ParkMe: Hazard Analysis

Group 5

Jan. 18, 2019

Kathryn Brownlee
brownlks@mcmaster.ca
001408416

Ben Petkovsek
petkovb@mcmaster.ca

Michael Bitzos
bitzosm@mcmaster.ca
1405050

Daniel Agostinho
agostd@mcmaster.ca
001414323

Anthony Chang
changa7@mcmaster.ca
001413615

Revision History

Rev 0: Jan 18, 2019

Table of Contents

Introduction

Although ParkMe has very little physical interaction with the environment and the users, like most products, there is still inherent risk that comes with the system. The assumption is that the user will be driving for most of the interaction of the system. The system needs to ensure that it does not pose a risk to the driver, nor cause the driver to be distracted and further cause damage with their vehicle.

Scope

The victims of these hazards are not limited to just the driver and others in cars. Damage may also occur to pedestrians, other stationary vehicles, the physical sensors for the system, and infrastructure of the parking lot. All of these potential victims must be accounted for in analyzing the hazards of the system. Although the system cannot directly harm the user, there are control actions that the system makes that can have consequences that will lead to an accident or a loss. The correctness of the system's sensing and output of the sensor data/ geographical location is imperative for the safe use of the system. Thus the control actions that are within the scope of the hazard analysis are the ones that are directly responsible for receiving and outputting the information to the user.

Purpose

This document serves to outline the hazards associated with the product ParkMe. The hazard analysis technique that will be used for this document is the STPA technique. First we will identify the main control actions that can be hazardous. Then for each control action we will determine the hazards that come with those actions. We will breakdown the system control actions by component as can be seen in Figure 1. Finally the consequences of the hazards will be shown in the consequence matrix in Table 2.

List of Figures

List of Tables

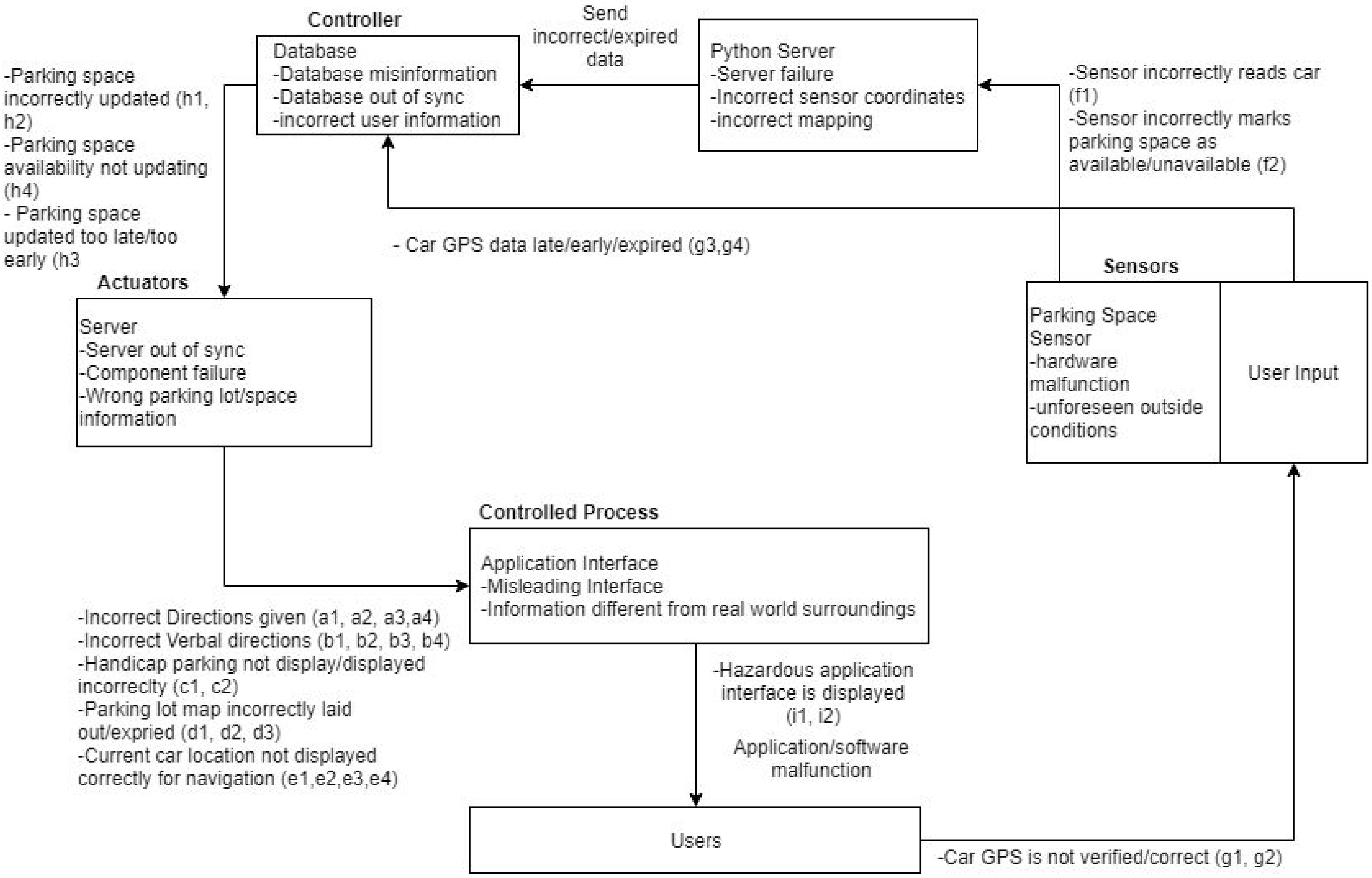
Controller
Database
-Database misinformation
-Database out of sync
-incorrect user information
Send incorrect/expired data
Python Server
-Server failure
-Incorrect sensor coordinates
-incorrect mapping
-Sensor incorrectly reads car (f1)
-Sensor incorrectly marks parking space as available/unavailable (f2)
-Parking space incorrectly updated (h1, h2)
-Parking space availability not updating (h4)
- Parking space updated too late/too early (h3
- Car GPS data late/early/expired (g3,g4)
Sensors
Actuators
Server
-Server out of sync
-Component failure
-Wrong parking lot/space information
Parking Space Sensor
-hardware malfunction
-unforeseen outside conditions
User Input
Controlled Process
Application Interface
-Misleading Interface
-Information different from real world surroundings
-Incorrect Directions given (a1, a2, a3,a4)
-Incorrect Verbal directions (b1, b2, b3, b4)
-Handicap parking not display/displayed incorrecltly (c1, c2)
-Parking lot map incorrectly laid out/expried (d1, d2, d3)
-Current car location not displayed correctly for navigation (e1,e2,e3,e4)
-Hazardous application interface is displayed (i1, i2)
Application/software malfunction
Users
-Car GPS is not verified/correct (g1, g2)

Figure 1: STPA breakdown of system control actions and hazards.

Control Action	**Category 1: A control action required for safety is not provided or is not followed.**	**Category 2: an unsafe control action is provided that leads to a hazard**	**Category 3: A potentially safe control action is provided too early, too late, or out of sequence**	**Category 4: A safe control action is stopped too soon.**
Display Map Directions (A)	Necessary direction is missing. (a1)	Provided direction of navigation is wrong. (a2)	Turns or stops are provided at the wrong time. (a3)	Directions are stopped while driving. (a4)

Provide voice navigation (B)	Verbal direction does not match physical location. (b1)	Verbal direction does not match physical location. (b2)	Verbal direction timing does not match physical location. (b3)	Verbal directions are stopped while driving. (b4)
Display Handicap Parking (C)	Handicap Parking spot not displayed to user. (c1)	Handicap parking spot is displayed incorrectly. (c2)	N/A	N/A
Display Available Parking Spots (D)	Map of parking lot is missing/ incorrect. (d1)	Map of parking lot is incorrect or misleading. (d2)	Map of parking lot is displayed while user is not within range of parking lot. Map of parking lot does not display on time when user is within range. (d3)	N/A
Update Car Location on Map (E)	Car is not displayed on screen. (e1)	Car location is not displayed to match current physical location within acceptable bounds. (e2)	Car location is not updated within acceptable timing range. (e3)	Car location display ends before user arrival. (e4)
Sense Car in Spot (F)	System fails to read data from sensor. (f1)	The sensors incorrectly sense the parking spot. (f2)	N/A	N/A
Get Car Location (G)	Car GPS coordinates are unavailable. (g1)	GPS coordinates do not match current physical location within acceptable bounds. (g2)	GPS coordinates are not updated within acceptable frequency. (g3)	GPS Coordinates stop being provided before arrival. (g4)
Update Spot Availability (H)	The availability of a spot is not updated when it changes. (h1)	A spot is said to be available when it isn't or vice-versa. (h2)	Spot is not updated within acceptable time range. (h3)	Spot availability is not updated. (h4)
Application interface display (I)	Application display is not functional (I1)	Application displays incorrect	N/A	N/A

		information. (i2)		

Table 1: STPA Chart showing control actions with hazard categories.

<table>
<tr><th>Control Action</th><th>Consequence of Hazard I</th><th>Consequence of Hazard II</th><th>Consequence of Hazard III</th><th>Consequence of Hazard IV</th></tr>
<tr><td>Display Map Directions (A)</td><td colspan="4">Could result in dangerous maneuvers or incorrect turns. May result in distracted driving, leading to crash, damage of property, personal harm or harms of others.</td></tr>
<tr><td>Provide Voice Navigation (B)</td><td colspan="4">Could result in dangerous maneuvers or incorrect turns. May result in distracted driving, leading to crash, damage of property, personal harm or harms of others.</td></tr>
<tr><td>Display Handicap Parking (C)</td><td>User may erroneously park in a handicap spot.</td><td>Handicap user may be led to non-handicap spot.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Display Available Parking Spots (D)</td><td colspan="3">May result in distracted driving, leading to crash, damage of property, personal harm or harms of others.</td><td>N/A</td></tr>
<tr><td>Update Car Location on Map (E)</td><td>May result in distracted driving, leading to crash, damage of property, personal harm or harms of others.</td><td colspan="3">Could result in dangerous maneuvers or incorrect turns. Driver may drive into vehicle, private property or physical obstruction if they are not vigilant.</td></tr>
<tr><td>Sense Car in Spot (F)</td><td colspan="2">Driver may drive into vehicle, private property or physical obstruction if they are not vigilant.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Get Car Location (G)</td><td colspan="4">Could result in dangerous maneuvers or incorrect turns. May result in distracted driving, leading to crash, damage of property, personal harm or harms of others.</td></tr>
<tr><td>Update Spot Availability (H)</td><td colspan="4">Driver may drive into vehicle, private property or physical obstruction if they are not vigilant.</td></tr>
<tr><td>Application</td><td colspan="2">May result in distracted driving,</td><td>N/A</td><td>N/A</td></tr>
</table>

Interface DIsplay (I)	leading to crash, damage of property, personal harm or harms of others.		

Table 2: Consequence matrix.