Hazard Analysis
Software Eng

Team #11, Mac-AR
Student 1 Matthew Collard
Student 2 Sam Gorman
Student 3 Ethan Kannampuzha
Student 4 Kieran Gara

Table 1: Revision History

Date	**Developer(s)**	**Change**
2023/10/16	All	Initial Revision
2023/10/17	Matthew	Filled in multiple failure modes in the FMEA table
2023/10/17	Ethan	Worked on all sections of document
2023/11/03	Ethan	Removed SAR and added HS requirement
2024/01/04	Ethan	Updated FMEA for server crash
...	...	...

Contents

1 Introduction

In order to make an application that is usable and safe for users, common hazards need to be thought about beforehand and ways for mitigating them need to be developed. A hazard is anything that fails or modifies the intended functionalities of the Mac AR application, as well as anything that could pose a danger to the user or cause system failure.

2 Scope and Purpose of Hazard Analysis

The purpose of the hazard analysis is to document potential hazards that may arise when the application is being used and find ways to prevent or mitigate them. The scope of the hazard analysis will involve outlining the system boundaries and components, and potential hazards related to the system itself as well as user interaction with the system. Additionally, it will include the mitigation methods that will be implemented to prevent these potential hazards along with the safety and security requirements that relate to each hazard. Accounting for every single combination of user hardware should not be possible, so the analysis will be generalized for all mobile devices that are able to properly run our intended product.

3 System Boundaries and Components

The system will be divided into the following components:

- The frontend and backend parts of the system:
  - Backend server
  - User interface
- Physical Device:
  - Smartphone

The backend server will be responsible for connecting users together in a room, and associating puzzles with the users. Additionally, the server will store the current game state of the user's puzzle. The user interface is responsible for providing the user with an interact-able game, and handling all the user's inputs. The physical device that the user will run the application on is a Smartphone.

4 Critical Assumptions

- Users will not intentionally try to injure themselves or others while using the application
- Users will respect warning messages related to proper use of the application

5 Failure Mode and Effect Analysis

The Failure Mode and Effect Analysis table breaks down the potential hazards/failures of the application, along with their effects and the causes leading to the failure. Additionally, each hazard has a recommended action that describes how the hazard will be mitigated, along with the specific safety and security requirements it relates to. The specific hazards also have a severity associated with them (low, medium, or high).

Design Functions	**Failure Modes**	**Effects of Failure**	**Causes of Failure**	**Recommended Action**	**SR**	**Ref**	**Severity**
Internet connectivity	Loss of internet connection	The user is unable to send or receive data from the server	The user's device has lost connection to the internet	Notify the user that they have lost internet connection.	UH2	H1-1	Medium
				Prompt the user to play the game in an area with good internet connection, and if they get disconnected, prompt the user to reconnect before play can resume.	UH4		
	Unstable Internet Connection	The user is not able to keep up-to date with the server and the other users	The user's internet connection is poor/weak	Prompt the user when poor connection is detected to connect to a more stable internet network.	UH5	H1-2	Medium
General	System Powerdown	The user's phone has shutdown	Some failure from the user's phone/device caused the device to shutdown	The user should turn their phone back on and when they launch our app again, they should be allowed to rejoin the room and continue playing the game.	UH7	H2-1	High
	Application Crash	The application has crashed on the user's device	A bug in the code or an issue with the user's device	The user can relaunch the application and reconnect to their game room.	UH7	H2-2	High
Backend Server	Server cannot respond within a reasonable time	Possible loss of data from users, status of game rooms not clear	Too many user's sending and receiving data from the server at the same time	Limit the amount of users to ensure the server always has enough time to handle requests.	PR1	H3-1	Low
	Server Crash	Server has crashed resulting in users being unable to send and receive data from the server	A failure in the backend server causes it to become unresponsive/crash	Limit users from playing the game until server has become responsive	PR2	H3-2	High

Table 2: **FMEA Table**

Design Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref	Severity
User Interface	User Exits the game room	The user is too far from the puzzles to complete them	The user leaves the pre-defined area set by calibration	Inform the user before they leave the area to not leave, and if they leave, inform the user to return.	UH6	H4-1	Low
	User is injured	The user has sustained an injury during the use of our application	The user was not aware of their surrounding during the use of the application and injured themselves from their surroundings	Prompt the user before the game starts to be aware of their surroundings, and play in an open area with no visible hazards.	HS1	H4-2	High
			User was using application in dangerous conditions	Warn the user about potentially dangerous weather and to exit the area if outside.	UH8	H4-3	Low
	User calibration setup fails	User is unable to start puzzle due to calibration setup not being able to map real life room into AR environment	Room is too bright resulting in camera not being able to accurately map environment, User exits room during calibration setup, User attempts to play game in unsuitable environment (ex. moving car)	Prompt the user before the game starts to let them know the suitable environments for playing the game.	UH6	H4-4	Medium
				Prompt user through pop up warning during calibration to let user know that their current environment is not suitable and they must change their environment before they can resume play.	UH6	H4-5	Medium

Table 3: **FMEA Table continued...**

6 Safety and Security Requirements

The following requirements include requirements in the Software Specification Document. It also lists new requirements which will be added to the Software Specification Document and have been written in **bold**.

6.1 Security Requirements

SR1. The system shall keep user data private
Fit criterion: The system shall not make user passwords or IP addresses

able to be publicly accessed

SR2. The users will only be allowed to see limited data. Unnecessary data will not be displayed to the user
Fit criterion: The system shall only show users any data required in order to play the game

6.2 Health and Safety Requirements

HS1. The system shall give a warning to the user to be aware of their surroundings while using the system, and to not bump into any objects or obstacles in their path
Fit criterion: The system shall produce a notification at the start of the game to let users know to be careful and aware of their surroundings

6.3 Usability and Humanity Requirements

UH2 The system shall notify the user if there is no network, or they get disconnected
Fit criterion: The system should produce a notification when network connection is lost

UH4 **The system shall prompt the user to re-enter an area with internet connection when it detects there is no network**
Fit criterion: The system should produce a notification for the user telling them to move to an area that allows for internet connectivity

UH5 **The system shall prompt the user if it detects that the existing network connection is weak**
Fit criterion: The system should produce a notification when network connection is weak

UH6 **The system shall prompt the user if their current environment is unsuitable to use the application**
Fit criterion: The system will produce a pop up notification during calibration setup to let user know of issues with their environment

UH7 **The system shall allow users to reconnect to their game session if they become disconnected**
Fit criterion: The system will prompt the user to reconnect to their game session through a reconnect button, which upon pressing will reconnect to the user's previous session

UH8 **The system shall alert users of potentially dangerous conditions**
Fit criterion: The system will notify the user about incoming dangerous weather when it is detected

6.4 Performance Requirements

PR1 The system shall respond to user interaction instantaneously as perceived by the user
Fit criterion: The system shall respond within 100ms of user interaction

PR2 The system shall be available for users at any time or display the reasoning for the system outage
Fit criterion: The system will be accessible 24 hours a day unless the server is under-going maintenance or experiencing an outage. If there is maintenance or an outage an error message is displayed stating the respective issue

7 Roadmap

It is expected that all of the safety and security requirements listed above will be implemented before the Revision 0 demonstration (Feb 5 - 16). If there are any updates regarding scope, documentation will be updated to match current expectations.