Hazard Analysis
LiDart

Team 10
Jonathan Casella
Kareem Elmokattaf
Michaela Schnull
Neeraj Ahluwalia

Contents

1 Reference Material **1**
1.1 Abbreviations and Acronyms 1

2 Background **1**

3 Introduction **1**
3.1 Purpose 1
3.2 Scope 1

4 Assumptions and Definitions **2**
4.1 Assumptions 2
4.2 Definitions 2
4.2.1 Hazard 2

5 System Overview **2**
5.1 System Boundary 2
5.2 System Processes 3

6 Failure Modes and Effects Analysis **4**

7 System Requirements **4**
7.1 New System Requirements 5
7.2 Existing System Requirements 6

8 Roadmap **6**

A Failure Modes and Effects Analysis **7**

List of Figures

1 Setup and Installation Process Diagram 3
2 Operation Process Diagram 4

List of Tables

1 Failure Modes and Effects Analysis 7

Revision History

Date	Version	Authors	Notes
10\Oct\2022	1.0	Michaela Schnull Kareem Elmokattaf	Initial Release

1 Reference Material

This section records information for easy reference.

1.1 Abbreviations and Acronyms

Symbol	Description
A	Assumption
ALARA	As Low as Reasonably Achievable
FMEA	Failure Modes and Effects Analysis
GUI	Graphical User Interface
H	Hazard
POST	Power-On Self-Test
SR	System Requirement

2 Background

3D scanning is a versatile technology that is used across many industries, but its uses are often limited by high cost and complexity. LiDartaims to build a low cost, simple to use 3D scanning robot. A software suite will process data obtained from the robot and provide a user interface. LiDart's end product will be a wheel based mobile robot with all required sensors on-board that can be connected to over WiFi.

3 Introduction

3.1 Purpose

The purpose of this document is to identify and provide actions to eliminate or mitigate hazards associated with the setup and operation of LiDart. This document is intended to identify failure modes, effects, and causes related to system hazards. Recommended actions have been assigned to each failure mode and new requirements have been created to mitigate and eliminate hazards.

3.2 Scope

The LiDart system consists of a graphical user interface that allows the user to remotely drive a robot, initiate 3D scans, and download the final stitched 3D scan. Hazard analysis will be performed on all processes relating to the installation and operation of the LiDart system. Hazard analysis will not be completed for software components such as licensing, user authentication, security, and data storage as these considerations are not within the

scope of the project. Failure modes due to human performance factors are not included in this hazard analysis.

4 Assumptions and Definitions

4.1 Assumptions

The following assumptions were used in the development of this process FMEA:

A1: The LiDart system is in good condition. All maintenance activities have been properly completed.

A2: The LiDart system has not been damaged or modified by the user.

A3: The user will follow operating instructions as provided in the user manual.

4.2 Definitions

4.2.1 Hazard

The definition of a hazard used throughout this document is based on Nancy Leveson's work. A hazard is defined as any property or condition of a system coupled with an environment that has the potential to cause harm, damage, or adverse effects.

5 System Overview

The LiDart system is a 3D scanning solution in the form of a mobile robot. The system includes location markers, a remote-controlled robot, and a graphical user interface.

5.1 System Boundary

Hazard analysis is performed on LiDart system, which consists of:

- The physical robot, including the hardware and firmware running on the robot
- Location markers
- The GUI application
- A WiFi network

The physical device running the GUI application and the environment surrounding the robot are not controlled by LiDart. Hazard analysis will not be performed on elements external to the system.

5.2 System Processes

The processes executed by the LiDart system can be broken into the following categories:

H0 General Failure Modes
Consists of the failure modes that may occur at any time.

H1 System Setup and Installation
Before performing scanning operations, the robot must be powered on, and communication must be established between the robot and the user interface over WiFi. A series of functional checks are performed after communication is established to ensure the robot is in an operational state. Furthermore, location markers must be installed. Figure 1 illustrates the setup and installation processes.

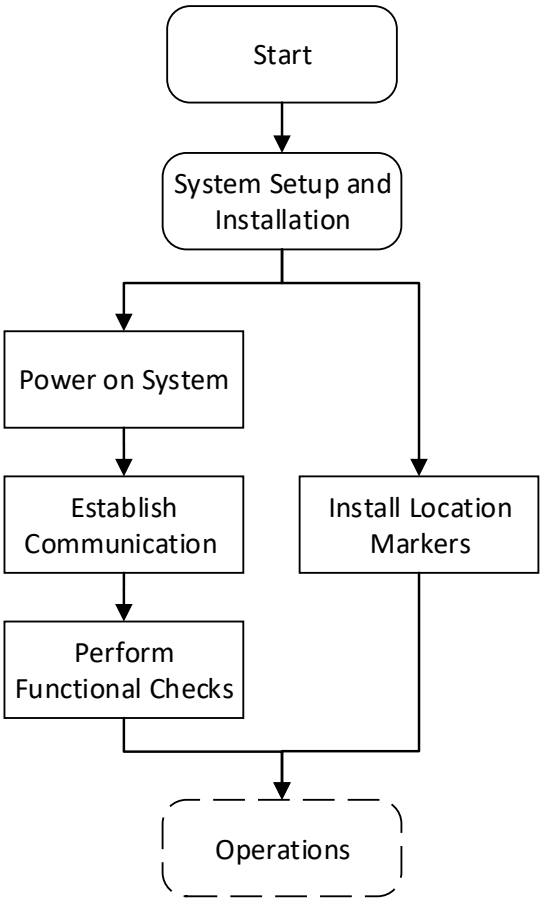

Figure 1: Setup and Installation Process Diagram

H2 Operation
While in operation, the robot must respond to inputs from the user and perform scanning operations. The system must perform state estimation, acquire sensor data, and output 3D models. Figure 2 illustrates the operational process logic.

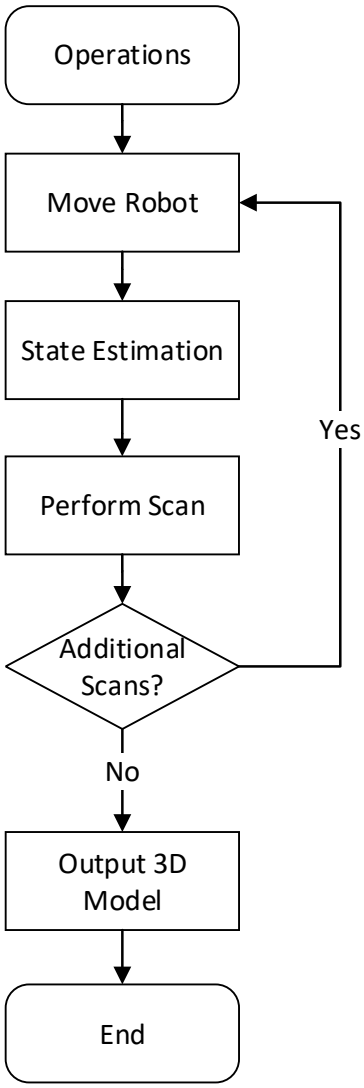

Figure 2: Operation Process Diagram

6 Failure Modes and Effects Analysis

A Failure Modes and Effects Analysis (FMEA) is used to perform hazard analysis of the LiDart system. The table is included in Appendix A.

7 System Requirements

New system requirements have been created based on failure modes identified in the FMEA. Existing system requirements that mitigate or eliminate hazards identified in the FMEA have been included for reference.

7.1 New System Requirements

SR1 The system shall prevent the robot from driving into an obstacle. An error message should be displayed if the user attempts to move the robot into an obstacle.
Rationale: Driving into an obstacle could damage the robot and/or the surrounding system. The system should prevent the user from driving the robot into an obstacle and have a means of notifying the user about the obstacle.

SR2 The system shall prevent the robot from moving during scanning operations.
Rationale: The data acquired by the sensor may not be correct if the robot is moving during data acquisition.

SR3 The system shall automatically save data from scanning operations.
Rationale: Data should be saved automatically without requiring the user to manually save it in case of unexpected events that cause data loss.

SR4 The system shall validate all user inputs on the GUI.
Rationale: Incorrect inputs may cause unexpected system behaviour.

SR5 The robot's electrical system shall use short circuit protection devices.
Rationale: Short circuit protection should be implemented as a safety precaution and to protect electrical devices.

SR6 An adequate number of location markers shall be used such that the robot can determine it's location in any position.
Rationale: The system must be able to perform localization in any position in order to stitch point cloud data.

SR7 The robot shall perform a power-on self-test (POST) to check the functionality of system components prior to operation.
Rationale: The POST will identify functional issues and mitigate downstream functional and performance issues.

SR8 The system shall display a warning if there is insufficient data acquired to create a 3D model.
Rationale: The point stitching algorithm requires sufficient data to create a 3D model. The accuracy of the model may decrease or a model may not be able to be created if there is insufficient data.

SR9 The system shall be able to retroactively correct stitched point cloud models given new data.
Rationale: If there is an issue with a certain section of a 3D model, the system should be able to correct the model given new data for that section. The user should not have to re-scan every section.

7.2 Existing System Requirements

SR10 The robot shall be placed in a safe-state if communication with the GUI is lost.
Rationale: The robot must not be able to move if communication with the user is lost.

SR11 All hardware and electronic components shall be easily accessible.
Rationale: Electrical components should be easily accessible for trouble-shooting and maintenance purposes.

8 Roadmap

New system requirements created from the hazard analysis will be implemented throughout the design phase of this project to eliminate and mitigate hazards. The principle of ALARA will be used to reduce risk and decide which requirements will be implemented.

A Failure Modes and Effects Analysis

Table 1: Failure Modes and Effects Analysis

Design Component	Ref.	Failure Mode	Cause of Failure	Effect of Failure	Detection	Recommended Actions	SR
General Failure Modes							
GUI	H0-1	GUI crashes	1. Poor software memory management and performance 2. Unexpected error handling	1. Communication with the robot is lost 2. The robot continues to move after communication is lost 3. Current scanning data is lost	The GUI closes unexpectedly	1. Validate all user inputs to the GUI 2. Place the robot in safe-state if communication is lost 3. Provide an auto-save feature to ensure data is not lost	SR4
System Power	H0-2	Power is lost	1. Battery died 2. Cables/wires become disconnected	1. The robot no longer functions and may be completely halted	The system will not power-on or powers down	1. Charge or replace the battery 2. Connect any disconnected cables/wires	SR11
	H0-3	Short circuit	1. Loose electrical connections 2. Damaged electrical components 3. Buildup or surges of electricity	1.Electrical components may be damaged 2. The robot stops working	Sparking and power system issues	1. Power off the robot and investigate the cause of the short circuit 2. Replace damaged components 3. Use circuit protection devices	SR5, SR11
System Setup and Installation							
Establish Communication	H1-1	Cannot establish communication with the robot	1. Incorrect network settings 2. Robot is not in the range of the network 3. Hardware/system power failure	1. Delay to investigate and fix network issues	Error message on the GUI when attempting to connect to a network	1. Move the robot to a location with a strong network signal 2. Check the network settings, and correct the settings if necessary 3. Reset the network 4. Power cycle the robot	SR11
Functional Checks	H1-2	Functional checks (e.g. check that all required devices are connected, sensors are calibrated) are not successful	1. Checks fail when they should pass	1. Delay to investigate and fix any errors	An error message on the GUI stating which checks failed	1. Display a warning on the GUI stating which checks failed 2. Investigate and fix system components that have failed	SR7, SR11
Operation							
Communication	H2-1	Communication between the GUI and the robot is lost	1. The WiFi signal is too weak 2. The WiFi signal intermittently cuts out	1. The robot will not be able to be controlled by user 2. Data loss	Error messages on the GUI that the robot cannot connect to a network	1. Keep the robot within the range of the WiFi signal	SR3, SR10
Movement of Robot	H2-2	The robot crashes	1. The robot does not respond to user input 2. The robot is not capable of stopping in time	1. Damage to the surrounding environment 2. Damage to the robot	Visual inspection	1. Display a warning on the GUI when the robot is getting too close to an obstacle 2. Use software controls to prevent user input from instructing the robot to drive into an obstacle	SR1
State Estimation	H2-3	The location of the robot cannot be determined	1. The location markers are not in the camera(s)' field of view 2. The object detection algorithms cannot identify the location markers 3. Inadequate number of location markers	1. The system cannot stitch point cloud data and create a 3D model	The GUI displays a message that the state cannot be estimated	1. Re-calibrate the system 2. Ensure enough markers are used 3. Adjust the position of the location markers so that they are visible to the robot 4. Move the robot to a new location	SR6
	H2-4	False positive that the state is correctly estimated	1. State estimation filtering error	1. The 3D model output is incorrect	Visual inspection of 3D model output	1. Automatically save data so that the scans performed prior to incorrect localization are not lost 2. Re-scan the affected area	SR3, SR9
Perform Scan	H2-5	Insufficient amount of data acquired	1. Not enough scans are performed	1. A 3D model cannot be created 2. The accuracy of the 3D model may decrease	An error message on the GUI stating not enough scans when the system attempts to process data	1. Perform additional scans	SR8
	H2-7	The data acquired is not correct	1. Sensor malfunction 2. The robot moves during data acquisition	1. 3D models are inaccurate	Visual inspection of 3D model output	1. Use software controls to prevent the robot from moving during scanning	SR2