Hazard Analysis
Park'd

Team #29, caPstOneGroup
Albert Zhou
Almen Ng
David Yao
Gary Gong
Jonathan Yapeter
Kabishan Suvendran

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct 13 2022	Albert, Almen, David, Gary, Jonathan, Kabishan	Revision 0
Apr 3 2023	Albert, Almen, David, Gary, Jonathan, Kabishan	Revision 1

Contents

1 Introduction **1**

2 Scope and Purpose of Hazard Analysis **1**

3 System Boundaries and Components **1**

4 Critical Assumptions **2**

5 Failure Mode and Effect Analysis **3**

6 Safety and Security Requirements **6**

4.6.1 Access Requirements 6

4.6.2 Integrity Requirements 6

4.6.3 Privacy Requirements 7

4.6.4 Audit Requirements 7

4.6.5 Immunity Requirements 7

7 Roadmap **7**

List of Tables

1 Revision History i
2 Failure Mode and Effect Analysis Table 3
3 Failure Mode and Effect Analysis Table, Part 2 4
4 Failure Mode and Effect Analysis Table, Part 3 5

1 Introduction

This document is the hazard analysis of Park'd. A hazard is a property or condition in the system together with a condition in the environment that has the potential to cause harm or damage = loss (From Nancy Leveson's work).

2 Scope and Purpose of Hazard Analysis

The scope of the system encompassed by this hazard analysis of the Park'd application. Hazards imposed by outer environment and society are beyond the scope of this document.

This document identifies hazards including security, feature authorization, user authentication, input correctness, and error handling as well as discusses the plans for hazard mitigation, and safety and security requirements that arise from the analysis of these hazards.

3 System Boundaries and Components

The system boundary and components consists of the following:

- Camera
  - An external hardware that captures the video and images of parking lots and transmits this information as input for our machine-learning model
- Park-d web application Band-end server system
  - Communication System (Communication protocol library for different system components)
    - A system responsible for the communication of the different components of the application. (Communicating through HTTP call or RPC call)
    - A system responsible for recovery when a communication failure occurs.
  - Driver Navigation System
    - A system Provides the user with the navigation information for our application when a user arrives at the parking lot
  - Administrative Map System
    - A system specifically designed for parking lot owners to allow them to upload the physical layout of their parking lot
  - Machine-Learning Model
    - This system serves to analyze the real-time video data of the parking lot and outputs vacant parking spot information upon user request.
  - Database Storage System

        * The data storage system stores the necessary user information and parking lot information for our backend services

- Cloud server
    - The cloud server provides the ability to host our services remotely, load balancing, and take web requests from users.
- Local machine
    - The local machine including a cellphone or laptop allows user to check parking lot information and sending requests to our services.

4 Critical Assumptions

There are no critical assumptions being made.

5 Failure Mode and Effect Analysis

Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref.
Navigation	No driving instructions provided	Driver cannot navigate to desired parking space	a. User location access lost b. Map lost connection to remote service c. Specified destination is unreachable	Inform the driver that driving instructions could not be found and to try again later to avoid driver frustration	SR.13	H1-1
	Impossible driving instructions provided	Driver cannot navigate to desired parking space	Path finding algorithm provided directions that are blocked by obstacles	Add functionality to allow driver to report the obstacle and request another route	SR.4	H1-2
	Lengthy driving instructions provided	Driver travels a distance that exceeds the minimum distance required to reach the parking space	Path finding algorithm could not find an optimal path in the requested amount of time	Inform the driver that driving instructions with least travel could not be found and to try again later to avoid driver frustration	SR.13	H1-3
Spot detection	System classifies reserved or accessibility parking spaces as normal parking spaces	Driver unknowingly parks in a parking space that is not available to them	a. Painted indicator for reserved or accessibility parking has faded or obscured by nearby vehicles or shadows b. Some spaces are converted to reserved spaces	Allow parking lot managers to edit the parking lot layout to fix the errors. Warn users to verify that they are allowed to use the spot before parking.	a. SR.2, SR.3, SR.4, SR.10 b. SR.2, SR.3, SR.4	H2-1
	System unable to detect any parking space	User cannot park at any parking space in the parking lot	Weather conditions, such as snow, have hidden the parking space boundaries	Use backup data if a large percentage of parking spots become obscured	SR.7	H2-2

Table 2: Failure Mode and Effect Analysis Table

Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref.
Selecting Parking Space	System associates selection with wrong parking space	a. Driver is provided with wrong directions b. Wrong space is marked as occupied until camera marks the space as still empty	Space database error; Selection does not translate to the same space in the database	The system must not deviate from the format it uses to store other parking spaces	SR.8	H3-1
	System allows selection of reserved parking spaces while unauthorized	Driver is directed to spaces they are not authorized to use	a. Image recognition algorithm mislabels spot b. Interface fails to hide unauthorized spaces	Invalid spaces should be marked accordingly in the app; Spaces should be stored along with any of their special properties	a. SR.9 b. SR.9	H3-2
Parking Lot Mapping	System maps a parking space where there is none	Driver is directed to park illegally	Image recognition algorithm fault	Allow for manual corrections to the constructed map	SR.2, SR.3	H4-1
	Recognized parking space is not associated with the database	Gaps exist in the displayed map on a valid parking space	Space database error; Parking space is recognized but not made accessible in the database	Raise an error if the system fails to associate a key with a given parking space. Ensure database entries always contain data for both the camera view and the map view.	SR.10	H4-2
	Paths leading to parking spaces are not mapped	Driver cannot navigate to desired parking space	a. No driving instructions provided b. Driving instructions are impossible to follow	Driving paths through the parking lot should already be stored for any potential space	a. SR.12 b. SR.12	H4-3

Table 3: Failure Mode and Effect Analysis Table, Part 2

Functions	Failure Modes	Effects of Failure	Causes of Failure	Recommended Actions	SR	Ref.
Viewing Parking Lot	System displays wrong parking lot layout	Driver does not see accurate information about the layout of the parking lot	Fault in Parking Lot Mapping algorithm	Add functionality to allow driver to manually mark layout mistakes as feedback to the system	SR.4	H5-1
	System displays wrong parking spot information	Driver does not see accurate information about the status of parking spots	Fault in Parking Spot Detection algorithm	Add functionality to allow driver to report incorrect parking spot status as feedback to the system	SR.4	H5-2
Editing Parking Lot Layout	System does not save the changes made to the layout	Parking lot manager is not able to apply changes they made to the parking lot	Database not updated properly with changes made to the layout	Allow parking lot manager to force an update to the layout stored in the database; Ensure database is checking for manual changes to the layout of the parking lot	SR.5, SR.6 SR.11	H6-1
	System does not display tools to edit the layout of the parking lot	Parking lot manager is not able to edit the layout of the parking lot	System not displaying user interface for editing	Allow parking lot manager to restart or refresh the editing view/interface	SR.5, SR.6, SR.11	H-2

Table 4: Failure Mode and Effect Analysis Table, Part 3

6 Safety and Security Requirements

The requirements that should be added to Park'd's SRS based on the FMEA analysis are written in red.

4.6.1 Access Requirements

SR1. The system's parking lot data shall be accessible only to the team and to the parking lot owner(s).
Fit Criterion: The data is password protected.

SR2. Only the parking lot owner(s) shall have the option to edit the parking space layout
Fit Criterion: The administrative console is the only view that has the option to edit the parking space. Normal users are not given the credentials to log in to this console.

SR3. Only the parking space manager(s) of a parking lot are allowed to have access to the administrative console for their parking lot
Fit Criterion: The administrative console of a parking lot can only edit and view analytics of the parking lot. Normal users are not given the credentials to log in to this console.

4.6.2 Integrity Requirements

SR4. The system shall prevent inaccurate data from being stored.
Fit Criterion: Stress test the system with accurate and inaccurate data and measure the data's accuracy.

SR5. Unsaved parking layout information should be stored locally if the information cannot be uploaded to the server

SR6. Unsaved parking layout information should attempt to upload to the server every 30 seconds

SR7. Parking layouts will be automatically backed up daily

SR8. No parking space should be stored in a different format in the database from other parking spaces

SR9. The system should only allow a parking spot to have 1 special property
Fit Criterion: A parking space is either labeled as normal, accessible, or reserved

SR10. Parking lot managers must be prompted when there is a failed attempt to add a parking spot to the database

SR11. Parking lot owners should be able to prompt the upload of their parking lot layout to the database and server

SR12. Correct paths should be stored to all parking spaces

SR13. Users are informed when an error occurs when the system is determining the navigation path

4.6.3 Privacy Requirements

SR14. The system shall ask for permission to use the driver's location data.
Fit Criterion: The system has a driver location agreement form.

4.6.4 Audit Requirements

N/A

4.6.5 Immunity Requirements

N/A

7 Roadmap

Of the new requirements listed on this document, SR1-SR3 and SR8-SR14 were all successfully implemented in Revision 1. SR4, SR5, SR6, and SR7 are all slated for a future revision, after the Capstone Expo. Of these, SR5 is considered the highest priority, to prevent lost progress. These requirements are related to contingencies regarding unreliable connections, and are considered of lower priority relative to others which are related to main functionality.