation of PII.** The STM isolates the PII data inside S3 in compliance with the IRB protocol. The data goes through anonymization and aggregation steps. Data shared to applications outside the STM do not have any PII.

- **Data Retention.** PII data is isolated and retained in compliance with the IRB protocol.

Compliance

- **Data Management Plan and Data Privacy Plan.** Further details on data management and privacy practices are available in the SDD and the IRB protocol document.

Ongoing Security Measures

- **Security Audits.** The IRB protocol will be followed for ensuring data security. Limitation of access to data by external entities and requirement of authentication keys to access data is used to ensure data security. For system level security, no additional measures are taken beyond what is provided by AWS.

- **Vulnerability Scanning.** The system will rely on manual quarterly vulnerability scans conducted by GTRI.

5.3. STM Operations and Maintenance Roles and Responsibilities

The operations and maintenance roles and responsibilities for the STM are listed in **Table 12.**

Table 12. STM Operational and Maintenance Roles and Responsibilities

Role	Organization	Responsibilities
Software Maintenance	GTRI/GA Tech	Software maintenance, updates, and bug fixes.
Data Collection	GA Tech	Collection and maintenance of sidewalk data.
G-MAP Logging	Arcadis	Secure hosting of G-MAP logs for retrieval by STM.

5.4. Operational Modes

This section details the operational modes for the STM. It lists how the STM adjusts or mitigates the impact of degraded mode. The operational modes have been adapted from the ConOps (2024).

Normal Operation. During normal operations, the full system is functional and available to input and output subsystems. All objects in the environment are functioning normally and are being monitored by specified personnel.

Degraded Modes. In degraded mode, some or all of the subsystems are not functioning as intended. The degraded modes are explained below.

- If communication via Waze or NaviGAtor event streams is disrupted or fails, existing event data already ingested by the STM is preserved and will continue to be used for impedance calculations until its expiration time, or until 15 minutes have passed without any relevant updates. Once the event is considered expired, it is removed from the STM database and no longer impacts impedance calculations. If event stream communication is resumed, any currently valid events are incorporated into impedance calculations. Extended periods of event stream communication failure will result in STM relying on default impedance values.

Failure Mode. In failure mode, the STM application is not available to the end user in an operational or degraded mode.

- If the STM experiences a loss of functionality in the AWS Neptune or API Gateway service, G-MAP users will not have functional access to the STM. Trip impedance will not be provided, and communications with the STM will be unavailable. The G-MAP will use the last updated Impedance API upload.

5.5. Operational Processes

This section describes the high-level operational processes that are applied to the STM subsystem. The processes include system monitoring, performance management reporting, and standard operational processes that occur periodically during operations.

5.5.1. System Monitoring

The STM system leverages a combination of AWS CloudWatch and AWS CodePipeline to monitor system operation and ensure optimal performance and reliability.

AWS CloudWatch plays a central role in monitoring the health and performance of the STM software. We utilize CloudWatch to:

- **Collect and Track Key Metrics.** CloudWatch collects metrics from various AWS services used in the STM infrastructure, including Lambda, Neptune, EC2, and API Gateway. These metrics include CPU utilization, memory usage, network traffic, error rates, and logging.

- **Detect and Identify Issues.** CloudWatch alarms are configured to automatically detect anomalies and potential issues. For example, alarms are set to trigger notifications if CPU utilization exceeds a certain threshold, error rates spike, or critical system components become unavailable.

- **Monitor Operational Performance.** CloudWatch dashboards provide a visual representation of key performance indicators (KPIs), allowing us to monitor uptime, identify performance bottlenecks, and track the overall health of the system.

- **Ensure Security.** CloudWatch logs are used to monitor security-related events, such API access attempts and potential security breaches. These logs are regularly audited by GTRI to ensure compliance and identify any suspicious activity.

AWS CodePipeline is used to monitor the CI/CD pipeline for the STM software. We utilize CodePipeline to:

- **Track the Progress of Code Deployments.** CodePipeline provides visibility into the different stages of the CI/CD pipeline, allowing us to monitor the status of builds, tests, and deployments.

- **Identify and Resolve Deployment Issues.** CodePipeline integrates with CloudWatch to provide alerts and notifications if any stage in the pipeline fails. This allows us to quickly identify and address deployment errors, ensuring that software updates are rolled out smoothly.

GTRI is primarily responsible for monitoring the system using CloudWatch and CodePipeline. They are responsible for configuring alarms, creating dashboards, analyzing performance data, and addressing any alerts or issues that arise, and ensure the ongoing security of the system.

5.5.2. Operational Performance Reporting

Operational performance data is captured and reported using a combination of AWS CloudWatch, AWS S3 monitoring tools, and AWS Backup.

AWS CloudWatch forms the core of the performance monitoring and data capture strategy.

- **Reliability (Uptime).** CloudWatch monitors the uptime and availability of critical system components. Metrics such as API latency, error rates, and service health checks are tracked to provide a comprehensive view of system reliability. CloudWatch alarms are configured to trigger notifications in the event of downtime or degraded performance, allowing for prompt response and mitigation.

- **Log Monitoring.** CloudWatch Logs collects and analyzes log data from the Neptune STM database and all of the Lambda functions. This data provides insights into system behavior, error occurrences, and potential performance bottlenecks.

AWS S3 Monitoring Tools are used to track storage usage and ensure efficient utilization of resources.

- **Storage Lens.** Storage Lens provides a centralized view of object storage usage and activity across the S3 buckets. It helps analyze storage trends, identify cost optimization opportunities, and ensure compliance with data retention policies.

- **S3 Metrics.** CloudWatch collects metrics related to S3 storage usage, request rates, and data transfer. This data is used to monitor storage capacity, identify potential issues, and optimize storage costs.

AWS Backup is used to manage and monitor the STM backup processes.

- **Backup Schedule.** AWS Backup provides a centralized view of the STM backup schedules and their execution status. This ensures that backups are performed according to defined policies and that data is protected in accordance with the STM disaster recovery plan.

- **Backup Monitoring.** CloudWatch monitors the status of backup jobs and sends alerts for any failures or issues. This allows us to proactively address backup-related problems and ensure data integrity.

5.5.3. Operational Processes

On a daily schedule, a snapshot of the STM database is generated and backed up to S3. Daily snapshots are generally retained for one week before being removed from S3, with the snapshot from the final day of the month being stored as a monthly backup and retained for twelve months.

Performance metrics are calculated on a weekly basis every Monday, incorporating data from the previous seven-day period (Monday to Sunday). Performance data is stored in the “its4us-public-export” S3 bucket. Performance metrics data is stored indefinitely.

STM logs are automatically monitored by AWS CloudWatch and associated triggers. In the event of communication failures with external data streams (e.g., Waze, NaviGAtor), alerts are sent to GTRI to investigate errors with associated data ingestion Lambda function(s).

Manual quarterly security audits are conducted against the STM, and any findings are tracked for GTRI to address. Any necessary security patches are typically applied within fourteen days of audit findings, dependent on severity of finding(s) and complexity of solution(s).

5.6. Operational Issue Handling Procedures

The operational issues handling procedures adopt the Change and Issue Management Processes without change.

5.7. Operations Backup, Shutdown, Restart/Recovery

Operations backup, shutdown, and restart / recovery processes are described in the subsections below.

5.7.1. Operations Backup

Snapshots of the STM Neptune database are backed up daily and discarded after seven days, and longer-term monthly database backups are retained for one year. Additional details about the STM backup configuration can be found in **Section 5.5**.

5.7.2. Operations Shutdown

While the STM is designed for continuous operation, there may be circumstances that require a planned or unplanned system shutdown. Planned shutdowns would typically be limited to planned maintenance activities, e.g., software upgrades or security patching. Unplanned shutdowns would typically be limited to emergency situations.

The decision to initiate a system shutdown will be made collaboratively between GTRI and GA Tech and other members of the system maintenance team. The decision-making process will consider the following factors:

- **Severity of the Issue.** The impact of the issue on system functionality and user experience.
- **Urgency of the Shutdown.** Whether the shutdown needs to be performed immediately or can be scheduled for a later time.
- **Potential Impact on Stakeholders.** The effect of the shutdown on users, partners, and other stakeholders.

Stakeholders will be notified of a system shutdown via email notification, with as much lead time as possible. These notifications will include a well-defined reason for the shutdown, as well as the expected duration that the STM is expected to be unavailable.

The system shutdown will be performed in a controlled and systematic manner to minimize data loss and disruption. Before any planned shutdown, a snapshot of the STM graph database will be generated. If the activity includes shutting down the database, all other AWS components will be shut down before the database itself.

The instructions for backing up, shutting down and restarting AWS components are available via AWS official documentation at: https://docs.aws.amazon.com. Most AWS services like Lambda function and API Gateway that execute on demand do not incur costs if the functions and the APIs are not being executed or used. These services do not need to be shut down and restarted. The order for shutting down the remaining AWS components of the STM are as follows:

1. Disable all of the AWS EventBridge schedulers (Do not delete)
2. Disable all of the AWS EventBridge rules (Do not delete)
3. Neptune - create a snapshot of the databases and delete the databases
4. Stop EC2 instances (Do not terminate)
5. S3 buckets backup - optional; currently ITS4US S3 buckets are not backed up. If they are backed up, the buckets could be deleted and restored.

5.7.3. Operations Restart/Recovery

Following a system shutdown, the STM will be restarted in a controlled and systematic manner to ensure data integrity, minimize disruption, and restore full functionality as quickly as possible.

The system restart will follow a structured approach to ensure a smooth and successful recovery. In the event of an operations restart after a planned shutdown, the AWS components will be enabled in the

reverse order they were disabled during the shutdown. Restarts after an unplanned shutdown will enable the STM graph database before any other components.

In the event of data corruption, the STM graph database will be restored from the most recent snapshot with verified functionality. In the case of planned STM restarts, this will typically be the snapshot manually generated just before the shutdown. In the case of unplanned shutdowns, this will typically be the most recent daily snapshot. Once the appropriate Neptune snapshot is identified, the database is recovered using the “Restore DB Cluster” functionality in the Neptune Console.

Stakeholders will be notified of a successful system restart via email notification. These notifications will include an update on the state of the STM, and information on any maintenance activities successfully completed (if applicable).

The order for restarting the AWS components of the STM are as follows:

1. Start EC2 instances
2. Restore a snapshot of Neptune databases
3. Restore a backup of S3 buckets if the buckets are backed up
4. Enable the AWS EventBridge schedulers
5. Enable the AWS EventBridge rules

5.8. Software Maintenance Updates and Upgrades

Software maintenance activities including updates and upgrades are included in this section. Maintenance activities include AWS application updates, STM OSS updates and upgrades and data updates as needed.

5.8.1. Infrastructure Software and Security Updates

The STM leverages serverless code hosted in AWS, so operating system updates/patches are a non-issue for STM update management. Neptune database engine updates and security patches are handled automatically by AWS, with configuration options for limiting downtime to off-peak hours.

5.8.2. OSS Updates and Upgrades

OSS updates (minor changes) are reviewed on a weekly basis and applied by GTRI during off-peak hours after testing against development/staging data.

OSS upgrades (major changes and upgrades) are reviewed on a monthly basis and applied by GTRI during off-peak hours after testing against development/staging data.

If the change impacts downstream subsystems (G-MAP or Public PMD), the issue will be subject to the software change process and documented in the software change bulletin as described in **Section 3**.

5.8.3. Data and Other Software Updates

OSM mapping data is generally updated on a monthly basis, or to address comments/feedback indicating synchronization issues between the STM and OSM. Upload and processing of updated OSM data is conducted during off-peak hours. Modifications to impedance values or calculations are conducted on an as needed basis and are conducted during off-peak hours.

Modifications to how Waze or NaviGAtor data is processed, ingested, or stored will involve software development tasks on the associated STM lambda functions, implemented by GTRI.

Any data or software modifications are implemented and tested in the STM development before being applied to the production environment. The software development process is described in the SEMP.

5.9. STM Operations and Maintenance Risks and Contingencies

Operational or maintenance risks and their associated mitigation measures are listed in **Table 13**.

Table 13. Operational and Maintenance Risks

Risk #	Risk	Mitigation Measures
1	Integration changes that impact OSS (Waze format change)	When a change to input data is anticipated, the GTRI team will review the change and assess the impact prior to implementation. The team will work with Waze to understand when the change will occur and apply the change management approach as described in **Section 3.** When a change is unknown in advance, the GTRI team will operate in “degraded mode” as defined in **Section 5.4**.
2	Incident management that occurs off-business hours and school breaks (winter)	When an incident to the software or data impacts the STM or its data, a person will be on call to address the issue and provide a timeline for its fix as described in the change management approach as described in **Section 3.**
3	GDOT format change to NaviGAtor	When a change to input data is anticipated, the GTRI team will review the change and assess the impact prior to implementation. The GDOT team is part of the monthly review team. To this end, the team expects that they will report when a change is imminent and work with the team to understand the change and when it will occur. To this end, the GTRI team will be able to apply the change management approach in a timely fashion and as described in **Section 3.** When a change is unknown in advance, the GTRI team will operate in “degraded mode” as defined in **Section 5.4** until the issue is fixed in the software.

6. Sidewalk Data Collection and Update Process

This section describes the maintenance of sidewalk data, OSM network updates, roles, responsibilities, and processes for managing changes to the OSM and Impedance API structure.

6.1. Configurable items

The sidewalk data collection occurs when an improvement or change to the sidewalk infrastructure occurs. It is anticipated that these changes will be minor and impact a small number of nodes or paths in the OSM network that is configured in the STM and G-MAP apps. In most cases, the sidewalk data collection tools will not be needed. Rather, facility maintenance plans or updated county maps will be used to apply the changes.

The configuration item requiring maintenance is the OSM network and Impedance API structure (e.g., the STM database as defined in **SDD, Section 5.4**). This data is located in STM OSS GitHub site (https://github.com/gti-gatech/STM4US/tree/main/asset_data).

Additional information about these maintenance processes can be found in the STM Admin Manual for Adding or Modifying the Locked-down OSM Network.

6.2. Maintenance Roles and Responsibilities

The roles and responsibilities for the data collection are listed in **Table 14**.

Table 14. Maintenance Roles and Responsibilities

Role	Organization	Responsibilities
OSM Graphical Editor	GA Tech System Administrator	• Perform changes to OSM network geometry based on OSM File Editor requests (e.g., add links, points) in the OSM *osmium* tool. Perform Editing, merging and cleanup of OSM network (as described in the Maintenance Processes). • Manage installation and version control of osmium tool on computer.

Role	Organization	Responsibilities
OSM File Editor	GA Tech System Administrator	• Manage (update/ add/ delete) OSM network to ensure consistency between STM and G-MAP OSM and Impedance API versions. • Coordinate changes to OSM network and impedance API with Arcadis.
G-MAP Data Manager	Arcadis (G-MAP administrator)	• Ingest OSM PBF file as directed by OSM File Editor. • Test impedance API against updated OSM PBF to ensure that the impedance layers correspond to the path-node format of the PBF.

6.3. Maintenance Processes

The process for updating the OSM and Impedance API structure are described in this section.

Editing the Public OSM Network. The Public OSM network is edited to add/modify ways/nodes by logging in to the OSM GUI editor. If a sidewalk is created, the highway:footway and footway:sidewalk tags must be added to the newly created “way”.

Once the edits are made, the changeset file corresponding with the edits is downloaded. The editor can go to the profile page and click on “My edits” to access the changeset repository.

If there is a node or “way” that needs to be included but was not edited by the editor and hence is not part of the editor’s changesets, the XML files corresponding to each individual node and “way” is downloaded.

Merging Changesets with Locked PBF. Next, the Changeset and node/way definition XML files are merged with the latest version of the Locked PBF file that is shared between G-MAP’s OTP engine and the STM using the following steps.

- The merge process involves the use of the *osmium* tool: https://osmcode.org/osmium-tool/ which can be installed as follows:
    - On an Ubuntu Linux computer, the tool can be installed using the Advanced Package Tool (APT) using a command such as: *sudo apt-get install osmium-tool.*
    - On a windows computer, it is necessary to first install Windows Subsystem for Linux (WSL), followed by installation of an Ubuntu subsystem in the WSL environment and installation of osmium using the above command.
- Once the osmium-tool is installed, it can be used to convert the Protocolbuffer Binary Format (PBF) file to human-readable format (and the reverse), merge OSM changes and files, check integrity of files, etc. First, the PBF file (binary format) is converted to an OSM file (XML format) for human readability.
- Next, the changeset and individual “way” and node definition files are merged with the OSM file.

Post-merge Clean-up. Once the merge is performed it is necessary to clean up the versions manually (or using a script) to reduce the risk of OTP ignoring the most updated version of the way and node definitions when the network is loaded from the PBF file. For this purpose, a text editor such as Notepad++ can be used.

For deduplication of network elements, the old record is deleted, and the version number of the new record is reset to 1. Note that this approach involves removal of version control information.

In addition to duplicate elements, there could be duplicate relations in the file, which are identified manually and deleted for deduplication.

Finally, the OSM file is converted back to the PBF format using the osmium tool.

Updating the "Way" Length Input Table. The length of any newly added "way" needs to be measured for impedance calculations either using measurement instruments at the site or using a mapping tool such as Google Maps.

A record corresponding to the "way" is added in the "link length" csv file that is used as input in the impedance calculations in the STM. For each "way", two rows, corresponding to travel from node A to B, and travel from node B to A, are added unless the "way" is a one-way.

The link length input table and the new PBF file is ingested in the STM and the base impedance values are recalculated to integrate the newly added network elements in the STM.

7. Integration Elements and Service Level Agreements

This section provides a high-level overview of the operations, maintenance, and governance of external systems integrated with G-MAP, including CV infrastructure, PED-X, Public PMD, Ride Request, and Indoor Navigation System (INS) components.

7.1. Introduction

The external systems including data feeds, software applications, and equipment will be operated and maintained by existing vendors or IOOs. Agreements or contracts are in place with these entities to ensure a service level that is consistent with the operational performance needs to ensure convenience and confidence by end users.

This section includes the five major external systems including systems related to Connected Vehicle operations (including traffic signal operations), PED-X, Public PMD, Ride Request, and Indoor Navigation.

7.1.1. Integration-Element Governance

Governance of these external systems are listed in **Table 15**. Each system (integration element), its description, organization responsible, and type of governance for ownership, operations or maintenance are summarized in the table. In addition, a reference to the section which describes the roles, responsibilities and / or management processes are included in the column labeled “Section”.

Table 15. Integration-Element Governance

Integration Element	Description	Organization(s) Responsible	Type of Governance	Section
CV Platform	The Connected Vehicle system operations and maintenance of software, hardware and configuration of the following items: • OBUs in the Ride Gwinnett buses, • RSUs that provide roadside information to vehicles, and • Connected Vehicle back-office equipment and services (data hub, security, etc.) • NaviGAtor • Enhanced TSP proxy server, software and services • External traffic data sharing program	GCDOT (manages local systems) GDOT (provides procurement vehicle)	Public Sector -- operations and maintenance contracts	7.2
PED-X	Operations and maintenance of: • Gwinnett traffic signal and pedestrian signal systems • PED-X Proxy Server • PED-X Proxy Server Software	Gwinnett Information Systems (server and security) GCDOT (signal equipment and configuration) GDOT (proxy software and configuration)	Public Sector -- operations and maintenance agreement	7.3
Public PMD	Operation and maintenance of public PMD commercial off the shelf (COTS)	ARC	Public sector operations Phase 3 Subconsultants	7.4

Integration Element	Description	Organization(s) Responsible	Type of Governance	Section
Ride Request	Operations and maintenance hardware and software related to: • Mobile data terminals (MDTs) in revenue vehicles providing messages to the operator • Brokage software that secures messaging between the back office and bus	Ride Gwinnett	Public sector – operations / maintenance contract	7.5
Indoor Navigation – Hardware and Facility Management	Maintenance of beacons installed at two Gwinnett Facilities in public areas: • Gwinnett Justice and Administration Center (GJAC) • Norcross OneStop	Gwinnett Facilities	Public sector – staff and resources	7.6.1
Indoor Navigation -- Software	Operations and maintenance of back-office tools and SDKs related to: • Managing beacon inventory and configuration • Operating SDK services • Maintaining SDKs for Android and iOS updates	CXApp	Phase 3 contract / license agreement	7.6.2

7.1.2. Integration Element Modes of Operation

Degraded mode of operation may disrupt G-MAP services. These degraded modes will be reported by external systems and incorporated into better understanding operational metrics. Although G-MAP enhanced services will be disrupted, alternative functionality or existing services will continue to operate in their original mode. If hardware or backend systems fail, then the services will no longer be available in any mode.

Degraded Modes: In degraded mode, some or all of the subsystems are not functioning as intended. Several degraded modes are explained below.

- If the GCDOT communications network experiences a loss of communications, the G-MAP broker will not be able to communicate with the enhanced TSP server or the PED-X proxy server. The enhanced TSP functionality will be limited to standard TSP functionality. Additionally, G-MAP will continue to track travelers, but the traveler will need to manually select the pedestrian actuation button at the intersection. G-MAP will be alerted when it sends the request to the proxy server that the message was not received for a pedestrian actuation request.

- If a Ride Gwinnett vehicle experiences a loss in functionality, through device malfunction or communication loss, enhanced TSP functionality and ride request for transit service may be interrupted. The user will still be able to board and alight a Ride Gwinnett vehicle but will not receive priority at intersections or alert the driver about their boarding and alighting stops.

- If the CXApp SDK services and back-end services experience a loss in functionality, possibly through malfunction or communication loss, indoor wayfinding functionality will be interrupted. The G-MAP subsystem including the G-MAP Mobile App will be able to function in a degraded mode by providing all services outside of indoor navigation.

7.2. CV Platform

The CV Platform is composed of serval systems. The major systems interfacing directly with G-MAP include the Enhanced TSP (**Section 7.2.1**), RSU (**Section 7.2.2**) and data access to several data sources supported under the CV Platform (**Section 7.2.3**).

7.2.1. Enhanced TSP

The major Enhanced TSP system components include the OBUs that are installed on board Ride Gwinnett revenue vehicles, the TSP software logic and the updates to the TSP logic to support enhanced TSP, and the proxy server to provide a secure gateway between the TSP software and G-MAP.

Table 16. Enhanced TSP Roles and Responsibilities

Roles	Organization	Responsibilities
Operate OBUs on board revenue vehicles	Ride Gwinnett / GCDOT and GCDOT / GDOT contractor	Ensure the OBUs operate effectively on-board the transit vehicle in revenue service. Operations include: • Monitor communications between the bus and external systems including with RSUs and TSP systems. • Review log files to monitor operations and security. Note: established SOPs are in place to perform these duties.

Roles	Organization	Responsibilities
Maintain OBUs	GCDOT / GDOT contractor	Ensure OBU maintenance includes: • Update OBU software and firmware as necessary. • Update configuration parameters if needed. Note: established SOPs are in place to perform these duties.
Manage TSP Software	GCDOT / GDOT contractor	Operate and maintain TSP software including additional logic to support enhanced TSP. Maintenance may be needed if the OBU configuration is changed, or the on-board functions / data feeds are updated by Ride Gwinnett.
Manage Enhanced TSP Proxy Server	GCDOT contractor	Operate Enhanced TSP secure gateway server. Maintain software and configuration of the Enhanced TSP secure gateway. Monitor operations and security of the Enhanced TSP secure gateway.

Any changes to the Enhanced TSP system will be presented to the Change Management Process and will be included in the software bulletin as documented in **Section 3**.

7.2.2. RSU

The RSU includes responsibilities for monitoring RSU, ensuring configuration is up-to-date, and managing RSUs at sites under construction, as listed in **Table 17**.

Table 17. RSU Roles and Responsibilities

Roles	Organization	Responsibilities
Operate and maintain RSUs	GCDOT / GDOT contractor	Ensure the RSUs operate effectively at intersections. Operations include: • Monitor communications between the signal system and message broadcast. • Store broadcast messages in the CV Data Hub. • Review log files to monitor operations and security. Ensure RSU maintenance includes: • Update RSU software and firmware as necessary. • Update configuration parameters if needed. Note: established SOPs are in place to perform these duties.
Install additional RSUs	GCDOT / contractor	Execute the process to install new RSUs at specified intersections including: • Identify details for location and configuration of the RSUs. • Manage and verify RSU configuration with back-office software (e.g., MaxTime and MaxTime CV) that includes specifications that support TIMS Pedestrian Presence Alert message.

The list of RSU sites can be found in the **Appendix, RSU Site Locations**.

Requests for additional RSUs at specific location should be directed to the GDOT CV manager and the Gwinnett IT liaison. These requests may be made at the Change and Issues Management meeting held monthly as described in **Section 3.**

7.2.3. CV Data Feeds

The CV and Traffic Operations data feeds includes:

- Waze data provided under the GDOT data agreement
- NaviGAtor data feeds
- TIMS Pedestrian Presence Alert log files

The Waze data is provided as a streaming service and is discussed in the Interface Control Document (ICD), Interface I-8. Any change to the Waze data will impact the STM updates and will be documented in the Software Bulletin. GDOT staff responsible for the data agreement will participate in the Change Control Meetings to inform them of the change.

The NaviGAtor and TIMS alerts are provided as data files through existing methods with GaTech staff.

7.3. PED-X

The PED-X function is composed of the proxy server and the interface with the MaxTime signal system. The pedestrian signal systems will operate without change. Roles and responsibilities are listed in **Table 18.**

Table 18. PED-X Roles and Responsibilities

Roles	Organization	Responsibilities
Proxy Server operations including system security and server management	Gwinnett IT with support from GDOT	• Monitor server operations and performance. • Manage firewall and monitor security. • Communications brokerage (incoming and outgoing).
Proxy Server software maintenance and updates	GDOT with GCDOT	• Access and configure timing, internet protocols, and triggers for proxy server. • Share information with G-MAP. • Manage software and update if needed. • GDOT /GCDOT representatives to participate in Change Control process if change to software is required. • GDOT to manage and update Open Source site with updated software if changes to the software are warranted.
Signal System (MaxTime) operations and maintenance	GCDOT	• Manage and monitor MaxTime operations. • Update signal system timing as needed. • Manage construction of field signal system hardware and connectivity.

The list of PED-X sites can be found in the **Appendix, PED-X Site Locations.**

Table 19 enumerates the process for updating or adding a new intersection to enable PED-X include activities performed by GDOT programming, GCDOT and G-MAP staff.

Table 19. PED-X Proxy Server Update Process and Responsibilities

Activity	Responsibility
1. Check intersection for pathway through intersection.	G-MAP Leads / GA Tech, update if needed (see **Section 1** for process).

Activity	Responsibility
2. Check signal system at intersection for connectivity to MaxTime.	GCDOT
3. Provide access to GDOT when changes to the software or update to configuration are needed.	Gwinnett IT, requested by GCDOT.
4. Configure Proxy Server with approach and timing information.	GCDOT provides information to GDOT. GDOT configures the information into the proxy server software lookup tables.
5. Configure G-MAP triggers.	GDOT shares with G-MAP developers who configure G-MAP with new intersection. Unit testing is required to check operations. Test software is pushed to app store testing sites (e.g., TestFlight) to perform end-to-end testing with GDOT and GCDOT.
6. End to end testing with log review and in-field review. Testing includes: a. Test trigger by persona at intersection from multiple approaches (review logs). b. Test receipt of trigger by proxy server (review logs). c. Test transmission and receipt of message to pedestrian signal system (review logs). d. Test extension for “extra time” at intersections (review logs and review at intersection).	In coordination with G-MAP developers, GCDOT and GDOT developer, in-field / back office testing is conducted. G-MAP sends message to proxy server (GDOT) and proxy server sends request to MaxTime (GCDOT).

7.3.1. Proxy Server OSS

Any time the proxy server software or interfaces change, the code and coding support tools (e.g., builder) will be updated on the OSS site. The OSS software is stored in the USDOT CodeHUB. Access to the Proxy Server OSS site can be found at:

The open source proxy server code is stored in the USDOT CodeHUB at https://github.com/usdot-jpo-codehub/PedX-Proxy.

7.3.2. Other Systems Undergoing Transition

GDOT and subsequently GCDOT may transition to a new signal system sometime in the next few years. It is not anticipated for the duration of the Phase 3 project. The transition will negate the need to use the proxy server to implement the actuation request, rather the trigger used to communicate with the proxy server will be used to communicate with the new system. The current APIs (see **ICD, I-12**) includes

requests for intersection and signal timing information. These interfaces will need to be tested through a testbed and in-field testing. As of the publication of this document, the estimated timing of this change is not yet known.

7.4. Public PMD

The public PMD is a configuration of the COTS Microsoft Power BI, Version: 2.138.1203.0 64-bit (November 2024) platform used to display and provide access to performance data.

The public PMD processes include the following:

- **Data Ingestion and Curation Processes**. Function to ingest data input from the private PMD. These include the anonymized metrics and metadata information which are securely held and made available from a private PMD S3 Bucket.
- **Visualization and Publication Processes.** Processes to visualize the metrics, generate reports and publish these artifacts to the public PMD website.
- **Data Access.** Processes deployed to allow the public to interact with or download the performance measurement data and reports.

These processes are supported by the Power BI administration console that provides the following services. Documentation and user support is provided by Microsoft online in a searchable format or in guided user training, Power BI get started documentation - Power BI | Microsoft Learn.

- Import data from private PMD S3 Bucket
- Configure quality control procedures
- Define and associate data fields to generate charts for data visualization
- Define and associate data fields to generate reports
- Save and publish charts or reports to web

The Power BI administration console provides the designer with customizable templates and configurable options to create visualizations and reports, dashboards, and apps. The Power BI basic concepts are described here: The Power BI service - basic concepts for beginners - Power BI | Microsoft Learn.

7.4.1. Roles and Responsibilities

The public PMD site will continue to operate without change during Phase 3 and will be migrated to ARC's Power BI platform in preparation for post-Phase 3 operations. The public PMD Roles and responsibilities are listed in **Table 20.**

Table 20. Public PMD Roles and Responsibilities

Roles	Organization	Responsibilities
Power BI service software maintenance and updates	ARC and ICF	• Maintain service subscription and access. • Monitor server operations and performance. • Communications brokerage (incoming and outgoing). • Update software as needed.
Operate Public PMD	ARC, ICF, and GA Tech	• Maintain connectivity to private PMD S3 Bucket. • Import data from private PMD S3 Bucket. • Coordinate any changes with STM system.
Implement quality control procedures and review data	ARC, ICF, and GA Tech	• ARC, ICF, GA Tech representatives to participate in Change Control process if change to software or private PMD data is required. • Monitor site and download historical data to review trends for quality assessment. • Review site each quarter after quarterly survey data is ingested and displayed.
Migrate Public PMD	ARC and ICF	• Set-up Power BI host site. • Gain access to private PMD S3 Bucket. • Migrate public PMD site to ARC. • Deactivate ICF public PMD site.
System security and server management	ARC and ICF	• Maintain Power BI security provisions. • Conduct annual employee training and follow agency best practices for privacy and cyber security. • Monitor audit logging and incident response logs to ensure site access as expected.

7.4.2. Public PMD Security and Privacy

Power BI offers a secure platform to design and display data with the following security provisions. These features are included in the Public PMD deployment.

- **Authentication and Authorization**. Open Authorization (OAuth) is used to authorize the user.

- **Data Encryption**. Hypertext Transfer Protocol Secure (HTTPS) for data in transit is used and ensures that any sensitive data is encrypted at rest.
- **Access Controls**. Role-based access controls (RBAC) are used to limit who can see and do what within the system.
- **Audit Logging**. Detailed logs of who accesses the public PMD and what actions they perform are kept.
- **Monitoring and Incident Response**. The site is continuously monitored for unusual access patterns or data breaches and an incident response plan is in place.
- **API Security**. For any API endpoints, rate limiting is used and considered when implementing an API gateway to manage and secure API traffic.
- **Data Integrity Checks**. Checksums or other data integrity checks are used to ensure that the data has not been tampered with during transfer.

The Private PMD ensures that all PII is removed or anonymized prior to being made available to the Public PMD as is described in **Section 5.2**.

7.4.3. Public PMD Operations and Maintenance Contract

The Public PMD site will be operated and maintained by ICF through existing Phase 3 contracts. It is anticipated that additional data or data presentation format may need to be modified during Phase 3 which will be coordinated by the project team and led by GA Tech. In addition, this contract includes efforts to migrate the site to ARC's Power BI platform in preparation for the five-year, post-deployment operations and maintenance phase which will be hosted, operated, and maintained by ARC.

7.5. Ride Request

The ride request module is supported under an existing contract between Ride Gwinnett and their Computer-Aided Dispatch / Automated Vehicle Location (CAD/AVL) vendor. The contract includes operations and maintenance of the services related to the ride request functionality. Existing software transmits the ride request message to the driver's terminal on-board the bus. Roles and responsibilities for Ride Request are listed in **Table 21.**

Table 21. Ride Request Roles and Responsibilities

Roles	Organization	Responsibilities
Ride Request process operations	Ride Gwinnett contractor	• Broker Ride Request message from G-MAP. • Operate message broker services and transmission of messages to driver terminal. • Secure interface from G-MAP. • Operate current CAD/AVL as designed: ○ Operational and maintenance terms and conditions are subject to the Ride Gwinnett contract.
Maintain Ride Request API and update software	Ride Gwinnett contractor with G-MAP developers	• Update API if changes are needed (none anticipated): ○ Updates will be subject to Ride Gwinnett discretion. • In cooperation with G-MAP design, code and test updated interface. • An update will require participation in the Change Control Process and publication in the Software Bulletin.
Maintain GTFS and GTFS-RT	Ride Gwinnett contractor	• Maintain the GTFS and GTFS-RT data feeds in order to generate accurate Ride Request API (and to support the Enhanced TSP functionality which depends on the Ride Request API).

7.6. INS

The INS is composed of two components, the back office which is subject to the annual license agreement with CXApp and the beacons installed at two Gwinnett facilities. **Table 22** lists the roles and responsibilities for the two components.

Table 22. Indoor Navigation System Roles and Responsibilities

Roles	Organization	Responsibilities
CXApp SDK	CXApp	• Update platform SDKs when operating systems are updated (e.g., Android, iOS and browser/web). • Work with GDOT team when issue arises with software.
Beacon Inventory	CXApp	• Manage beacon inventory throughout the duration of the license agreement. • Support changes to beacon placement.

Roles	Organization	Responsibilities
Beacon operations and maintenance	GDOT Team and GC Facilities Management	• Monitor beacon operations including physical security periodically annually. • Work to relocate and configure beacons during construction. • Replace beacons with spares and replace batteries as needed. • Manages Kontact.io app login (beacon battery and power settings).
Facility pathway management	GC Facilities Management	• Manage changes to facility (including construction, elevator / escalator operations, destinations, obstacles, etc.) to manage change in the Map Manager and Editor.

7.6.1. Beacon Operations and Maintenance and Facility Pathway Management

Periodically, Project staff will verify the configuration and operations of beacons at both Gwinnett facilities. Project staff will inform a designated person at the GC facility of the beacon audit. This activity will occur no more than twice annually. The audit will consist of:

- Locating the beacon on the INS facility map to verify its location.
- Monitoring the beacon signal configuration to ensure that device is operating, and if:
    - Not operating, troubleshoot the device to determine if the battery is still operating.
    - A replacement device is necessary, replace and test the device, record its placement, and relay the identifier to CXApp to update the inventory.
    - Note: replacement uses double-sided tape that adheres to the wall.
- Reviewing the pathways and destinations are still valid via the facility map (Map Manager).
- Documenting the audit in the software bulletin with any changes or updates to the beacons, beacon locations or facilities.

In order to maintain security and operational integrity, information regarding beacon inventory and placement will not be included in this document. Current beacon inventory and placement are included in an external file.

Map update training and procedures are located in the CXApp backoffice jibestream site. (https://support.cxapp.com/hc/en-us/articles/360033183511-Building-A-Mapping-Application-The-Complete-Guide; note access to training is granted by project team).

7.6.2. CXApp SDK and Back Office Software

Operations and maintenance including any updates or upgrades to the software are governed by the Agreement between CXApp and GDOT. Terms of the agreement are summarized as follows:

These include access to:

- SDK jibestream and ODP
- Back office jibestream with Map Manager and training materials for mapping updates
- System performance and monitoring
- Coverage of 130,000 across 2 sites.

The terms are updated annually. Next renewal is in August 2025.

8. Operations and Maintenance Risks and Contingencies

Any deployment in a live environment has operations and maintenance risks; those deployments that are integrated and have dependencies on multiple systems have increased risk. **Table 23** provides a summary of operational and maintenance risks and associated mitigation measures.

Table 23. Operational and Maintenance Risks and Mitigation

ID	Risk	Mitigation Measures
1	**Level of Service.** G-MAP, subsystem components, or integrated systems level of service is not maintained.	Operations and maintenance are included within the scope of work for Phase 3 contracts with all subsystem administrators. The operations and maintenance of integrated systems are covered by existing contracts.
2	**Degraded Functionality.** Modifications or maintenance activities degrade G-MAP functionality.	Developers will continue to perform unit and regression testing when changes are made to the code.
3	**Operating System Changes.** iOS or Android platforms implement significant changes that may impact the functionality of G-MAP.	Developers will continue to monitor iOS and Android changes in advance of the release and work to minimize any risk or impact to G-MAP functionality.
4	**Integration Dependencies with External Partner Systems.** External systems are changed or not maintained which may impact G-MAP functionality. This includes the RSUs, OBUs, TSP, GTFS data feeds, and signal control systems.	The project team has worked with the external partners to set up more efficient business processes where certain information is shared, and alerts are set up so that impacts related to external system changes can be addressed quickly. In particular, integrated systems like CV subsystems, Gwinnett DOT and Ride Gwinnett system changes, updates and degraded systems impact operations of the system. Monthly issues and change control meetings will help understand the impacts. Key contact information will also be designated as formal liaison to mitigate any issues that might arise.
5	**Staff Changes.** Staff changes risk a loss of knowledge and familiarity with the project.	The project team is preparing training materials and processes to share knowledge such that a single staff transition will not impact the operations and maintenance of G-MAP.

ID	Risk	Mitigation Measures
6	**Company Dissolution.** Significant changes to partner entities may impact continued operations and maintenance support.	The project team has taken significant measures to document system design, documentation, operations, and maintenance. Should a partner entity no longer be able to fulfill their obligations, the project team will seek to find and on-board a replacement partner who will leverage the documentation and support of teaming partners to minimize the impact. This is applies to commercial products and services such as subconsultants to GDOT and CXApp.

9. Related References

Table 24 lists the documents that were used to support and contribute to this document. References to these documents are identified with the acronym provided in brackets.

Table 24. References

ID	Referenced Documents
[ARCRTP]	Atlanta Regional Commission. “The Atlanta Region’s Plan: Regional Transportation Plan” Atlanta: Atlanta Regional Commission. (2021).
[CAP]	Georgia Department of Transportation. Deliverable Task 2D Comprehensive Acquisition Plan. (2023).
[CGCT]	Gwinnett County Department of Transportation. Connect Gwinnett Transit Plan - Existing Conditions Technical Memorandum. Duluth: Gwinnett County Government. (2017).
[CIP]	Georgia Department of Transportation. Deliverable Task 2D Comprehensive Installation Plan. (2023).
[ConOps]	Atlanta Regional Commission. Deliverable Task 2.3 Concept of Operations. Atlanta: U. S. Department of Transportation. (2021).
[CV1K]	Georgia Department of Transportation. "The Regional Connected Vehicle Program Scope of Work. " Atlanta: Georgia Department of Transportation. (2019).
[CVTMP]	AECOM. "Gwinnett County Connected Vehicle Technology Master Plan (CVTMP). " Duluth: Gwinnett County Department of Transportation. (2019).
[DMP]	Georgia Department of Transportation. Deliverable Task 2C Data Management Plan. Atlanta: U. S. Department of Transportation. (2023).
[DPP]	Georgia Department of Transportation. Deliverable Task 2C Data Privacy Plan. Atlanta: U. S. Department of Transportation. (2023).
[GBFS]	GitHub. General Bikeshare Feed Specification. Washington D. C.: GTFS. (2019).
[GCDOT]	Gwinnett County Department of Transportation. Transportation. Duluth: Gwinnett County Board of Commissioners. (2021).
[GTFS]	GTFS. General Transit Feed Specification Reference. Washington D. C.: GTFS. (2019).

ID	Referenced Documents
[GTFSP]	GTFS. General Transit Feed Specification Pathway. Washington D. C.: GTFS. (2019).
[GTFS-RT]	GTFS Realtime. GTFS Realtime Reference v2. Washington D. C.: GTFS Realtime. (2019)
[ICD]	Georgia Department of Transportation. Deliverable Task 2B Interface Control Document. (2024).
[OSM]	OpenStreetMap Foundation. Open Street Map. Washington D. C.: UCL, ByteMark. (2021).
[SAD]	Georgia Department of Transportation. Deliverable Task 2B System Architecture Document. (2024).
[SEMP]	Atlanta Regional Commission. Phase 1 Systems Engineering Management Plan (SEMP). Atlanta: U.S Department of Transportation. (2022).
[SDD]	Georgia Department of Transportation. Deliverable Task 2B System Design Document. (2024).
[SyRS]	Atlanta Regional Commission. Deliverable Task 6.1 System Requirements and Specifications Document. Atlanta: U.S Department of Transportation. (2021).

10. Acronyms and Abbreviations

Error! Reference source not found.Table 25 lists acronyms that have been used throughout the document for reference.

Table 25. Acronym List

Acronym	Definition
API	Application Programming Interface
ARC	Atlanta Regional Commission
AWS	Amazon Web Services
Avail	Avail Technologies
CAD	Computer-Aided Dispatch
CAD/AVL	Computer-Aided Dispatch / Automated Vehicle Location
CFT	Controlled Field Testing
CFT	Controlled Field Testing
CI/CD	Continuous Integration and Continuous Delivery
CMOP	Comprehensive Maintenance and Operations Plan
ConOps	Concept of Operations
COTS	Commercial off the Shelf
CV	Connected Vehicle
FHWA	Federal Highway Administration
G-MAP	Georgia Mobility and Accessibility Planner
GA Tech	Georgia Institute of Technology
GCDOT	Gwinnett County Department of Transportation
GDOT	Georgia Department of Transportation
GJAC	Gwinnett Justice and Administration Center
GOSystems	GO Systems and Solutions LLC
GTFS	General Transit Feed Specification
GTFS-RT	General Transit Feed Specification Real Time
GTRI	Georgia Tech Research Institute
iOS	iPhone Operating System
ICD	Interface Control Document
ICF	ICF International, Inc.
INS	Indoor Navigation System
IOO	Infrastructure Owner/Operator
ITS	Intelligent Transportation System
JPO	Joint Program Office

Acronym	Definition
KHA	Kimley-Horn and Associates, Inc.
KPIs	Key Performance Indicators
LEP	Limited English Proficiency
MARTA	Metropolitan Atlanta Regional Transit Authority
ML	Machine Learning
NCUs	Neptune Capacity Units
O&M	Operations and Maintenance
OBU	Onboard Unit
OSM	OpenStreetMap
OSS	Open Source Software
PED-X	Pedestrian Crossing
PII	Personally Identifiable Information
PMD	Performance Management Dashboard
PPA	Pedestrian Presence Alert
QA	Quality Assurance
RSU	Roadside Units
S3	Simple Storage Service
SAD	System Architecture Document
SDD	System Design Document
SDK	Software Development Kit
SE	System Engineering
SEMP	Systems Engineering Management Plan
SILCGA	Statewide Independent Living Council of Georgia
SOP	Standard Operating Procedures
SRB	Software Review Board
SSE-S3	Server-Side Encryption with Amazon S3-Managed Keys
ST-CTN	Safe Trips in a Connected Transportation Network
STM	Space Time Memory
STP	System Testing Plan
SW	Software
SaaS	Software as a Service
TSP	Transit Signal Priority
UI	User Interface
USDOT	U.S. Department of Transportation
UX	User Experience
VPC	Virtual Private Cloud

11. Appendix

This appendix contains RSU and PED-X site locations.

11.1. RSU Site Locations

The RSU site locations are listed in **Table 26**.

Table 26. RSU Site Locations

ID	Intersection
1	Indian Trail Lilburn Road at Georgia Belle Court
2	West Crogan Street at Langley Drive
3	SR 20 at Nash Street
4	SR 20 at Gwinnett Drive SW
5	SR 120 at Phoenix High School
6	SR 20 (Bufford Drive) at Hurricane Shoals Road NW
7	Phillip Boulevard at Hurricane Shoals Road NW
8	West Pike Street at Don's Way
9	SR 8/Lawrenceville Suwanee Road NW at Medical Center Boulevard
10	SR 8 at Old Norcross Road
11	Collins Hill Road at University Center Lane/Melody Lane
12	Collins Hill Road at Collins Industrial Way/Lendon Connector
13	Collins Hill Road at SR 316 EB Ramp
14	Collins Hill Road at Park Access Drive
15	Hurricane Shoals Road NW at Hillcrest Green Drive NW
16*	Sugarloaf Parkway at Old Norcross Road
17	Sugarloaf Parkway at Marathon Boulevard/Cruse Road NW
18	Sugarloaf Parkway at QuikTrip Driveway
19	Sugarloaf Parkway at SR 316 EB Ramp
20	Sugarloaf Parkway at SR 316 WB Ramp
21	Sugarloaf Parkway at Lakes Parkway
22	Sugarloaf Parkway at Gwinnett Technical College Driveway
23	Riverside Parkway at Lakes Parkway
24	Old Norcross Road at Brass Key Court
25	Old Norcross Road at Riverside Parkway
26	Old Norcross Road at Monfort Road/Raco Drive

ID	Intersection
27	Lawrenceville Suwanee Road NW at Greenvale Road NW
28	Lawrenceville Suwanee Road NW at central Lawrenceville Market Driveway
29	Lawrenceville Suwanee Road NW at southern Lawrenceville Market Driveway
30	SR 120 at SR 8 / Lawrenceville Suwanee Road
31	SR 120 at Parkside Walk Court

* Location is currently under construction and will be deployed during Phase 3.

11.2. PED-X Site Locations

The PED-X site locations are listed in **Table 27**.

Table 27. PED-X Site Locations

ID	Intersection
1	SR 20 at Gwinnett Drive
2*	SR 20/Perry Street at Nash Street
3	Beaver Ruin Road at Light Circle
4	East Crogan Street and east of North Clayton St
5	Old Norcross Road at Davenport Road
6	Jimmy Carter Boulevard at Hayes Drive
7	Jimmy Carter Boulevard at Dawson Blvd/Live Oak Pkwy
8	SR 141 at Forum Drive
9	Satellite Blvd at Gwinnett Plantation Way
10	Satellite Blvd at Merchants Way
11	Indian Trail Lilburn Road at Georgia Belle Court

* Location is currently under construction and will be deployed during Phase 3.

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-21-875



U.S. Department of Transportation