Hazard Analysis
Sayyara Automotive Matcher

Team 27, Kappastone
Tevis Doe, doet
Caitlin Bridel, bridelc
Gilbert Cherrie, cherrieg
Rachel Johnson, johnsr12
Harkeerat Kanwal, kanwalh
Himanshu Aggarwal, aggarwah

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct. 19th, 2022	All Members	Initial document creation. Revision 0.

Contents

1 Introduction

This document goes over the hazard analysis of the Sayyara Automotive Matcher. The Sayyara Automotive Matcher is a software that assists customers is finding and creating appointments with mechanics to perform maintenance on their vehicles.

For the purposes of this project, the definition of a hazard, based on Nancy Leveson's work is as follows: A hazard is any property in the system, that when paired with an event in the environment causes loss in the system.

2 Scope and Purpose of Hazard Analysis

The purpose of this Hazard Analysis is to identify possible hazards within the system. The hazards identified are analyzed to deduce causes, effects and steps for mitigation. Further safety and security requirements are developed to ensure hazards are avoided.

3 System Boundaries and Components

Within our hazard analysis, we will consider failures and hazards that could occur on the following system components:

1. The **progressive web application (PWA)** which facilitates the following services:
    - Account creation and deletion
    - Authentication
    - Sending and receiving quotes and quote requests
    - Booking appointments
    - Creating and deleting work orders
2. The **database** which stores information related to:
    - Shops
    - Shop owners
    - Shop employees
    - Customers
    - Quotes
    - Work orders
    - Appointments
3. The **user device** which is the medium through which users will interact with the PWA

4 Critical Assumptions

The only critical assumption being made is that the cloud provider we are using will have a 98% up time to allow us to achieve our non functional requirement for reliability and availability.

5 Failure Mode and Effect Analysis

A failure modes and effect analysis (FMEA) is performed below as a way to identify potential hazards, and provide recommended actions as a means to mitigate them.

5.1 Hazards Out of Scope

The final product our partner wishes to receive is meant to be an MVP that can be demoed to potential investors. Given this aim, it is imperative that performance, and up-time related hazards be thoroughly accounted for, however, this also means the following hazards are considered low priority and/or out of scope:

- Security concerns (unnecessary because the demos will be done using a dummy account, whose data is of no consequence)
- Long term data loss (unnecessary because the data is not required to be stored after the demos have been completed)

5.2 Failure Mode and Effects Analysis Table

The Failure Mode and Effects Analysis for the Sayyara Automotive Matcher-system is outlined in Table 2.

Table 2: Failure Mode & Effects Analysis

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	Severity	SR	Ref.
Shop Info	Appointment list is lost	Loss of business. Customers will show up for appointments that are not scheduled in the system, causing angry customers and overall loss of money.	• Host site for server unexpectedly goes down. • Server crashes from instability related to bugs.	Periodically backup database, allowing rollbacks to database on request from a shop owner.	High	IR-1	H1-1
	Services list is lost	Customers will not be able to request services from shops because they are not listed, causing the shop to lose out on business.	• Host site for server unexpectedly goes down. • Server crashes from instability related to bugs. • Database failure	Same as H1-1.	High	IR-1	H1-2
Quotes	Active quotes list is lost	Loss of customer quote data. Shop owners can potentially lose customers if customers lose their quote data or shop owners can lose information related to the quotes they are working on.	• Host site for server unexpectedly goes down. • Server crashes from instability related to bugs.	Periodically backup database, allowing rollbacks to database on request from a shop owner.	High	IR-1	H2-1
Employee Invitations	Employee invites are sent to incorrect emails	Authorized employees do not receive invitations and are unable to create account or login	• Emails inputted are not correctly stored in database • Database failure • Miscommunication between database and email-sending software	• Provide a way to verify emails are correctly received by app. • Same as H1-1	Medium	IR-1	H3-1

Component	Failure Modes	Effects of Failure	Causes of Failure	Recommended Action	Severity	SR	Ref.
Server	Server crashes unexpectedly	Complete loss of function in the system beyond front end interface. Current progress in app is essentially lost.	• Host site for server unexpectedly goes down. • Server crashes from instability related to bugs.	• If current host site proves unstable, research a new way to deploy the server. • Store current session of a user, allowing in-progress actions to be resumed when server access is restored. In the meantime, display an error to the user.	High	IR-2, IR-3	H4-1
Authentication	User credentials are lost	Shop owners will be denied access to the system. Loss of business. Cannot manage shops, nor respond to potential customers.	• Credentials of a given user do not match the hash stored in database • Database failure	• Provide a way to reset the user's password in a secure way, allowing them to use the system again. • Same as H1-1.	High	IR-1	H5-1
	Unauthorized user gains shop owner level of access to the system	The user could make unauthorized edits to shop profiles, employee accounts, quotes, work orders, and appointments.	• Failed authentication • The unauthorized user stole a real user's login information • The real user created a password that was not very secure	• Invest in a reliable method of authentication • Provide multi-factor authentication that does not rely solely on correctly entering login information • During account creation, prompt the user to create a secure password and advise them on how to do so	High	AR-1, IR-4, IR-5	H5-2
Database	Users gain direct access to the database.	The user could query private data and make unauthorized changes. The user could also steal emails and passwords of other users.	• The backend server has a flaw that allows direct access to the database.	• Store encrypted passwords. • Use a different database for storing user details and passwords.	High	IR-6, IR-7, PR-1	H6-1

6 Safety and Security Requirements

6.1 Access Requirements

AR-1 Only shop owners shall be allowed to edit shop profiles, employee accounts, quotes, work orders, and appointments.

6.2 Integrity Requirements

IR-1 The databases shall be backed up every 12 hours.

IR-2 Any pending tasks paused due to a server crash shall be resumed automatically when the server is back up.

IR-3 Any errors that cause the server to crash shall be logged.

IR-4 The system shall require users to create a strong password when registering.

IR-5 The system shall provide support for multi-factor authentication.

IR-6 The system shall encrypt passwords before storing them.

IR-7 The system shall store user details and credentials in a different database.

6.3 Privacy Requirements

PR-1 Users shall not be able to query data related to other users directly through the database.

6.4 Audit Requirements

N/A

6.5 Immunity Requirements

N/A

7 Roadmap

All of the safety requirements will be implemented as part of the capstone timeline because they are required by our partner (excluding requirements explicitly stated as out of scope in section 5.1).