Hazard Analysis
MECHTRON 4TB6

Team 25, Formulate
Ahmed Nazir, nazira1
Stephen Oh, ohs9
Muhanad Sada, sadam
Tioluwalayomi Babayeju, babayejt

Table 1: Revision History

Date	**Developer(s)**	**Change**
10/12/2022	Ahmed	Added FMEA analysis
Date2	Name(s)	Description of changes

Contents

1 Introduction

A hazard is the combination of a system property with an environmental condition that can cause harm to the intended user.

Hazard analysis is a critical consideration in the design of all systems. When done correctly, hazards to the end user are identified and can be mitigated or eliminated completely. While it is not possible to guarantee the safety of a system, applying hazard analysis methods is a neccesary step in supporting the safety of the system.

Formulate's area of work combines hardware and software sub-systems and as a result, requires hazard analysis to obtain a comprehensive understanding of the overall system.

2 Scope and Purpose of Hazard Analysis

In this document, Formulate details the hazards a user can experience through the Failure Mode and Effect Analysis method. As a result, the group systematically outlined the hazards and measures that were considered to mitigate or eliminate the hazard.

3 System Boundaries and Components

The device that is referred to in this document is made up of 5 major components that hazard and failure analysis would have to be done for:

1. Hardware
2. Desktop Application
3. Database
4. Data Website Analytics
5. The Physical Device

Each component has there own system boundaries based on the software and hardware we use. Since this is the case we will have to design the system based on the type of the test that is required to be performed by the MAC Formula Electric Team. An example of this would be if the client had to test their motor at an operating speed we would choose hardware components that are within that temperature range to avoid any failure reading the data correctly or damaging the component.

4 Critical Assumptions

- The user understands the safety precautions of operating and working with a Formula Electric vehicle
- The user has a basic understanding of handling electrical and mechanical components
- The user aims to always correctly operate the testing device

5 Failure Mode and Effect Analysis

Component	Ref	Failure Mode	Effects of Failure	Cause of Failure	Recommended Actions
Hardware	H1.1	Sensor data is not sent to PC	Test data is not captured by our device	• Wi-Fi Module is broken • USB Device is not connected • Device is not connected to Wi-Fi network	Using the LCD display show the systems connectivity
	H1.2	System does not have power	Device is off and not operational	• Battery died • Power cables are disconnected • Too much current is drawn from Arduino	• Add a battery indicator to the screen to alert the user if the battery is low • Make the sensors get their power directly from the power source and not the arduino
	H1.3	Hardware falls off the mount	• Hardware device breaks/gets damaged • Sensors capture incorrect data • Potential injury to those in vehicle	• User didn't affix Hardware properly • Mounting mechanism failed	The mounting mechanism should give the user feedback when the device is mounted correctly
	H1.4	Display turns off	Cannot view the status of the device	• LCD display failure • LCD is improperly connected • Arduino is drawing too much current	
	H1.5	Threshold alert not displaying	User will not be notified	• Sensor failure • Refer to H1.4 • Threshold not set up by user in the Desktop App	
Desktop Application	H2.1	App cant see hardware device	Refer to H1.1	• Refer to H1.1 • COM Port is being used by another application	

	H2.2	Data from the hardware device is lost	Test results will all be lost	• Application suddenly closes during test • Hardware device disconnects from PC	Store last test data into local storage
	H2.3	Cannot view live data	User will not be able to see data during test runs	• Sensors are not connected • Refer to H1.1	
	H2.4	Data cannot be sent to database	Test results will all be lost and will not be viewable in the analytics platform	• Database failure • Connection failure • PC not connected to the internet	
Database	H3.1	Too much data is sent to the database	The database is getting overloaded with data causing it to crash or freeze	User submits too much data within a very short time period	Add a cool down timer after the user submits the data to the database so they wont be able to spam it constantly
Data Analytics Website	H4.1	User cannot login	User will not have access to dashboard	• User does not have an account • User's credentials don't match	
	H4.2	User cannot view the dashboard	Users cannot view KPIs of tests	• User does not have required permissions	
	H4.3	Data not being displayed		• Database failure • Authentication error	

6 Safety and Security Requirements

SR 1: The device should validate a connection between sensors, device, and application before starting measurements.

Rationale If the connections are not validated, then data might be lost as it never gets send to either the device, application and/or database.

Associated Hazards H1.1, H2.1, H2.2, H2.3, H2.4

SR 2: The device should give a warning indicating that battery is low after a certain time amount of usage.

Rationale If the battery dies during testing, measurement values will be lost as it is power source of the device.

Associated Hazards H1.2

SR 3: In order to send values to the database from the application, user must log into the application.

Rationale This ensures that only testers have the ability to send and write values to the database.

Associated Hazards H4.1, H4.2, H4.3

SR 4: Every user should have a login when accessing the data analytics website which would be the same login as the application's.

Rationale This ensures that only testers have view access to values on the website.

Associated Hazards H4.1, H4.2, H4.3

SR 5: The device should save a certain amount of values in case the connection to application fails during testing.

Rationale This ensures that the most recent data is not lost if there is a system failure.

Associated Hazards H2.2

SR 6: The device should have an audible click to indicate that the device has mounted on the vehicle correctly.

Rationale The audible click aids the user in mounting the device correctly to ensure that it does not fall off.

Associated Hazards H1.3

7 Roadmap

All these requirements will try be implemented during the course of the capstone. The safety and security requirements are important for a complete and safe testing device. As this is the case most, but hopefully all of them will be implemented but if we can not implement all of them due to our time constraint the ones essential to the design will be implemented while the others that only improve user functionality will be added towards the end.