

# Hazard Analysis LiDart

Team 10

Jonathan Casella

Kareem Elmokattaf

Michaela Schnull

Neeraj Ahluwalia

# Contents

<b>1</b>	<b>Reference Material</b>	<b>1</b>
1.1	Abbreviations and Acronyms . . . . .	1
<b>2</b>	<b>Background</b>	<b>1</b>
<b>3</b>	<b>Introduction</b>	<b>1</b>
3.1	Purpose . . . . .	1
3.2	Scope . . . . .	1
<b>4</b>	<b>Assumptions and Definitions</b>	<b>2</b>
4.1	Assumptions . . . . .	2
4.2	Definitions . . . . .	2
4.2.1	Hazard . . . . .	2
<b>5</b>	<b>System Overview</b>	<b>2</b>
5.1	System Boundary . . . . .	2
5.2	System Processes . . . . .	2
<b>6</b>	<b>Process Failure Modes and Effects Analysis</b>	<b>4</b>
<b>7</b>	<b>Recommended Actions and Safety Requirements</b>	<b>5</b>
<b>8</b>	<b>Roadmap</b>	<b>5</b>
<b>A</b>	<b>Failure Modes and Effects Analysis Table</b>	<b>6</b>

# List of Figures

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

# List of Tables

1	Failure Modes and Effects Analysis . . . . .	6
---	----------------------------------------------	---

## 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 Effects Analysis
GUI	Graphical User Interface
H	Hazard

## 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. LiDart aims 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

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.

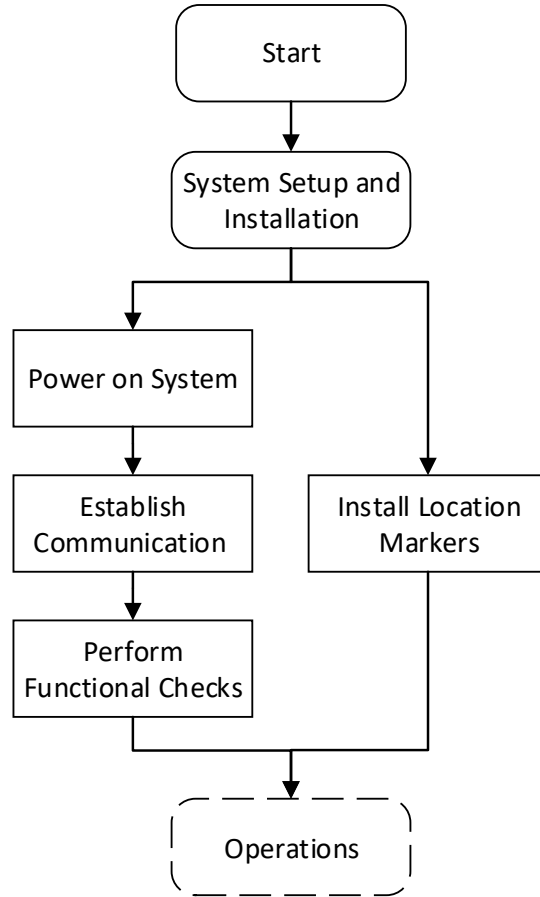


Figure 1: Setup and Installation Process Diagram

## 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.

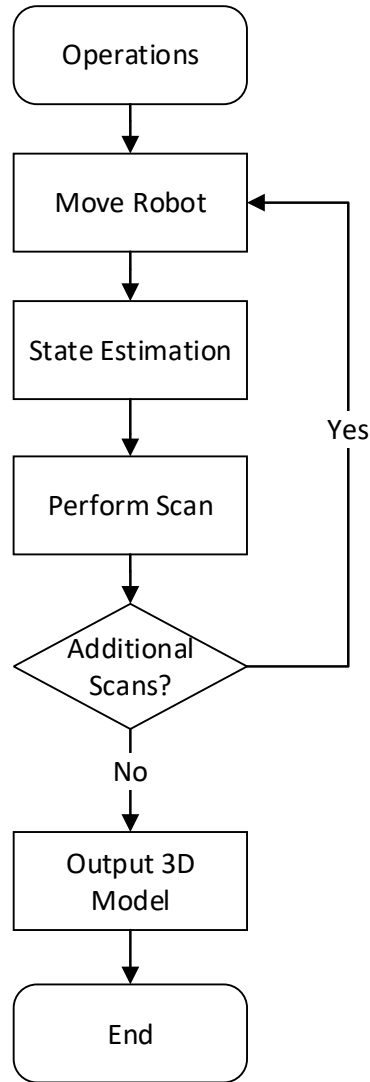


Figure 2: Operation Process Diagram

## 6 Process Failure Modes and Effects Analysis

A process 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 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	Effect of Failure	Cause of Failure	Detection	Recommended Actions	SR
General Failure Modes							
LiDar Sensor Calibration	H0-1	Sensor doesn't scan the object	3D scanning can't take place	LiDar Ssnor hasn't been calibrated properly	Software checks for calibration confirmation from sensors	Following steps to calibrate the sensor	
Robot location calibration	H0-2	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	
System Power	H0-3	Robot does not have any power	Robot can't operate	Damage to the power supply	System no longer functions and is completely halted	Damaged power supply is replaced	
System Setup and Installation							
Power On System	H1-1	- Robot does not power on	- Robot does not function  - Robot does not move	- Battery died  - Short Circuit	Through GUI	- Charging the battery  - Powering robot off	*Something to be inserted here* *Insert*
Establish Communication	H1-2	- Robot does not receive input - Robot does not give output	- Robot will not be controlled by user - User will not be able to assess the processing of the robot	- Wifi signal being too weak - Bluetooth signal is too weak	Through GUI	- Keeping robot closer to the WIFI signal - Keeping robot closer to bluetooth communication source	*Insert*
Functional Checks	H1-3						
Operation							
Move Robot	H2-1	Robot does not move as instructed by user input	Robot could end up in the wrong location	Communication strength not being strong enough (wifi or bluetooth signals)	Software checks the strength of the signal between host and robot	Limiting robots movement to keep signal strength with the host	
State Estimation	H2-2	Robot is not properly calibrated in	Robot will have the scan incorrectly	*Undecided*	Software displays location of robot	Robot to be recalibrated	