Hazard Analysis
Digital Twin Forest

Team 8, Forest Mirror
Yichen Jiang, jiany34
Bowen Zhang, zhangb82
Junhong Chen, chenj297
Jiacheng Wu, wuj187
Tingyu Shi, shit19

Table 1: Revision History

Date	**Developer(s)**	**Change**
October 18	All team members	Initial documents

Contents

List of Tables

List of Figures

1 Introduction

This document is the hazard analysis of the project Digital Twin Forest. Digital twin forest is a virtual representation of the natural world, specifically a real forest. The detailed introduction of our project can be found here.

2 Scope and Purpose of Hazard Analysis

The scope of this document is to analyze and identify the hazards may occur in our system in order to minimize the cost and harm of them when they occur.

Safety is always the top requirement of ours. Though we are developing a software which may not lead to any physical harms to our users, we would make an effort to examine and then avoid any other kind of possible harms. We care about not only our users but also our development and maintenance team, which will provide long-term support for our users.

The purpose of our product is to display visualized forest information to users. As a result, users would be able to better make their strategies based on the information we provided in the product, which means, inaccurate data might mislead the users when making decisions. Thus, different with many other products, the information accuracy is another one of our top concerns. Regarding to the purpose of the product and the requirements of information accuracy, we will also include the analysis of possible source of data inaccuracy in this document.

With the hazard analysis recorded in this document, we expect our product to avoid mentioned possible hazards and provide a safer using experience for our users. 100% safety is not achievable in a project. However, we believe that it is still essential to avoid predictable unsafe situations and try our best to prepare for unpredictable ones. In this document of hazard analysis, it identifies unsafe behaviours while accomplishing the application, and it makes sure such behaviours are eliminated. We would raise several recommended actions for each hazard we mentioned, which provides possible solutions to avoid hazards.

3 System Boundaries and Components

3.1 System Boundaries

Our system includes the following contents:

- Entire application
- Computers or laptops that execute our application
- Mobile devices like iPad that execute our application
- backup data files

3.2 System Components

The application will be divided into the following 5 components, in order of importance:

1. Data collection and analysis
2. Model construction
3. Data presentation
4. Data storage
5. Future update and maintenance

The following is the justification of our components division:
As the functions and the whole system of our product are integrated, dividing components according to the different features or subsystems seems unreasonable in this case. In contrast, we divide the components regarding to the development phases, which cover data collection and analysis, model construction, code implementation(including data presentation and storage), future update and maintenance. In each phase, there are several possible hazards which might lead to safety and security concerns or data inaccuracy.

4 Critical Assumptions

We assume the data stored in data store classes should always match the data collected.

5 Failure Mode and Effect Analysis

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Data Collection and Analysis	Scanning device cannot support the data collection	a. Data collection process is more time-consuming than expected b. Inaccuracy in data collection	The scanning devices (iPad or iPhone) are limited by electricity and memory space	a. Provide power banks for the data collection team b. Store the data collected in other devices during the collection process and release the memory	SR2.6	H 1-1
	Misinterpretation for tree types	a. Errors in final product in models and data representation b. Misrepresent the absolute and relative amount of each type of tree	Lack of domain knowledge about trees	a. Gain the basic information of the target forest before the data collection process b. Learn relative knowledge before the data collection process.	SR2.6	H 1-2
	The statistics obtained in the data collection process lack accuracy	Inaccurate data can mislead the user when they do research or make decisions	a. Errors in the scanning and modeling b. The workload of measuring every tree is huge c. The sample size is not large enough to estimate reliable forest parameters	a. Use scanning devices with higher resolution b. Improving statistical analyzing methods the team uses to get more accurate statistics c. User larger sample size	SR2.6	H 1-3
	Trees with small diameters have low-quality scanned models	Losing data about certain types of trees	LiDAR sensors from iPhone or iPad are not capable of scanning thin trees	a. Using scanning devices with higher resolution	SR2.6	H 1-4
	Ground area is not calculated properly from the scanning	Tree density cannot be calculated properly	Scanned forest models have irregular ground shapes. It is difficult to estimate irregular shapes' areas	a. Put irregular scanned grounds into rectangles, then use the area of rectangles to calculate tree density.	SR2.6	H 1-5

Figure 1: FMEA for Data Collection and Analysis

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Modeling	The terrain of the virtual forest is different from the actual one	The virtual forest cannot provide accurate models to users. This may cause forest owners to make the wrong decisions or meteorologists to do wrong analysis about the forest	a. Lack of information about the actual terrain of the forest b. The change of terrain after scanning due to natural and human factors	a. Use more advanced devices with wider scanning range and higher resolution to scan the actual forest	SR2.4	H 2-1
	The virtual forest may have different tree representations from actual trees.	The virtual forest cannot provide accurate models to users. This may cause forest owners to make wrong decisions or meteorologists to do wrong analysis about the forest	The scanning devices are not set to or do not have high-resolution	Refer to H 2-1	SR2.4	H 2-2
	Scanned models do not support post-processing well	a. The process of loading models is slow b. The crash happens when Unity is running	More computation resources are needed to support the post-process model elements, such as rendering the colors of trees according to different seasons and adding fog and light.	a. Use machines with higher computation power b. Lower model resolutions c. Give users options to disable post-processing	SR2.2	H 2-3

Figure 2: FMEA for Modeling

Component	Failure Modes	Effects of failures	Causes of failures	Recommended Action	SR	Ref.
Data presentation	The system does not include GUI for some data	Hard for users to make decisions based on the limited amount of data presented	a. Poorly designed GUI may not utilize screen space efficiently and some data can not be presented	a. Design better GUI and utilize screen size more efficiently b. Implement data presentation as a hierarchy so that the system can use more pages to illustrate the data	SR2.5	H 3-1
	GUI implemented, but the corresponding data are missing	Application will crash since Unity GUI can not find the corresponding data	a. Missing data from data collection process b. Data Store classes unintentionally deleted	a. Backup data storage b. Implement code to check the existence of data before presenting them.	SR2.5	H 3-2

Figure 3: FMEA for Data Presentation

Component	Failure Modes	Effects of failures	Causes of failures	Recommended Action	SR	Ref.
Data Storage	Data Store classes unintentionally deleted	a. Data analysis fail b. GUI cannot present data	Data storage failure	a. Backup data storage b. Users cannot delete the data	SR1.2 SR2.5	H 4-1

Figure 4: FMEA for Data Storage

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref.
Update	Inappropriate User Inputs	a. Possible application crash caused by wrong user inputs b. Application may not crash, but irrational phenomenons may happen in the virtual forest	a. Users may input data with the wrong data type b. Users may make irrational modifications such as logging 110 trees when there are only 100 trees	a. Implement code that can check user inputs and then accept user inputs	SR 1.2 SR 2.3	H 5-1
	Original data is not fully overwritten by new data because the update process is interrupted.	a. Users can not update data successfully b. Data integrity may be damaged c. Data may be lost	a. Computers are out of battery when updating b. Application crashes during the updating	a. Remind users to connect to power before updating data from data files	SR2.2 SR2.6	H 5-2

Figure 5: FMEA for Data Update

6 Safety and Security Requirements

New added requirements are shown in blue and will be updated into SRS document.

6.1 Access Requirements

SR1.1 The product shall only be accessed by users who download the product from our website.

SR1.2 Tree and forest data shall only be modified through the interface provided by developers.

6.2 Integrity Requirements

SR2.1 The system shall not propagate errors throughout the users' devices in case of failure.

SR2.2 The product shall avoid crash when being used.

SR2.3 The product shall check if user updates(user inputs) are legal before updating them to the system.

SR2.4 Data displayed in the application shall be consistent with the data stored.

SR2.5 The system shall provide one-to-one mapping relationships between each data and GUI.

SR2.6 The data integrity of the system shall be maintained.

6.3 Privacy Requirements

SR3.1 The product shall not ask the users to provide personal information.

SR3.2 The product shall not send notifications to the users without permissions.

6.4 Audit Requirements

N/A

6.5 Immunity Requirements

N/A

7 Roadmap

7.1 Data collection and analysis

Unsafe behaviours related to data collection and analysis are identified and eliminated before the hazard analysis revision 0 on October 19. This component has the greatest importance in the failure mode and effect analysis. The team accomplished most of the data measurement during the reading week with Dr. Gonsamo's guidance.

7.2 Model construction

Unsafe behaviours related to modeling will be identified and solved before the proof of concept demonstration on November 14. The model is the basic visual representation of the real forest. Failures may occur while the team using the technique of parametric modeling in Unity. It is necessary to eliminate or mitigate all of them during the early phase of the project.

7.3 Code implementation

Unsafe behaviours related to coding will be identified and solved before the proof of concept demonstration on November 14. The team may encounter challenges and unpredictable failures while implementing the project. Actions shall be taken to ensure the outcome of the demo is satisfying.

7.4 Future update and maintenance

The solution of unsafe behaviours related to future updates and maintenance will be postponed to the end of the project. According to the failure mode and effect analysis, this component is the least important. Therefore, the team shall focus on the implementation of the project first, and defer the mitigation of unsafe maintenance behaviours.