

Hazard Analysis

Plutos

Team #10, Plutos

Payton Chan

Eric Chen

Fondson Lu

Jason Tan

Angela Wang

Table 1: Revision History

Date	Developer(s)	Change
10/23/2024	Angela	Initial draft
...

Contents

1	Introduction	1
2	Scope and Purpose of Hazard Analysis	1
3	System Boundaries and Components	1
4	Critical Assumptions	1
5	Failure Mode and Effect Analysis	2
6	Safety and Security Requirements	3
7	Roadmap	3

1 Introduction

A hazard in the context of this document is any property or condition that may lead to harm or damage to the Plutos system or its users. The following sections will identify hazards within the system and discuss the controls in place for their mitigation.

2 Scope and Purpose of Hazard Analysis

This document aims to provide a comprehensive hazard analysis of the Plutos system. It identifies hazards within the system, outlines measures to mitigate them, and specifies the safety and security requirements derived from this analysis. The analysis will follow the Failure Mode and Effect Analysis (FMEA) approach. Potential losses due to these hazards may include breaches of user privacy and data, loss of application functionality, and data loss. The analysis aims to discover the potential failure modes within the system and develop a mitigation plan to reduce the risk of failure.

3 System Boundaries and Components

The system will be divided into the following components:

1. The Plutos application, which consists of:
 - (a) **The database:** The database is where the user's receipts and profile data will be stored.
 - (b) **The backend server:** The backend server is responsible for handling and serving requests from the client. It will interact with all the other components listed here.
 - (c) **The frontend/user interface:** The frontend/user interface is responsible for displaying the appropriate views to the user and handling user interactions.
 - (d) **The machine learning (ML) model:** The ML model is responsible for parsing and categorizing items from a picture of an itemized receipt.
2. The user's mobile device and camera setup

4 Critical Assumptions

The project will be making the following critical assumptions:

1. The users will be using a mobile device running an up-to-date version of iOS or Android.
2. Users are not expected to repeatedly input invalid images into the system (i.e., images that do not contain a receipt). While it is anticipated that users may occasionally submit an invalid image, it is assumed to not be a significant concern.

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: Failure Mode and Effect Analysis Table

Design Function	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
...

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

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?