Hazard Analysis
LiDart

Team 10
Jonathan Casella
Kareem Elmokattaf
Michaela Schnull
Neeraj Ahluwalia

Contents

List of Figures

List of Tables

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
SR	Safety 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 the safety of the system. Recommended actions have been assigned to each failure mode.

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 functionality 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.

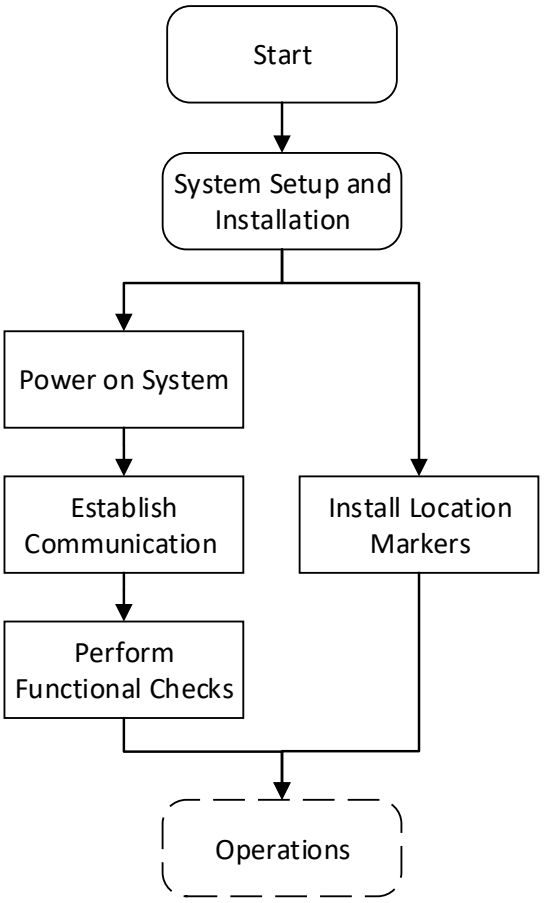

Figure 1: Setup and Installation Process Diagram

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.

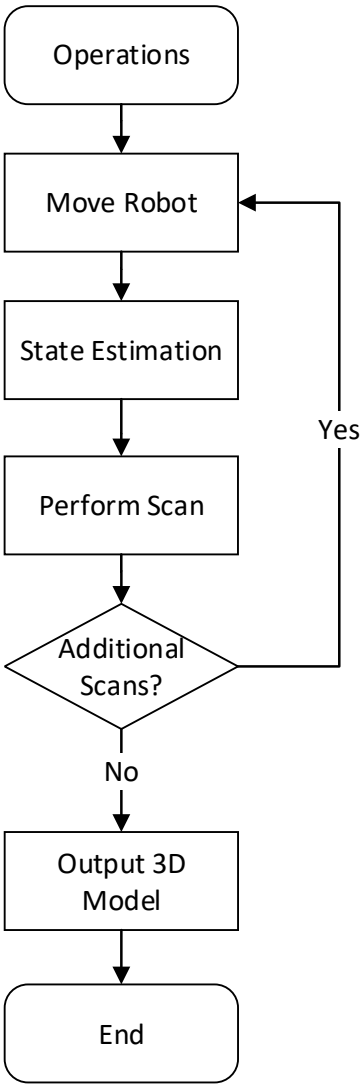

Figure 2: Operation Process Diagram

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 Recommended Actions and Safety Requirements

8 Roadmap

New safety requirements created from the hazard analysis will improve the safety of the LiDart system. Additionally, recommended actions from the FMEA 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 recommended actions will be implemented.

A Failure Modes and Effects Analysis Table

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							
Robot location calibration	H0-1	Robot can't calibrate its location	Robot can't start scanning	- Tags are not in visible range of the robot - Not enough tags are placed to calibrate the robot	Software checks for calibration confirmation	- Adjusting the placement of the tags to be visible by the robot - Ensuring enough tags are placed around the space	
GUI	H0-2	GUI crashes	- Bugs in software due to memory management - Performance issues	- Communication with robot is lost - Robot continues to move after communication is lost -Current scanning data lost	Visual inspection	- Provide auto-save feature - Place the robot in safe-state if communication is lost	
System Power	H0-3	Power is lost	- Damaged battery - Battery died - Short circuit	-Robot no longer functions and is completely halted	Visual inspection	- Charge the battery - Replace the damaged battery - Fix short circuit	
System Setup and Installation							
Establish Communication	H1-1	Cannot establish communication with robot	Network connectivity issue	Delay to investigate and fix network issues		Reset the network	
Functional Checks	H1-2	Functional checks (e.g. check that ll required devices are connected) are not successful	- Checks fail when they should pass - Checks pass when they should fail	Delay to investigate and fix error Potential downstream functional and performance issues			
LiDar Sensor Calibration	H1-3	Sensor doesn't scan the object	3D scanning can't take place	LiDar Sensor hasn't been calibrated properly	Software checks for calibration confirmation from sensors	Following steps to calibrate the sensor	
Operation							
Communication	H2-1	Communication between the GUI and the robot is lost	- Wifi signal is too weak - WiFi signal intermittently cuts out	- Robot will not be able to be controlled by user - Data messages are lost	Through GUI	- Keep the robot closer to the WiFi signal - Use networking protocols that check for missed messages	
Movement of Robot	H2-2	Robot crashes	- Robot does not respond to input - Robot is not capable of stopping in time	- Damage to the surrounding environment		- Display warning when the robot is getting too close to an obstacle - Use software controls to prevent user input from instructing the robot to drive into an obstacle	
	H2-3	Robot does not move as instructed by user input	Robot could end up in the wrong location	Communication strength not being strong enough (WiFi signals)	Software checks the strength of the signal between host and robot	Limiting robots movement to keep signal strength with the host	
State Estimation	H2-4	State cannot be estimated	- Markers are not in the camera(s)' field of view - Camera cannot identify markers -No encoder feedback Inadequate number of markers	System cannot correctly perform scanning operations	Software checks for calibration confirmation	- Re-calibrate the system - Ensure enough markers are used - Adjust the position of markers so that they are visible to the robot - Move the robot to a new location	
	H2-5	False positive that the state is correctly estimated	State estimation filtering error				
	H2-6	False negative that state has not been correctly estimated	State estimation filtering error				
Perform Scan	H2-7	Incorrect amount of data acquired	Insufficient amount of data acquired	Accuracy of output may decrease			
	H2-8	Data acquired is not correct	- Sensor malfunction - Robot moves during data acquisition	3D models are inaccurate		-Use software controls to prevent the robot from moving during scanning - Validate output of sensor data	