yoGERT GIS Library

Capstone 4G06

Hazard Analysis

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

April 5, 2023

Contents

List of Tables

List of Figures

1 Revisions

Table 1: Revision History

Date	**Developer(s)**	**Change**
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
03/04/2023	Moksha Srinivasan	Final Documentation Runthrough

2 Definitions

2.1 Naming Conventions and Terminology

Term	description
CSV/.csv	Comma Separated Value is a file type that contains large amounts of data separated by commas. All user inputs and outputs of the yoGERT toolbox, other than the Mapping output will be in this file format.
GB	Gigabyte, a unit of information commonly used within this document.
GIS	Geographical Information Systems.
Github	Is a version control software that will be used to distribute the stable version of the yoGERT library to future users.
GUI	Graphical User Interface.
GPS	Global Positioning Systems.
MIS	Module Interface Specification.
SRS	System Requirement Specification.

3 Introduction

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

4 Background

yoGERT is a python library that will be used by geo-researchers to derive meaningful insights from GPS data. The library will be cloned from github and then installed locally using pip. Users will call various library functions and use their CSV GPS data as input. The functions in turn will output files within the user's local file system, where they can be further analyzed or perused by the user.

5 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.

6 System Boundary

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

- The library (installed on users' personal computers) consisting of the following major modules:
  - Pre-processing
  - Episode Generation
  - Fetch Activity Locations
  - Shortest Route
  - Alternative Route
  - Mapping
- The user's personal computer

7 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 [1]. In yoGERT, there are hazards with regard to safety (to data preservation) and security (restricted data access). Additionally, hazards can be also found due to human-errors (incorrect user actions that interrupt the system).

8 Critical Assumptions

Some critical assumptions we make in this document are that:

1. The user knows how to upload a file using a file path.
2. The user has python installed on their local machine.

9 Failure Modes and Effects Analysis

9.1 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.

9.2 Failure Modes Effects Analysis Table

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

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref.
Store user GPS data.~~Storage of users geo-location.~~	User's location data is corrupted	Unable to process data	a. Invalid data inputted by user b. Corrupted files being load into system	a. Data is checked and sanitized before being added into system	SR6	H1-1
	User's location data is not saved	User must input data again	a. Disconnection from internet b. Computer crashes while calling a function	a. Prompt user to retry after internet connection is reliable b. Last actions made by user in the software are saved.	SR4 SR8	H1-2
Process large GPS Datasets~~Memory usage of the system~~	Unprocessed csv file not correctly processed	Unable to process the gps data for future functions	a. Incomplete system functionality b. System has too little memory to store file c. Truncated Output	a. State file size restrictions for the system, if followed suggest creating a Github bug b. Prompt user to clean up system files to create space for file c. Do not create output and provide error message to user	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. System has too little memory to store file	a. Prompt user to clean up system files to create space for file	SR7	H2-2
Correctly output results~~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. Prompt user to reinstall using "pip install ." b. Prompt user to charge their 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	a. State accepted input data formats for the system. b. Prompt user to reinput valid data	SR5 SR3 SR10	H3-2
	~~An unauthorized action~~ Actual output fails to meet the user's expectation	Data can be corrupted and the produce wrong output	a. An unauthorized or an unexpected~~Unexpected~~ action made by the user	a. Revert the changes made by the unauthorized action	SR1, SR10	H3-2

Table 2: FMEA TABLE

10 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.

10.1 Access Requirements

SR1: The system must allow users to have access to read and modify 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 (9.2)

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 (9.2)

10.2 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 (9.2)

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 (9.2)

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 (9.2)

SR6: The system shall provide warning log messages of ~~proper or expected~~ improper or unexpected 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 (9.2)

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 (9.2)

10.3 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 (9.2)

10.4 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 (9.2)

SR10: The system should pass audit requirements for producing correct and reliable data.

- **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 (9.2)

10.5 Immunity Requirements

N/A

11 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.