Hazard Analysis The Nursery Poject

Aaron Billones, billonea
Gillian Ford, fordg
Juan Moncada, moncadaj
Steven Ramundi, ramundis

October 19, 2022

Date	Version	Notes
2022-10-19	Juan Moncada, Aaron Billones, Steven Ramundi, Gillian Ford	Initial release

Contents

1 Introduction

This document is the hazard analysis of the Pot-Pulator. This machine will be built for Sheridan Nurseries, filling trays with pots, preparing them to be populated with soil and seeds, to reduce the manual labour of the workers at the farm. The hazard analysis will consider each part of the Pot-Pulator, including the respective tray and pot droppers, the sensor verification section, and the conveyer belt.

The definition of a hazard used in this document is any issue or property in the Pot-Pulator that will cause a risk to the ideal result of the system. In this system, most hazards will be concerning safety of the workers collecting the trays at the end of the conveyer, and the effectiveness of the verification system.

This document will include the Scope and Purpose of Hazard Analysis, System Boundaries and Components, Failure Mode and Effect Analysis, and Safety & Security Requirements.

2 Scope and Purpose of Hazard Analysis

The scope of this document is to identify the components of the Pot-Pulator that could have harmful consequences to the users or the results and reduce each risk to a level where the overall system will be safe and acceptable.

Hazards will be analyzed based on research of similar systems, and any specific hazards occurring throughout the development process of the machine.

3 System Boundaries and Components

The hazard analysis will be conducted based on the Pot-Pulator, which is restricted to the components below.

1. Conveyer belt
2. Tray allocation
3. Pot dropping
4. Verification system

The hazard analysis will be based on these critical elements of the system. The system boundary includes a conveyer belt moving the system along, tray allocation to place the trays on the conveyer, a pot dropper to place the pots into the trays, and a verification system to confirm the correct placement of the components.

The conveyer belt will be controlled by a sensor based on the other components. At the end of the process, the conveyer belt will bring the completed trays to the end of the line, to be collected by a worker. This will all be accounted for in the hazard analysis.

4 Critical Assumptions

There are no critical assumptions for this system.

5 Failure Mode and Effect Analysis

Component	Failure Mode	Effect of Failure	Cause of failure	Recomended action	SR	Ref
Tray Dispensing	Tray is not dispensed	Machine is unable to continue operation, tray may be damaged	(a) Tray stack software/hardware failure (b) Tray dispenser software/hardware failure (c) Parts failure	(a) Sensor will recognize if tray has not been dispensed, error message will be displayed and operator will be notified. (b) Refer to H1-1a (c) Refer to H1-1a		H1-1
	Trays placed incorrectly on conveyor	Tray is unable to move forward on conveyor, pot dispenser is unable to place pots correctly. May damage pots/trays	Tray dispenser software/hardware failure	Guiding rods will be placed on the conveyor to centre trays into correct position. If trays are unable to move forward, error message will be displayed and operator will be notified.		H1-2

	Trays dispensed are stacked, 2+ trays dispensed at once	Tray storage becomes out of sync with pot storage, may damage pots/trays	1. Parts failure 2. Trays loaded incorrectly	1. Sensor will recognize if multiple trays have been dispensed, error message will be displayed and operator will be notified 2. Operator will be trained to properly load trays into machine"	H1-3
	Tray dispenser damages tray	Tray is unable to hold pots and be sent for distribution (will depend on severity of damage to tray)	Quality issue in trays	Operator will be trained to perform 60 second visual check of Pot-pulator, trays, and pots before each refill to note and eliminate trays with any noticeable defects	H1-4
Pot Dispenser	Pots are not dispensed	Tray will be dispensed empty	Software/hardware failure	Sensor post pot dispensing will sense that the tray has not been populated, error message will be displayed and operator will be notified	H2-1

Conveyor	Conveyor does not move	Tray is unable to move to soil filling machine, trays may be damaged	(a) Software/hardware failure (b) Parts failure	(a) Sensor will recognize if conveyor is not moving for extended period of time, error message will be displayed and operator will be notified (b) Operator will be trained to perform 60 second visual check of Pot-pulator before pots and trays refill to note any damage to conveyor or belt wear	H3-1
	Conveyor does not stop when it is meant to	Pots are unable to be placed properly in trays, pots and/or trays may be damaged	Software/hardware failure	If tray is in view of pot dispenser, refer to H2-2a. If tray is not in view of pot dispenser, refer to H2-3	H3-2

	Trays slide on conveyor when conveyor is accelerating/deccelerating	Pots are unable to be placed properly in trays, trays may be damaged	(a) Software/hardware failure (b) Belt failure	(a) Sensor will recognize if conveyor is accelerating/deccelerating at a magnitude greater than specified, error message will be displayed and operator will be notified (b) Refer to H3-1b	H3-3
	Conveyor is unable to reach desired speed	Machine is unable to meet production standards	(a) Software/hardware failure (b) Parts failure	(a) Sensor will recognize if conveyor is not reaching desired speed for extended period of time, error message will be displayed and operator will be notified (b) Refer to H3-1b	H3-4

6 Safety and Security Requirements

6.1 Existing Requirements

The following are listed as non-functional requirements that can be found in the Software Requirements Specification (SRS) document (reference in square brackets). These requirements are related to the safety and security of the system which are necessary during operation.

SR1: All electrical equipment and electronics must be well covered and protected. The user must not have access to equipment. [NFR1]

SR2: All wiring must be tucked away and not accessible to avoid potential electrical failure. [NFR2]

SR3: All moving parts must be covered and protected. Moving parts should be covered to protect both the mechanism and the safety of the operator. [NFR3]

SR4: System must have both audible and visible signal outputs for each system status. [NFR7]

SR5: Conveyor system must not accelerate in a manner that would shift the position of the tray on the conveyor belt. A shift in the position of the tray could result in a misalignment and potential error. [NFR8]

SR6: System must have emergency cut off. In case of any emergency, this will trip off all power to the Pot-Pulator. [NFR11]

SR7: System must be able to locate and identify failures within each independent subsystem. [NFR12]

SR8: SR8: System must follow electronic component safety requirements. [NFR25]

6.2 New Requirements

The following are listed as non-functional requirements related to safety and security of the system that were formulated upon performing hazard analysis. Reference to the new requirements in the SRS are shown in square brackets.

SR9: System must be able to withstand a sufficient physical force to keep from falling over. [NFR26]

SR10: System must obtain a user login system or physical start key. [NFR27]

SR11: Clear physical emergency instructions and labels located on the device. [NFR28]

SR12: System must have surge protection. [NFR29]

7 Roadmap

There were some new non-functional requirements (safety and security) discovered, after performing hazard analysis on the system. The safety and security requirements that will be implemented in the future beyond the timeline of the capstone are SR7, SR10, and SR12. These requirements will be apart of a future implementation due to time-related and financial reasons. The remaining non-functional requirements related to safety and security will be implemented within the timeline the capstone project.