Hazard Analysis Report
MECHTRON 4TB6

Group 1, UWheeledChair,
Lisa Ji
Haoyu Lin
Yuntian Wang
Zichun Yan

November 7, 2023

Table 1: Revision History

Date	Editor(s)	Rev	Description
2023-10-26	Haoyu Lin, Lisa Ji Yuntian Wang, Zichun Yan	0	Created initial draft

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

This Hazard Analysis Report (HAR) has been prepared for the delivery robot project of Group 1. This project is to develop a fully-autonomous delivery robot based on the existing Wheeled Bipedal Robot (WBR) robot provided by the MacRobomaster Club. We are in charge of developing the software component of the project, while the hardware design and supply is handled by the MacRobomaster Team. The project will be mentioned as WBR in the following documents.

1.2 Purpose

This document describes the components of the system; identifies; assesses probability of potential hazardous behaviours that could cause functional failure or safety issues.

1.3 Scope

The scope of this HAR is to include all hazards only related to the software component of the WBR project, while the MacRobomaster Team is responsible for the hardware design and provision.

2 Components

2.1 Robot Posture and Movement Control

The robot is designed to move in various ways, including moving up ramps, bypassing or jumping over obstacles, moving across asymmetric terrains in altitude or friction behaviours. As the fundamental criterion of its movement control, it shall maintain balance of chassis; responsively follow the commanded trajectory; avoid obstacles dexterously.
The smoothness and reliability of the movements stands as a pivotal criterion to uphold the safety of its locomotion.

2.2 Inter-Module Communication

Ensuring the uninterrupted and less-delayed transmission of signals in between all system modules is of paramount importance. It is necessary for our robot to promptly execute commands and respond to sensor-derived information regarding the environment. Minimizing the response time of the control system necessitates optimizing data exchange procedures to mitigate any potential issues or disruptions that may impede the system's seamless operation.

2.3 Environment Sensing

Our robot will need to know what kind of environment it is in order to know where it is and where to go. Since the environment is changing all the time, a high frequency and low delay system is required to keep the robot updated in real-time, so it supports the importance of the previous component, IMC.

2.4 Path Finding and Tracking

This robot needs to figure out how it can get to the delivery location while following the provided map and shall log its path in the mean time.
Since our robot will be running on public areas, a great local and global obstacle avoidance will be necessary in our scenario. It will need to dodge human, animal, car, and any obstacle that originally did not show on the path finding algorithm for local obstacle avoidance.

2.5 User Interface

This component shall provide a comprehensive communication interface between system and user.

2.6 Delivery Security

This component will ensure only the authorized user will receive the package.

3 Critical Assumptions

Critical Assumptions (CA) are,

1. All mechanical components provided by the MacRobomaster Team are reasonably robust and reliable, and can almost behave like rigid bodies in the control analysis.

2. All electronic components provided by the MacRobomaster Team from market are reasonably robust and reliable.

   (a) All measurement instruments provides reasonably accurate results or results with appropriate uncertainty distributions.

   (b) All actuators act responsively and accurately according to instruction by controller. Delays, repeatability, accuracy, etc. are reasonable.

   (c) Cameras, LiDAR, Developer Boards are good to use in outdoor environment.

3. The overall robot assembly built by the MacRobomaster Team is reasonably robust and reliable.

4. Only people authorized by MacRobomaster Team is able to use our delivery robot.

4 Hazard Analysis

4.1 FMEA Worksheet

Table 2: FMEA Table

Components	**Failure Modes**	**Causes of Failure**	**Effects of Failure**	**Severity**	**Recommended Actions**	**SR**	**Ref**
Robot Posture and Movement Control	Unable to follow the instructed path	a. Terrain complexity out of controllable range of the system b. Battery and/or motor overheated after prolonged operation period c. Controller Failure	Robot cannot reach the target location	High	a. Bypass dangerous terrain b. Let robot rest for some time before tackling the tough terrain c. Extensively validate control system in different scenarios	SR1	H1-1
	Unable to maintain safe posture	a. Terrain complexity out of controllable range of the system b. Controller Failure	a. Vulnerable to system disturbance b. Potential damage to the cargo	High	a. Bypass dangerous terrain b. Extensively validate control system in different scenarios	SR3	H1-2
	Unable to reach safe posture	a. System properties changed, e.g. center of mass changed by cargo load b. Controller Failure	a. Cargo is prone to fall out of robot b. Cargo is held at improper inclination	Low	a. Implement dynamic adaptive control b. Extensively validate control system in different scenarios	SR3	H1-3
Inter-Module Communication	Intermittent loss of IMC	a. Electro Magnetic Interference (EMI) b. Low battery c. Crowded network	a. System being blind of environmental change b. System becomes open-loop or closed-loop with garbage data, thus divergent c. etc. (Depends on particular type of IMC)	Medium	a. Implement Emergency stop after prolonged offline status b. Implement redundancy check, e.g. CRC, and ignore corrupted data	SR2	H2-1

Continued on next page

Table 2 – continued from previous page

Components	Failure Modes	Causes of Failure	Effects of Failure	Severity	Recommended Actions	SR	Ref
		d. (Depends on particular type of IMC)					
	Corrupted IMC data	a. EMI b. Overloaded serial network	Same as H2-1	Medium	Same as H2-1	SR2	H2-2
	Invalid module response	a. Invalid request message data field b. Invalid order of request messages	Same as H2-1	High	a. Extensively validate control system in different scenarios b. Same as H2-1	SR2	H2-3
Environment Sensing	Unable to form surrounding view(point cloud)	Distance out of hardware specification or part broken	Unable to react according to environmental change	Strongly High	Emergency stop and send back error code to server for diagnostic.	SR1	H3-1
	Unable to perform object detection	Bad machine learning model or faulty information from camera or LiDAR	Unable to react according to environmental change and fail to dodge moving obstacle with higher priority	Strongly High	Emergency stop	SR1	H3-2
	Unable to localize itself	a. Image processing software failure b. LiDAR/IMU offline c. Dirty camera/liDAR	Unable to react according to environmental change	Strongly High	a. Sensor Fusion and emergency stop. b. Use more than at least 3 sensors together for localization. c. protection on Camera and LiDAR	SR6	H3-3
Path Finding and Tracking	Unable to find path	a. Software logic failure b. Unstable connection to server	Robot cannot reach target	HIGH	a. Stop right away and get back to original location b. Restrict area for robot can delivery to	SR4	H4-1

Continued on next page

Table 2 – continued from previous page

Components	Failure Modes	Causes of Failure	Effects of Failure	Severity	Recommended Actions	SR	Ref
	Improper selection of path	a. Communication failure with sensor b. Algorithm failure	a. Crash into obstacles b. Higher battery consumption c. Robot stop mid way. d. Robot could try to go under obstacle that it couldn't pass.	Strongly High	a. Change sensor mounting location on the robot b.add more sensors	SR6	H4-2
	Path logging failure	Server down, connection issue, or Software bug b. Lost historical data.	a. Lost track of robot on APP.	Medium	a. Store log locally	SR2	H4-3
	Unresponsive path planning	a. Software logic failure b. Insufficient Computational Power	Robot could run on undesired route	Strongly High	a. Restart program for re-calibration b. use at least 3 sensors to fuse and onboard processing c. Use soft padding around robot to avoid damage	SR4	H4-4
User Interface	App crash	Network issues in client side	information lost	High	store log information	SR2	H5-1
	Password transmission failure	Poor Network Connection	package locked	High	Have a special way to unlock the space(master key, disassemble package box)	SR2	H5-2
	Unauthorized access	Insufficient encryption and possible security check bypass.	Package lost or data leaking.	Strongly High	Set for the restriction of logging in and give permission only to limited user accounts or 2FA.	SR5 SR7	H5-3

Continued on next page

Table 2 – continued from previous page

Components	**Failure Modes**	**Causes of Failure**	**Effects of Failure**	**Severity**	**Recommended Actions**	**SR**	**Ref**
Delivery Security	Package theft	Inadequate Security Measures and high-crime geographical Location	The package is stolen from its intended location.	High	Use hard material for package box and alarm system with siren.	SR6	H6-1
	Robot theft	Inadequate Security Measures and high-crime geographical Location	The robot is stolen from its intended location.	High	Have GPS on the robot keep location updated	SR6	H6-2

5 Safety and Security Requirements

5.1 Safety Requirements

5.1.1 SR1

The device shall stop if there exists any unintended movements or loss of control.
Rationale: It should be able to set a detector for the device. As long as the movement exceeds the range, send an error and auto stop the device.
Associated Hazards: H1-1, H3-1, H3-2

5.1.2 SR2

The device shall try to reconnect and return an error message when the connection is unstable.
Rationale: The user should be notified if the connection is unstable or offline. Users should not have access to hardware.
Associated Hazards: H2-1, H2-2, H2-3, H4-3, H5-1, H5-2

5.1.3 SR3

The device shall rest or stop right away if the motor is overheated, and it should have sufficient battery to return to base.
Rationale: A temperature sensor and a CPU usage monitor should be set for the device. As long as the temperature or usage exceeds the range, send an error.
Associated Hazards: H1-2, H1-3

5.1.4 SR4

The device shall stop and recalculate path if the robot is on a wrong path or can not avoid obstacle.
Rationale: The robot shall stop right away if sensors have big disagreement on obstacle detection, then attempt to find a solution for the issue.
Associated Hazards: H4-1, H4-4

5.2 Security Requirements

5.2.1 SR5

The device shall reject unauthorized login.
Rationale: The user should be notified with the issue, and may attempt to reset the credentials.
Associated Hazards: H5-3

5.2.2 SR6

The device shall continuously send out GPS location.
Rationale: In case of theft or loss, the user should be able to know the location of the robot.
Associated Hazards: H3-3, H4-2, H6-1, H6-2

5.2.3 SR7

User Interface shall encrypt all data.
Rationale: In case of data leaking, UI shall encrypt all the data and only allow authorized user to access.
Associated Hazards: H5-3

6 Roadmap

The effects delineated within the hazard analysis document will be subject to thorough consideration, with a strong commitment to taking decisive actions aimed at reducing and eliminating the hazards throughout the course The prioritization of these actions will be determined based on the severity of each hazard, ensuring that the most critical issues are addressed as a matter of utmost importance.

A Glossary

CA Critical Assumptions. 5

CRC Cyclic Redundancy Check. 6

EMI Electro Magnetic Interference. 6, 7

HAR Hazard Analysis Report. 4

IMC Inter-Module Communication. 4, 6, 7

WBR Wheeled Bipedal Robot. 4