Hazard Analysis
MECHTRON 4TB6

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

April 3, 2023

Table 1: Revision History

Date	Developer(s)	Change
10/12/2022	Ahmed	Added Failure Mode and Effect Analysis
10/13/2022	Stephen	Added Introduction and Scope
10/13/2022	Muhanad	Added Critical Assumptions and Safety Requirements
10/14/2022	Tioluwalayomi	Added System Boundaries and Roadmap
10/19/2022	All	General edits
04/02/2023	Ahmed	Added REV1 changes

List of Tables

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 Analytics Website

Each component has their 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 the car under specific conditions, we would choose hardware components that are within that temperature range to ensure data is read correctly.

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	Connection Failure	Test data is not captured by our PC	• The Wi-Fi module is broken • USB Device is not connected to PC • PC is not connected to the device Wi-Fi	Using the device's yellow LED to convey the system's 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 Power indicator to the device to alert the user if the device has power • 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 physical feedback when the device is mounted correctly
Desktop Application	H2.1	Application cannot read hardware device output	Refer to H1.1	• Refer to H1.1 • COM Port is being used by another application	Ensure that the COM port is open for communication

	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 live data during test runs	• Refer to H2.1 • Refer to H1.1	Device will default to record the entire test run and save the test data into local storage
	H2.4	Data cannot be sent to database	Test results will not be saved to the database and will not be viewable in the analytics platform	• Database failure • Connection failure between Desktop App and Database • PC not connected to the internet	Verify connection between desktop app and database to ensure data will be sent correctly
Database	H3.1	Database Overload	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 will not be able to spam test submissions
Data Analytics Website	H4.1	User cannot login	User will not have access to dashboard	• User does not have an account • User's credentials do not match	Redirect user to either create a new login or to reset their login
	H4.2	User cannot view the dashboard	Users cannot view KPIs of tests	• User does not have required permissions	User can request permission which needs to be approved by an admin

	H4.3	Data is not displayed on the dashboard	Refer to H4.2	• Database does not contain test data • Authentication error	Validate that the database contains data

Table 2: Failure Mode and Effect Analysis

6 Safety and Security Requirements

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

Rationale If the connections are not verified, 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 have a power LED indicating to the user if the battery is working.

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

Associated Hazards H1.2

SR 3: Every user should have a login when accessing the data analytics website.

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

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

SR 4: The device should save a certain amount of values in case the connection to the application fails during testing.

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

Associated Hazards H1.1, H2.2

SR 5: The device should have an audible click to indicate that the device and sensors have mounted correctly.

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

Associated Hazards H1.3

7 Roadmap

These requirements will be implemented during the course of the capstone. The safety and security requirements are important for a complete and safe testing device. Due to the time constraint we face, some requirements will take priority over others. Over the course of our capstone we will continuously update this document with any other hazards that might arise. We aim to mitigate all the hazards by the end of the term.