4TB6: Hazard Analysis
Stonecap Solutions - Smart Serve

Max Turek *turekm*
Ryan Were *werer*
Sam Nusselder *nusselds*
Peter Minbashian *minbashp*
David Bednar *bednad*1

10/19/2022

Contents

List of Figures

List of Tables

Table 1: Revision History

Date	**Developer(s)**	**Change**
10/19/22	Max Turek Sam Nusselder Ryan Were Peter Minbasian David Bednar	Initial Draft
04/05/23	Max Turek	Removed some security requirements and updated some failures in the FMEA table

1 Introduction

This document is the Hazard Analysis for StoneCap Solutions - Smart Serve. Smart Serve is an autonomous bartending robot that aims to streamline the process of a customer ordering a drink up to them receiving it. The system would automate the tasks of taking customer orders, making the drinks, and alerting the end user when the drinks are ready. This would result in a system that creates consistent, accurate and timely drinks while avoiding unnecessary spillage.

2 Scope and Purpose of Hazard Analysis

The scope of this document is to conduct a Hazard Analysis on the proposed Smart Serve System using a Failure Modes and Effects Analysis (FMEA). We aim to identify possible failures, their modes, effects, and causes. Knowing these, we will be able to recommend actions to mitigate these hazards.

3 System Boundary

The boundary of the system will include a variety of different components that work together to create our autonomous drink creator called Smart Serve. They will consist of :

1. The physical hardware that makes up the autonomous bartending system can be divided into two main sections:
    - The physical frame that encapsulates the system
    - The computer, pumps and tubing
    - The drink ingredients
2. The users and/or operators phone used for the web application
3. The web application both front and back end which is used for users and operators to interact with the system
4. The container used to house the cocktail

All the hardware of the system excluding the WiFi network and the users phone, are the responsibility of StoneCap Solutions. All these systems work together to create the overall system boundary profile of Smart Serve for every use case.

4 Definition of Hazard

As defined by Nancy Leveson's work a hazard is a condition, property or state of a system coupled with a state in the environment that has the potential to cause harm or damage.

5 Critical Assumptions

Critical assumptions of the system include:

- Smart Serve is not intentionally tampered with or physically damaged by anyone
- Smart Serve is set up on a well balanced surface that users aren't able to easily knock over
- All people who have access to the system are of legal drinking age
- All drinking containers used with the system are made of plastic
- Internet service within the system environment is assumed to be working consistently at high-speed
- All containers are filled with the drink specified in the Web App

6 Failure Modes and Effects Analysis

The following is a table depicting failure modes and effects analysis (FMEA) table:

6.1 Hazards Out of Scope

Hazards out of scope will include:

- The physical location of a bar or restaurant environment
- The user's mobile device to connect to the web application and works as intended
- Human behaviour from the result of intoxication or alcohol use

6.2 Failures Modes and Effects Analysis Table

Failure Mode and Effects Analysis						
Design Function	Failure Modes	Effects of Failures	Causes of Failures	Recommended Action	SR	Ref.
Pouring drinks	Over pouring of alcoholic ingredients into drink	User could become intoxicated or fall ill	a. Pump malfunctions b. Web app sends wrong information	a&b. Add a flow-meter to sense if the amount of liquid dispensed is as expected	ODR11	H1-1
	Under pouring of ingredients	Drinks would be made with much less volume than expected, or have an incorrect mix ratio	a. Refer to H1-1a b. Leak in the lines liquids are being pumped through	a. Same as H1-1a b. Sense that this error is occurring and send a notification to the operator so a new line can be swapped into place	ODR11	H1-2
	System dispenses improper drink ingredients	User could become ill	a. Software sends the wrong drink order	a. Notify operator of issue, and run our test suite to validate drink orders	ODR11	H1-3
	Cup is misaligned	Water could spill in the machine, on the user, or on the table	a. User does not place glass in machine correctly	a. Clean up mess and dry machine	ODR11	H1-4
Hardware of System	Failure of electrical components	Undefined System behaviour would result	a. Damage to smart serve could loosen components, or a spill/leak as described above	a. Notification to web app with an error message corresponding to the component failure	ODR14 ODR15	H2-1
	Front panels for chassis are not water tight	Damage to key components can result in system failures, i.e. short circuiting	a. Spillage of internal or external liquids of the system may be able to permeate into key electrical/hardware components	a. Use an epoxy to seal key areas that spills are likely to occur in that lead to electrical components of the Smart Serve System	ODR14	H2-2
	Smart Serve gets bumped into	Damage to the chassis of Smart Serve and other mechanical/electrical components may result	a. Smart Serve is at a risk of being pushed off of the surface it is sitting on	a. Add a rubber mat to the bottom of Smart Serve to increase its grip b. Add mounting e to Smart Serve so that it may be screwed into place	ODR15	H2-3

Table 2: FMEA for Smart Serve System.

Failure Mode and Effects Analysis						
Design Function	Failure Modes	Effects of Failures	Causes of Failures	Recommended Action	SR	Ref.
Web Application	User is given operator privileges	User can access all information on drink ingredients and user info	a. Authentication error	a. Operator is notified, who will then disable the web app. and remove permissions for that user	ODR13 ODR2	H3-1
	User cannot login	User is unable to order drinks	Login credentials do not match what is stored in the database	a. Reset user credentials	ODR12	H3-2
	Queue of drinks is reset	Ordered drinks are not made by Smart Serve	Operator accidentally clears all orders	a. Reset to old database	ODR3 ORD6	H3-3
Ordering Drinks	QR code is unable to be scanned	The user will not be able to order a drink using Smart Serve	a. QR code surface gets damaged	a. Add a link underneath our QR code that leads to the web app b. Same as H4-1a	ODR1	H4-1

Table 3: FMEA for Smart Serve System.

7 Safety and Security Requirements

Note: New Safety Security Requirements not found in Version 0 are **bolded**

7.1 Ordering Drinks

ODR1: User can scan QR code launching smart-serve web app

ODR2: User can access the menu and select drinks to order

ODR3: User can view place/time remaining for the drink to be made

ODR5: User is notified if drink ingredients are out of inventory

ODR6: User is notified when drink is done

ODR8: Operator is notified if drink ingredients are out of inventory

ODR9: Operator inputs all ingredients available for drinks into the web app

ODR10: Operator inputs dispenser location of each ingredient into web app

ODR11: User's drink is the same drink they ordered on the app

ODR12: User can login successfully into the app

ODR13: User has user permissions

ODR14: Electrical components with high exposure to liquids are separated from liquid

ODR15: Have a robust and durable architecture/components

8 Roadmap

Throughout the course of the project, the hazard analysis will be an important tool that will be used to mitigate any risks and prevent failures of design components. Although there is a possibility that not all source of risk can be or will be mitigated by our final revision, it is important that level of risk assessed is within our tolerable limits. The project will plan on implementing all safety requirements listed above given the time constraints.