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 conveyor 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 conveyor, 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. Conveyor 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 conveyor belt moving the system along, tray allocation to place the trays on the conveyor, a pot dropper to place the pots into the trays, and a verification system to confirm the correct placement of the components.

The conveyor belt will be controlled by a sensor based on the other components. At the end of the process, the conveyor 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

It is assumed there will be no damage to the system by water, pressure, or similar external factors, considering the machine will only be used within the nursery in ideal conditions.

5 Failure Mode and Effect Analysis (FMEA)

Table 1: FMEA

Component	Failure Mode	Effect of Failure	Cause of Failure	Recommended 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	(a) SR4, SR7, SR9 (b) SR4, SR7, SR9 (c) SR4, SR7, SR9	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.	SR4, SR7, SR9	H1-2

	Trays dispensed are stacked, 2+ trays dispensed at once	Tray storage becomes out of sync with pot storage, may damage pots/trays	(a) Parts failure (b) Trays loaded incorrectly	(a) Sensor will recognize if multiple trays have been dispensed, error message will be displayed and operator will be notified (b) Operator will be trained to properly load trays into machine"	(a) SR4, SR7, SR9 (b) SR17	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	SR17	H1-4
Pot Dispensing	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	SR4, SR7, SR10	H2-1

	Pots dispensed are not flush with tray openings	Pots will be damaged by Pot-pulator or soil filling machine	(a) Software/hardware failure (b) Quality issue in pots (c) Quality issue in trays	(a) Sensor will recognize that pot is not flush with tray opening, error message will be displayed and operator will be notified (b) Operator will be trained to perform 60 second visual check of Pot-pulator, trays, and pots before each refill to note and eliminate pots with any noticeable defects (c) Refer to H1-4	(a) SR4, SR7, SR10 (b) SR17 (c) SR17	H2-2
	Pots dispensed when tray is not present	Pot storage becomes out of sync with tray storage	Software/hardware failure	Sensor will recognize if pots are dispensed without tray present, error message will be displayed and operator will be notified	SR4, SR7, SR10	H2-3

	Pots dispensed are stacked	Pots will be damaged by Pot-pulator or soil filling machine	(a) Parts failure (b) Pots loaded incorrectly	(a) Sensor will recognize if multiple pots have been dispensed, error message will be displayed and operator will be notified (b) Operator will be trained to properly load pots into machine	(a) SR4, SR7, SR10 (b) SR17	H2-4
	Pot dispenser damages pots	Pots are unable to be filled with soil and sent for distribution	Quality issue in pots	Refer to H2-2b	SR17	H2-5

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	(a) SR4, SR7, SR11 (b) SR17	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	SR10	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	(a) SR4, SR5, SR7, SR11 (b) SR17	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	(a) SR4. SR7, SR11 (b) SR17	H3-4

Verification System	Tray with less than 10 pots passses through verification system	Trays are unable to be sent for ditribution, trays are wasted, pot and tray storage will become out of sync	(a) Software/hardware failure (b) Verification sensors are obstructed/damaged	(a) Soil machine operator will be inspecting all trays leaving the soil machine. If a tray with less than 10 pots is identified, soil machine operator will be trained to manually stop Potpulator (b) Operator will be trained to perform 60 second visual check of Potpulator before pots and trays refill to note any obstructions/damage to sensors	(a) SR12 (b) SR17	H4-1

	Verification system does not stop machine process when required to	Trays are unable to be sent for distribution, may cause damage to trays	(a) Software/hardware failure (b) Verification sensors are obstructed/damaged	(a) Refer to H4-1a (b) Refer to H4-1b	(a) SR12 (b) SR17	H4-2

General	Person comes into contact with moving parts of machine	Potential risk of serious injury or death	(a) Operator wearing loose clothing or jewellery (b) Operator places hand in machine during operation	(a) Moving parts will be covered and protected. Emergency cut off switch will be implemented to cut all power to Pot-pulator. Physical emergency instructions and labels will be placed on the device. Operators will complete safety training before operating the Pot-pulator (b) Refer to H5-1a	(a) SR3, SR6, SR15, SR17 (b) SR3, SR6, SR15, SR17	H5-1

	Person comes into contact with electronics of machine	Potential risk of serious injury or death	Operator makes accidental contact with electrical wiring or electronics of machine	Electrical equipment and electronics will be covered and protected. Emergency cut off switch will be implemented to cut all power to Pot-pulator. Physical emergency instructions and labels will be placed on the device. Operators will complete electrical safety training before operating the Pot-pulator	SR1, SR2, SR6, SR8, SR15, SR17	H5-2
	Machine is subject to unexpected external force	Potential risk of injury to operator, may damage machine components, pots, or trays, may interrupt machine operation	Accidental bump from person/equipment passing by machine	Pot-pulator base will be reinforced to ensure it is able to withstand a reasonable unexpected external force	SR13	H5-3

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

SR9: The tray dispenser must stop when an error arises (verification failed, pot dispenser malfunction/empty, conveyor malfunction). [TDR6]

SR10: The pot dispenser must stop when an error arises (verification failed, tray dispenser malfunction/empty, conveyor malfunction). [PDR7]

SR11: The conveyor must stop when an error arises (verification failed, pot dispenser malfunction/empty, tray dispenser malfunction/empty). [CR5]

SR12: The verification must notify all other systems if verification fails, such that $n_{traysout} \neq 1$ *or* $n_{potsout} \neq 10$ [VR2]

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.

SR13: System must be able to withstand a sufficient physical force to keep from falling over. [NFR26]

SR14: System must obtain a user login system or physical start key. [NFR27]

SR15: Clear physical emergency instructions and labels located on the device. [NFR28]

SR16: System must have surge protection. [NFR29]

SR17: Operators must be properly trained in general safety, electronic safety, and system operation. [NFR30]

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, SR14, and SR16. 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.

8 List of Tables