



# LazyBots

McMASTER UNIVERSITY

Hazard Analysis

SE 4GA6 & TRON 4TB6

GROUP 9

Karim Guirguis	001307668
David Hemms	001309228
Marko Laban	001300989
Curtis Milo	001305877
Keyur Patel	001311559
Alexandra Rahman	001305735

# Table of Contents

<b>1</b>	<b>Revisions</b>	<b>3</b>
<b>2</b>	<b>Introduction</b>	<b>4</b>
2.1	Document Purpose . . . . .	4
2.2	Definitions . . . . .	4
<b>3</b>	<b>Component Overview</b>	<b>4</b>
3.1	Drink Ordering System . . . . .	4
3.2	Login System . . . . .	4
3.3	Administrative Map System . . . . .	4
3.4	Error Management System . . . . .	4
3.5	Backend Server System . . . . .	4
3.6	Alfred Manager System . . . . .	5
3.7	Drivetrain Subsystem . . . . .	5
3.8	Alfred Pumping System . . . . .	5
3.9	Image Processing Subsystem . . . . .	5
<b>4</b>	<b>Safety Considerations</b>	<b>5</b>
4.1	Drink Ordering System . . . . .	5
4.2	Login System . . . . .	5
4.3	Administrative Map System . . . . .	5
4.4	Error Management System . . . . .	6
4.5	Backend Server System . . . . .	6
4.6	Alfred Manager System . . . . .	6
4.7	Drivetrain Subsystem . . . . .	6
4.8	Alfred Pumping System . . . . .	7
4.9	Image Processing Subsystem . . . . .	7
<b>5</b>	<b>FMEA Worksheet</b>	<b>8</b>

## List of Tables

1	LazyBots Table of Revisions . . . . .	3
---	---------------------------------------	---

## List of Figures

1	FMEA Table Part 1 . . . . .	8
2	FMEA Table Part 2 . . . . .	9
3	FMEA Table Part 3 . . . . .	10
4	FMEA Table Part 4 . . . . .	11
5	FMEA Table Part 5 . . . . .	12

## 1 Revisions

Table 1: LazyBots Table of Revisions

Date	Revision Number	Authors	Comments
November 24 <sup>th</sup> , 2017	Revision 0	Karim Guirguis David Hemms Marko Laban Curtis Milo Keyur Patel Alexandra Rahman	-

## 2 Introduction

### 2.1 Document Purpose

The purpose of this document is to identify the components of Alfred which could potentially have hazardous consequences, and either eliminate them or reduce its risk to an acceptable level. Hazard analysis should be performed for all the major phases of the software development lifecycle, including requirements, architectural design, detailed design, and actual code. In particular, this document will look at the hazardous potential when the system works correctly, as well as when the system works incorrectly.

Hazards will be identified based on hazards from similar systems, as well as any hazards that occur during development/lifecycle of the system.

For this report we will analyze the hazards which can be affected by our mechanical and software systems.

### 2.2 Definitions

<b>System Hazard</b>	The system is in a condition/state from which an accident can occur.
<b>Accident</b>	Unplanned event which can lead to unacceptable consequences.
<b>Risk</b>	A measure that combines the likelihood that a system hazard will happen, the likelihood that an accident will happen, and the severity of the worst potential accident.
<b>Critical System</b>	System whose failure can lead to unacceptable consequences.
<b>Safety Critical System</b>	A critical system whose failure can lead to injury, death, or environmental damage.

## 3 Component Overview

The components can be divided into ten components;

### 3.1 Drink Ordering System

An android application that allows customers and consumers to order drinks. The order is then relayed to Alfred.

### 3.2 Login System

A web application that allows users such as administrators or servers to login into the system and modify the restaurant map or close orders.

### 3.3 Administrative Map System

An android application that allows an administrator to change the layout of the restaurant. This map is then relayed to Alfred.

### 3.4 Error Management System

An application that allows users and administrators to view and track ongoing issues with Alfred. Users can also close issues once they have been resolved.

### 3.5 Backend Server System

The backend server serves as a method of communication between Alfred and other applications and components.

### 3.6 Alfred Manager System

This system serves as Alfred's drink order manager. The system will place the orders in a queue and assign them to the corresponding table number so that Alfred may complete the drink order.

### 3.7 Drivetrain Subsystem

This is the basic mechanical and electrical components of Alfred that allow motion and movement.

### 3.8 Alfred Pumping System

The system that deals with the fluid dynamics. Receives necessary information from Alfred Manager System to dispense correct type of drink, with the correct amount for the corresponding table.

### 3.9 Image Processing Subsystem

Alfred will be utilizing this subsystem to assure that all pathways are clear and to relay better error reports in case on an accident.

## 4 Safety Considerations

### 4.1 Drink Ordering System

#### Software Issues:

- An order is not sent within the desired time

#### Hardware Issues:

- None

### 4.2 Login System

#### Software Issues:

- The ability to perform attacks the server software to prevent access to the system
- The ability to perform attacks the server software to pose as store manager
- The ability to snoop information in order to obtain information about clients
- The ability to attack the system by injecting code

#### Hardware Issues:

- Server is not able to perform functionality to properly verify users due to internet issues or component failure

### 4.3 Administrative Map System

#### Software Issues:

- The ability to inject false information while data is being transferred to the server

#### Hardware Issues:

- Computer is not able to perform functionality due to internet issues or component failure

## 4.4 Error Management System

### Software Issues:

- Errors are injected into the communication to be able to provide incorrect information to the manager's system
- Errors are not received within the desired time

### Hardware Issues:

- Computer is not able to perform functionality due to internet issues or component failure

## 4.5 Backend Server System

### Software Issues:

- The ability to perform attacks the server to prevent access to the system
- The ability to perform attacks the server system to pose as a manager or administrator
- The ability to snoop information in order to obtain information about clients
- The ability to attack the system by injecting code
- Issues with response and processing time of the subsystem

### Hardware Issues:

- Server is not able to perform functionality to properly verify users due to internet issues or component failure

## 4.6 Alfred Manager System

### Software Issues:

- Attacks where incorrect drink orders are sent to Alfred

### Hardware Issues:

- Issues within micro-controller that would prevent computation functionality
- Issues such as faulty wiring or noise would prevent proper communication to the drink subsystem

## 4.7 Drivetrain Subsystem

### Software Issues:

- Correct command to the motor is obtained and is regulated for things such as slew rates and max capacities
- The system is within a stable control state of operation and if not the ensuring that there is no motion
- Detection of obstacles blocking Alfred's path of motion

### Hardware Issues:

- Encoders are operating within the normal suggested operating range
- Motors are performing the correct path of motion based on the control systems specifications
- Motors are performing within the recommended operating range
- Ultrasonic sensors are providing information within the recommended operating range
- Electrical components being leaked on by liquid storage devices
- Insufficient power is supplied from the battery to the drive system

## 4.8 Alfred Pumping System

### Software Issues:

- The software system is not able to validate command from the Alfred manager system

### Hardware Issues:

- There is a leak within the pumping system
- There is a leak within the storage of the liquids
- Alfred is not able to pump liquid using the pump
- Micro-controller is not able to receive information due to broken communication lines
- Micro-controller components fail and is not able to process drink request

## 4.9 Image Processing Subsystem

### Software Issues:

- The software image processing Library is not able to properly process the image due to poor lighting conditions

### Hardware Issues:

- The image is not able to be captures properly due to a broken or blocked camera
- Micro-controller processor is broken and not able to perform functionality

## 5 FMEA Worksheet

Function	Failures	Effect(s) of failure	Severity of failure (0-10, 0 being least likely)	Cause of failure	Likelihood of occurrence (0-10, 0 being least likely)	Controls in place	Likelihood of failure detection (0-10, 0 being most likely to detect)
AF1: Movement of Alfred	Battery not able to power DC Motor.	Alfred is unable to move.	6	Battery has ran for an extended period of time. Battery is malfunctioning.	7	Voltage sensors to see if voltage is within operating range.	3
	Not able to sense speed of Alfred.	Will be unable to be controlled properly.	8	Encoder is malfunctioning. DC motor brush failure.	2	Have a diagnostic to determine if the speed from the encoder is in range.	1
	Micro-controller is not able to power motor.	Will be unable to be controlled properly.	8	Micro-controller failure. PWM comparator failure.	3	Timeout conditions on server. Diagnostics for speed.	4
	Movement Path is obstructed.	Crashing or not being able to move.	9	People moving in front of the robot, obstacles around the restaurant.	9	Ultrasonic sensors and Camera are used to be able to navigate around obstacles.	5

Figure 1: FMEA Table Part 1



AF2: Correlate drink order to correct table	Alfred pours the incorrect drink for the table.	Unsatisfied customer	4	Communication failure for orders.	3	Communication Protocols. Cyclic redundancy check.	3
AF3: Navigate to table successfully	Alfred does not make it to the table.	Customer does not receive drink.	6	Something has incapacitated Alfred. Unable to navigate around objects.	1	Monitor whether Alfred's fallen over. Timeouts of attempting to navigate around objects.	8
	Alfred does not make it to the correct table.	Unsatisfied customer	4	Image processing changed path incorrectly. Incorrect operating map.	3	Continuously compare CV calculation to mapped layout. Having obstacle avoiding software to move around objects.	2
AF4: dispense correct drink for the order	Dispenses the wrong drink.	Unsatisfied customer	4	Communication failure for orders.Failure in PCB trace	2	Communication Protocols. Cyclic Redundancy Check	5

Figure 2: FMEA Table Part 2

AF5: Dispense correct amount	Underfills drink.	Unsatisfied customer.	4	Pump does not run long enough or cup grabbed too soon.	2	Weight sensor, LED to display when drink is ready.	2
	Overfills drink.	Liquid could leak onto electronics.	9	Pump runs for too long or cup put back with liquid.	2	Weight sensor, internal cups.	2
AF6: Determine when liquids are not correct temperature	Drinks are over desired temperature.	Could be harmful to customer.	8	Warmer ambient temperature	10	Adding thermal wrapping to container and having temperature sensors.	4
AF7: Notify staff when errors or warning occurs	Staff will not know when to help Alfred.	Customers do not receive drinks.	7	Any of the issues stated in AF1 and AF2.	5		3
AF8: Determine when liquid supply is lower than desired level	Alfred is not able to dispense drinks.	Customers do not receive drinks.	7	Too many people requesting drinks so it must be refilled.	10	Add behaviour to send warnings to the kitchen warning them that Alfred needs to be refilled and have Alfred Navigate home.	2

Figure 3: FMEA Table Part 3

AF9: Moving the storage container of liquid to locations	Storage container is put on its side.	Liquids spills onto electronics.	9	People knocking Alfred over.	8	Get leak proof containers to prevent leaking. As well as using silicone to seal any cracks. Having separation between liquids and electronics with some form of dividing wall.	5
	Movement of liquid in storage container.	Liquid spills onto electronics.	9	People knocking Alfred over.	8	Get leak proof containers to prevent leaking. As well as using silicone to seal any cracks. Having separation between liquids and electronics with some form of dividing wall. Adding a slew rate for speed controller to prevent fast acceleration.	3

Figure 4: FMEA Table Part 4

AF9: Moving the storage container of liquid to locations	Container is cracked and leaking.	Liquid spills onto electronics.	9	People knocking Alfred over.	8	Get leak proof containers with thick plastic to prevent leaking. As well as using silicone to seal any cracks. Having separation between liquids and electronics with some form of dividing wall. Having on board diagnostics to determine when a leak is occurring by using a weight sensor.	3
AF10: Dispense drink for the customer	Dispenses the wrong drink.	Unsatisfied customer.	4	Communication failure for orders. Failure in PCB trace.	2	Communication Protocols. Cyclic redundancy check.	5
	Not able to pump liquid.	Customers not able to receive drinks.	7	Voltage pin from micro failure, Mosfet failure. Pump failure.	2	Have diagnostics to determine when the weight of the cup is not rising by using a weight sensor.	2

Figure 5: FMEA Table Part 5