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
Nov 23rd	Zihao Du	Add the new requirement IDs in the new SRS
Jan 8th	All	Revision 1: Resolve TA feedback and update the FMEA table

Contents

1 Symbols, Abbreviations, and Acronyms

symbol	description
STPA	System-Theoretic Process Analysis
SRS	Software Requirement Specification
SQL	Structured query language
AR	Augmented Reality
UI	User Interface

2 Introduction

Based on the STPA Handbook [1], 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 Unity-based AR 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.

3 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 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.

4 System Boundaries and Components

The system will be divided into the following components:

1. The application's in-game feature components:
    - Friends Component

- Map and Location Component
- AR Camera Component
- Event/Lecture Management Component
- User Profile Management Component
- General application features

2. Firebase real-time database which will store all of user, event and lecture data

   General app features include a user login system, which will be responsible for user login and account creation, as well as notification and user accessibility management. The other features are 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.

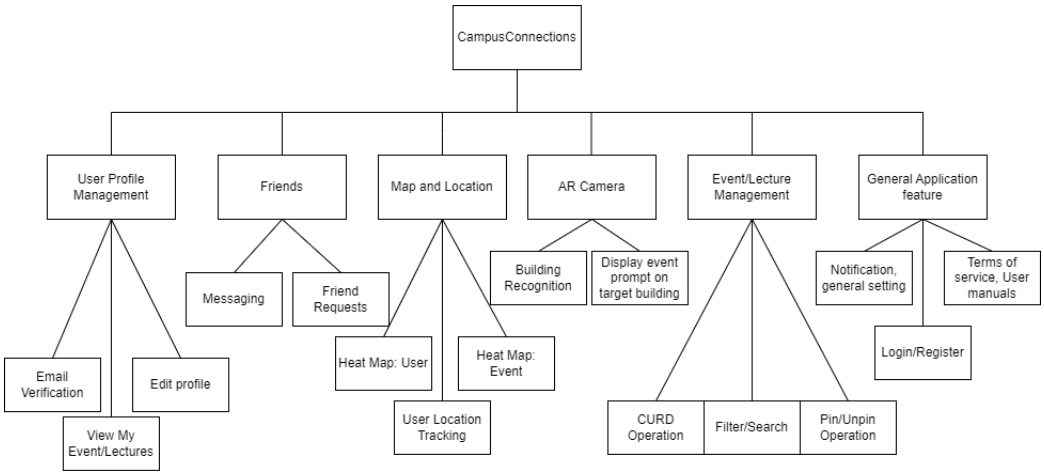

Figure 1: System Components

5 Critical Assumptions

- Assume the administrators of the application (the developers) and the provider of lecture/event information (McMaster official website) do not intend to misuse or hack into the system (e.g. SQL injection when adding new events).
- Assume the user's device will have all necessary hardware components and the device OS is compatible with the application.

- Assume data can be transmission and storage is secure under the protection of Firebase database security rules.
- Assume the routes to the backend of the system will always be ready to serve requests and not blocked due to unnecessarily locked resources
- Assume the regular maintenance of the server and database takes very short time and does not affect users from using the application

6 Failure Mode and Effect Analysis

Design Functions	**Failure Modes**	**Effects of Failure**	**Causes of Failure**	**Detection**	**Recommended Action**	**SR**	**Ref**
AR Camera	Building recognition fails	The corresponding AR objects set on the target cannot be loaded	a. Poor lighting conditions (e.g. in the evening)	a. Users cannot see any designed AR objects on the screen even if they try from different angles	a. Notify the user that they AR camera may have a poor performance in poor lighting condition or bad weather, give them developer's contact information for more questions	a. XX	H1-1
			b. Bad Weather (e.g. foggy)	b. Same as H1-1a	b. Same as H1-1a	b. XX	
Backend Server	Server crashes	All services related to server (chatting, real time location map) are down	a. Server-side Software Error	a. Users cannot chat with friends or see other users on the map and error messages are found in the server logs	a. Let server attempt to restart once it crashes due to unknown errors	a. XX	H2-1
	Server fails to respond	All related services fail to render new changes	a. Server reaches max capacity	a. Error messages complaining about server over capacity are found in the log	a. Estimate potential user number and get an appropriate plan	b. NFR-P-C1	H2-2
Internet connectivity	Internet connection is lost	The user is unable to send or receive data from the server	a. The user runs out of mobile data	a. The device shows there is no internet connection	a. Notify the user that they have lost internet connection	a. XX	H3-1
			b. The internet connection is poor/weak	b. Same as H3-1a	b. Same as H3-1a	b. XX	
Database	SQL injection attack	Personal information leakage and database information corruption	a. Inputs like user email and nick name are not validated	a. Database log shows malicious SQL statements are inserted as input	Limit the use of special characters for all vulnerable user input fields	a. XX	H4-1
			b. Users bypass checks in the application and access database directly	a. Same as H4-1a	a. Add protection rules from the database side	a. NFR-P-SC2	
Map and Location	Distracted walking when watching the screen	Users may block the traffic or even get injured because of distracted walking	The game-play of real time location map (User tends to walk and check the map simultaneously)	a. Users walk and use the application map at the same time	Show a warning message when using the map that tell the user to be aware of the surroundings	a. XX	H5-1

Table 2: **FMEA Table**

Design Functions	Failure Modes	Effects of Failure	Causes of Failure	Detection	Recommended Action	SR	Ref
Map and Location	Unintentional location sharing	The real time location of user outside campus is shared with other users using the map	a. User forgets to disconnect from real-time map session	a. User is marked outside of campus on the map	a. Check if the user location is on campus. If not, disconnect him from the map session and hide his location from other users	a. XX	H5-2
User Profile	User account is hacked	Sensitive personal information leakage	a. Week password protection rules	a. User report	a. Add password rest through email functionality b. Allow users to contact administrators to suspend target account	a. FR2-4 b. NFR-S-A1	H6-1
	Malicious user creates bot accounts	Database and authentication system have less capacity for normal users	a. Lack of human verification during account creation process	a. lots of fake accounts are created at the same time in the authentication system log	a. Add human verification in account creation process	a. FR2-5	H6-2

Table 3: **FMEA Table cont**

7 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.

7.1 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, public events, map without other users' locations and account recovery pages. We call the first level guest, user persona: a grade 12 student on a university tour.

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. We call them user. A User will have full access to all features except writing access to the database, which means a user cannot edit or create new lectures or events. User persona: a software engineer undergrad student.

The third level will the the administrator account, used for adding, deleting, or editing official events, lectures and all users. 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. Administrators are responsible to bring up-to-date information to all users and manage all users, including help users get their password back, answer user questions and suspend malicious accounts (e.g. bot accounts).

7.2 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.

7.3 Privacy Requirements

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.

7.4 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.)

7.5 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.

7.6 New Requirements

The following requirements in bold are the new requirements added to our SRS document.

NFR-P-RF4. **AR Camera should have a notification available in the UI telling users possible reasons the target is not recognized.**

- **Rationale:** The user should get a notification telling them that AR camera may have a bad performance in some cases, and they should be able to report that to the developer if they want the problem to be solved.
- **Fit Criterion:** The product should show the user a list of possible reasons that the camera does not work and the contact information of maintainers once they have trouble using the AR camera and click the help button.

NFR-P-RF2. **The server shall attempt to restart when it crashes.**

- **Rationale:** This requirement enhances robustness of the backend server and prevents it from going down for a long time because of some intermittent minor errors.
- **Fit Criterion:** The server should try to restart after it crashes due to unknown errors.

NFR-P-RF5. **There must be a fail-safe for the product to function if server or internet connection 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 functionalities without connecting to the internet or server.

NFR-P-RF3. **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.

NFR-P-SC4. **The product shall display a message upon map startup warning the user to be aware of their surroundings.**

- **Rationale:** The game-play of real-time location map may lead to distracted walking, therefore we need to warn the user for their safety.
- **Fit Criterion:** A message telling the user to be aware of their surroundings is displayed upon map startup.

NFR-P-SC5. **The product shall hide user location if the user leaves campus.**

- **Rationale:** Users may stay connected and share their location even they leave the campus. To prevent personal information leakage, we need to hide that information and disconnect the user.
- **Fit Criterion:** A user's information shall not be shared once he or she leaves campus.

NFR-P-SC6. **The product shall prevent user entering special characters in all text input field.**

- **Rationale:** When creating accounts, users can perform SQL injection attack by inputting some SQL statements.
- **Fit Criterion:** Any text input with special characters will give the user an error

NFR-P-SC7. **The product shall validate email format when creating an account.**

- **Rationale:** When creating accounts, users can perform SQL injection attack by inputting some SQL statements.
- **Fit Criterion:** An input in email field that's not in the format of an email will give the user an error when creating a new account.

8 Roadmap

The hazard analysis has identified lots of safety and security requirements, but due to time constraints, not all of the requirements can be fulfilled. Our team thinks the following requirements have higher priority and will implement them for the capstone:

- AR Camera should have a notification available in the UI telling users possible reasons the target is not recognized.
- The server shall attempt to restart when it crashes.
- There must be a fail-safe for the product to function if server or internet connection takes too long or fails.
- The product shall display a message upon map startup warning the user to be aware of their surroundings.
- The product shall hide user location if the user leaves campus.
- The product shall prevent user entering special characters in all text input field.
- The product shall validate email format when creating an account.

Requirements to be implemented after capstone:

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

References

[1] Nancy G. Leveson and John P. Thomas. *STPA Handbook*. March 2018.