Hazard Analysis
Room8

Mohammed Abed
Maged Armanios
Jinal Kasturiarachchi
Jane Klavir
Harshil Patel

2024-10-25

Table 1: Revision History

Date	**Developer(s)**	**Change**
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Contents

[You are free to modify this template. —SS]

1 Introduction

[You can include your definition of what a hazard is here. —SS]
Room8 is a suite of tools aimed at reducing the occurrence of frustrating situations between roommates. Room8 is expected to be implemented as a mobile application and interact with the physical world using a camera and as a result, is expected to handle sensitive user data such as addresses, names, birthdays, images, and financial details. This document aims to outline the scope, critical assumptions, potential failures, and mitigation strategies for Room8. Hazards in the system can be caused by data privacy issues, system malfunction / misuse, and legal / compliance issues.

2 Scope and Purpose of Hazard Analysis

[You should say what **loss** could be incurred because of the hazards. —SS]
The purpose of this hazard analysis is to identify, be aware, and mitigate losses that can be incurred as a result of hazards in the system. There a multiple ways to mitigate the losses such as following appropriate regulations, implementing thorough testing, and informing users how to properly use the system. By examining as many scenarios as possible where the system can cause harm and recording it in this document, the development team aims to minimize the harm dealt to users, stakeholders, and development team. Possible loss that can occur from hazards includes financial loss, loss of reputation, and service disruptions.

3 System Boundaries and Components

This section goes over the components that the system can be divided into.

3.1 User Device

Smart phone the user is using with the supported version of Android or iOS.

3.2 Camera

Responsible for taking picture for cleanliness detection analysis when sensor sends information of user.

3.3 Motion Sensor

Detects movement in the shared space to determine if user has entered or exited shared space signaling the camera for a picture.

3.4 PWA Interface

A mobile application installed on smart phones which have versions of Android and iOS that is currently being supported mobile providers. This includes front-end of the system where users can see details and change settings of various back-end components listed below.

3.5 Authentication

Authentication using OAuth of user credentials and house details are processed in this component including the update of information mentioned previously.

3.6 SMS ChatBot

ChatBot responsible for sending messages to group chat of home members for notifying them of cleanliness assessment, expenses from bill splitter, or reminders to complete tasks.

3.7 Calendar Tool

Allows users to add events to calendar and display to other housemates, if involved in event, in their respective calendars. Also houses logic for generating chore/cleaning schedule and adding in calendars of users.

3.8 Cleanliness Manager

Runs algorithm for detecting change in environment through input received from hardware and stores user's information for the user to view on application along with history of cleanliness.

3.9 Bill Splitter

Calculate charges due from a shared expense and keeps track of which expenses are due from each user and who they owe using the SMS ChatBot to notify users. Also stores history of expenses and charges paid for user to view.

3.10 Database

Used to securely store user and house information, calendar events, expense history, and pictures for cleanliness calculator.

4 Critical Assumptions

[These assumptions that are made about the software or system. You should minimize the number of assumptions that remove potential hazards. For instance, you could assume a part will never fail, but it is generally better to include this potential failure mode. —SS]

- **CA1**: Homes will have a consistent and uninterrupted supply of electricity available.
- **CA2**: Homes will have internet speeds capable of streaming video.
- **CA3**: Every resident of a shared home will have their own personal electronic device.
- **CA4**: Users have used other applications before and are familiar with common signifiers, mappings, and UI metaphores (ex. Heart implies like).
- **CA5**: External services, such as location services, map integrations, and calendar APIs will be available and reliable.
- **CA6**: Users' devices will have additional free storage beyond the what's required for the applications install.
- **CA7**: Camera setup in shared environment will not be moved or blocked to ensure clear pictures of space.

5 Failure Mode and Effect Analysis

[Include your FMEA table here. This is the most important part of this document. —SS] [The safety requirements in the table do not have to have the prefix SR. The most important thing is to show traceability to your SRS. You might trace to requirements you have already written, or you might need to add new requirements. —SS] [If no safety requirement can be devised, other mitigation strategies can be entered in the table, including strategies involving providing additional documentation, and/or test cases. —SS]

Table 2: **FMEA Table**

Design Functions	**Failure Modes**	**Effects of Failure**	**Causes of Failure**	**Recommended Action**	**SR**	**Ref**	**Severity**
Camera Takes Picture	Takes picture while space is blocked	Inaccurate picture for Cleanliness Calculator.	User is covering too much of space that needs to be analyzed.	If picture before use differs too greatly from "clean" state take picture again.	SR?	H1.1	BLANK
	Takes final picture while user in frame.	User privacy is breached	Sensor does not detect movement	Remove picture from database and retake final picture when no motion is detected and analyze again for user.	???	H1.2	BLANK

Design Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref	Severity
Motion Sensor Detects Motion	Motion should not be detected (false positive) Motion is not detected although it is occurring (false negative)	Unnecessary computation and notifications Cleanliness detection does not occur	a. Motion sensor is overly sensitive b. Some brief/light movement that should not be classified as motion occurred (e.g., insect flew by) c. Continuous movement that should not be classified as motion is occurring (e.g., air conditioner causing curtain to move) a. Motion sensor is underly sensitive b. Motion sensor is out of battery c. Signal not detected Motion sensor has disconnected from system d. Motion sensor is broken	a. Include regular motion-calibration testing in system design b. Have a clause in the cleanliness detection algorithm to check for false positives (i.e., if the before/after pictures do not meet a threshold to be considered dissimilar) c. Replace with alternative response for false positives/negatives	SR?, SR?	H2.1	Medium

Design Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref	Severity
System Authenticates User	Bad actor logs in to a user's account	Bad actor alters account credentials. Sensitive user information is revealed, such as full name and address. Unauthorized use of services occurs. Account lockout. Bad actor impersonates user, allowing them to disrupt services for other users within the same house.	Data breach. Weak account password. Lack of multi-factor authentication. Out-dated/insecure methods of storing user credentials. Man-in-the-middle attacks. Brute force attacks.	Check for unusual login patterns, such as different geolocations, IP addresses, and repeated failed attempts on the same login. Require all account passwords to satisfy a minimum password strength criterion. Impose rate limits on failed authentication attempts. Recommend multi-factor authentication to users.	SR?, SR?	H3.1	Medium
Cleanliness Detection System Detects Changes in the Cleanliness of a Room	System falsely concludes that a room has become more dirty. System falsely concludes that a room has become more clean. System concludes that there are no changes despite there being changes. The system concludes that there are changes when there are no changes.	Conflict amongst roommates. Trust in the system declines.	Obstructions in the images captured by the camera. Improper calibration and timing of the motion sensor. Object detection algorithm has errors and classifies items incorrectly in an image.	Create base case tests for the cleanliness detection system, including no change, increase, decrease, and no room state change cases. Alert and instruct users to clear camera obstructions before setting up the system.	SR?, SR?	H4.1	Low

Design Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref	Severity
ChatBot	Texts user about deleted event	False information sent to user and user gets annoyed	ChatBot SMS did not get update from calendar that event was deleted and no longer needs to inform user.	Have test cases covering testing if ChatBot SMS is updated when calendar events update.	NFR222	H5.1	Medium
Bill splitter	Amount owing not accurate or Bill splitter crashing	Users receiving false information. Inputs to bill splitter are not being saved/processed	a. There has been an update to the bill (i.e., amount or people owing). a. User has poor internet connection. b. Room8's server is down.	a. Provide users with a mechanism to edit previously input bill. a. Warn users that their internet is not working and to try again when they have a proper connection. b. Warn users that Room8's server is down and provide updates.	SR?, SR?	H6.1	Medium
Scheduling a chore in the calendar	Event cannot be scheduled	User is frustrated, and important information is not being sent to roommates	a. User has poor internet connection. b. Room8's server or calendar API server is down. c. Conflict occurred due to multiple users scheduling events simultaneously	a. Same as H6.2a. b. Same as H6.2b. c. Put a lock on the calendar resource.	SR?, SR?	7.1	Medium
NEW	NEW	NEW	NEW	NEW	SR?, SR?	H??	Medium

6 Safety and Security Requirements

[Newly discovered requirements. These should also be added to the SRS. (A rationale design process how and why to fake it.) —SS]

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

Appendix — Reflection

[Not required for CAS 741 —SS]

The purpose of reflection questions is to give you a chance to assess your own learning and that of your group as a whole, and to find ways to improve in the future. Reflection is an important part of the learning process. Reflection is also an essential component of a successful software development process.

Reflections are most interesting and useful when they're honest, even if the stories they tell are imperfect. You will be marked based on your depth of thought and analysis, and not based on the content of the reflections themselves. Thus, for full marks we encourage you to answer openly and honestly and to avoid simply writing "what you think the evaluator wants to hear."

Please answer the following questions. Some questions can be answered on the team level, but where appropriate, each team member should write their own response:

1. What went well while writing this deliverable?
2. What pain points did you experience during this deliverable, and how did you resolve them?
3. Which of your listed risks had your team thought of before this deliverable, and which did you think of while doing this deliverable? For the latter ones (ones you thought of while doing the Hazard Analysis), how did they come about?
4. Other than the risk of physical harm (some projects may not have any appreciable risks of this form), list at least 2 other types of risk in software products. Why are they important to consider?