yoGERT GIS Toolbox

Capstone 4G06

Hazard Analysis

Team 19,
Smita Singh, Abeer Alyasiri, Niyatha Rangarajan,
Moksha Srinivasan, Nicholas Lobo, Longwei Ye

November 24, 2022

Contents

List of Tables

List of Figures

1 Revisions

Table 1: Revision History

Date	Developer(s)	Change
Date1	Name(s)	Description of changes
10/19/2022	Niyatha Rangarajan	Failure Modes and Effects Analysis
10/18/2022	Smita Singh	Safety and Security Requirements
10/13/2022	Moksha Srinivasan	Sections 3-8.1
10/18/2022	Abeer Alyasiri	Safety and Security Requirements, Roadmap
10/18/2022	Longwei Ye	Failure Modes and Effects Analysis
10/19/2022	Nicholas Lobo	Failure Modes and Effects Analysis
11/22/2022	Longwei Ye	Format changes based on feedback
11/23/2022	Longwei Ye	Update FEMA Table

2 Definitions

2.1 Naming Conventions and Terminology

symbol	description
GPS	Global Positioning Systems.
GIS	Geographical Information Systems.
MIS	Module Interface Specification.
GUI	Graphical User Interface.
CSV/.csv	Comma Separated Values is a file type that contains large amounts of data separated by commas.
SRS	System Requirement Specification.
GB	Gigabyte

3 Introduction

This document is the hazard analysis of the yoGERT GIS toolbox. The toolbox is a software that aids in deriving insights from transportation data. This includes route choice estimations, travel mode detection, and travel episode identification/analysis.

4 Scope and Purpose of Hazard Analysis

The scope of this document is to identify possible hazards within the yoGERT system, the causes and effects of failure, steps for mitigation, as well as safety and security requirements.

5 System Boundary

The system referred to in this document that the hazard analysis is conducted upon consists of:

- The toolbox (installed on users' personal computers) made up of the following major components:
  - Data Pre-processing
  - Travel Episode Identification
  - Travel Mode Detection
  - Activity Location Identification
  - Route Choice Analysis
  - Visualization Module
- The user's personal computer

6 Definition of the Hazard

The definition of a hazard is from Nancy Leveson's work as follows: A property or condition in the system along with a condition in the environment that has the potential to cause harm or damage. In yoGERT, there are hazards with regard to safety (to data preservation) and security (restricted data access). Besides, hazards can be also found due to human-errors(wrong actions to the system).

7 Critical Assumptions

One critical assumption is regarding the system boundary. For example, if the stretch goal of adding a GUI and GIS software plug-in is completed, the hazard analysis will have to be extended. Another critical assumption is that the user knows how to upload a file using a file path.

8 Failure Modes and Effects Analysis

8.1 Hazards Out of Scope

The hazards out of scope would be:

- The user's personal computer
- The validity of input data

The user's personal computer and validity of input data are integral parts of our system's correctness. It is out of scope to develop a mechanism to verify that data is correct/applicable, and hence hazards with respect to correctness and validity of data are out of scope. To ensure that we can process the user's data we will be sanitizing and normalizing data before applying functions. The user's personal computer is managed by the user and software updates are applied by the manufacturer, hence we cannot control all hazards.

8.2 Failure Modes Effects Analysis Table

8.2.1

System: GERT toolbox
Subsystem:N/A
Phase/Mode:System Requirements

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref.
Storage of users geo-location data	User's location data is corrupted	Unable to use program without clearing out corrupted data	a. Bad data inputted by user b. Corrupted files being load into system	a. Data is checked and sanitized before being added into system	a:SR6	H1-1
	User's location data is not saved	User must input data again	a. Disconnection from internet b. Computer crash while using software	b. Last actions made by user in the software are saved	a:SR4 b:SR8	H1-2
Memory usage of the system	Unprocessed csv file for gps input is too large	Unable to process the gps data for other functions	a. Incomplete system functionality b. File if produced might be inaccurate or skewed c. Uncertainity in output	a. State file size restrictions for the system	a. SR7	H2-1
	Processed gps data is too large to be stored in the output directory	Unable to use the system for creating episodes, routes and activities	a. Useful data manipulation can be attained b. The system is incomplete in functionality c. Benefits of analysing episodes is prevented	b. Produced file can be compressed to meet storage requirements	b. SR7	H2-2
General use of the system	Program crashes unexpectedly	Program is terminated, unable to continue current progress, data of the current progress could be lost	a. Crash due to lack of supported libraries b. User device runs out of power	a. Check if the supported libraries are installed at the start of the program b. Charge the device so that the system can work again	SR2	H3-1
	Output does not meet the desired accuracy	Unusable output, unable to proceed to the next step	a. Input data is in wrong format b. Input file is corrupted	b. Same as H1-2 c. Validating against requirements and mathematical specifications	SR5 SR3 SR9	H3-2
	~~An unauthorized action~~ Actual output does not meet the user's expectation at all	Data can be corrupted and the produce wrong output	a. An unauthorized or an unexpected~~Unexpected~~ action made by the user	d. Revert the changes made by the unauthorized action	SR1, SR9	H3-3

Table 2: FMEA TABLE

9 Safety and Security Requirements

The section lists the newly formulated requirements. The new requirements will be added to the SRS document and the previous requirements will be removed before Revision 1 milestone.

9.1 Access Requirements

SR1: The system must allow users to have access to the data they've uploaded

- **Rationale:** This would allow users to edit inputted data and make any necessary changes. If a problem occurs, the user should be able to retrieve their data instead of having to restart the process or software which would be time consuming
- **Associated Hazards:** H3-3 (8.2.1)

SR2: The system shall allow access to all system services and data outputs.

- **Rationale:** This is the main objective to the application to satisfy user goals. If a problem occurs, the system will be completely ineffective and not workable.
- **Associated Hazards:** H3-1 (8.2.1)

9.2 Integrity Requirements

SR3: The system shall output correct calculated or modified data

- **Rationale:** The user should not have to question the accuracy of the data outputted. If the data is not accurate or correctly calculated it is contrary to the goal of the system.
- **Associated Hazards:** H3-3 (8.2.1)

SR4: The system will only modify necessary data

- **Rationale:** The system would be wasting resources and time if any other modification or unnecessary calculations occur. It would also be unethical to use the data in a way that the user is unaware of and has not consented to.
- **Associated Hazards:** H3-3 (8.2.1)

SR5: The system shall produce accuracy of 80% when graphing location data points on a map.

- **Rationale:** The graphics produced to the system should be consistent to produce valuable information to be reused. When the graphic points deviate from the actual location the system will be counterproductive and user will be alarmed.
- **Associated Hazards:** H3-2 (8.2.1)

SR6: The system shall provide warning log messages of proper or expected system uses.

- **Rationale:** The system should provide helpful information when navigating around the system. This ensures a mitigation response to unexpected user activity.
- **Associated Hazards:** H1-2 (8.2.1)

SR7: The system shall confirm upload and output files are not larger than 1GB.

- **Rationale:** The system needs to provide secure methods of handling system files. This ensures safe saving and uploading of files.
- **Associated Hazards:** H2-1, H2-2 (8.2.1)

9.3 Privacy Requirements

SR8: The system will only store data locally.

- **Rationale:** The data does not have to be hosted on a remote location such as online database; which would mean better security and protection for the user's data. Failure to store makes the system unresponsive and idle.
- **Associated Hazards:** H3-4 (8.2.1)

9.4 Audit Requirements

SR9: The system should be verifiable against the requirements and MIS

- **Rationale:** The system must be verified with logical and deductible methods. Failure to meet the requirement results with poor demonstration of requirements.
- **Associated Hazards:** H3-1, H3-2, H3-3 (8.2.1)

9.5 Immunity Requirements

N/A

10 Roadmap

The document outlined new safety and security requirements to mitigate and avoid system hazards. The project aims to implement all the safety requirements. However, a priority guideline has been decided that leaves SR4, SR5, and SR6 requirements to be more likely than 50% implemented in the future due to constrained capstone timeline.

References

[1] N. G. Leveson, Safeware: System Safety and Computers. Addison Wesley, 1995.