MECHTRON 4TB6: Hazard Analysis
LifeLine

Group 30
Emily Crowe, crowee
Arthur Faron, farona
Danushka Fernando, fernad12
Yerin Thevarajah, thevaryn
Phillip Truong, truonp1

December 6, 2021

Contents

1 Introduction

When designing a product it is of paramount importance to account for all potential behaviours of the system, both intended and not intended, and ensure that they meet or exceed all safety requirements. A thorough hazard analysis needs to be performed on the product to determine all the ways in which the device can malfunction, what impact the malfunction will have on the performance of the product, how it may affect the safety of the users, and what needs to be done to prevent the malfunction from occurring or to minimize its effect. This is especially important for a medical device such as the LifeLine which may be critical to the treatment and survival rate of the casualty. This document includes a comprehensive overview of all the components in the system, how the functionality of the device can be compromised, important safety considerations regarding the user and casualty, as well as a Failure Mode and Effects Analysis (FMEA) to determine potential system faults and their severity.

2 Definitions and Key Terms

- First responders: EMS, firefighters, paramedics, or police officers.
- First aid: Emergency care given to an individual in the case of serious injury with the aim to keep the individual alive and prevent further injury.
- First-aider: Individual performing first aid. For instance, a person trained in first aid arriving on a scene to treat an injured person.
- Casualty: Individual receiving first aid treatment.
- Vitals: The four vitals are body temperature, blood pressure, heart rate, and respiration rate. Vital signs are used to detect and monitor medical issues. Lifeline will measure three vitals: body temperature, blood pressure, and heart rate.

3 Background

The Portapres system by Finapres Medical Systems was a portable blood pressure monitoring device. It recorded finger arterial blood pressure, provided real-time visualization and could export data via serial port. A failure mode and effects analysis (FMEA) was performed on the existing device in hyperbaric conditions, and identified [1]:

- Potential for spark formation from electrical components such as connections to battery supply and the carbon brush motorized pump
- Overheating due to increased power consumption
- Hyperbaric implosion hazard of the gas-filled electrolytic capacitors

This device has also been recalled through the FDA for reasons of the battery may become hot and leak [2].

The Apple watch was designed with electrocardiogram (ECG) and irregular heart rhythm features that were approved by the FDA. Those features provided continuous monitoring of ECG, data processing and analysis for the user. Though the FDA risk to health factors included [3, 4]:

- Poor quality ECG signal resulting in failure to detect arrhythmia
- Misinterpretation and/or over-reliance on device output, leading to: Failure to seek treatment despite acute symptoms. Discontinuing or modifying treatment for chronic heart condition
- False negative resulting in failure to identify arrhythmia and delay of further evaluation or treatment
- False positive resulting in additional unnecessary medical procedures

4 Component Overview

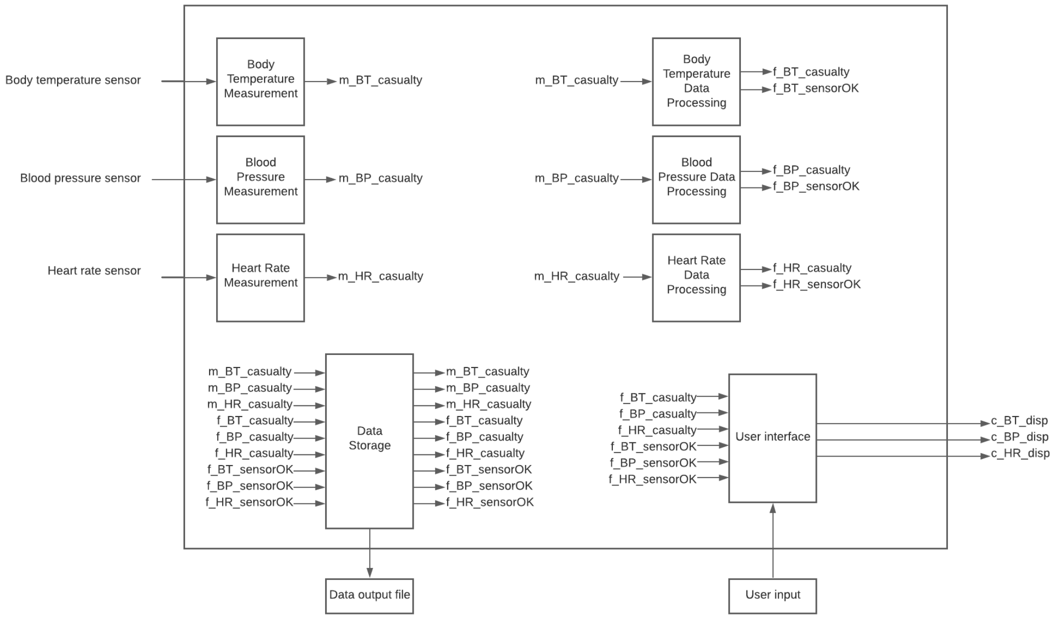

Figure 1: Component overview

4.1 Components

4.1.1 Body Temperature Measurement

The subsystem that measures a casualty's body temperature and passes it to the micro-controller.

4.1.2 Blood Pressure Measurement

The subsystem that measures a casualty's blood pressure using a Pulse Express Pulse-Ox & Heart Rate Sensor with MAX32664 and passes it to the micro-controller.

4.1.3 Heart Rate Measurement

The subsystem that measures a casualty's heart rate using a Pulse Express Pulse-Ox & Heart Rate Sensor with MAX32664 and passes it to the micro-controller.

4.1.4 Body Temperature Data Processing

The subsystem that checks whether the body temperature is within a valid range. If valid, the body temperature data is filtered and output to the display, otherwise the user is notified the data out of range.

4.1.5 Blood Pressure Data Processing

The subsystem that checks whether the blood pressure data is within a valid range. If valid, the blood pressure data is filtered and output to the display, otherwise the user is notified the data out of range.

4.1.6 Heart Rate Data Processing

The subsystem that checks whether the heart rate data is within a valid range. If valid, the heart rate data is filtered and output to the display, otherwise the user is notified the data out of range.

4.1.7 Data Storage

The subsystem that stores the data from all three vitals (body temperature, blood pressure, and heart rate) before and after processing. The data must be available after the device is powered off.

4.1.8 Data Export

The subsystem that exports the data from the device's internal memory to an external device such as a USB memory drive or computer.

4.1.9 User Interface

The subsystem contains two components: display and input. The display must show the filtered vitals after processing. The input must allow the user to give commands to delete or store data, export data, and switch between profiles for multiple casualties.

5 Main Hazards to Casualty and User

5.1 Casualty

(a) Electric shock

(b) Burns

(c) Misinterpretation of data by the user could lead to misdiagnosis

(d) Leaked medical data

5.2 User

(a) Electric shock

(b) Burns

6 Device Functionality Considerations

6.1 Body Temperature Measurement

6.1.1 Software

None

6.1.2 Hardware

(a) Incorrect readings caused by faulty sensor or wiring.

(b) Ambient temperature is too cold or too hot for the sensor to operate correctly.

(c) Current and power ratings of body temperature sensor are exceeded.

(d) Motion artifact from casualty causes incorrect readings.

(e) Physical damage to the body temperature sensor causes incorrect readings.

(f) Body temperature sensor do not work and are unresponsive.

(g) Body temperature sensor reaches end-of-life and no longer functions correctly.

6.2 Blood Pressure Measurement

6.2.1 Software

None

6.2.2 Hardware

(a) Incorrect readings caused by faulty sensor or wiring.

(b) Ambient temperature is too cold or too hot for the sensor to operate correctly.

(c) Current and power ratings of blood pressure sensor are exceeded.

(d) Motion artifact from casualty causes incorrect readings.

(e) Physical damage to the body temperature sensor causes incorrect readings.

(f) Blood pressure sensor does not work and is unresponsive.

(g) Blood pressure sensor reaches end-of-life and no longer functions correctly.

(h) Blood pressure readings are incorrect due to the limitations of PPG (photoplethysmogram). For instance, nail polish needs to be removed.

6.3 Heart Rate Measurement

6.3.1 Software

None

6.3.2 Hardware

(a) Incorrect readings caused by faulty sensor or wiring.

(b) Ambient temperature is too cold or too hot for the sensor to operate correctly.

(c) Current and power ratings of heart rate sensor are exceeded.

(d) Motion artifact from casualty causes incorrect readings.

(e) Physical damage to the body temperature sensor causes incorrect readings.

(f) Heart rate sensor does not work and is unresponsive.

(g) Heart rate sensor reaches end-of-life and no longer functions correctly.

(h) Heart rate readings are incorrect due to the limitations of PPG (photoplethysmogram). For instance, nail polish needs to be removed.

6.4 Body Temperature Data Processing

6.4.1 Software

(a) Overflow errors cause incorrect readings or prevent the device from displaying the data completely.

(b) Calculation errors and rounding errors cause incorrect readings.

(c) Error within comparison between out-of-range values and measured data.

6.4.2 Hardware

(a) Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values.

6.5 Blood Pressure Data Processing

6.5.1 Software

(a) Overflow errors cause incorrect readings or prevent the device from displaying the data completely.

(b) Calculation errors and rounding errors cause incorrect readings.

(c) Error within comparison between out-of-range values and measured data.

6.5.2 Hardware

(a) Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values.

6.6 Heart Rate Data Processing

6.6.1 Software

(a) Overflow errors cause incorrect readings or prevent the device from displaying the data completely.

(b) Calculation errors and rounding errors cause incorrect readings.

(c) Error within comparison between out-of-range values and measured data.

6.6.2 Hardware

(a) Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values.

6.7 Data Storage and Export

6.7.1 Software

(a) Encryption error causes a privacy breach of the casualty's medical data.

(b) Export file becomes corrupted.

(c) Overflow errors causes portions of data to be deleted.

(d) Volatile memory interrupted by accidental device shutdown results in loss of data.

6.7.2 Hardware

(a) Ambient temperature, either too hot or cold, affects device memory.

(b) Port malfunctions or physical damage to the port prevents it from operating properly.

6.8 User Interface

6.8.1 Software

(a) Communication error between user input and micro-controller prevents user input from being picked up by the device.

6.8.2 Hardware

(a) Overheating causes device to crash.

(b) Wire malfunction results in data displayed intermittently.

(c) If the touchscreen doesn't work or buttons are stuck, it prevents the first aider from switching between multiple patients, saving or deleting data, and exporting data. It could also affect the performance of the first aider as it will create a more stressful situation.

(d) The screen malfunctions and stops working when the ambient temperature is too cold. This too can affect the performance of the first aider.

(e) If the sunlight creates the issue of seeing the screen, this could affect the performance of the first aider.

6.9 Micro-controller

6.9.1 Software

(a) Unscheduled software updates results in the device being unable to record and save data. If this happens during an assessment out in the field, it could create a more stressful situation for the first aider.

6.9.2 Hardware

(a) Ports of the micro-controller are faulty.

(b) Wire issues between the micro-controller and its peripherals.

6.10 Power

6.10.1 Software

(a) Device does not monitor the power supply level and inform the user of low battery.

6.10.2 Hardware

(a) Battery leaks.

(b) Power supply degrades over time.

(c) Ambient temperature affects the performance of the power supply.

(d) Battery overheats.

7 Casualty and User Safety Considerations

7.1 Casualty Applied Parts

(a) Current and power ratings are exceeded by device.

(b) Sensor overheats and burns casualty.

(c) Sensors placed on casualty's body shock the casualty electrically.

(d) Sensors induce medical shock from the casualty due to burning or electrical shock.

7.2 Data Privacy

(a) Encryption error causes a breach of casualty's private medical data.

7.3 Power Supply

(a) Casualty is not electrically isolated from the power supply.

(b) Battery leaks and acid corrodes casualty or user's skin.

(c) Battery enclosure is pierced causing it to combust.

(d) Battery overheats.

7.4 Misinterpretation of Data

(a) Over-reliance on device output causes user to not seek treatment even if it is required.

(b) False positive data results in prioritizing a casualty over others even if they are not in as much danger.

7.5 Environment

(a) Device is wet.

(b) Casualty is wet or lying on a conductive surface.

(c) Automated External Defibrillator (AED) damages device and poses risk to patient.

8 FMEA Worksheet

Scale	Severity
0	no impact
1	low - some loss of functionality
2	moderately low - affects performance but not permanent
3	moderate - some permanent issue, poses no harm, device loses key functionality
4	moderately high - device loses key functionality and there is harm to a person
5	high impact - pose deadly harm to user or casualty

Causes of Hazards	**Severity** Out of 5
Body Temperature Measurement	
Hardware	
6.1.2.a Incorrect readings caused by faulty sensor or wiring	3
6.1.2.b Ambient temperature is too cold or too hot for the sensor to operate correctly	2
6.1.2.c Current and power ratings of body temperature sensor are exceeded	4
6.1.2.d Motion artifact from casualty causes incorrect readings	1
6.1.2.e Physical damage to the body temperature sensor causes incorrect readings	3
6.1.2.f Body temperature sensor does not work and are unresponsive	3
6.1.2.g Body temperature sensor reaches end-of-life and no longer functions correctly	3
Blood Pressure Measurement	
Hardware	
6.2.2.a Incorrect readings caused by faulty sensor or wiring	3
6.2.2.b Ambient temperature is too cold or too hot for the sensor to operate correctly	2
6.2.2.c Current and power ratings of blood pressure sensor are exceeded	4
6.2.2.d Motion artifact from casualty causes incorrect readings	1
6.2.2.e Physical damage to the body temperature sensor causes incorrect readings	3
6.2.2.f Blood pressure sensor does not work and is unresponsive.	3
6.2.2.g Blood pressure sensor reaches end-of-life and no longer functions correctly.	3
6.2.2.h Blood pressure readings are incorrect due to the limitations of PPG (photoplethysmogram). For instance, nail polish needs to be removed.	3
Heart Rate Measurement	
Hardware	
6.3.2.a Incorrect readings caused by faulty sensor or wiring	3

Causes of Hazards	**Severity**
6.3.2.b Ambient temperature is too cold or too hot for the sensor to operate correctly	2
6.3.2.c Current and power ratings of heart rate sensor are exceeded.	4
6.3.2.d Motion artifact from casualty causes incorrect readings.	1
6.3.2.e Physical damage to the body temperature sensor causes incorrect readings.	3
6.3.2.f Heart rate sensor does not work and is unresponsive.	3
6.3.2.g Heart rate sensor reaches end-of-life and no longer functions correctly.	3
6.3.2.h Heart rate readings are incorrect due to the limitations of PPG (photoplethysmogram). For instance, nail polish needs to be removed.	3
Body Temperature Data Processing	
Software	
6.4.1.a Overflow errors cause incorrect readings or prevent the device from displaying the data completely.	3
6.4.1.b Calculation errors and rounding errors cause incorrect readings.	3
6.4.1.c Error within comparison between out-of-range values and measured data.	3
Hardware	
6.4.2.a Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values.	3
Blood Pressure Data Processing	
Software	
6.5.1.a Overflow errors cause incorrect readings or prevent the device from displaying the data completely.	3
6.5.1.b Calculation errors and rounding errors cause incorrect readings.	3
6.5.1.c Error within comparison between out-of-range values and measured data.	3
Hardware	
6.5.2.a Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values.	3
Heart Rate Data Processing	
Software	
6.6.1.a Overflow errors cause incorrect readings or prevent the device from displaying the data completely.	3
6.6.1.b Calculation errors and rounding errors cause incorrect readings	3
6.6.1.c Error within comparison between out-of-range values and measured data.	3
Hardware	

Causes of Hazards	**Severity**
6.6.2.a Analog LC filter parts malfunction. For instance, capacitors and resistors short and cause incorrect values	3
Data Storage and Export	
Software	
6.7.1.a Encryption error causes a privacy breach of the casualty's medical data	4
6.7.1.b Export file becomes corrupted	3
6.7.1.c Overflow errors causes portions of data to be deleted.	3
6.7.1.d Volatile memory interrupted by accidental device shutdown results in loss of data	3
Hardware	
6.7.2.a Ambient temperature, either too hot or cold, affects device memory.	3
6.7.2.b Port malfunctions or physical damage to the port prevents it from operating properly.	3
User Interface	
Software	
6.8.1.a Communication error between user input and micro-controller prevents user input from being picked up by the device.	2
Hardware	
6.8.2.a Overheating causes device to crash	2
6.8.2.b Wire malfunction results in data displayed intermittently.	1
6.8.2.c If the touchscreen doesn't work or buttons are stuck, it prevents the first aider from switching between multiple patients, saving or deleting data, and exporting data. It could also affect the performance of the first aider as it will create a more stressful situation	2
6.8.2.d The screen malfunctions and stops working when the ambient temperature is too cold. This too can affect the performance of the first aider.	2
6.8.2.e If the sunlight creates the issue of seeing the screen, this could affect the performance of the first aider.	1
Micro-controller	
Software 6.9.1.a Unscheduled software updates results in the device being unable to record and save data. If this happens during an assessment out in the field, it could create a more stressful situation for the first aider.	 3
Hardware	
6.9.2.a Ports of the micro-controller are faulty.	2
6.9.2.b Wire issues between the micro-controller and its peripherals.	2
Power	
Software	

Causes of Hazards	**Severity**
6.10.1.a Device does not monitor the power supply level and inform the user of low battery.	3
Hardware	
6.10.2.a Battery leaks.	4
6.10.2.b Power supply degrades over time	1
6.10.2.c Ambient temperature affects the performance of the power supply.	1
6.10.2.d Battery overheats.	3
Casualty Applied Parts	
7.1.a Current and power ratings are exceeded by device.	4
7.1.b Sensor overheats and burns casualty.	4
7.1.c Sensors placed on casualty's body shock the casualty electrically.	4
7.1.d Sensors induce medical shock from the casualty due to burning or electrical shock.	4
Data Privacy	
7.2.a Encryption error causes a breach of casualty's private medical data	4
Power Supply	
7.3.a Casualty is not electrically isolated from the power supply	4
7.3.b Battery leaks and acid corrodes casualty or user's skin.	4
7.3.c Battery enclosure is pierced causing it to combust.	4
7.3.d Battery overheats.	4
Misinterpretation of Data	
7.4.a Over-reliance on device output causes user to not seek treatment even if it is required.	3
7.4.b False positive data results in prioritizing a casualty over others even if they are not in as much danger	4
Environment	
7.5.a Device is wet	3
7.5.b Casualty is wet or lying on a conductive surface.	2
7.5.c Automated External Defibrillator (AED) damages device and poses risk to patient.	4

9 Roadmap

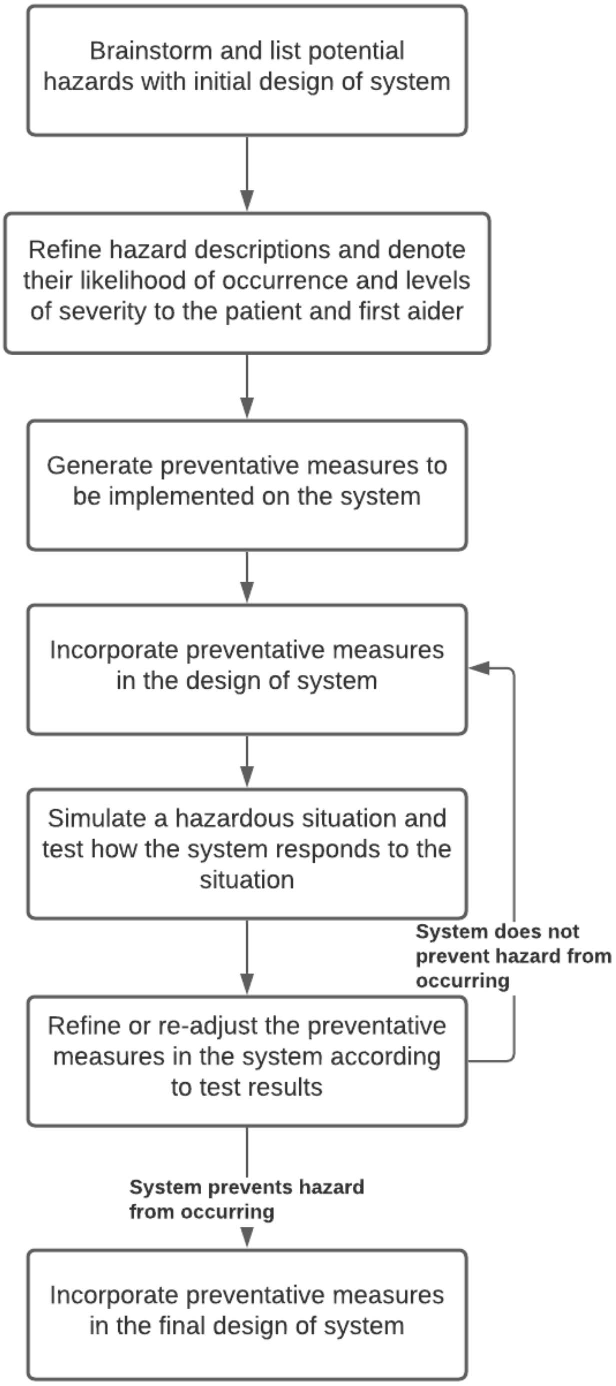
Brainstorm and list potential hazards with initial design of system
Refine hazard descriptions and denote their likelihood of occurrence and levels of severity to the patient and first aider
Generate preventative measures to be implemented on the system
Incorporate preventative measures in the design of system
Simulate a hazardous situation and test how the system responds to the situation
System does not prevent hazard from occurring
Refine or re-adjust the preventative measures in the system according to test results
System prevents hazard from occurring
Incorporate preventative measures in the final design of system

Figure 2: The iterative process of hazard analysis

10 Appendix

References

[1] R. Van der Bel. *A modified device for continuous non-invasive blood pressure measurements in humans under hyperbaric and/or oxygen-enriched conditions.* (accessed December 02 2021). URL: https://www.researchgate.net/publication/299469821_A_modified_device_for_continuous_non-invasive_blood_pressure_measurements_in_humans_under_hyperbaric_andor_oxygen-enriched_conditions.

[2] FDA. *Class 2 Device Recall Finapres Portapres Ambulatory Continuous NonInvasive Blood Pressure Monitor.* (accessed December 2 2021). URL: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=110979#3.

[3] FDA. *DE NOVO CLASSIFICATION REQUEST FOR ECG APP.* (accessed December 2 2021). URL: https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN180044.pdf.

[4] FDA. *DE NOVO CLASSIFICATION REQUEST FOR IRREGULAR RHYTHM NOTIFICATION FEATURE.* (accessed December 2 2021). URL: https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN180042.pdf.