Hazard Analysis
Mechtronics Enigeering

Team 32, Wingman, SmartVault
Edward He
Erping Zhang
Guangwei Tang
Peng Cui
Peihua Jin

2022-10-19

Table 1: Revision History

Date	Developer(s)	Change
2022-10-19	Edward He, Erping Zhang Guangwei Tang, Peng Cui Peihua Jin	Revision 0
2022-12-22	Edward He, Erping Zhang Guangwei Tang, Peng Cui Peihua Jin	Revision 1.0, change the structure of the Hazard analysis document, easy to follow and understand
2022-04-01	Edward He, Erping Zhang Guangwei Tang, Peng Cui Peihua Jin	Revision 1.1, fix the content to match with other documentations

Contents

List of Tables

1 Introduction

This document describes the components making up the system and identify the possible hazardous behavior that could cause functional issue and safety problem. The Failure Modes and Effects Analysis method are being used in this document to clearly identify possible hazardous behaviors and the recommended actions that could be done to reduce the risk level. The system is meant to be implemented to help people locate items they have difficulty remembering. The mean function of this system are object recognition and item tracking which is used to satisfy daily-life need instead of industrial level. Safety requirement is crucial to be satisfied in the case users are considered to be non-professional. In the follow sections, all components of the system and hazards caused by the failure will be taken into consideration and methods can be applied in each case to solve the issue will also be clarified.

2 Scope

The scope of this hazard analysis document is to include all potential hazard relating to both hardware and software component of the project.

3 Component Overview

The project can be divided into five different main components. Those components are listed in the paragraphs below.

3.1 Movement of Camera

A stable and accurate motorized camera mount is necessary for the movement tracking. The servos need to move in a appropriate speed and angle in order to make the camera capture the best view of both objects and user.

3.2 Human Body Detection

A good detection method should be used so that the human body can be detected by the program in the images provided by the camera. The movement of the human body should also need to be detected to help the camera to judge its angular position.

3.3 User Interface

This component provides a communication layer between the system and the user through a computer app.

3.4 File Transfer and Storage

A fast and accurate data flow is the cornerstone for a system to be able to work properly and meet and requirements. The design and implementation of this module is playing a major role in the whole system design.

3.5 Objection Detection

This system is responsible for detecting any moving object in the area and identifying each object with unique set of characteristics. The is the main logical system for SmartVault to help locate a "lost" item.

4 Critical Assumptions

Critical assumptions that are made are:
CA1: Camera is mounted in a safe environment.
CA2: The computer device deploying SmartVault is in good condition.

5 Hazard Analysis

5.1 FMEA Worksheet

Failure Mode and Effects Analysis							
Components	**Failure Modes**	**Causes of Failure**	**Effects of Failure**	**Severity**	**Recommended Actions**	**SR**	**Ref**
Movement of Camera	Servo motor overload	Servo gear or components stuck	Motor overheat and damage	Strongly High	Lubricate the parts when hear uncommon noise	SR1	H1-1
	Short circuit	Liquid spill	The camera stop moving, and the whole system may stop working	Strongly High	Need technician to repair and have protection employed.	SR8	H1-2
	Unstable connection	Loosen connection during rotation	Whole system stop working, cannot tracking new objects	High	Unplug the connections and plug in again then restart the whole system	SR2	H1-3
	Risk of falling	Loosen assembly	The parts will disassembly and may cause injury	Strongly High	Concern about any abnormal movement or noise of the camera, technician may needed depend on situation	SR3	H1-4
	Abnormal rotation speed of camera	Caused by the control algorithm error	High	System will lose the tracking of user and objects	Restart the system	SR1	H1-5

Table 2: FMEA Table Part 1

Failure Mode and Effects Analysis							
Components	**Failure Modes**	**Causes of Failure**	**Effects of Failure**	**Severity**	**Recommended Actions**	**SR**	**Ref**
Human Body Detection	Human body detection failure	a. Detection method Failure b. Wrong Human Body Detected c. Wrong postures of human body	a. Wrong position description of the objects	High	a. Restart the program b. Compare detected body with human body database stored inside the system	SR4	H2-1
	Body movement detection failure	a. Detection method failure b. Wrong movement detected	Hard to associate movement of objects with movement of human body	High	a. Restart the program b. Rejudging movement zone around the human body	SR3	H2-2
User Interface	App closes unexpectedly	Host device loses power, or Crash due to instability	Current progress is lost	High	a. Store unsaved data locally on user's device	SR9	H3-1
	User cannot log in to the app successfully	User's credential is unmatched	User is unable to use the system	High	a. Reset user's credentials	SR5	H3-2
	An unauthorized user logs in as a privileged one with high-level access	Authentication issue	User could view or modify data even he/ she is not allowed	Strongly high	a. Fix the account permission and undo changes made by unauthorized user	SR10	H3-3

Table 3: FMEA Table Part 2

Failure Mode and Effects Analysis

Components	**Failure Modes**	**Causes of Failure**	**Effects of Failure**	**Severity**	**Recommended Actions**	**SR**	**Ref**
File Transfer and Storage	Overflow	Files of frames are stored without size restriction	Program crash	High	Set a strict time period for the camera to capture picture for each task	SR6	H4-1
	Mismatch	Object information are not collected completely	Inaccurate behavior done by the system	Medium	Fist ensure the functionality of camera is in good condition then re-enter information about the object	SR6	H4-2
	Miss time requirement	Too much items in one frame and takes the program longer time to proceed	Long time delay of the system behavior	Medium	Increase search frame and prioritize the assigned area	SR7	H4-3
Object Detection	Connection lost with camera live feed	a.Temporary internet lost b.Camera system faults	a.There will be no video frames for SmartVault to process and monitoring object movement b.Same as H5-1a	High	a.System output error message to user and retry connecting b. Refer to H1-3	SR2 SR9	H5-1
	Object detection faults	a. Unable to detect moving object b.Unable to uniquely identify an object (sharing all characteristics with two or more recorded item)	a.SmartVault will not be able to update the specific item's new position b. same as H5-2a	High	a.Well rehearsed image processing and detection method will be implemented to mitigate the chance of this event b. Refer to H5-2a	SR3 SR4	H5-2

Table 4: FMEA Table Part 3

6 Safety and Security Requirements

6.1 Safety Requirements

6.1.1 SR1

The device will stop if the motor is overloaded or has an abnormal rotation speed.
Rationale: It should be able to set a maximum and minimum speed for the motor. As long as the speed exceeds the range, send an error and auto adjust the speed.
Associated Hazards: H1-1, H1-5

6.1.2 SR2

The device will return an error message when the connection is unstable and tries to reconnect if possible.
Rationale: The user should be notified if the connection is unstable or loose. Users should not have to manually reconnect for every connection issue.
Associated Hazards: H1-3, H1-4

6.1.3 SR3

The device will return an error message if the object or human is unable to be detect or false detection.
Rationale: Detection may fail due to various reasons, and the user should be made aware of the issue. If detection is failed, system will be unable to find lost item.
Associated Hazards: H2-2, H5-2

6.1.4 SR4

The device will return an error message when the image processing is failed.
Rationale: Object identification may fail due to various reasons, and the user should be notified if the identification is failed, and notice the underlying cause behind it.
Associated Hazards: H2-1, H5-2

6.1.5 SR5

The device will return an error message if there is an issue with the user's credential.
Rationale: The user should be notified with the issue, and may attempt to reset the credentials.
Associated Hazards: H3-2

6.1.6 SR6

The device will return an error message if the database has an overflow or mismatch.
Rationale: The user should be notified with the issue, and may attempt to find a solution for the issue.
Associated Hazards: H4-1, H4-2

6.1.7 SR7

The device will return an error message when the database cannot proceed large numbers of items in one frame.
Rationale: The system should have an opportunity to slice the job into small pieces and redo the task again.
Associated Hazards: H4-3

6.1.8 SR8

The device should have short circuit prevention.
Rationale: Short circuit prevention is employed to protect electrical devices.
Associated Hazards: H1-2

6.2 Security Requirements

6.2.1 SR9

The device will save user's data periodically to the local file.
Rationale: In case of unexpected shutdown or loss of power. The user should be able to keep all information from the last step.
Associated Hazards: H3-1, H5-1

6.2.2 SR10

The device will return an error message if there is an authentication issue detected.
Rationale: The user should be notified that there is another user who logins in as a superuser. Then fix the account permission and undo all changes.
Associated Hazards: H3-3

7 Roadmap

The requirements outlined in this hazard analysis document will be implemented throughout the project's time line. The order of implementation of the failure listed in the following section will be determined by their severity, where higher severity failure would have higher priority.