Hazard Analysis
Software Engineering

Team #2, Campus Connections
Waseef Nayeem
Zihao Du
Matthew Miller
Firas Elayan
Abhiram Neelamraju
Michael Kim

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct 20th	All	Revision 0
...	...	...

Contents

1 Introduction

Based on the STPA Handbook, a system hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions will lead to a loss. Regarding CampusConnections, our AR-based social networking application, a hazard can be a condition in the game when it fails to perform the intended functions or performs unexpected behaviors when coupled with environmental conditions. This document aims to detect, analyze, assess, and eliminate or migrate potential safety and security hazards that are applicable to this application.

2 Scope and Purpose of Hazard Analysis

The scope of hazard analysis is to specify all potential system hazards that may arise when using the application and discover safety and security requirements to migrate and eliminate the effects of those hazards. However, it will not include hazards related to the hardware the application is running on. It will be the choice of the user and we cannot account for all mobile devices on the market. Hazard to the user and the society will be out of the scope as well. We will assume users intend to run the application on a normally functioning mobile device properly and efficiently. The purpose of the document is to highlight various hazards associated with the system, effects and causes of corresponding failures along with new requirements for further mitigation steps.

3 System Boundaries and Components

The system will be divided into the following components:

1. The application's in-game feature components:
    - Social Media
    - AR & Location Services
    - Event/Lecture Management
    - General application features
2. The database being used which will store all of users' data

    General app features include user login system, it will be responsible for user login and account creation, as well as notification and user accessibility management. The other three features are just responsible for corresponding in-game functionalities, more details can be found in the figure below. The database and user interaction are considered external to the system, the interaction between the system and external systems is described in the previous document.

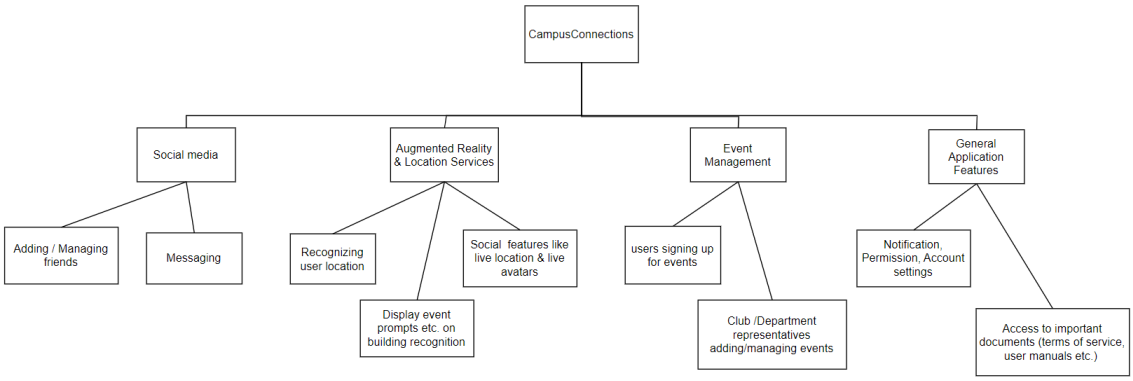

Figure 1: System Components

4 Critical Assumptions

- Assume the users of the application do not intend to misuse it
- Assume the user's device will have all necessary hardware components with sufficient computing/output power such as sensors, processors, etc.
- Assume the routes to the backend of the system will always be ready to serve requests and not blocked due to unnecessarily locked resources

5 Failure Mode and Effect Analysis

Design Function	Failure Modes	Causes of Failure	Effects of Failure	Detection	Recommended Action	SR	Ref. No.
AR Object Recognition	App is unable to detect object	Poor lighting conditions Camera angle	User is unable to view information from the AR element	Keep track of prior incomplete scan attempts	Implement a failsafe mechanism that shows the scannable information if enough previous attempts have failed	RFT2 AVR1	H1
Backend Server	Server is inaccessible	No internet connection Hosting service is down Invalid access key	Users are unable to make changes to their profile Users cannot receive updated information from the server	Keep track of the connection to the server using periodic heartbeats or similar methods	Display an error message stating that the connection the the server has been lost	RFT1	H2
User Profile View	Sensitive user data is publicly visible	Invalid visibility permissions Access control software malfunction	Confidential user information could be exposed and used for malicious purposes	Software failsafes and checks that verify the integrity of the permission structure	Prevent other users from accessing unauthorized information by creating a robust permissions system	SR	H3
App Performance	App performance is poor	Large amounts of assets to be rendered Slow internet connection App is running on an old phone	User experiences lag or slowdown App feels unresponsive	Track of frame times or other performance metrics	Only show up to a maximum number of avatars or lower the level of detail	SLR	H4

User Safety	App is used where and when it is not intended	User is distracted by the app	User could get into an accident	N/A	Display a warning message when opening the app that tells the user to be aware of their surroundings at all times while using the app	RFT2	H5
AR Module	Device is not compatible with AR features	Device is missing required hardware or software	User cannot use the AR features	Check if device supports the required feature set using API functions.	Display a warning message if the user's device is not compatible	RFT3	H6
Account Creation	Duplicate ID Creation	1. Account login failure 2. Function returns incorrect results 3. Incorrect user added as friend	1. Duplicate ID was used during account creation 2. Duplicate ID was used during account update	Compare ID with existing ID in database	Checks whether the ID is duplicate or not when entered and when saving	IR	H7

F7: Share location with friends	Location shown unintentionally	1. Location known without application being focused 2. Incorrect location display on other users	1. User did not turn off their GPS and application	Application only sends location information for too long	If user has not interacted with the application for a prolonged period, check for activity, and turn off all processes if no response is received	PR SR1	H8
Unauthorized user activity	1. Incorrect login attempts 2. Account activity in unknown devices 3. Unknown administrator activity	1. Account locked for user until further checks 2. Compromise of user and friend data	1. Predictable passwords allowed, improper password change rules 2. Security measures such as second factor authentication not used 3. Account lock features were not used	1. Accounted used from previously unknown account 2. Suspicious activity in the logs	1. Too many incorrect passwords will result in account lock. The lock can be undone from email. The account ID and password can be changed with rules preventing predictable passwords such as cannot use same password. 2. Recommend all users to use multi-factor authentication and have logs of their previous activity available to them. 3. Notify users of the security measures of the application and procedures of using them	AR	H9

Maintenance and updates of features	Update cannot be finished in time or major error is found	1. Users could experience unexpected down times 2. Features could be delayed	1. Update was not properly tested	Maintenance expected time exceeds allocated time	Rollback to previous update and do the update sequencially in smaller patches at low usage times	MR	H10

6 Safety and Security Requirements

The following requirements includes previous non-functional requirements in the Software Requirements Specification document that are referred in the previous section and new requirements added to handle potential hazards.

6.1 Access Requirements

There will be three levels of access.

The first will be before login and account creation, where anyone can access. They must not have access to anything beyond the login, account creation, and account recovery pages.

The second will be after login that verifies their identity, where the user has provided information matching the McMaster student or faculty member with McMaster email account. Only the user can access this page.

The third level will the the administrator account, used for adding, deleting, or editing official events. This account can be accessed by login that verifies that they are the maintainer, this will be used by the maintainers to check the functionality of the product and pull logs that are not accessible to users.

6.2 Integrity Requirements

The product will prevent introduction of duplicate data, to guarantee that all user identities are unique.

In the future, the database and server can protect itself from excessive use with a load balancer and additional servers being added.

6.3 Privacy Requirements

All data collected must be encrypted on disk in the server by standard encryption algorithm. All data collected must be encrypted on transit by industry standard encryption algorithm.

The product will require users to agree on the terms prior to account creation and additional data submission. The product must erase all data if the user requests, or when account is deleted. Additionally, accounts that are inactive for a certain period of time will have their account deleted after notice to prevent unnecessary data being held.

6.4 Audit Requirements

N/A (This currently does not apply, once the product is ready to be used in multiple universities and regions, audit requirements will be reconsidered.)

6.5 Immunity Requirements

The product must only use open source libraries with many users and continuous security updates. As open source libraries are used by millions of people, vulnerabilities are found and patched much earlier.

The product must undergo vulnerability checks before a build is pushed to the users. This will prevent vulnerabilities from inadequate codes from being introduced to user devices.

Security updates must be done as soon as possible when they are announced for used packages. This will reduce the chances of novel attacks from affecting the product.

6.6 New Requirements

PR1. **The product shall not transmit information while not in use.**

- **Rationale:** This requirement prevents the application from unnecessarily communicating with the server and taking up resources. This will improve the privacy and data protection of the application. This also reduces the battery usage of the product.
- **Fit Criterion:** The product will not execute any code that involves the transmission of information outside of the product.

AVR1. **There must be a failsafe for the product to function if main method takes too long or fails.**

- **Rationale:** This will allow the product to function to some degree even during high traffic or bad internet connection situations.
- **Fit Criterion:** The product must be able to provide rudimentary navigation functionality using its offline functions.

RFT1. **The product shall display an error message when there is no internet connection.**

- **Rationale:** When there is no internet connection, the user should be made aware.
- **Fit Criterion:** An error message stating that there is no internet connection is displayed when the product fails to connect to the internet.

RFT2. **The product shall display a message upon startup warning the user to be aware of their surroundings.**

- **Rationale:** Ensures the safety of the user.
- **Fit Criterion:** A message telling the user to be aware of their surroundings is displayed upon startup.

RFT3. **The product shall display a warning message if the user's device is not compatible with the AR features.**

- **Rationale:** Tells the user that the AR features of the app cannot be used with their device.
- **Fit Criterion:** A warning message is displayed if the user's device is incompatible with AR.

7 Roadmap

Safety Requirements to be implemented for capstone:

- The product shall not transmit information while not in use.
- The product shall display an error message when there is no internet connection.
- The product shall display a message upon startup warning the user to be aware of their surroundings.
- The product shall display a warning message if the user's device is not compatible with the AR features.

Safety Requirements to be implemented after capstone:

- None