Hazard Analysis
Mechatronics Engineering

Team #1, Back End Developers
Jessica Bae
Oliver Foote
Jonathan Hai
Anish Rangarajan
Nish Shah
Labeeb Zaker

Table 1: Revision History

Date	**Developer(s)**	**Change**
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Contents

[You are free to modify this template. —SS]

1 Introduction

[You can include your definition of what a hazard is here. —SS]

2 Scope and Purpose of Hazard Analysis

3 System Boundaries and Components

The system consists of several components that make up the entire system

3.1 Battery/Power Management system

This component facilitates stepping down/up the source voltage from the battery to the necessary values required by different parts of the device. Moreover, it consists of a charge protection circuit for battery protection (Over-voltage and Discharge). Finally present is a battery level indicator that will generate an alert should the battery life fall below a certain threshold.

3.2 Sensor Array system

This component represents all the various sensors that will be used to collect the state information about the user. Also consists of various filters to facilitate smooth and accurate data collection.

3.3 Prompt generation system

This component handles all prompt generation, from the detection of when a prompt occurs, to its specific creation and finally its display on the screen.

3.4 Display System

This system manages all functionality of the device's display, such as prompt display, showing basic user feedback such as date, time, temperature, etc.

3.5 Data Storage system

This system handles all logging and storage of data collected by both the sensor array and the prompt generator. Data is stored along with an indication of which system it came from and all prompts will be stored with the data and time of entry.

3.6 Device Manager

This system handles all connection and communication between the device and the host software.

3.7 Error Handler - Hardware

This component constantly checks the states of every system present and ensures that if any of them fail or return an error, an alert is generated. Moreover the system will also try to fix the problem wherever possible.

3.8 Error Handler - Software

This component monitors the state of the host software and will attempt to solve any errors that arise and will alert the user should the attempts fail.

3.9 Host Software

This system is the primary interface for the researchers to analyze the data collected by the device. It consists of several features that allows the researcher to set different thresholds for activity tracking, calibrate all the sensors, update and create new records for participants, and finally interact with the data stored on the device.

3.10 Calibration

This system allows researchers to calibrate the sensors on the device , set and modify the different thresholds for activity tracking and create new prompts.

3.11 Records

This system stores all information about users present in the study. Moreover it provides functionality for researchers to create new records for new users.

3.12 Data View

This is where all data stored on the device can be viewed/ analyzed by the researchers in a graphical manner. The system also contains some functionality for data sorting/parsing and statistical analysis.

3.13 System Boundary Diagram

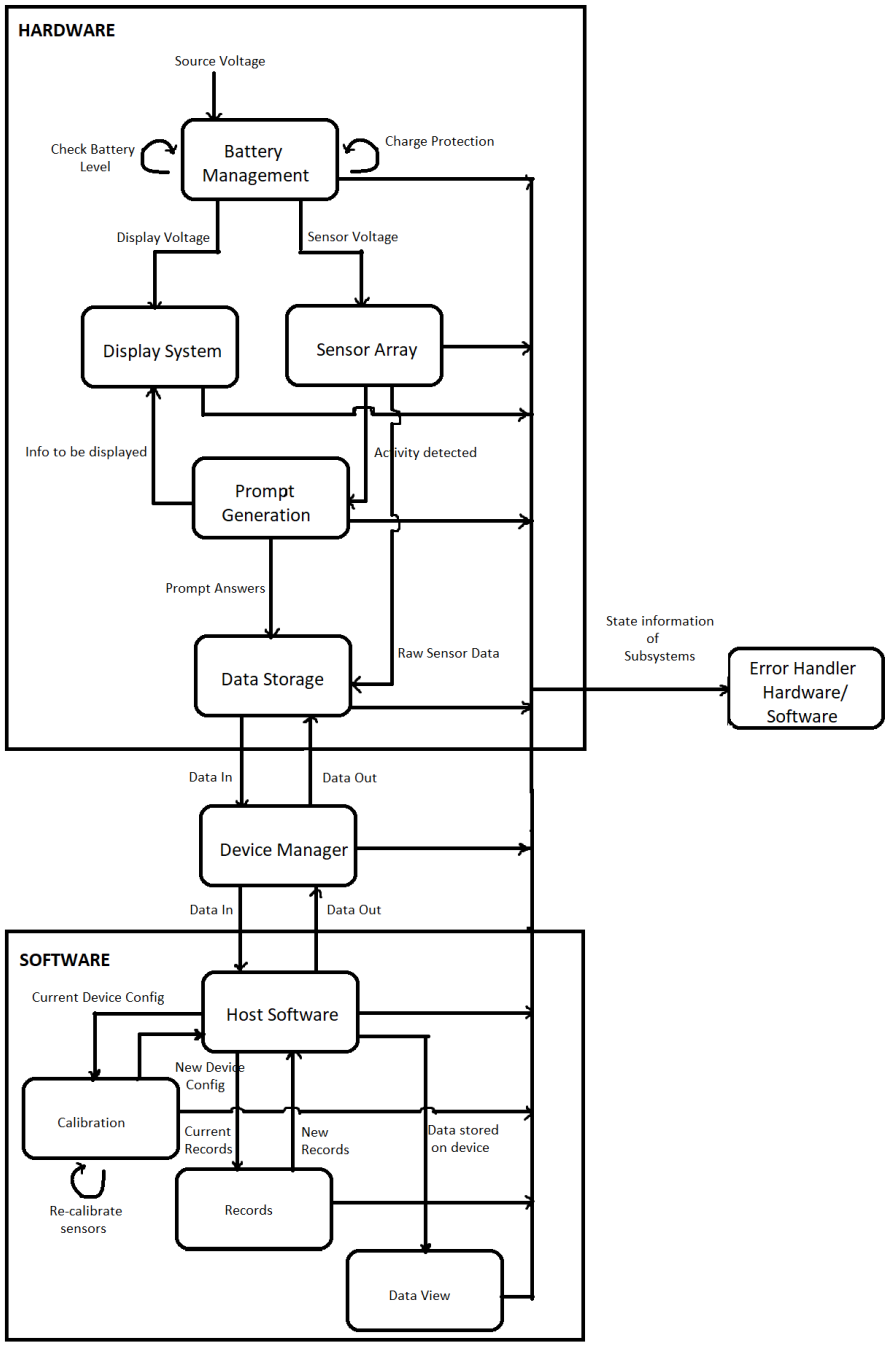

Figure 1: System Boundary Diagram

4 Critical Assumptions

[These assumptions that are made about the software or system. You should minimize the number of assumptions that remove potential hazards. For instance, you could assume a part will never fail, but it is generally better to include this potential failure mode. —SS]

5 Failure Mode and Effect Analysis

Design Component	Failure Modes	Causes of Failure	Effects of Failure	Detection	Recommended Action
Display System	Display not working	• Improper circuit connection • Battery Level too low • Code malfunction	• Users cannot answer prompts. • Users cannot view any information on the display	Display system returns an error code. Display Led is OFF	Check wiring and run a diagnostic on the display system
	Incorrect information displayed	• Display Driver faulty • Improper interaction between Display system and Prompt generation	Users face unexpected outputs causing imporper use of device	Display system returns an error code.	• Let Error Handler try to solve issue. • Perform a manual overview of code. • Perform a system reboot.

Prompt Generation System	Prompt not generated	• Prompt generation code faulty • System stuck in an idle state where no activity is detected.	• Display system will not produce an output. • Users will be unable to provide feedback regarding activity	Prompt Generation system returns an error code.	Let Error Handle try to solve the issue
	Incorrect Prompt Generated	• Prompt generation code faulty • Improper interaction between Prompt generation and Sensor Array	Prompt generated produces unexpected outputs causing imporper use of device	Prompt Generation system returns an error code. Test prompt produces unexpeted outputs	• Let Error Handler try to solve issue. • Check System Array State • Perform a system reboot.

6 Safety and Security Requirements

[Newly discovered requirements. These should also be added to the SRS. (A rationale design process how and why to fake it.) —SS]

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

8 Appendix

8.1 Error Codes

To facilitate error handling, every system will return an error code that represents the status of that system. These error codes follow the following format, BED_ERR_ERRORTYPE For example BED_ERR_NONE represent that the system is working correctly. Some more examples of error codes are:

- BED_ERR_PARAM_ERR : Represents an error with the paramaters of the function.
- BED_ERR_GENERAL : Represents a generic error that hasnt been catalogued yet.
- BED_ERR_INVALID_DATA_SIZE : Represents an error related to a size mismatch in what is stored within a block of memory or variable.