BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

EEE 416 (July 2023)

Microprocessors and Embedded System Laboratory

Final Project Report

Section**: A1** Group: **06**

IOT based Safety Device

Course Instructors:

Dr. Sajid Muhaimin Choudhury
Assistant Professor
Department of EEE, BUET

Ayan Biswas Pranta
PT
Department of EEE, BUET

Signature of Instructor: ______________________________

Academic Honesty Statement:

IMPORTANT! Please carefully read and sign the Academic Honesty Statement, below. Type the student ID and name, and put your signature. ***You will not receive credit for this project experiment unless this statement is signed in the presence of your lab instructor.***

"In signing this statement, We hereby certify that the work on this project is our own and that we have not copied the work of any other students (past or present), and cited all relevant sources while completing this project. We understand that if we fail to honor this agreement, We will each receive a score of ZERO for this project and be subject to failure of this course."

Signature: ________________ **Full Name: Shahan Bin Sharif Hirock** **Student ID: 1906012**	**Signature:** ________________ **Full Name: Md. Sumon Howlader** **Student ID:1906018**
Signature: ________________ **Full Name: Progna Dipto Saha** **Student ID:1906027**	

Table of Contents

1 Abstract

Title: IoT-Based Safety Device for Ensuring Personal Security

Abstract:

Since Internet of Things (IoT) technology is becoming more and more widespread, there is a great potential to design new systems that improve personal safety. This article therefore introduces one of our projects; an internet-based security device designed to protect vulnerable individuals from imminent danger.

Our system works by continuously monitoring people in real-time and taking immediate action when necessary. Our framework consists of sensors that detect falls, quick movements or any distress signal hence allowing the alarm to go off. It means that once the device identifies such cases, it can then wait no further time before it facilitates their rescue in time.

One of its main features is its ability to send out emergency SMSs to pre-stored contacts. Through GSM or other relevant communication protocols, information about emergencies can be transmitted urgently to specific targets. This further entails uploading essential information including where the affected person may be found on cloud based services. Thus enabling timely rescue efforts due to minimization time wasted on searching for victims who need urgent help.

In addition, user-friendliness and accessibility are at the top list of our safety device based on IoT. It is small in size and user-friendly which makes it a product that can be used by people of different ages. Additionally, the device can be connected to a smart home ecosystem thus improving general convenience as well as interoperability.

To wrap up, our project represents a crucial stride towards leveraging IoT technology to improve personal safety. Our device provides an efficient solution for ensuring security of vulnerable individuals through powerful sensor abilities combined with cloud communication systems. Going forward, we imagine a future where connected devices and real-time monitoring will significantly contribute to personal safety with time.

2 Introduction

If especially the disadvantaged individuals such as the seniors and also the sick people are not considered, the safety and wellbeing as the top priorities in contemporary societies cannot be guaranteed. Although we have made huge improvements towards their conservation, ensuring their security remains an intricate concern. The issue of safely crossing the road has led to this project being that of developing an IoT-based Safety Device to solve this important concern. The objective of this device is to assist the bill-of-vital moments by forwarding the important message to some designate contact and then uploading the important data to the cloud. The rapid response and rescue operations are possible through the objective due to immediate help.

Reasons Why It is a Complex Engineering Problem:
The project we are working on is a multifaceted engineering challenge that is built around multiple technical domains such as hardware design, embedded systems programming, sensors, the integration and communication protocols, and cloud computing. The complexity resides in that it is

vital to have all parts connected seamlessly forming a reliable system that detects emergencies, transmits messages, and falls within security and privacy guidelines.

1. Hardware Design: finalising the physical product to find appropriate components (microcontrollers, sensors eg. accelerometer for fall detection, communication modules eg. GSM or Wi-Fi, power management system and so on) and the way in which they are integrated together (eg. size, power consumption, durability) poses a big engineering challenge.

2. Embedded Systems Programming: The microcontroller of a smart nightlight requires firmware that needs to be programmed from scratch. At a low enough level, most embedded systems rely on programming in C or assembly language. This includes implementing algorithms for sensor data processing, event detection, communication protocols, etc.

3. Sensor integration: Sensors need to be able to accurately and reliably detect emergency scenarios (eg, if the person has fallen, if they identify themselves as in distress). Calibrating sensors, removing noise and reducing false positives/negatives are key challenges in sensor integration.

4. Communication Protocols: Choose communication protocols (GSM, SMS, TCP/IP) for sending emergency alerts to guardian phone numbers. Ensure reliable transmission from device to cloud, as well as in protecting information (error handling and encryption).

5. Cloud Integration: Providing access to location information from the cloud to emergency responders requires integration to cloud providers (AWS, Azure, etc). This involves accommodating secure authentication, data encryption, and scalable storage to create a robust foundation.

Possible Alternative Solutions:

Several alternative approaches can be considered to address the safety needs of vulnerable individuals:

1. Wearable Gadgets: In place of standalone safety monitors, items like smartwatches or pendants with GPS tracking and emergency-button functionality can fulfil most of the same capabilities.

2. Smartphone Applications: Create a smartphone application making use of the built-in sensors as well as the Internet and network communication capabilities that would enable the detection of an emergency and notifying the designated contacts by sending a message.

3. Home Monitoring Systems: Providing domestic sensors and cameras to make regular observations of and, when required, attend to the activities of the vulnerable for the identification of emergency events.

4. Community-based Alert Systems: Set up community networks where neighbours or volunteers alert each other in case of an emergency, offering a helping hand until professional help arrived.

Every alternative is a trade-off between the benefits and drawbacks. Cost, usability, reliability and scalability all come into play. Our IoT-based Safety Device combines elements of several alternatives to provide a sophisticated response to the special needs of vulnerable individuals, all within the capabilities of IoT devices that deliver assistance in responsive time.

3 Design

3.1 Problem Formulation (PO(b))

3.1.1 Identification of Scope

Our project, Safety Device by the Internet of things, seeks to fill a gap in the society by establishing security of the vulnerable people through utilization of the microprocessors, embedded systems and IoT systems. The scope of our project encompasses several key components and functionalities:The scope of our project encompasses several key components and functionalities:

1. Hardware Development: Creating PCB as well as testing and prototyping the physical device will include identification of specific microprocessors (for example, this includes accelerometers for fall detection), communication modules (e.g., GSM, Wi-Fi), as well as power management systems. The subscription model should be in the form of SaaS (software as a service) and hardware must be miniaturized, ruggedized, and energy-efficient.

2. Embedded Systems Programming: Selecting, designing and building the hardware and the firmware for the microcontroller to make it possible to control the operations in real-time, alerting mechanisms for events happening and the communication with external systems. This is done by the application of low level programming languages such as C or assembly for implementation of algorithms for real time operating systems purposes and emergency detection.

3. Sensor Integration: Integrating the sensor instrument to identify a range of emergencies, including falls, sudden planes or signs of trouble. To establish it as reliable, consistent and free from the false positives/negatives it should be ensured that sensors are accurately calibrated, while their reliability should be improved.

4. Communication Protocols: Developing communication routine which allows the device to send SOS messages to number of predefined phone numbers. These include choosing applicable methods (e.g. GSM, SMS) and ensure that reliable transfer, error handling, and encryption for secure data transfer are done.

5. Cloud Integration: Install the functionality to upload positioning information stored on the cloud that may be possible to access remotely by the emergency responders. This entails embracing cloud technologies (e.g., AWS, Azure) as a means to guarantee proper authentication, encryption, as well as elastic data storage.

6. User Interface: Defining an intensive user-friendly interface for configuring device settings, keeping emergency contacts, showing device status. This incorporates among others accessibility, usability, and feedback components to ensure that victims of abuse and other vulnerable members benefit from the services offered.

7. Testing and Validation: Performing comprehensive tests to ensure the product is indeed dependable, reliable and provides adequate protection in different real life eventualities. These tests encompass the areas of sensor accuracy, communication reliability, battery life, and emergency response time, among others.

8. Documentation and Deployment: Recording the design, development, and functioning of the safety device for future usage/to be called upon for later reference and reproduction. Use of the tool in real-life scenarios to test its efficacy in making communities safe for those with needs.

The focus of our project is the development and testing of the IoT-based Safety Device under accordance of the laboratory condition. While down the line, additional tests may be performed concerning scalability, interoperability and compliance of those systems for use in real-world settings.

3.1.2 Literature Review

Keeping vulnerable individual people safe and ensuring their welfare is the objective that has gained much attention in both research and industrial spheres. The provision of Internet of Things enabled safety equipment constitute an exciting way forward that will help us deal with this burning problem. We will scrutinize the studies and the technologies related to smart safety devices that are based on IoT where various aspects such as location tracking and emergency communication systems will constitute the target of our research.

1. IoT-Based Safety Devices:
Due to IoT technology development, there is a great many IoT devices being created to monitor the situation and react to emergencies in a timely manner. The devices are designed with sensors to detect falls, quick movements, or coughing. Usually they also transmit vital signs information. Researchers have diverged into different areas in terms of design and implementation, which consists of wearable devices, home monitoring facilities, and automotive safety technologies.

2. Emergency Communication Systems:
Well established communication is a really important factor in mercy work. Current research into this particular area has looked into creating protocols as well as communication technologies for passing messages to the representative contacts of the situation. The technologies of SMS, GSM and voice calls have been mainly used for urgent messaging via the pre-assigned mobile phone numbers. Moreover, there has been a large scale of development of mobile phone appliances as far as emergency communication is involved.

3. Location Tracking Solutions:
Tracking server of the location will be useful for the emergency responders via which they can pinpoint the exact location of people in danger. A GPS technology utilizes the concept of real-time location tracking, which works well indoors as well as outdoors. Nevertheless, specific obstacles, in this case, the signal attenuation in indoor situations, as well as the high consumption of electrical power have made exploration of alternative technologies possible as an example, equal to wireless positioning system, bluetooth beacons and inertial navigation systems.

4. Integration with Cloud Services:4. Integration with Cloud Services:
The benefits of cloud computing that include storage and processing of huge amounts of data hence for the IoT devices come together to allow this kind of analytics realization. While doing researches, IoT safety devices have been integrated with cloud platforms so that they will help to make remote monitory, data storage, and analytics. Cloud services empower services providers with the opportunity to immediately access important information like location information and sensor data, which allows the services to be ready and efficient.

5. User Interface Design:
Whether consumers utilize the internet of things to enhance their safety or not, is a key player which is heavily relied upon to guarantee correct adoption and abundant use of the technology. The research of this field is dedicated to developing user interfaces that are extremely convenient for the users from any age or level of disabilities. Human-based design practices are used in designing interfaces that allow resourceful scope of powers like authority, emergencies contact operations, and diagnostics checking to be conducted by the centre of the device.

In general, the literature stresses the significance of the connectedness of that type of IoT safety equipment in the provision and security of safety systems of vulnerable persons. Sensing technology, communication systems, location tracking engagement and cloud services all make up the several systems of the device that is an overall solution to emergency response and assistance. But difficulties e.g. sensor accuracy, communication reliability and users` acceptance are still the point of focus for skepticism and further studies.

3.1.3 Formulation of Problem

The aim of our project is the creation of the Safety Device based on the IoT technology, which would be the answer to the increasing number of emergency cases that take place among the risk individuals. undefined

1.Emergency Situations:
The safety mechanism should have the ability to precisely release the emergency situations in which the individual's safety is exposed. The emergencies may be fall detection, autonomous movement suggesting the young is in distress, or anything else that has been defined upfront. Drawing a line between what is regular and what really needs attention is the biggest hurdle here. The edge needs to be very precise with no false calls of either type.

2. Real-Time Alert Mechanism:
In case an emergency has been detected, the safety gadget will automatically alert a specified contact informing of the crisis. This implies creating consistent communication channels, for instance, GSM and SMS, through which emergency alert messages incorporating specific details (for instance, the nature of the emergency or the individual's location) are sent. Establishing true-to-factness and punctualty of these warnings is of particular concern as they are needed to provide timely help and intervention.

3.Data upload:
Apart from sending emergency messages, the device has to be cloud storage linked to so that the rescuers could track the person's exact position in real-time. Therefore, the technology used for tracking locations should be incorporated into the device (e.g., GPS) and safe communication with the cloud-based platforms should be set up. Providing the data accuracy, also confidentiality and safety of the uploaded data are needed to speed up the operations process for search and rescue.

4. Power Management and Efficiency:4. Power Management and Efficiency:
The fact that the safety device has the purpose of continuous monitoring calls for good power management that is aimed to provide enough power for the battery life and the beacon to be always on. This process asks for very enhanced engineering skills that could optimize the device`s power consumption for as long as functionality and responsiveness remains. Doing so is likely to entail multiple means such as order-power modes, intelligent sensor sampling and energy-efficient communication sequences.

5. User Interface and Accessibility:
The device needs to be simple to operate and should not require special knowledge, or training for the user, the interface should therefore be intuitive and should support the configuration, control and monitoring of contacts and device status. Creating an interface that puts users into central position in distribution and their particular needs accounting as its principles are fundamental for rendering the program successful and transparent.

In overall, we are the key technical hurdles that to coming up with a smart IoT device with the capacity to register what the situation is, generate an emergency alert quickly, pick the location, optimize power, and provide user-friendliness interface. Our project attempts to address the issue of administering health care safely and comfortably by means of technological provisions in healthcare solutions for vulnerable groups.

3.1.4 Analysis

Our Safety Device project which uses IoT, Microprocessors and Systems on a Chip addresses a fundamental safety need of vulnerable individuals by harnessing the vast potential of IoT technologies to achieve a more secure environment. Below is an analysis of various aspects of the project:Below is an analysis of various aspects of the project:

1. Technical Complexity:
The project integrates between the technical components involved, like microcontrollers, sensors, communication modules, and cloud tools. For each one of them there is a choice, configuration , and putting together in order to arrive at smooth operation. The complexity of the process further is augmented by need of writing firmware for the microcontroller, creating emergency detection algorithms, and setup of power management correctly.

2. Sensor Integration:
Among the technical obstacles influencing the developing of a mobile application of this nature is the incorporation of sensors that allow to detect different emergency circumstances i.e. falls or distress calls. Ensuring that the sensors are correctly set up and configurated to reliably differentiate between regular activities and emergencies is the prerequisite for this gadget to work well effectively. As one of the main objectives of the sensor design is to detect on the basis of a variation in a certain measurand, the engineering challenge of minimizing the numbers of false positives and false negatives and at the same time to ensure that the sensors are reliable as well is a significant one.

3. Communication Protocols:
Sending emergency messages to the specified phone numbers with trusted communication methods has to be done very carefully paying attention to things like the network availability, error handling as well as the relative message delivery delay. To obtain fault-tolerant communications it is important to have selection of proper communication modules (can say as eg.GSM, Wi-Fi) and also by optimizing communication protocols for better data transmission timing then onwards alerting and effective emergency response can be expected.

4. Cloud Integration:
To provide uploaded location data in the cloud for remote access by rescuers it will be necessary to integrate the presence of the security device within the cloud platforms, and to implement encrypting and authentication systems. Providing data with an adequate level of security in order for data flow and storage in the cloud to continue smoothly means that there is a technical challenge that needs to be dealt with in detail.

5. User Interface Design:
It is vital for usability and accessibility also that we design an interface that is intuitive and offers configuring of settings in the device, a management of emergency contacts, and a status monitor of the device. Human centered design concepts need to be incorporated into the architecture to ensure that the interface is easy to use and navigate, especially for the prone group that have little technical proficiency and physical impairments at the fore.

6. Power Management:
By optimizing power consumption towards longevity of battery life and maintaining constant operations, a safety device for continuous monitoring must comply with safe operating

procedures. Among seamless power optimization strategies, medium consumption of power including low-power mode and smart sensor sampling are necessary for better device application in real world conditions.

In overall, the statistics show the technical complexity and challenges which may be faced in the same while developing a safety device that uses the IoT to ensure the safety of all vulnerable individuals. We strive to solve these difficulties with the help of picking out an appropriate design, implementation, and testing models, which will lead us to the conclusion of the making urban environment safer and better to live for all people who are seeking for help.

3.2Design Method (PO(a))

To summarize our work on the project of IoT-based Safety Device, we used the study material from these fields such as mathematics, science, and engineering. Here's how we utilized each of these domains to solve the problem:Here's how we utilized each of these domains to solve the problem:

1. Mathematics:
a. Algorithm Development: With the use of mathematical science, we designed computer programs which helped us detect emergency situations based on observed sensor data. Doing so meant to make use of the math basics like signal processing, statistical analysis, and patterns identifying, which are related to emergency signals, such as falls or distress signals, and it will be done accurately.
b. Data Analysis: We implemented mathematical approaches of the processing of the sensor data which allowed us the reframing of the data into the signals and patterns that correspond to the emergency events. These comprised of solutions related to data normalization, filters, and feature extraction in order to increase the precision of the algorithms as well to ensure a high level of accuracy.
c. Optimization: Mathematics has been the most significant determinant of the success/ failure of various components of the network, including power consumption, communication protocols, and algorithm's efficiency. Then the by linear programming, numerical and mathematical methods optimization was applied by us to our safety device and we were able to this device performance in a final as to be more productive as well as effective.

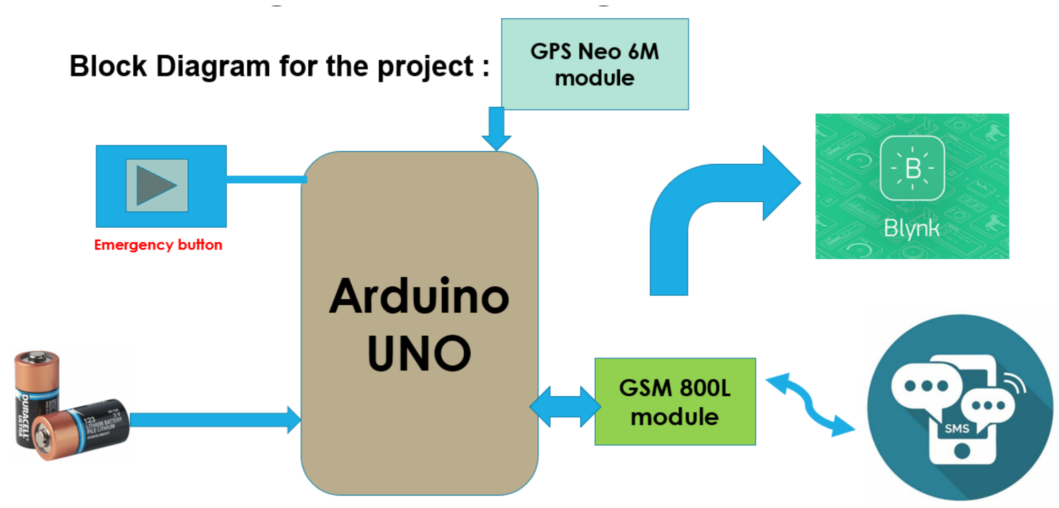
2. Science:
a. Sensor Technology: Scientific principles like accelerometers, gyroscopes, and proximity assumption rules to learn the behavior and capabilities of the sensors we used for our safety gadget was utilized in application. This was doing the research which includes topics such as sensor physics, signal processing, and sensor fusion techniques to ensure that the accuracy and reliability of our sensor data remains great.
b. Communication Systems: We deployed scientific procedures of designing and employing emergency communication systems that would be channeled to the groups or individuals TBA. Here among others, I gained knowledge into the key aspects of wireless communication, modulation techniques, and error codes; which ensured reliable data transmission in the face of diverse environmental situations.
c. Location Tracking: The GPS, satellite systems, and signal processing methodology principles were integrated into the safety device and led to the development of accuracy location tracking capabilities.

3. Engineering:
a. System Design: In case we applied engineering principles to the security device, this would affect its main architecture and design, involving components selection process, integration, and software and hardware co-design. This required to be dealt with, taking into account the elements like

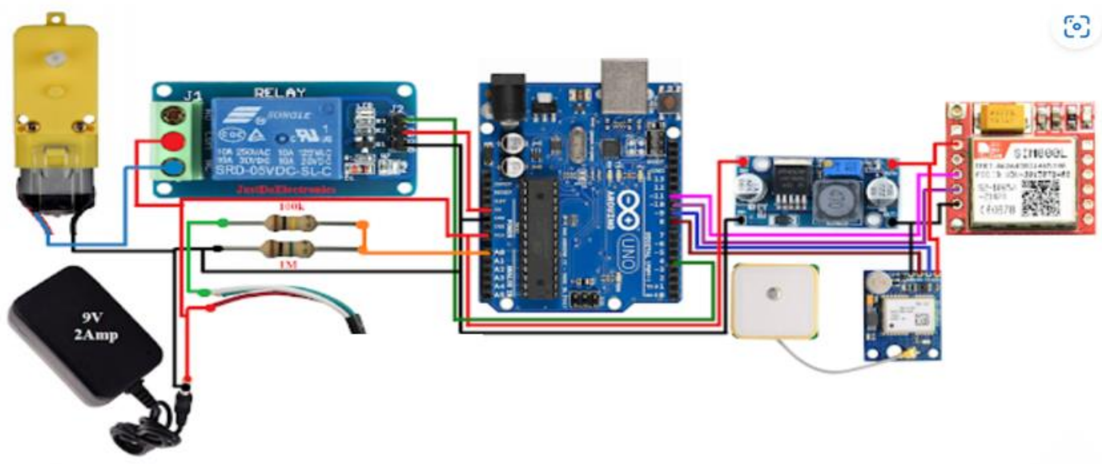
performance demand, cost pressures, and the expansion possibility to achieve a stable and efficient solution.
b. Embedded Systems Programming: Through implementing coding for a given microcontroller, our team comprised firmware engineers who used engineering fundamental to build sensors data processors with event detection and communication protocols. The ability to code using a low-level programming language, such as C or assembly language, and an exhaustive baggage of knowledge about embedded systems design principles and guidelines was mandatory.
c. Testing and Validation: Compilation of engineering concepts guided us through the testing, validation, and final checking of device to make it more reliable, safe, and functional. This consisted in carrying out the numerous tests designed to detect problems and to determine whether the instrument had the prescribed characteristics, such as the unit testing, integration testing and field testing.

By learn from mathematics, science and engineering our solution had been developed to reduce the level of safety for vulnerable people using our IoT-based Safety Device.

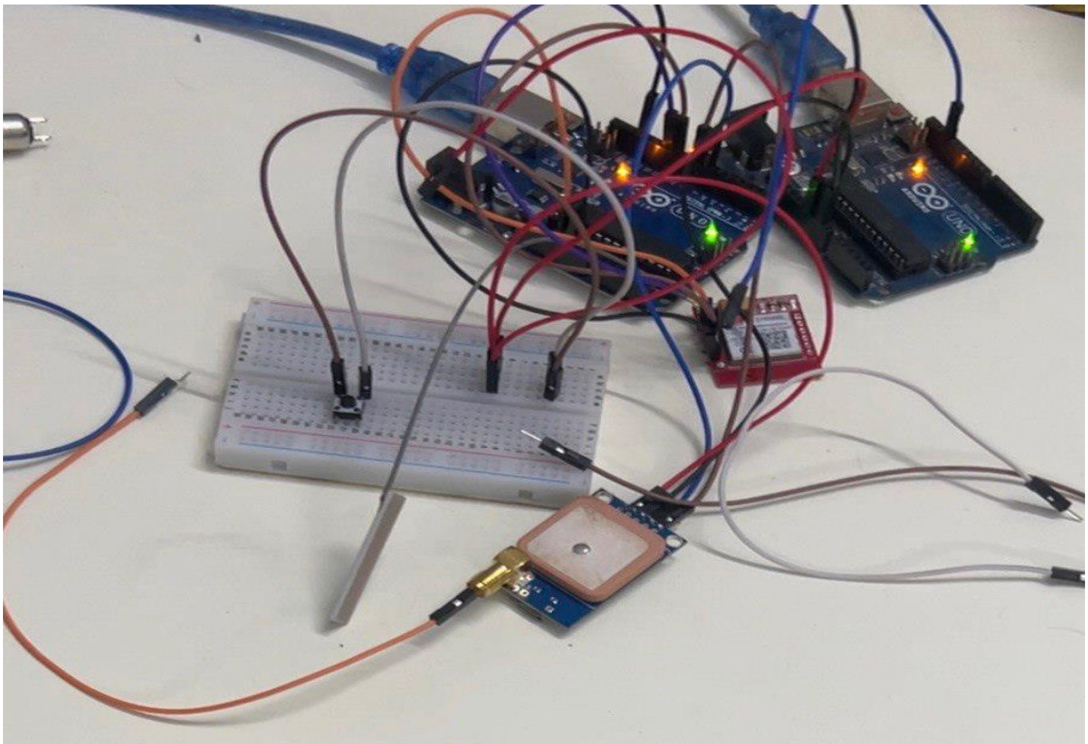
3.3Block Diagram



3.4Circuit Diagram



3.5CAD/Hardware Design



3.6Full Source Code of Firmware

```
//Prateek
//https://justdoelectronics.com
//https://www.youtube.com/@JustDoElectronics

#include <SoftwareSerial.h>
#include <AltSoftSerial.h>
#include <TinyGPS++.h>

const String PHONE = "+9188305848xx";

#define ignition_switch 4
#define ignition_sensor A0

//GSM Module RX pin to Arduino 3
//GSM Module TX pin to Arduino 2
#define rxPin 2
#define txPin 3
SoftwareSerial sim800(rxPin, txPin);

//GPS Module RX pin to Arduino 9
//GPS Module TX pin to Arduino 8
AltSoftSerial neogps;

TinyGPSPlus gps;

String sms_status, sender_number, received_date, msg;
boolean ignition_status = false;
boolean tracking_status = false;
boolean reply_status = true;
boolean anti_theft = false;

unsigned long previousMillis = 0;
long interval = 60000;

void setup() {
  delay(7000);
  Serial.begin(115200);

  sim800.begin(9600);
  neogps.begin(9600);

  pinMode(ignition_switch, OUTPUT);
  pinMode(ignition_sensor, INPUT);

  sms_status = "";
  sender_number = "";
  received_date = "";
  msg = "";

  sim800.println("AT");
  delay(1000);
  sim800.println("ATE1");
  delay(1000);
  sim800.println("AT+CPIN?");
  delay(1000);
  sim800.println("AT+CMGF=1");
  delay(1000);
  sim800.println("AT+CNMI=2,2,0,0,0");
  delay(1000);
}


void loop() {

  ignition_status = getIgnitionStatus();

  if (tracking_status == true && ignition_status ==
true) {
    unsigned long currentMillis = millis();
    if (currentMillis - previousMillis > interval) {
      previousMillis = currentMillis;

    }
  }
  if (anti_theft == true && ignition_status == true) {
    digitalWrite(ignition_switch, HIGH);
  }

  while (sim800.available()) {
    parseData(sim800.readString());
  }

  while (Serial.available()) {
    sim800.println(Serial.readString());
  }
```

```
}

void parseData(String buff) {
  Serial.println(buff);

  unsigned int len, index;
  index = buff.indexOf("\r");
  buff.remove(0, index + 2);
  buff.trim();
  if (buff != "OK") {
    index = buff.indexOf(":");
    String cmd = buff.substring(0, index);
    cmd.trim();

    buff.remove(0, index + 2);

    if (cmd == "+CMTI") {
      index = buff.indexOf(",");
      String temp = buff.substring(index + 1,
buff.length());
      temp = "AT+CMGR=" + temp + "\r";
      sim800.println(temp);
    } else if (cmd == "+CMGR") {
      extractSms(buff);
      if (sender_number == PHONE) {
        doAction();

      }
    }
  } else {
    //The result of AT Command is "OK"
  }
}
void extractSms(String buff) {
  unsigned int index;
  Serial.println(buff);

  index = buff.indexOf(",");
  sms_status = buff.substring(1, index - 1);
  buff.remove(0, index + 2);

  sender_number = buff.substring(0, 13);
  buff.remove(0, 19);

  received_date = buff.substring(0, 20);
  buff.remove(0, buff.indexOf("\r"));
  buff.trim();

  index = buff.indexOf("\n\r");
  buff = buff.substring(0, index);
  buff.trim();
  msg = buff;
  buff = "";
  msg.toLowerCase();

  Serial.println(".........");
  Serial.println(sms_status);
  Serial.println(sender_number);
  Serial.println(received_date);
  Serial.println(msg);
  Serial.println(".........");
}

void doAction() {
  //case sensitive
  if (msg == "bike on") {
    digitalWrite(ignition_switch, HIGH);
    Serial.println("Bike has ON");
    if (reply_status == true) {
      sendSms("Bike has ON");
    }
  } else if (msg == "bike off") {
    digitalWrite(ignition_switch, LOW);
    Serial.println("Bike has OFF");
    if (reply_status == true) {
      sendSms("Bike has OFF");
    }
  } else if (msg == "get location") {
    sendSmsGPS("Location");
  } else if (msg == "anti theft on") {
    anti_theft = true;
    if (reply_status == true) {
      sendSms("Someone Trying to start your bike");
      sendSms("Bike Has OFF");
    }
  } else if (msg == "anti theft off") {
```

```
    anti_theft = false;
    if (reply_status == true) {
      sendSms("Anti-Theft has OFF");
    }

    else if (msg == "reply on") {
      reply_status = true;
      sendSms("Reply has ON");
    }

    else if (msg == "reply off") {
      reply_status = false;
    }
  } else if (msg == "tracking on") {
    tracking_status = true;
    if (reply_status == true) {
      sendSms("Live Tracking has ON");
    }
  }
  //yet to be implemented
  else if (msg == "tracking off") {
    tracking_status = false;
    if (reply_status == true) {
      sendSms("Live Tracking has OFF");
    }
  } else if (msg == "tracking status") {
    if (tracking_status == false) {
      sendSms("Live Tracking has OFF");
    } else {
      sendSms("Live Tracking has ON");
    }
  }
  sms_status = "";
  sender_number = "";
  received_date = "";
  msg = "";
}
void deleteSms() {
  sendATcommand("AT+CMGD=1,4", "OK", 2000);
  Serial.println("All SMS are deleted.");
}
void sendSmsGPS(String text) {
  // Can take up to 60 seconds
  boolean newData = false;
  for (unsigned long start = millis(); millis() - start
< 2000;) {
    while (neogps.available()) {
      if (gps.encode(neogps.read())) {
        newData = true;
      }
    }
  }
  if (newData)
  {
    float flat, flon;
    unsigned long age;
    Serial.print("Latitude= ");
    Serial.print(gps.location.lat(), 6);
    Serial.print(" Longitude= ");
    Serial.println(gps.location.lng(), 6);
    newData = false;
    delay(300);
    ///*
    sim800.print("AT+CMGF=1\r");
    delay(1000);
    sim800.print("AT+CMGS=\"" + PHONE + "\"\r");
    delay(1000);
    sim800.print("http://maps.google.com/maps?q=loc:");
    sim800.print(gps.location.lat(), 6);
    sim800.print(",");
    sim800.print(gps.location.lng(), 6);
    delay(100);
    sim800.write(0x1A);
    delay(1000);

  }
}
void sendSms(String text) {
  sim800.print("AT+CMGF=1\r");
  delay(1000);
  sim800.print("AT+CMGS=\"" + PHONE + "\"\r");
  delay(1000);
  sim800.print(text);
  delay(100);
  sim800.write(0x1A);
  delay(1000);
  Serial.println("SMS Sent Successfully.");
}
int8_t sendATcommand(char* ATcommand, char*
expected_answer, unsigned int timeout) {

  uint8_t x = 0, answer = 0;
  char response[100];
  unsigned long previous;

  memset(response, '\0', 100);

  delay(100);

  while (sim800.available() > 0) sim800.read();

  if (ATcommand[0] != '\0') {
    sim800.println(ATcommand);
  }


  x = 0;
  previous = millis();
  do {
    if (sim800.available() != 0) {
      response[x] = sim800.read();
      x++;
      if (strstr(response, expected_answer) != NULL) {
        answer = 1;
      }
    }
  } while ((answer == 0) && ((millis() - previous) <
timeout));

  return answer;
}

boolean getIgnitionStatus() {
  float val = 0;
  for (int i = 1; i <= 10; i++) { val = val +
analogRead(ignition_sensor); }
  val = val / 10;
  //Serial.println(val);
  if (val > 90) {
    return true;
  } else if (val < 50) {
    return false;
  }
}
void setIgnition() {
  ignition_status = getIgnitionStatus;
  if (ignition_status == false) {
    sim800.print("AT");
    sendATcommand("AT+CSCLK=0", "OK", 1000);
  } else if (ignition_status == true) {
    sendATcommand("AT+CSCLK=2", "OK", 1000);
  }
}
```

Table: Source Code for the main program

4 Implementation

4.1 Description

Sure, here's a description of the circuit design for your IoT-based Safety Device using Arduino Uno, GPS module Neo 6m, and GSM 800L module:Sure, here's a description of the circuit design for your IoT-based Safety Device using Arduino Uno, GPS module Neo 6m, and GSM 800L module:

1. Arduino Uno: Instead of time-consuming procedure, it is the main unit for control of a safety device. It shall serve a role of communicating with GSM, GPS biased and other peripheral modules as well as deciding what high emergency alerts to trigger.

2. GPS Module Neo 6m: The GPS-module is the one to take the latitude-longitude data of the gadget. This is achieved through the use of UART (serial communication) that enables it to send location data to Arduino Uno.

3. GSM 800L Module: With the GSM module, SMS to predetermined phone numbers can be sent out in case of incidences that are considered life-threatening. It also has a communication with the Arduino via UART to send messages, it does.

4. Power Supply: You'll have to consider an Arduino Uno power source plus the modules to add up the right voltage. Options range from direct connection to a USB port or a self-contained power source, based on the operating scenario requirements.

5. Connections: Arduino Uno module will be employed to execute serial data transmission between a GPS module and a GSM module by utilizing UART communication. Inside the module, make sure RX pin is supplied with TX pin of the Arduino Uno and vice versa. Just like that, RX and TX of the GSM module should connect to the same TX and RX TX of the Arduino Uno.

6. Antenna: There is GPS module and the GSM module that are claimed to be dependent on antennas for the purposes of them being functional. Be sure your each module is fitted with the correct antenna.

7. Integration: Develop code for the Arduino Uno that connects with GPS sensors, determining whether there is any cause for danger (defined as GPS beacons along predetermined unsafe locations and manual triggering), and sends SMS in case of need using a GSM module. Make sure that the code stands a good structural review, takes reasonable time to execute and has appropriate comments for easy maintenance and understanding.

8. Testing and Debugging: Once you have integrated all the components of the circuit and written the code, thoroughly test its performances in various tests for you to know the device’s effectiveness and reliability. Eliminate any occurrences of errors characteristic

during testing and continue perfecting the design to match up the requirements.

9. Cloud Integration: The next step is to set up the cloud environment, which may include AWS, Google Cloud, or Azure, allowing you to store the victim's location data online. Furthermore, this will involve additional coding to transmit this data to the cloud during an internet connectivity (such as Wi-Fi or GSM) as well as employ data safety strategies to secure the data.

The completion of these actions would give you a chance to construct a Safe and Operational Internet-of-Things (IoT) Safety device which will be an effective alert platform as well as an uploader of location data to the cloud machines.

5 Design Analysis and Evaluation

5.1 Novelty

1. Integration of IoT Technology with Arduino:
- Arduino has been a common choice for projects of all kinds, but when it comes to IoT integration it goes a step further by allowing any device to communicate over the internet.
- Through the integration of IoT, your safety device will be able to communicate with other machines or systems; therefore, it will be possible to have remote sensing and control abilities.
- This integration enables to transfer data in real time, for analysis and decision making processes. It becomes possible to increase the safety device’s functionality and effectiveness.

2.Automatic Alert System:
- The automatic emergency alert system is based on the function of the sensors, mainly it is a GPS. They detect pre-defined dangerous situations or trigger events.
- Different from emergency alert systems that use manual activation, the system is based on the fact that automatic detection of emergencies with the help of criteria that are already defined is conducted, which results in faster response times.
- The device will automatically alert designated contacts/authorities of the incident whether the user is unable to trigger the alert or is incapacitated.

3. Cloud-Based Location Tracking:
- Cloud-based location tracking adds to the feature set of the safety device with cloud storage of location data as well.
- Through this element, one can watch the location of the device in real-time from the Internet-connected device like a smartphone or PC.
- The cloud-based system, which is safe and easily accessible, ensures that location data is securely backed up from anywhere, maintains user's piece of mind himself and his loved ones.

4. User-Centric Design:
- User-focused design strives on meeting the demands and anticipation of the users, thus producing a favorable user experience.

- In regards to your safety device, user-centric design principles are utilized to make it user-friendly, easy to use, and dependable in case of emergencies.

In summary, the novelty of your project lies in its integration of IoT technology with Arduino, the implementation of an automatic emergency alert system, the use of cloud-based location tracking for real-time monitoring, and the adoption of user-centric design principles to ensure a seamless and effective user experience.

5.2 Design Considerations (PO(c))

5.2.1 Considerations to public health and safety

1. Accessibility:
   Providing that the Safety Device implementing the IoT is available to all individuals, comprising the disabled persons or the individuals having special needs, is of primary importance for public health and safety. The devices interface design should give consideration to such features as a large font size, voice commands and the provision of tactile feedback to accommodate those with visual, auditory and motor impairments.

   2. Reliability:
   The device of reliability is the main thing that let a quick help in case of emergency to be assured. Vigorous test procedure and rigorous quality assurance processes should be employed to validate a device working under conditions like extreme temperature, humidity and even physical impact. Furthermore, the replacement of key components should be reduced through implementing redundant systems and fail-safe mechanisms which could minimise the risk of a device failure.

   3.Privacy:
   Privacy and confidentiality of user data are the key issue since it is the public health and safety. The devise should be conform to industrial regulations and standards for data security, for instance encryption, authentication and access controls, so that the sensitive information can’t leak out or be misused and unauthorized access can be prevented. Users should be provided with understandable policies and consent mechanisms to give them the tools and establish the basis for future interaction.

   4. Emergency Response Coordination:
   Coordination of emergency response agencies and healthcare providers is important factor of systematic approach and response to emergency situations. The safety device should unite smoothly with preexisting emergency response system and enable the emergency responders to get real time information on location and speak with people who are in danger. Training programs together with protocols should be established to educate emergency people on handling and abilities of the safe device.

5. Community Engagement:
Letting communities and stakeholders involved is mandatory for celebrating the indicators of safety device and encouraging it use. The publicity of the campaign should include the device and how its features benefit individuals to the maximum. Feedback systems should be implemented to collect input from users and other stakeholders, by which the product can be tunned up, and get polished.

6. Regulatory Compliance:
Adherence to regulatory requirements and norms in medicine, telecommunication, and encryption is one of the crucial tasks to maintain unity, safety and security of public. The safety device shall be required to pass all the necessary regulatory controls and documentation such as certifications to show that it is effective, safe and complies with the existing regulations. Ongoing monitoring, as well as compliance management, should be conducted in order to implement corrective measures concerning new regulations' or updates' emergence.

Considering the latter health and security of the marginalized individuals, our project, relying on IoT-based Safety Device, strives to improve the living conditions of the said people. We achieve this by partnering with key players, complying with best practices and a long-term improvement on health.

5.2.2 Considerations to environment

1. Energy Efficiency:
Such kind of IoT-based Safety Device requires having energy-efficient components and algorithms to decrease its environmental imprint. Low power microcontrollers, sensors and communication modules that optimize power consumption and facilitate longer battery lives should be integrated into the design. Moreover, power-saving characteristics in the form of standby modes and dynamic power management can contribute to the improvement of energy efficiency.

2. Sustainable Materials:
The utilization of environment-friendly material and processes for the structuring of the safety apparatus leads to a little impact on the environment. If there are options, elements and items should be produced from renewable and recycled sources. Developing a disassembly and recycling model for a device at the end-of-life ensures that resources are used up efficiently and waste is minimized.

3. Reduced Emissions:
Mitigating electromagnetic interference (EMI) and radio frequency (RF) emissions is a step forward in environmental stewardship. With the use of shielding technology, circuit design optimizations, and obeying emission regulations, the electromagnetic pollution can be controlled. Another factor is the selection of communication protocols and technologies which have reduced output power which would in turn reduce RF emissions.

4. End-of-Life Considerations:
Engaging in the closing-life planning and recycling of the safety tool is necessary of environmental sustainability. Creating the designing of the device from the start for easy disassembly and separation of the components helps recycling and reusing the materials. By giving directions on proper disposal techniques and working with recycling facilities we assure that e-waste is being handled in a sustainable way and contributes to avoid environment pollution.

5. Lifecycle Assessment:
An environmental life cycle assessment of the safety device would assist in evaluating its impact from the time of manufacture till disposal of the product. The consideration of aspects such as the consumption of energy, material, emissions, and waste contribute a great deal in defining improvement strategies and green design solutions. Life cycle assessment also help build a basis for informed decision making and constant improvement of device's environmental efficiency and sustainability.

6. Environmental Regulations:
The compliance with the environmental regulations and standards is absolutely vital for ensuring the ecological safety device sustainability. Fulfillment of regulations like the RoHS (Restriction of Hazardous Substances) and the WEEE (Waste Electrical and Electronic Equipment) directives helps eliminate the use of hazardous substances and introduces responsible recycling and disposal methods. By understanding the emerging environmental regulations and having compliance measures in place during device design and manufacturing processes, is a vital thing to protect the environment.

The aim of this consideration of environmental factors is to reduce the impact of the IoT-Based Safety Device production, operation, and end-of-life on environment and support more sustainable production for the benefit of people and the world.

5.2.3 Considerations to cultural and societal needs

1.Cultural Sensitivity :
The device should be designed with consideration of cultural preferences, beliefs and practices concerning personal safety and emergency response. To cater for different cultural backgrounds the user interface, language options and symbols on the device should be culturally sensitive and inclusive.

2 Accessibility

Inclusivity is promoted by ensuring that the safety device is accessible to individuals with diverse cultural and social needs. This can entail creating human-machine interfaces as well as functionalities which are accessible to those who cannot see or hear properly. By providing alternative communication means like text-to-speech or braille support, users with different requirements are able to access the system.

3 Community Engagement:

Community involvement in development as well as implementation process fosters trust, collaboration and social cohesion. Running community outreach programs, focus groups, cultural sensitivity training sessions helps raise awareness about the safety device while drawing input from diversified viewpoints. The concerns of locals are essential if this device is expected to appreciate their societal background

4. Privacy and Confidentiality:
Privacy and confidentiality preservation deliberately to clients is the base in shaping the level of trust between the culturally diverse site and its users that could play a role in the device adoption. Besides, it's also crucial to ensure transparency regarding how the device is data collected, stored and shared which will dispell any doubt about privacy and as a result provided users wih comfort while using the device. Because of the fact that users are provided with ability to govern their private details by editing privacy settings they gain confidence and feel more itly among them.

5. Gender and Identity Considerations:5. Gender and Identity Considerations:
A series of safety approaches for various types of gender and expressions will make the campus inclusive and will provide solutions tailored to specific safety needs of people. An award-winning safety device will feel welcoming to everyone if uses gender neutral language and images in designing it to prevent the reinforcement of stereotyping attitudes, and as a result, the mix of experiences. Providing an opportunity to individuals to display their gender orientation and have the tailored settings accommodate these preferences will help users to exercise user autonomy and enhancing the coveted user autonomy.

6. Cultural Competence Practice

Such process enables the trainer to understand the civil factors which can influence the users either in comfort or in discomfort and create their own lifestyle when using the product. In training programs, topics like cultural comprehension and dialogue need interpersonal communication and management specialized interface with minorities should be taught. Employees that can understand each other's cultural differences will be able to have a clear understanding on different users' requests depending on the set cultural dimensions.

Our goal is formulizing a solutions-oriented, comprehensive approach based on the culture-aware and all-inclusive principle by taking into account these cultural and social requirements during IoT based Safety Device design, developmental and deployer activities for more vulnerable individuals/communities.

5.3Limitations of Tools (PO(e))

Technological Limitations and Constraints:

Hardware Failures:
- Technological Limitation: The type of chips applied to our programmed Safety Device might encounter sporadic data-reading faults owing to hardware imperfections or weak performance.
- Maximum Limit: Although the topmost reading failure chances may differ from one chipset to the rest and conditions, the failure of data ensure the safety perfection and success.
- Tolerances: Correspondingly, the tolerances for data read failure should be kept at the least possible level to maintain the functionality and integrity of the device. The loss of any kind of redundancies beyond the safety system requirements will lead to the loss of backup safety monitoring capabilities.
- Probable Errors: Ranging from sporadic connections to data corruption to faulty hardware, the

most frequent mistakes related to chip data read failures include the following. Those mistakes make inaccurate readings, delayed emergency messages or complete devices failures possible.

2. GPS Limitations:
- Technological Limitation: On the other hand, humanize the principle of accuracy and precision of the GPS module integrated into the safety device should be practically achievable and doable.
- Maximum Limit: The distance GPS could measure was 300 meters maximum, meaning there was a chance that the platform could not get the right location of the user. Such shortcoming can however change depending on other elements, for example the number of satellites in operation, interference, and atmospheric conditions.
- Tolerances: The GPS inaccuracies may be values and should be considered when designing devices for functions or emergency response procedures. Users and emergency responders have to understand limitations of location tracking during emergencies to construe no confusion and misinterpretation.
- Probable Errors: The devices with GPS functionality also have minor defects such as position shift, signal multi-path impacts and satellite signal blockage. The mistakes may lead emergency services to delayed or erroneous locations, which will affect the efficiency and accuracy of emergency response and resuscitation.

3. Sensor Failures:
- Technological Limitation: There can be technical failures from time to time in the sensors when they are unable to detect vibrations accurately owing to the issue of sensitivity or the level of fluctuation present in the environment.
- Maximum Limit: The possible failure of the sensor vibration sensing limit must be minimized in order for reliable reading of emergency cases such as falls or distress signals.
- Tolerances: Limitations for vibration sensing failure among sensors must be thoroughly addressed in order to differentiate real emergency events from false alarms. By running calibration procedures and sensitivity adjustments sensor inaccuracies can be reduced to a suitable level.
- Probable Errors: Signal noise, calibration drift, and mechanical failures are the typical faults related to the sensor vibration sensing.

Incorporating into the design quality management systems, error handling strategies, and the development of supplementary approaches will supply the robustness and resilience to the IoT based Safety Device. The permanent testing and assessment process is indispensable for detecting the weakness and finding the solutions to facilitate the device's positive effects in safeguarding the security of vulnerable groups.

5.4Impact Assessment (PO(f))

5.4.1 Assessment of Societal and Cultural Issues

1. Privacy Concerns:
Privacy issue is one of the most important concern today, mainly because of the impact made by personal data collection and sharing in the digital universe. The end user may be skeptical over their location being transmitted up to the cloud and further shared with emergency services.
The issue of varied notions about privacy and the sharing of information is a common phenomenon in different cultures. Individuals in certain societies might be determined to protect personal privacy rather than privacy of others which could be collectively viewed as infringing on safety and security. since privacy is always an issue, the security device will integrate a strong data encryption and security mechanisms meant to ensure data security. In addition, clarity on data hamdling methods and user consent mechanisms that employ transparency in communication can help build trust, ease privacy issues and consequently increase adoption levels by users.

2. Trust and Acceptance:
Societal Issue: With such a device, trust and acceptance are all-important for the proper use and implementation. The user should have the facility of using the device with confidence that it is accurate, responsive, and reliable, especially in urgent circumstances.
Cultural Consideration: Peopleís cultural attitudes, beliefs, and values can determine the way people think about technology and the rate at which they choose to embrace newly introduced innovations. One cultural factor may be the mistrust of technology or commitments to traditional methods among the target group, which can influence their acceptance of the safety technology.
Mitigation: Participation in intercultural programs that are linguistically and culturally valuable brings trust and support from the inhabitants and the stakeholders. Giving users a chance to feed-back and participate in design and development may also provide the user with an extra level of confidence and the acceptance of the safety device is promoted.

3. Accessibility and Inclusivity:
Societal Issue: Providing access for all and taking into account the variable lifestyles of, for example, disabled or completely different individuals, are key points of addressing the multidimensional problems.
Cultural Consideration: It varies within cultural perspective towards disability and accessibility which has a big impact on the successfulness of the safety device. Cultural responsive approaches are also needed to be able to relate with diverse cultural views on the disease and also disability access.
Mitigation: Integrating the safety tool with the modified interface and communication techniques, and multiple languages, will catcall for more inclusiveness. Engaging in discussions with advocacy groups for disabled people and cultural specialists will certainly furnish with good background experience on culturally relevant accessibility measures.

4. Gender and Social Dynamics:4. Gender and Social Dynamics:
Societal Issue: Both men and women can view the safety device with either a positive or a negative inclination, which can provoke to the social dynamics and gender-related issues. Concerning the usage of social media and related cultural constraints such as norms and expectations which involve gender roles, power dynamics, and social hierarchies may affect the utilisation patterns and also user experiences.
Cultural Consideration: Attitudes to gender equality and positional hierarchy also differ in various cultures in a way that makes the development and application of the safety device difficult. The indispensable feature of the gender-sensitive and culture-centric strategy is the aim to empower girls and women to participate equally in using the Internet.

Mitigation: Incorporating safety device with gender neutral features can help to create a non gender specific fences and this can help promote inclusiveness and avoids reinforcing the gender stereotypes. Inter cultral sensitization of the staff that will be involved in the rollout and support of the product is a vital thing that can be done to make the work of dealing with gender and social dynamics effective.

Having done this we will try to solve these social and cultural problems with our proactive actions and culturally sensitive approach as we certainly want the project to become really effective, liked and accepted by people all across the globe.

5.4.2 Assessment of Health and Safety Issues

1. Emergency Response Time:
Health Issue: Indeed, fast action can be crucial in such instances as health or falls response due to risks of mortality in elderly people.
Safety Issue: The transmission of the emergency message can be delayed or the location data uploaded to the cloud can take time which make the effectiveness of the safety device low with its effect being lack of timely responses to emergency.
Mitigation: In order to reduce the response time to the levels possible, the safety device has to be developed on the basis of the optimized communication protocols and data transmission routes. Moreover, the device's testing and maintenance after-sale is also a crucial step to ensure durability and proper functioning in emergency cases.

2. Reliability of Sensors:
Health Issue: The reliability of the sensors used in safety equipment can provide enough information to appropriate departments in order to permit the emergency services to offer quick and efficient responses to instances such as falls or distress signals.
Safety Issue: The sensor might fail to detect or send inaccurate readings, which wind up as missed detections or false alarms, undermining the entire intend of the safety device for early detection and response to emergencies.
Mitigation: Carrying out circumstantial checkup and calibration of sensors so as to verify correctness and reliability becomes a must. Implementation of the system backup using redundant sensors, attached mechanisms or implement the fallback will provide alternate options in case of the sensor failure. Upgrading the sensor accuracy and taking calibrations in a periodic base should contribute to lessening the decline in sensor performance.

3. Data Security and Privacy:
Health Issue: Protection of both the security and privacy information of user data is the primary concern that could be used for the purpose of illness information confidentiality and personal safety.
Safety Issue: Illegal access to the user's location data or emergency messages stored in the cloud can impart heedlessness of their privacy whilst even risking their safety by hackers and criminals.
Mitigation: Establishing good data encryption, access controls, and authentication means, sharing sensitive data becomes more secure and only well-known people, having permission to access information, obtain it. Compliance to data protection legislation and market standards is the guarantor of privacy since they are the guarantees that privacy rights are not violated. The best way to remain secure is to conduct regular security audits and provide updates to eliminate emerging angles and vulnerabilities.

4. User Interface Design:
Health Issue: An intuitive interface that allows users to navigate without challenges is vital as people may die of stress or lose consciousness during emergency situations. This especially applies to those

who may have problems with their health or have psychological issues.
Safety Issue: Users can have trouble functioning well the unknown interfaces of the safety device because of its complexity or unintuitive interface design and may impede immediate and efficient emergency response efforts.
Mitigation: User Interface (UI) designing with simplicity, transparency and accessibility as founderation principles is mandatory. Such mechanisms as big buttons, very clear icons, and understandable navigation pathways introduces the element of accessibility, which is very much important for people who are less tech savvy or suffer from cognitive dysfunction. Usability tests conducted by a set of user groups that are heterogeneous help us unearth and sort out usability problems in the interface.

By implementing the preventive and conscientious measures and designing approaches, the purpose of the Safety Device with IoT in this project is directed at the safety of at-risk people during critical moments.

5.4.3 Assessment of Legal Issues

Acquiring and storing personal data including specific addresses and contacts increases a fear of invading personal space and violating regulations on privacy and data protection.
Adherence to regulation is a must. The EU's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA) are necessary amongst others. The implementation of secure data encryption, access controls, and predetermined consent policies will ensure that users' information is treated safely and accordingly to the law.

In the case of a device hazard or shutting down of emergency system, issues of liability coverage to any likely harm or injuries may define.
Defining, in first place, the responsibilities and liabilities of the device manufacturer, service provider and user in this artifact (device) terms of service or user agreement is of the utmost importance. Letting users know that the device has limitations in functionality and could be affected by service disruptions, clarifies user's expectations and reduces the possibility of being legally blamed.

Sending messages through mobile phone numbers can potentially subject the SMS campaign to telecommunications regulations, for instance, delivering the message, protecting privacy, and ensuring reasonable access to telephone emergency services.
It is of crucial importance to comply with the telecommunications regulations specifying the area where the device is being set up. Securing a license or a permit for broadcasting emergency messages and conforming to commercial quality standards for message transmission and privacy protection will be the steps taken to eliminate legal risks and guarantee proper operations.

Preservation of IP for the design, technology and software architecture of the safety device is of prime importance in order to avoid copying or misappropriation by competitors.
Applying for patents, trademarks, or copyrights for the innovations in terms of design, production, technology or general aspects of the safety device helps to protect intellectual rights. Reaching an agreement where both parties acknowledge the non-disclosure of data and trade secrets in combination with restricted access to private information stop

unauthorized use or leaking.

With the application to medical devices, telecommunications equipment, and data protection legislation, there is a need to follow the guidelines appropriate to medical devices, telecommunications equipment, and data protection.
Performing rigorous regulatory assessment and getting the certification if needed, which could be a CE marking in European Union or an FCC certification in United States, serves as a verification that the product is compliant with appropriate regulations. Creating mechanisms for the end-to-end monitoring of compliance and regulations in upgrades is what guarantees the device remains as per the evolving legal requirements.

Through reputable strategies of legal compliance and risk mitigation, our Safety Device project based on internet of things seeks to make this product legal with regard to the safety rules and reduce a threat of legal liability.

5.5 Sustainability Evaluation (PO(g))

1. Environmental Impact:
   - Energy Efficiency: The IoT-based Safety Device shall include low power components and shall utilize the power management techniques to maximize the battery life and to achieve low environmental impact.
   - Sustainable Materials: Sustainable resources and processes must be an integral part of device production to diminish both the resource depletion and pollution level associated with device production and disposing.
   - End-of-Life Disposal: Constructing the safety network which is simple to disassemble and recyclable helps to dispose materials responsibly at the end of life ensuring resource conservation.

   2. Social Impact:
   - Accessibility: Considering accessibility features in the design of a safety device is the key to inclusive safety device, catering for the diverse needs of each individual, including those with disabilities or special requirements.
   - Community Engagement: By involving the communities and other stakeholders throughout the project life cycle, trust, collaborations and social cohesion will be encouraged thus leading to acceptance and adoption of the device.
   - Cultural Sensitivity: Adding the cultural sensitivity into the construction and operation of the safety equipment serves to reflect the various cultural perspectives and values, thereby strengthens the relevance and effectiveness of the safety equipment no matter where it is deployed.

3. Economic Viability:
- Cost-Effectiveness: Through optimization of costs in the process of developing the safety device, the product will be available to the customers in particular in settings lacking of resources or among underprivileged communities.
- Scalability: The designing of safety device bearing scalability in mind excludes an easy way of deployment for large number of users now as well as a long-term sustainability with a consideration of future growth and user's needs will also be addressed within those designs.
- Return on Investment: Through the appraisal of the monetary advantages and the return of investment associated with the safety device wherein you get to have reduced healthcare cost or improved work skills, investment would be justified and fund would be raised security for the sustainability initiatives.

4. Ethical Considerations:
- Data Privacy: Firstly, User privacy and data protection are essential measures for users' rights protection, as well as for ensuring safety devices' popularity owing to the ethical principle of user's autonomy and confidentiality safeguarding.
- Transparency: Communication being open about drug's functions, capacities, limitations, and the way data is used and handled ensures ethical and responsible behavior in its application and deployment.
- Equity: Maintaining fair and just emergency situations and health care delivery systems regarding equality are ensured by allocating the device to all people without the prejudices of socioeconomic status or geographic location.

5. Long-Term Impact:
- Maintenance and Support: Implementing robust maintenance and operation plans for system safety ensures the enduring operationality and effectiveness of the life-saving device, thus the lifespan is extended and public health and safety expectations are met.
- Continuous Improvement: Continually committing to the process of discussing, monitoring, finding issues, and fixing them is important to keep the relevance and resilience of the safety device in the face of new community norms and concerns.

By considering these sustainability factors in the design, implementation, and deployment of the IoT-based Safety Device, we aim to create a solution that not only addresses immediate safety concerns but also contributes to long-term societal well-being and environmental stewardship.

5.6Ethical Issues (PO(h))

1.Encryption:
Ethical Principle: Privacy and user's information security while designing and using the safety device is the utmost responsible issue.
Application: We have developed encryption and controls for access data on the cloud to secure data transmitted by the user. Also indeed we provided transparency of information on users' data processing.

2. Inclusivity and Accessibility:
Ethical Principle: Various approaches can be used to make the safety feature to be easily understood

and used by individuals coming from different backgrounds and with different levels of capabilities. This, in turn, creates opportunities for inclusivity and fairness.
Application: We made the user interface of the safety appliance with features that enhance the usability. For example, we included large buttons, clear icons, and voice commands to serve persons with disabilities or specific needs. It is also worth pointing out that we featured multiple language versions and provided an interface that is compatible with the screen readers for the visually impaired users.
Ethical Challenges: Adding the equalized access to interaction and communication with the product for all the people, including those of the physical or the cognitive disabilities during the development became a moral task. This was solved by consulting the accessibility experts, conducting user tests on many different user groups, involving their feedback to finally create top-quality accessibility features.

3. Transparency and Accountability:
Ethical Principle: Preservation of transparency and accountability in all processes of the project, including data management, decision making, and stakeholders interaction, is an important aspect in trust building and ethical integrity.
Application: We create standard channels of communication for the stakeholders to narrate their concerns and stakeholders views continually during project implementation. Additionally, we kept all design arguments, testing procedures and implementation steps open to public scrutiny for proactiveness and accountability in project management.
Ethical Challenges: Ethical quandaries arose where the demand for secrecy was meant intertwined with that of disclosure of proprietary information and intellectual property rights. While dealing with these problems, we applied selective transparency policy by providing information only to the stateholders whose actions were directly connected to the project and on a need to know basis. Also, by signing of the non-disclosure agreements and other safeguards, the confidential and sensitive information was protected.

6 Reflection on Individual and Team work (PO(i))

.

6.1 Individual Contribution of Each Member

Student ID No.	Individual Contribution
1906012	Circuit Simulation , design , making circuit hardware and writing report
1906018	Writing Algorithm for Arduino code , Buying Components and writing Report
1906027	Writing Arduino Code , Making Embedded System, Debugging and Writing Report

6.2 Mode of Team Work

Our Mode of teamwork was mostly Face to face collaboration. We also some times used virtual collaborations according to our needs. We did circuit simulation ,design and report via virtual teamwork. Again we did the circuit making and embedded system with face to face collaboration .

6.3 Diversity Statement of Team

Student ID No.	**Diversity Statement**
1906012	Creative Hard worker and circuit designer
1906018	Circuit solver and software related problem solver
1906027	Creative problem solver ,hardware implementer and Code debugger

6.4 Log Book of Project Implementation

Date	**Milestone achieved**	**Individual Role**	**Comments**
15-1-24	Project Proposal	1906027,1906012,1906018	Task completed
25-1-24	Building circuits and simulation	1906012	Task completed
2-2-24	Writing algorithm and code	1906018	Task completed
8-2-24	Uploading the code and making embedded system	1906027	Task completed
16-2-24	Debugging	19906027,1906012	Task completed
23-2-24	Making this user-friendly ,making PCB and others	1906027,1906018	Task completed

7 Communication to External Stakeholders (PO(j))

.

7.1 Executive Summary

Introducing the Next Generation of Safety: IoT-Based Safety Device Ensures Protection for Vulnerable Individuals

The team that we are excited to introduce at this time the inauguration of our project for the course on Microprocessors and Embedded Systems Laboratory – the IoT enabled Safety Device dedicated to response to individuals facing threats and danger. This unique system is a source of emergency notifications that will be sent by text messages to identified phone numbers whenever there is danger. Location will also be uploaded to the cloud for the quick deployment of assistance. For the Safety Device to be successful, we have designed a user-interface that will be secure and straightforward. Its seamless functionality offers peace of mind to families and communities who care. Take part in shaping up new protective systems and solving the problems of those who have nowhere else to seek help.

For more information, please contact [1906027@eee.buet.ac.bd].

Project Group 6
Members : i) Progna Dipto Saha
ii) Shahan Bin sharif Hirock
iii) Md. Sumon Howlader

Date;24-02-24

7.2 User Manual

<u>IoT-Based Safety Device User Manual :</u>

Thank you for making us your selection of the IoT based safety device which will guarantee safety of people from risks and hazards. The present manual is tailored in such a way that it offers you every information of how to install and properly use the device.

1. Introduction:
Thus the device uses IoT technology to transmit emergency alerts to designated telephone lines when you are inst the danger. i;e does it as well as the location data is sent to the cloud for the fast and effective isolation.

2. Getting Started:
- Unboxing: Instruments were taken off carefully and everything is included in package verification was done.
- Setup: After dropping the SIM card into the device, power it on using the predefined source of energy.
- Connectivity: Connect the device to a legitimate wireless network or ensure HTTP traffic is enabled for perfect functioning. Languages used in these messages are often adapted to reflect

cultural linguistic traditions and colloquial expressions.

3. Device Operation:
- Emergency Activation: Upon any emergency, touch the intended emergency button on the device to turn an automatic message into the phone numbers that are your pre-selected numbers.
- Location Tracking: The included feature with my device will automatically upload the user"s location to the cloud and will help responders identify the victim's whereabouts.
- Status Indicators: Pay attention to the LED lit on the device which shows if it is on or not. The indicators will also tell if the device is connected to your network or to the internet.

4. Configuration:
- Phone Numbers: Utilize the given configuration interface to include the emergency contacts by numbers.
- Cloud Upload: Provide the cloud storage service and bring to bear the right authentication mechanisms, which provide the secured upload of data.

5. Maintenance:
- Power Management: This device features a battery life indicator. It can warn you if the battery level is low and needs to be recharged.
- Software Updates: Try to find any updates that your software has and install them to keep the devices in good working condition.

6. Troubleshooting:
- Connectivity Issues: It is recommended to confirm device's connection to network and properly configure the device for Wi-Fi or cellular communication mode.
- Power Problems: Be sure to look over the power source and connections to eliminate any difficulties of devices power or charging.

7. Support:
For any questions, technical support, or assistance, please contact our customer support team at [1906027@eee.buet.ac.bd].

We hope this user manual helps you effectively utilize our IoT-based Safety Device to ensure the safety and well-being of vulnerable individuals. Thank you for trusting us with your safety needs.

Project Group 6
Section A1

7.3 Github Link

https://github.com/PrateekSinghRajput

7.4 YouTube Link

https://youtube.com/shorts/2fCjwPVwIm0?feature=share

8 Project Management and Cost Analysis (PO(k))

8.1Bill of Materials

Name of Component	Price/Cost (Tk)
Arduino UNO	800
Wifi module	600
GPS Neo 7M	400
SIM 800L Module	500
Resistors	30
Battery	30
Breadboard	150
Jumpers	40
Push Button	10
Total	2560

8.2 Calculation of Per Unit Cost of Prototype

So , The per Unit cost of the prototype is around 2500 Tk

8.3 Calculation of Per Unit Cost of Mass-Produced Unit

For Mass Production it should be developed for being more portable and efficient. Then we can make compact Circuit and the possible cost for per unit will be around 2000 Tk

8.4 Timeline of Project Implementation

Week No.	**Milestone achieved**	**Individual Role**	**Percentage Work Completed**
15-1-24	Project Proposal	1906027,1906012,1906018	10%
25-1-24	Building circuits and simulation	1906012	20%
2-2-24	Writing algorithm and code	1906018	30%
8-2-24	Uploading the code and making embedded system	1906027	50%
16-2-24	Debugging	19906027,1906012	75%
23-2-24	Making this user-friendly , making PCB and others	1906027,1906018	100%

9 Future Work (PO(l))

To develop the IoT-based Safety Device project into an industry-standard solution, several future works and improvements can be considered:To develop the IoT-based Safety Device project into an industry-standard solution, several future works and improvements can be considered:

1. Enhanced User Interface (UI) and User Experience (UX):1. Enhanced User Interface (UI) and User Experience (UX):
- Bring modifications in the device's UI/UX design so it suits individual needs and simple to use.
- Invite an end-user to participate in user testing sessions and get feedback to learn where modifications are required to augment usability and functionality.

2. Advanced Data Security Measures:2. Advanced Data Security Measures:
- Deploy top-class encryption technologies and defend secure protocols to shield user data that goes into the cloud.
- Aim at the fulfilment of the industry standards and the data privacy and security regulations. This implies, to mention a few, the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA).

3. Scalability and Reliability:
- Ensure proper designing of a scaling device to handle a larger audience and more data over time.
- The fault tolerance capability of the device may be improved by implementing the redundancy and failover feature to reduce the device downtime to zero or minimize the downtime to the level that can meet performance requirements.

4. Integration with Emergency Response Systems:4. Integration with Emergency Response Systems:
- Develop a system that integrates the device to be used with the emergency response systems currently associated with existing emergency response services.
- Make a real-time and interactive connection among the device and emergency responders for the sake of immediate help possible.

5. Geolocation Accuracy and Precision:5. Geolocation Accuracy and Precision:
- Increase the accuracy of the device's geolocation system by the use of technology to provide reliable location information during livesaving operations.
- Proposing the employment of sophisticated positioning solutions which include GPS augmentation systems or indoor positioning systems is paramount in that they should ensure seamless location tracking.

6. Real-time Monitoring and Analytics:6. Real-time Monitoring and Analytics:
- Integrate real-time screen waching and analytical interfaces to monitor device working, user behavior, and emergency response related metrics.
- Data analytics can help to find answers to questions, addressing how well the device is functioning and whether the performance can be improved.

10 References

Demo video : https://youtube.com/shorts/2fCjwPVwIm0?feature=share

Github Link : https://github.com/PrateekSinghRajput

Other Links : https://youtu.be/4A5U0igktGE?si=7LUxK8NyQDpaMnVZ