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
April 2	All team members	Final Draft

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 that 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 software that may not lead to any physical harm to our users, we would make an effort to examine and then avoid any other kind of possible harm. 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, 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 the possible sources 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 user 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 behaviors while accomplishing the application, and it makes sure such behaviors 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
- JSON files to store the data

3.2 System Components

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

1. Forest Model Construction
2. Data Visualization
3. Data Storage
4. Data Update from users

4 Critical Assumptions

We assume that Unity game engine will always work properly.

5 Failure Mode and Effect Analysis

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Forest Model Construction	System lag or crash when loading tree models	Users cannot use the system anymore	• Excessive accuracy of the model • Loading too many models at the same time	• Reduce the accuracy of the model as a trade-off • Use parametric modeling to solve the problem of loading too many models at the same time	SR 2.2	H 1-1

Table 2: FMEA Forest Model Construction

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Forest Data Visualization	The user interface is missing for some of the forest data	Users will not be able to collect or analyze the data if the interface is not presented.	The space is not large enough for the interface or the Unity UI the system does not work properly.	Check if the Unity UI panel and buttons are finished. Make sure the space is big enough to present all data.	SR2.4, SR2.5	H2-1
	UI was implemented, but the corresponding forest data are inaccurate or missing.	The system may crash due to calculations using non-exist or wrong data.	The lab and the team do not have or upload the latest forest data.	Download the latest forest data from ArcGIS and update the data. Add scripts for fault tolerance when the data is missing.	SR2.2, SR2.5	H2-2

Table 3: FMEA Forest Data Visualization

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Data Storage	Data Storage classes were unintentionally deleted.	• Data analysis fails • User interfaces fail to represent data	Missing data storage	Users can download the backup data storage from GitHub of our project.(As we cannot prevent the users from deleting the data.)	SR1.1 SR1.2 SR2.2 SR2.3	H 3-1

Table 4: FMEA Data Storage

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Data update from users	Inappropriate user inputs	• Possible application crash caused by invalid data input. • Invalid data input may disable some of the features like pie charts, due to the failure of necessary calculations	Invalid input with wrong data type	Implement a feature to check the data type of the input before forwarding it to the storage.	SR2.2 SR2.3	H 4-1

Table 5: FMEA 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 GitHub website.

SR1.2 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 crashing 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.

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 permission.

6.4 Audit Requirements

N/A

6.5 Immunity Requirements

N/A

The corresponding fit criteria can be found in the SRS document

7 Roadmap

7.1 Data storage

Unsafe behaviours related to data storage are identified and eliminated before 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 measurement during the reading week with Dr. Gonsamo's guidance.

7.2 Forest 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 Data visualization

Unsafe behaviours related to data visualization will be identified and solved before the POC demonstration on November 14. The team may encounter challenges and unpredictable failures while implementing the user interface of the project. Actions shall be taken to ensure the user experience of the demo is satisfying.

7.4 Data update

The solution to unsafe behaviours related to data updates will be postponed until 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.