Hazard Analysis

Group #12 – Botanica

SproutBot

Arun Mistry

Mina Demian

Nicholas Levantis

Usman Minhas

Table 1: Revision History

Date	Developer(s)	Change
October 27, 2023	Arun Mistry, Mina Demian, Nicholas Levantis, & Usman Minhas	Hazard Analysis Rev 0
March 25, 2024	Arun Mistry	Added Feedback Integration table along with comments. Added unique IDs for all Hazards Modified all Hazards to follow feedback, eliminating mention of manual control

Table of Contents

List of Figures

List of Tables

Introduction

The purpose of this document is to identify the different components of our project, SproutBot, that could cause potential harm or loss to a system and identify their respective hazards. We will be using Fault Tree Analysis (FTA) to break them down further and identify strategies to mitigate them to an acceptable level.

Project Overview

SproutBot is a project aimed at users who want to or need to water house plants while they are away. In order to achieve that, a robot will be developed with a few major components. The robot shall have a movement system, the robot shall have a means of navigating through the environment to reach a plant, the robot shall have a watering mechanism to deliver water to the plant, and the robot shall have a companion application to serve as an interface for the user to control the robot when needed.

Definition and Purpose of Hazard Analysis

Conducting a hazard analysis in any engineering project, such as our project of developing a plant-watering robot, serves several critical objectives. A hazard analysis is a fundamental component of responsible engineering and a critical step in ensuring the safety, compliance, and overall success of a project. It is also meant to be a systematic and thorough examination of potential risks and safety concerns associated with the project, allowing us to address potential hazards, reduce risks, and ensure the project's safety and reliability. This Hazard Analysis serves quite a few different purposes.

Safety Assurance

Safety is important in any project. A hazard analysis helps identify, assess, and mitigate potential hazards and risks that can result in harm to users, damage to the robot, or environmental impacts. By addressing safety concerns early in the project, robust safety measures and safeguards can be designed to ensure that the robot operates without posing undue risks to users or the surroundings.

Risk Reduction and Management

Hazard analysis allows systematic assessment of risks. By understanding the likelihood and severity of potential hazards, resources can be allocated efficiently. This proactive approach reduces the likelihood of costly and time-consuming issues arising during or after project implementation.

Enhanced Reliability

By identifying potential failure points, vulnerabilities, and safety concerns, a hazard analysis can contribute to the overall reliability of the robot. It assists in designing redundancy, fail-safes, and robust safety protocols, enhancing the performance and dependability of the system.

Improved Project Planning

Hazard analysis is an ongoing process, and regular assessments during the project's lifecycle help in adapting to changing conditions and emerging risks. It supports better project planning and management, as resources can be allocated appropriately and safety measures can be implemented in a targeted and efficient manner.

Scope of Hazard Analysis

For the purposes of this document, the scope of hazard analysis will be limited to 4 major components. These components and their subsections are described below. The X within brackets stands for the hazard number within that specific subsection.

1. Robot **(HRX)** – This is the main actor that will be analyzed in this document. All other components can be considered to be supporting actors that the robot will interact with. The robot navigates the environment to reach a plant and provides water to it.
2. Plant **(HPX)**– This is the supporting actor that the robot directly interacts with due to its main functionality. The plant acts as the robot's target during movement and receives water from the robot.
3. Environment (**HEX)** – The robot must navigate to the plant, where the environment is what the robot has to navigate through. The environment plays an indirect role within the whole system as the robot must interact with it to navigate towards the plant.
4. Human **(HHX)** – This component includes the user and any person that may interact with the robot at any point. As the goal of the robot is to achieve autonomous navigation and operation, this component is interacted with the least, but is still important from the scope of a Hazard Analysis due to a Human being required for any special or unforeseeable circumstances.

System Boundary

With respect to the major components identified within the scope of Hazard Analysis, the system's boundaries must be defined to limit the scope of what will be investigated to relevant aspects.

1. **Internal Actors -** The main components of the system, and the system boundary for actors will be the robot and the different elements of it.
2. **External Actors -** The actors present outside the system boundary are the Plant, User (Human) and the environment. This document will still consider the interactions between the robot and the external actors.
3. **Movement Boundary -** The robot's operations will be limited within a single rectangular room for the purposes of this document. The maximum dimensions of the room can be considered to be safely within range of communication with the robot.

Critical Assumptions

When conducting the Hazard Analysis, we need to consider that some critical assumptions will always hold, which are given below.

- **Stable Power Supply to Components -** For the purposes of this document, we will assume that the power supply will be sufficient for all components the robot to function as expected.
- **Nominal Room Conditions -** The room can be assumed to have average room conditions, such as a standard room temperature, pressure, humidity, and any other environmental factors.
- **Minimal Connection Attenuation -** The connection between the robot and any other components it needs to communicate with, such as sensors and the companion application, should be considered to have enough power usually needed for steady communication.

- **Basic Obstacles -** The obstacles present in the environment will be similar to what can be found commonly in rooms, and they must not be complex or unusual. The terrain must also be mostly traversable between different points.
- **Similar Plant Pot Height -** The soil of plants being watered are assumed to be at a similar height, and there are no major obstructions between the robot and the soil when the robot is near the plant.
- **Plants Set Up by User -** We will assume that the plants are already set up with the necessary amount of soil and nutrients, and placed in an area with ample light. Thus, we assume that the only requirement for the plant will be water at regular intervals.

Robot

FTA

The major harms identified that can occur to the robot are as follows. The basic events of the FTA are mitigated under Mitigation Strategy, as shown in the FTA – Robot figure below.

- Water Damage to the robot
- Environmental Damage to the robot
- Electrical Damage to the robot
- Navigational Failure
- Communication/Connection Failure

Mitigation Strategy

HR1 **Water Leak** – Adding water resistant casing around the robot and insulating any connections would be an ideal way to mitigate this hazard.

HR2 **Improper Water Delivery** – Only allow water to flow or be delivered under very specific conditions, such as when it is at the plant's soil.

HR3 **External Fluid Spills** – Ensure that all external robot components are water resistant to some extent.

HR4 **Environmental Collisions** – Increase stopping distance between the robot and any obstacles it detects. If the environment can't be identified, and the robot is unable to navigate without colliding, alert the user through the companion app and prompt for assistance.

HR5 **Plant is Relocated** – Follow the signal of the signal emitter placed in the plant's pot. If no signal can be found, follow a pre-determined movement pattern ensuring obstacle avoidance and randomness. Alert the user if it can't find a route within a certain duration.

HR6 **Miscalculation of Position/Orientation** – Implement a negative feedback system for the movement to keep the robot directed towards the plant. Add more sensors to act as redundancy mechanism.

HR7 **Movement System Malfunction** – Usage of a rigid wheel system will help mitigate this issue, where the movement depends on multiple motors, acting as redundancy in case one fails.

HR8 **Unexpected Motor Output** – If the robot's expected movement does not match the actual movement, the user should be notified through the companion app for maintenance. The robot can also attempt to overcompensate on the damaged side, unto a predefined limit.

HR9 **Foreign Object Interference** – The robot should stop and alert the user if it is unable to move normally with the motors running.

HR10 **Robot Slippage** – The implementation of a track based movement system will increase traction and reduce the possibility of slipping.

HR11 **Navigation Failure** with Robot Movement – Improve the navigation software to reduce collision count. If collisions keep on being detected, stop the robot and alert the user through the companion app.

HR12 **Robot Unable to Move** – Alert the user through the companion app.

HR13 **Sensor Failure** – Implement several sensors to serve as redundancy, and implement different navigation routines with the use of different sensors.

HR14 **Tipping over Uneven Floor** – Use tracks and a large base to reduce the chances of tipping over. Alert the user if any tipping is detected.

HR15 **Tipping Over through Human/Pet Interactions** – Stop robot movement if any obstacle is detected to approach it. Alert the user if any tipping is detected.

HR16 **Battery Issues** – Inform the user about the battery levels through the companion app, and alert the user when the battery is low, for instance around 10%.

HR17 **Loose Connections within Robot** – Run a simple test at startup to ensure all components receive power and can communicate internally.

HR18 **Unauthorized Access to Robot** – Use a Login/Password system to prevent unwanted agents from accessing the robot.

HR19 **Loss of Signal** – Robot should follow the last schedule set by the user, and operate offline.

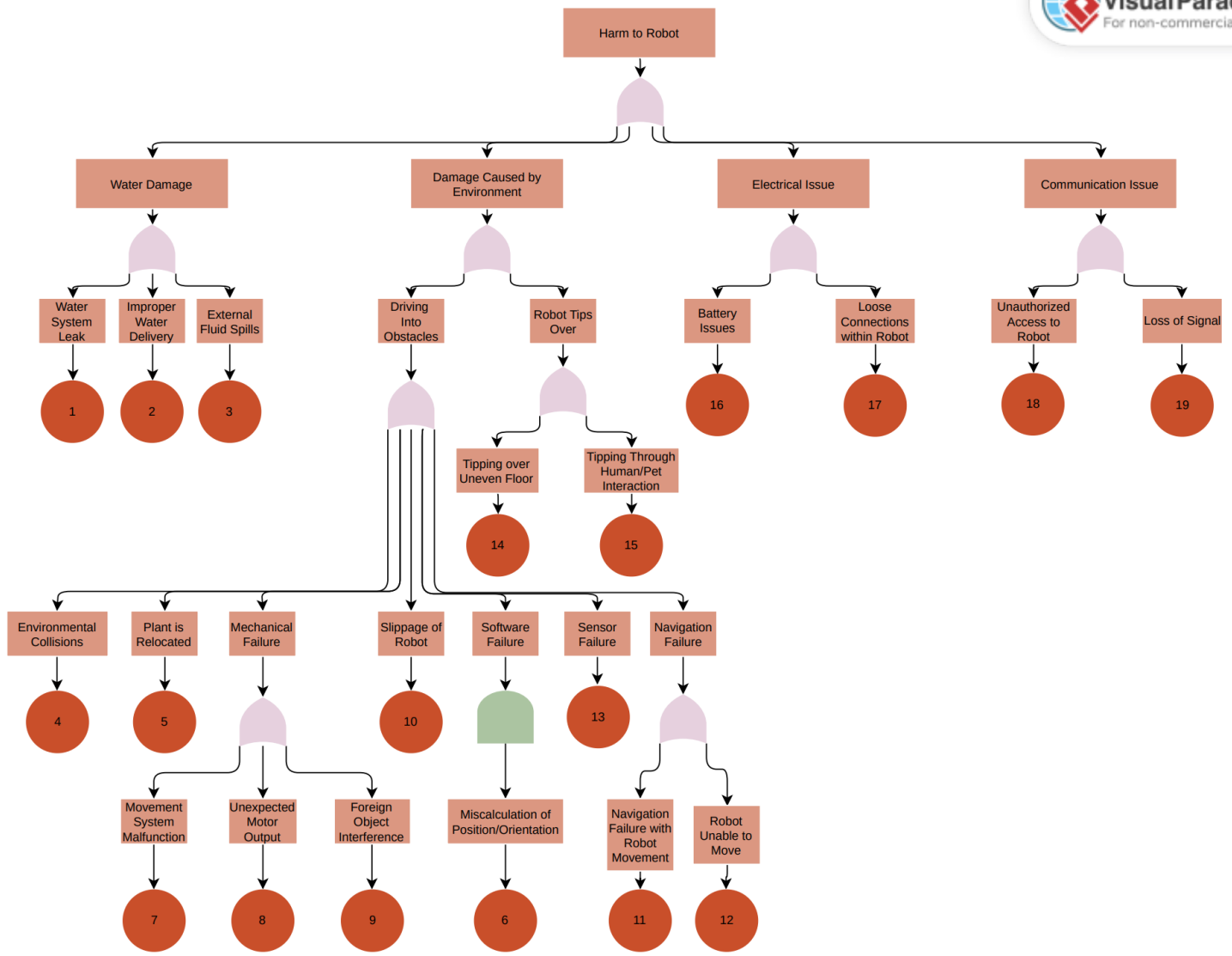

Figure 1: FTA of Robot

Plant

FTA

The major harms identified that can occur to the plant are as follows. The basic events of the FTA are mitigated under Mitigation Strategy, as shown in the FTA – Plant figure below.

- Water is not supplied correctly
- Collision of the robot with the plant

Mitigation Strategy

HP1 **Miscalculation of Water Needed** – A mitigation strategy would be to have additional sources of data required for this calculation. A sensor could be added to measure the amount of water coming out of the robot and into the plant.

HP2 **Incorrect Plant Identification** – For this hazard, signal emitters with unique IDs could be placed into each plant's pot. These could then be recognized by the robot and compared to saved information in its database on how much water it actually needs.

HP3 **Watering Schedule not Followed** – Implement software checks to confirm how often a specific plant must be watered and skip a plant if it doesn't not require water as frequently as other plants.

HP4 **Pump Does Not Stop** – A mitigation strategy would be to add a physical shut off mechanism, such as a valve.

HP5 **Pump Does Not Start** – There are 2 possible reasons water may not flow. If it is due to software, additional software checks could be implemented to see if the pump is supplied power to operate properly. If it is a hardware issue, the pump may be damaged, and the mitigation strategy here would be to replace the pump.

HP6 **Water Misses Target** – Assuming the robot is at the right plant, additional software checks can be implemented to confirm the robot's water delivering mechanism is aligned towards the plant's soil using different sensors. Add additional checks that ensure foliage is avoided. Warn the user if this process fails.

HP7 **Dead Battery** – The companion app must notify the user that the battery is about to be depleted at about 10% of the maximum capacity and require that the user recharges the battery.

HP8 **Robot Misses Target** – Alert the user and implement several software movement implementations to reorient and find the plant again.

HP9 **Robot Collides with Plant** – Increase the distance of detection between a robot and an obstacle, allowing the robot to stop further from an obstacle and prevent collision, before performing smaller, slower movements in order to reach the plant safely.

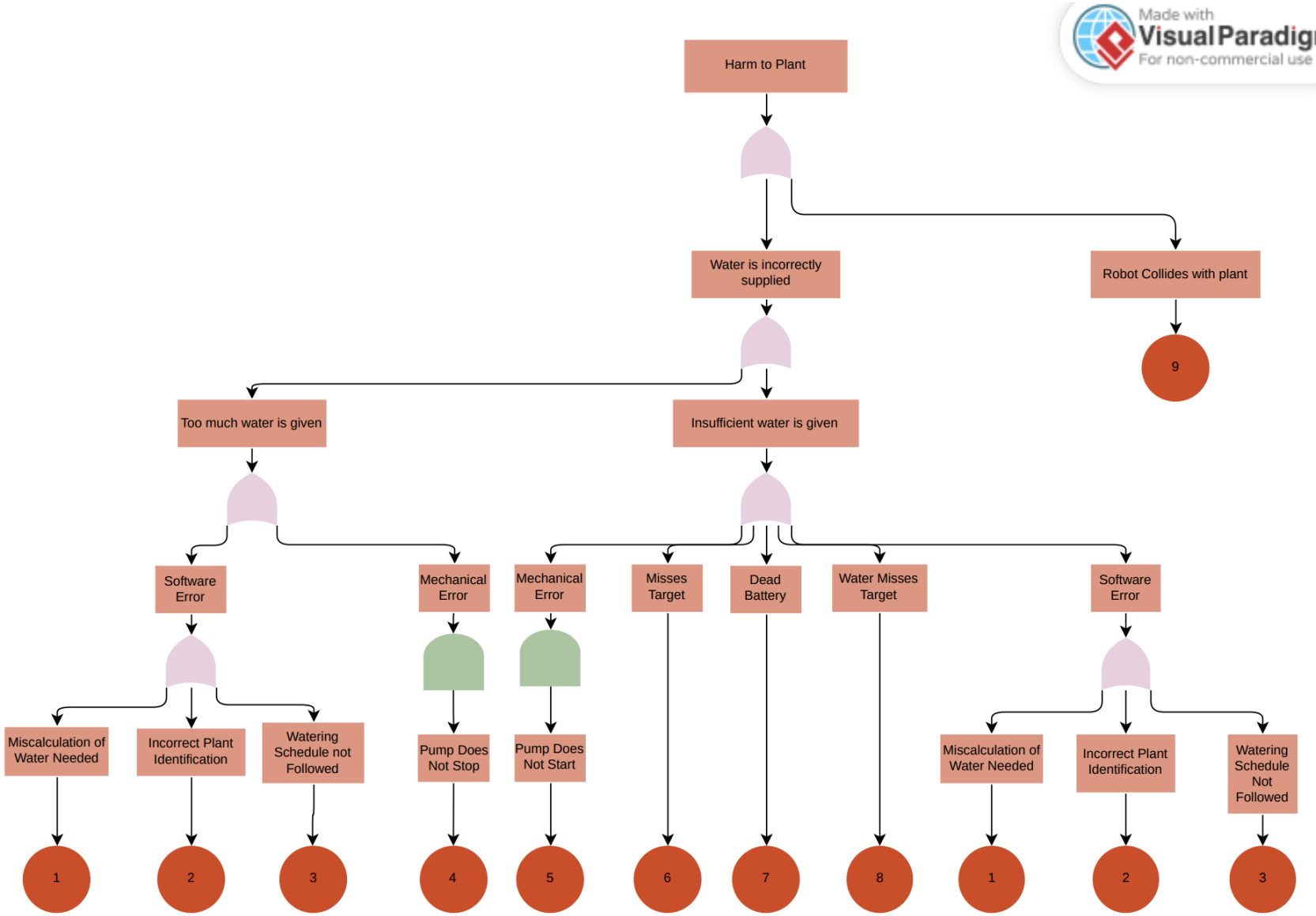

Figure 2: FTA of Plant

Environment

FTA

The major harms identified that can occur to the environment are as follows. The basic events of the FTA are mitigated under Mitigation Strategy, as shown in the FTA – Environment figure below.

- Collision Damage
- Water Spillage

Mitigation Strategy

HE1 **Robot Collides with Obstacles** – Increase the stopping distance between the robot and any obstacle it encounters, before it tries to navigate around the obstacle.

HE2 **Valve Software Failure** – Add additional software checks to ensure that the valve is fully closed and waits for a while before it starts moving.

HE3 **Valve Hardware Failure** – Add a secondary valve to act as a redundancy mechanism. If required, additional cameras can be used to detect if there is any water present on the ground along the robot's path.

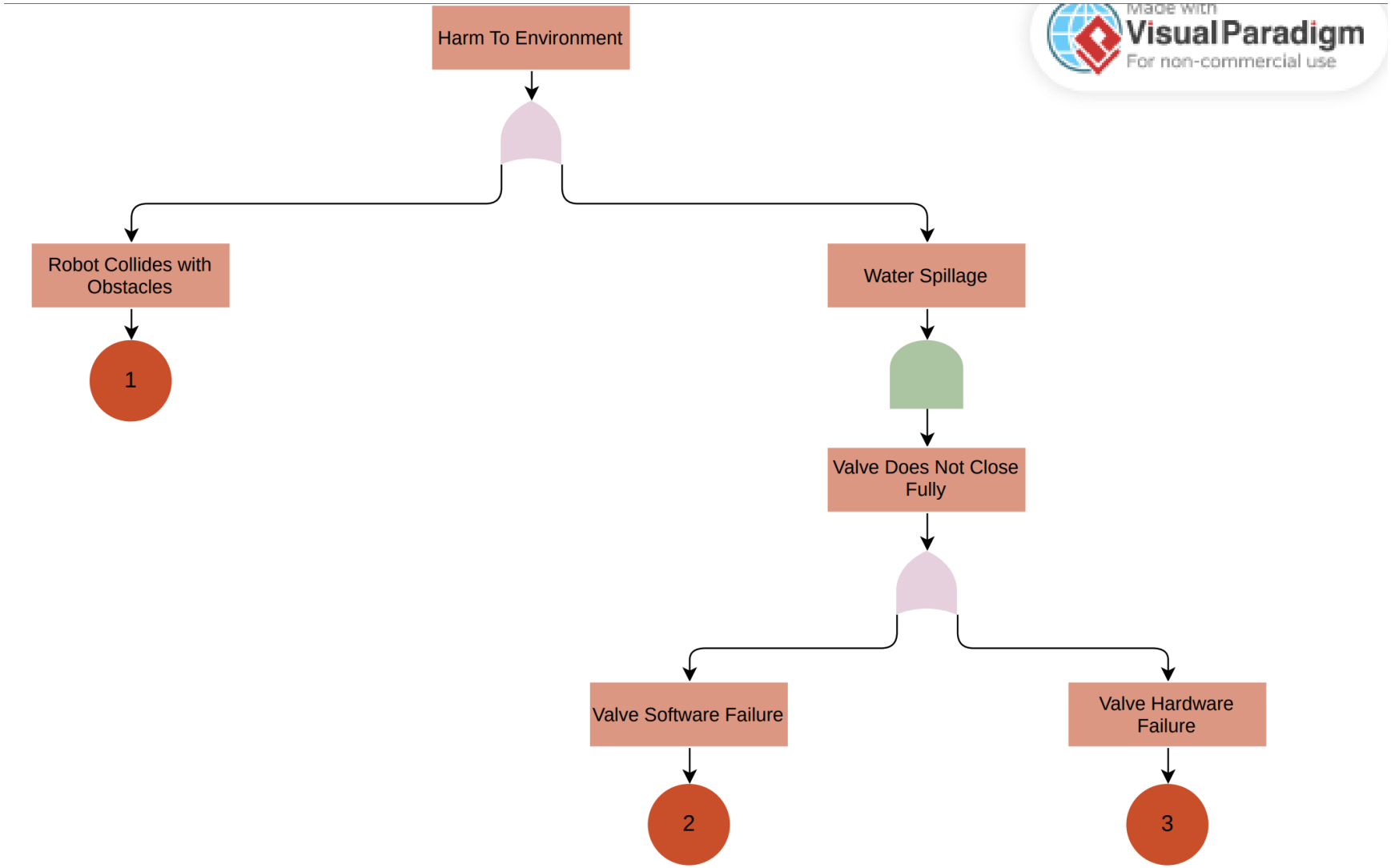

Figure 3: FTA - Environment

Human

FTA

The major harms identified that can occur to the environment are as follows. The basic events of the FTA are mitigated under Mitigation Strategy, as shown in the FTA – Human figure below.

- Tripping
- Water Spillage
- Loss of Control over Robot

Mitigation Strategy

HH1 **Robot in Human's Path** – A mitigation strategy would be to make the robot big enough to be easily visible from a distance, so the user can avoid it. Obstacle detection could also be developed to stop or reverse when a user is detected in its path. If humans are detected, a sound could be played during its movement in order to make the user aware of its presence

HH2 **Slipping on Water Spills** – The water delivery mechanism should only be enabled when it is located near a plant and aligned towards the soil. If the water delivery mechanism is triggered anywhere else accidentally, notify the user through the companion app.

HH3 **Electrical Shocks** – Hide away all electrical components within casing, ensuring that no internal components are exposed. Electrically insulating material such as electrical tape must be used around connections present outside any casing.

HH4 **Complex Companion Application** – Build the UI to be simplistic, with any complex features present under well-defined menus.

HH5 **Robot Stops Responding to Instructions** – Add a physical kill switch on the robot to shut it down.

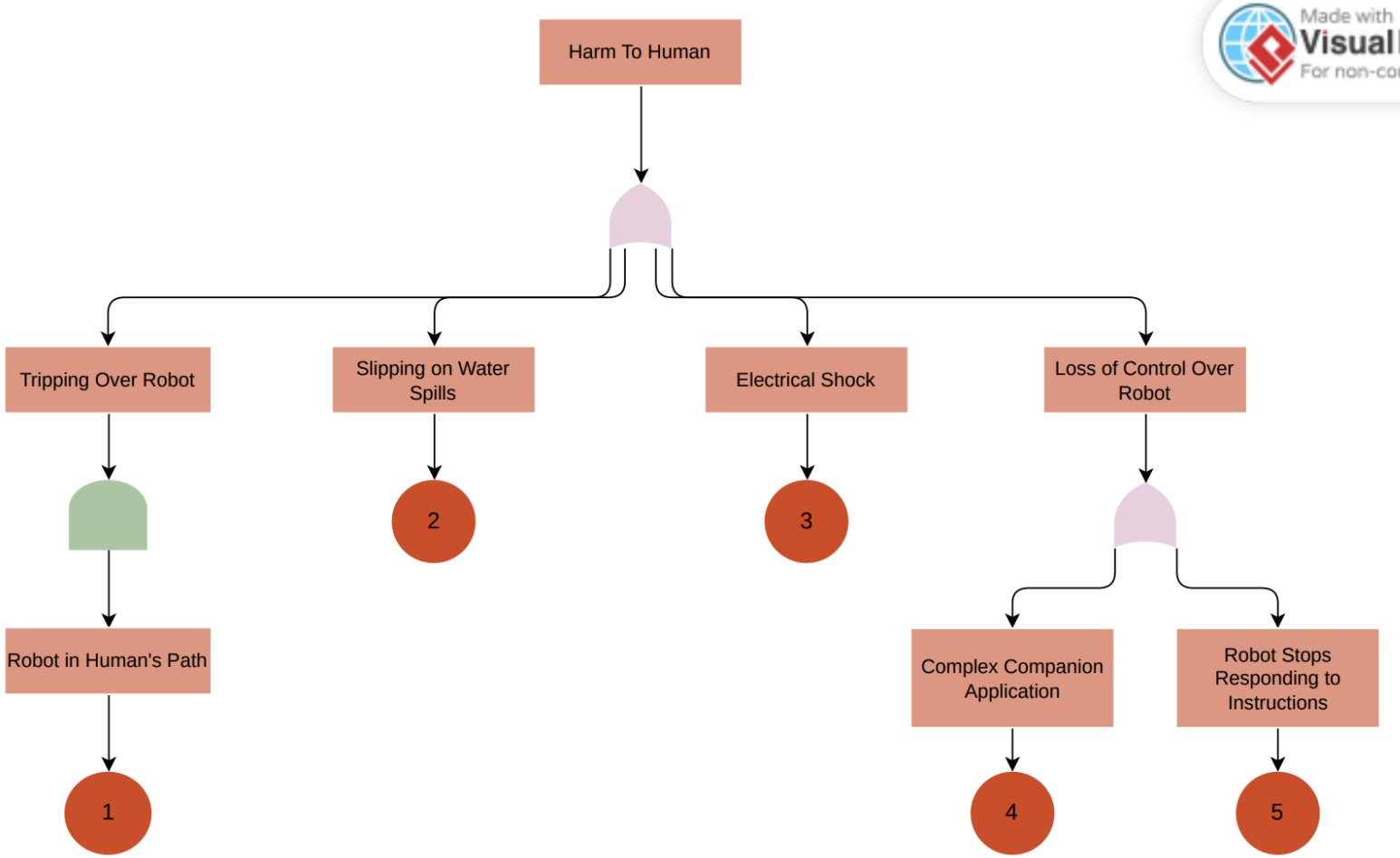

Figure 4: FTA of Human

Feedback Integration

TA Feedback	Integration Comments
Translate mitigation strategies to safety requirements using Unique IDs.	Unique IDs added to all hazards.
Possibility of plant foliage blocking soil when watering.	Added as a hazard and tackled in other documents.
Don't ask user to control robot, as system is designed to be automated. Safety requirements should focus on ensuring confidence about robot position.	Removed or reworded hazards mentioning manual control, and ensured automation is more robust.
Real world considerations on soil not absorbing water and pots having holes in bottom for water to drain out.	This would be good for future modifications but will not be considered right now. This would involve significant work in adding a pump at pot plate to remove water and pass onto robot.

Table 1: Feedback Integration