Hazard Analysis
Flick Picker

Team 7, 7eam
Talha Asif - asift
Jarrod Colwell - colwellj
Madhi Nagarajan - nagarajm
Andrew Carvalino - carvalia
Ali Tabar - sahraeia

October 20, 2022

Contents

Revision History

Table 1: Revision History

Date	Developer(s)	Change
October 17	Jarrod Colwell	Created document structure
October 17	Talha Asif	Modifying Doc Structure
October 17	Talha Asif	Added introduction section content
October 17	Jarrod Colwell	Added scope and purpose section content
October 19	Andrew Carvalino	Definition of Hazard and Critical Assumptions
October 19	Talha Asif	Adding Section 8
October 19	Ali Tabar	Adding Sections 5 and 6
October 19	Madhi Nagarajan	Adding Sections 3 and 4
October 19	Jarrod Colwell	Section 1-4 editing
October 19	Jarrod Colwell	Section 5 editing

1 Introduction

Before going any further with system design, it is crucial to conduct a hazard analysis of the system from an engineering perspective. The goal is to identify critical safety concerns the users of the application could face, and the solutions to them. Hazards will be identified and eliminated or mitigated using the Failure Modes and Effects Analysis (FMEA).

2 Scope and Purpose

This document covers the various areas in which the system is most vulnerable, including but not limited to:

- External Resource Integration Points
- Server Communication
- TODO: Add more here or delete

Along with identifying the vulnerable areas of the system, this document also covers the strategies, both elimination and mitigation, and new security requirements to reduce or eliminate the impact that these hazards have.

3 Background

Flick Picker is a web application that finds the most compatible movie, TV show, or Anime for an individual user or a group of users. Users will have the ability to set their preferences related to TV Shows, Movies, or Anime. Based on these preferences, the system will produce personalized recommendations for the individual user or the group.

4 System Boundary

The list below identifies the various components of the system:

1. Web Application
    (a) Authentication: Verifies and logs the user into the system.

(b) Profile Management: Stores and manages the user's profile, including their username, preferences, groups etc. Note that this data is stored

(c) Recommendation System: Provides movie/TV show recommendations to users and groups.

2. The user's Physical Device (Laptop or Phone)
3. External APIs (OMDb, MyAnimeList etc.): Our application requires these APIs to collect movie and TV show records.
4. Database: Storing user data on our database, through Firebase.
5. Deployments: Builds and deployments will be managed by Jenkins/GitHub Workflow.

The system boundary includes the entire Flick Picker Application, and application database. Note that user's device and APIs are external elements, therefore not part of the system boundary. Firebase/Google maintains the uptime of our application and database. We also make use of Jenkins/GitHub Workflow for CI/CD of our application.

5 Scope of Hazard Analysis

This document will identify safety concerns and solutions that users may face via:

- Defining what a hazard is in this context
- Stating the critical assumptions that are being made by the system
- Providing a Failure Modes and Effects Analysis of the components of the system
- Outlining the safety requirements that are a byproduct of that analysis
- Outlining a roadmap of when the hazard analysis may be consulted or further adjusted

6 Definition of Hazard

A hazard, as defined by Nancy Leveson, is a property or condition in the system, that may cause some sort of loss when combined with an environmental condition.

7 Critical Assumptions

1. System will not have direct access to users' hardware (ex. specific CPU registers)
2. Files will not be downloaded onto the users' device without the explicit consent of the user (should that be a feature of the system)
3. Users' private information will not be sold or intentionally disclosed to any third parties

8 Failure Modes and Effects Analysis

Below are tables containing the full Failure Modes and Effects Analysis.

Table 2: Failure Modes and Effects 1

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR
Database	Data is deleted on accident	All user data is lost	Database Failure	Regular backups exist where data can be rolled back on demand	IR2, IR3
	Data is unavailable	User cannot access data	Database Failure	Refer Above	IR7
	Data is modified incorrectly	User data is not updated	Database Failure	System alerts if data is not modified when requested	IR2
Authentication	User cannot login	User cannot view recommendations or friends	Invalid Credentials	Use the correct credentials	AR1, PR1

Table 3: Failure Modes and Effects 2

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR
Authentication	Impersonated Superadmin manipulates user's database	User data is changed on back-end, or deleted	Database Security Failure	Reset superadmin password and roll-back database	AR2
Show Selection	Show selection misses preferences	Group will be given a recommendation which does not match all preferences	Algorithmic Error	Group has to try a new recommendation or modify their preferences as none would match	PR2
	Show selection takes too long	Group is given recommendations too slowly	Algorithmic Error	Server must be able to handle influx of requests at busy times	PR2

Table 4: Failure Modes and Effects 3

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR
Browser	Application Crashes	Unsaved user data can be lost	General browser crash	Reopen browser application and fill in any data that was not saved	IR6
Github Automation	Pipeline Not Automatically Run	The current build of will look like it has no issues but the tests were not run	GitHub Error	Manually start pipeline	IR4, IR5

9 Safety Requirements

Below are the Requirements that have been formed by the above analysis.

9.1 Access Requirements

- AR1: Users can only access and modify their own data
- AR2: Only a superadmin can modify the database directly, which there is only one of

9.2 Integrity Requirements

- IR1: User data is not modified without their permission
- IR2: Database backups occur daily
- IR3: Database backups are kept for at minimum one month
- IR4: CI/CD Pipeline is run before every deployment to ensure a healthy application state
- IR5: CI/CD Pipeline is run on every new code change before it can be merged
- IR6: Application crashes will not cause the device to stop working
- IR7: Database will be available as long as the service is available

9.3 Privacy Requirements

- PR1: Users have to login with their credentials to access application data
- PR2: Algorithm to choose shows shall be protected

9.4 Audit Requirements

- AT1: Requirements shall be easy to read and verify across the system

10 Roadmap

The safety requirements determined within this document will be considered throughout the development of the project. After completion of key components (Frontend, Backend, Database etc.), hazard analysis will be conducted to ensure that potential risks are mitigated. If any issues or risks are discovered, action will be taken immediately to resolve them.