

VEHICLE THEFT CONTROL AND ACCIDENT LOCATION INTIMATION USING IOT

Submitted in partial fulfilment of the requirements for the award of

**Bachelor of Engineering degree in
Electronics and Communication Engineering**

By

V SIVA NAGA MALLESWARA RAO (38130239)



**SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade “A” by NAAC
JEPPIAAR NAGAR, RAJIV GANDHI
SALAICHENNAI – 600119**

MAY-2022



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **V SIVA NAGA MALLESWARA RAO (38130239)** who carried out the project entitled "**VEHICLE THEFT CONTROL AND ACCIDENT LOCATION INTIMATION USING IOT**" under our supervision from August-2021 to May-2022.

Internal Guide

(Dr. L.MEGALAN LEO, M.E., Ph.D.)

Head of the Department

(Dr. T.RAVI M.E., Ph.D.)

Submitted for Viva voce Examination held on_____

Internal Examiner

External Examiner

DECLARATION

I, V SIVA NAGA MALLESWARA RAO (38130239) hereby declare that the Project report entitled “**VEHICLE THEFT CONTROL AND ACCIDENT LOCATION INTIMATION USING IOT**” is done under the guidance of **Dr.L. MEGALAN LEO M.E.,Ph.D** is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING**.

DATE: **V SIVA NAGA MALLESWARA RAO (38130239)**

PLACE: **SIGNATURE OF THE CANDIDATE**

ACKNOWLEDGEMENT

We are pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey our thanks to **Dr .N.M.NANDHITHA, M.E., Ph.D.**, Prof & Dean of school of Electrical and Electronics Engineering and **Dr .T.RAVI, M.E., Ph.D.**, Heads of the Department, Department of Electronics and communication Engineering for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr .L.MEGALAN LEO, M.E., Ph.D.**, for their valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

We wish to express our thanks to all Teaching and Non-teaching staff and also panel members of the Department of Electronics and communication engineering who were helpful in many ways for the completion of the project.

ABSTRACT

According to this project when a vehicle meets with an accident immediately Vibration sensor will detect the signal or if a car rolls over, and vibration sensor will detects the signal and sends it to NODEMCU controller. Alcohol detection, eye blinks monitoring is performed by the NODEMCU Microcontroller sends, it alert mail through the IOT including the location to police control room or a rescue team. So the police can immediately then after conforming the location necessary action will be taken. If the person meets with a small accident or if there is no serious threat to anyone's life, then the alert message can be terminated by the driver by a switch provided in order to avoid wasting the valuable time of the medical rescue team. This paper is useful in detecting the accident precisely by means of both vibration sensor and Alcohol detection content and eye blink monitoring.

TABLE OF CONTENT

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	vi
1	INTRODUCTION	1
2	LITERATURE SURVEY	2
3	EXISTING SYSTEM	4
4	PROPOSED SYSTEM	5
	4.1 BLOCK DIAGRAM	5
	4.2 REQUIRED COMPONENTS	7
	4.3 INTERNET OF THINGS	6
	4.4 ENVIRONMENTAL MONITORING	10
	4.5 ENERGY MANAGEMENT	13
	4.6 UNIQUE ADDRESSABILITY OF THINGS	16
	4.7 EMBEDDED SYSTEMS	32
5	RESULTS AND DISCUSSION	51
6	SUMMARY AND CONCLUSION	52
	REFERENCES	53

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
4.1	Block diagram of a typical embedded system	34
4.2	General Block of Power Supply Unit	36
4.3	Node MCU	39
4.4	Gas Sensor	41
4.5	Flaw Detection Using Ultrasonic Sensors	46
4.6	Sonic Sensor	47
4.7	Variables	48
4.8	Synthetic Variables Engine	48
4.9	Note that default variables are yellow, and Synthetic Variables are green	49
4.10	Variable is inactive during a specific amount of time	50
4.11	When a device enters or exits a specific area (geofence):	50
5.1	Circuit connection view	51
5.2	Circuit connections view 2	52

CHAPTER 1

INTRODUCTION

The amount of road accidents in India has been increasing at an alarming rate. In 2018, the Ministry of Transport (MoT) India reported a total of 548598 road accidents; where 6,284 of them were casualties that resulted in death. The life and death status of a victim is decided by the response time of the emergency response department (ERD) which varies depending on the speed the accident information is received by the ERD. The importance of having a faster response time when an accident has occurred is crucial to accident victims. Extensive analysis has shown that by decreasing the accident response time by a minute, it would help increase the chances of saving an individual of up to 6%. Characteristically, the response time of an accident is associated with the location and severity of an accident coupled with the congestion caused around the location of accident. During minimal traffic congestion, the occurrence of an accident would increase the response time for the ERD to be notified about the accident, sometimes up to 24 hours.

CHAPTER 2

LITERATURE SURVEY

Title 1: Electric Vehicle Intelligent Control System-Hardware modules configurations

Author: Gan Yu Han; Leong Chee Ken; Chew Kuew Wai

Content: The Electric Vehicle Intelligent Control System(EVICS) project where the EVICS is a 2-in-1 system for an Electric Vehicle(EV) which consist of Monitoring System for the front seat driver and Infotainment System for the rear seat passengers. The Monitoring system consist of battery voltage, current and temperature monitoring modules, battery energy status(%), distance left(km), km/h and rpm meter, offline and online Global Positioning System(GPS) and Contour Positioning System(CPS).

Title 2: An intelligent automotive climate control system

Author: K.C. Wei; G.A. Dage

Content:An intelligent automotive climate control system based on human-sensory response is developed and described in this paper. The system uses the skin temperature of the vehicle occupant, measured by a passive remote infrared sensor, and an intelligent controller to improve the perceived thermal comfort of the occupant. Thermal comfort is characterized in terms of a set of comfortable skin temperatures for different climate conditions. The controller monitors and regulates the skin temperature and air temperature to maintain the desired thermal comfort level. The new system not only increases the robustness of the controller, also renders a structure for a fully automatic (with minimal human intervention) climate control system.

Title 3: Smart temperature-controlled infant car seat using thermoelectric devices

Author: Roshni Senthilkumar, Mohamed Al Musleh

Content: The thermal comfort for children and adults inside the car is a crucial issue to improve as the hot environmental conditions can be irritable and uncomfortable.

Being inside an extremely hot car for a prolonged time can lead to major health problems. This paper focuses on the thermal comfort of infants. Traditionally air conditioning systems are used to cool down an infant car seat which is not effective due to the portability and cooling duration. In this paper, heat relief for the child is researched using a thermoelectric cooling system. This paper reviews various factors concerning the development of a temperature-controlled infant car seat. This study focuses on the health and safety of children inside the cars, the subjective needs of the parent, heat management in the car cabin environment, thermoelectric modeling, and the methods for precise temperature control for effective thermoelectric cooling. In-depth research has been conducted on the contributions of other researchers on the thermoelectric cooling system in a car

Title 4: IoT based Smart Vehicle Ignition and Monitoring System

Author: Fathima Jabeen; Sudhir Rao Rupanagudi; Varsha G Bhat

Content: With the advancements in technology, several smart innovations are being introduced by automobile manufacturers across the world to enhance their product portfolio. These can vary from implementing simple solutions such as navigation systems, to more complex ones such as driver assistance systems, which in turn could monitor multiple parameters of the vehicle in order to assist the driver. This paper focuses on one such driver assistance solution which not only intimates the driver on the well-being of his or her car but also adds additional layers of security to prevent vehicular theft. Keeping in mind driver safety, the paper also proposes an idea to prevent the vehicle from starting in case of alcohol consumption by the driver and also incorporates an emergency alert system in case of accidents.

CHAPTER 3

EXISTING SYSTEM

When a car meets with an accident, immediately the car's number and the GPS co-ordinates of the location are messaged to the nearby hospitals, thereby ensuring timely help to the needy. When the car is tried to crank, a text message is sent to the owner thereby intimating the status of the car. While during a long drive, if the car's engine goes faulty. The error signals from the dash board of the car and the GPS co-ordinates are captured and sent to the near-by service center, thereby saving time. Here the GSM is used to send the text message and the GPS is used to track the exact coordinates of the car. The serial communication interface UART is used for the communication between the Microcontroller (PIC 16F877A), GSM and GPS module. The RS232 communication standard is used for the following purposes. Electrical signal characteristics such as voltage levels, signaling rate, timing and slew-rate of signals, voltage withstand level, short-circuit behavior

CHAPTER 4

PROPOSED SYSTEM

In our country, many people have lost their life by accidents, because of causalities or improper communication. So an automatic vehicle accident and theft detection system are implemented. Also, it is used in the theft detection. To minimize deaths and to treat people with high injury due to accidents, immediate action would be take place by rescue teams. The project is built around the Nodemcu. This micro controller provides all the functionality of the mail alert system. The vibration sensor, Eye blink sensor, alcohol detection sensor transmitting the information to the mail.

4.1 BLOCK DIAGRAM

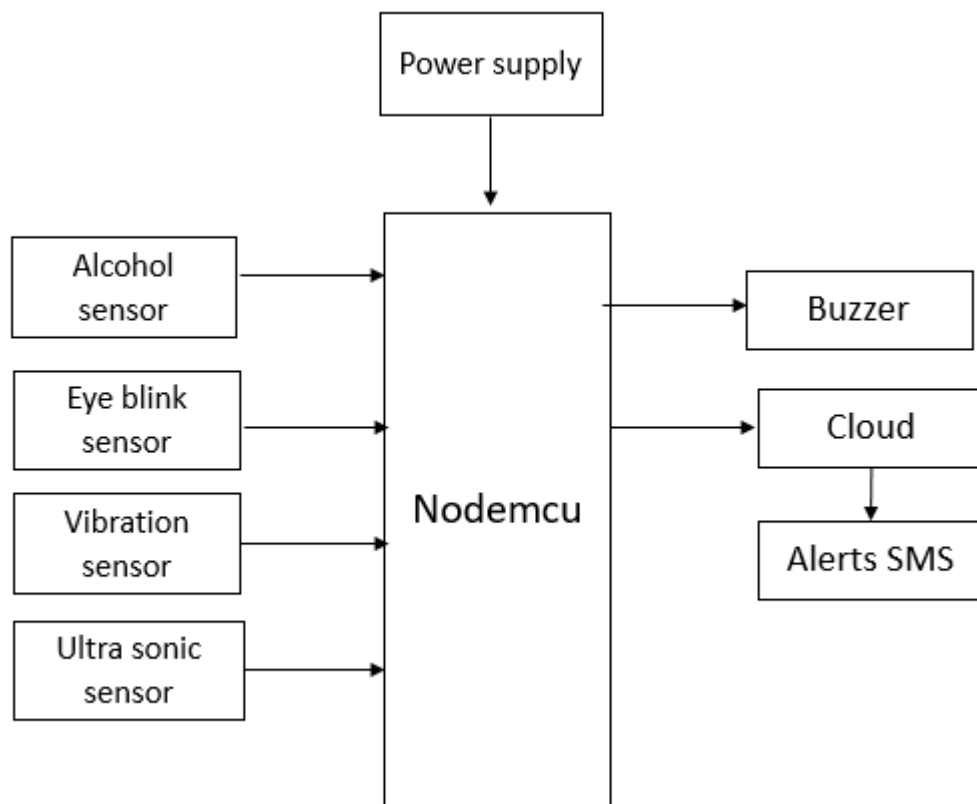


Fig 4.1 Block diagram

4.2 Required components

➤ Hardware required:

- Nodemcu
- Eye blink sensor
- Vibration sensor
- Alcohol detection sensor
- Ultrasonic sensor
- Buzzer

➤ Software required

- Arduino ide
- Embedded C

4.3 INTERNET OF THINGS

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks". The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology

becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to areas such as smart cities. "Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist firefighters in search and rescue operations. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service". These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include home automation (also known as smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring. As well as the expansion of Internet-connected automation into a plethora of new application areas, IoT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems.

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems.

This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IoT). The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994 Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the Internet of things became popular in 1999, through the Auto-ID Centre at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Centre) as a prerequisite for the Internet of things at that point. Ashton prefers the phrase "Internet for Things. "If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking. In its original interpretation, one of the first consequences of implementing the Internet of things by equipping all objects in the world with minuscule identifying devices or machine-readable identifiers would be to transform daily life. For instance, instant and ceaseless inventory control would become ubiquitous. A person's ability to interact with objects could be altered remotely based on immediate or present needs, in accordance with existing end-user agreements. For example, such technology could grant motion-picture publishers much more control over end-user private devices by remotely enforcing copyright restrictions and digital rights

management, so the ability of a customer who bought a Blu-ray disc to watch the movie could become dependent on the copyright holder's decision, similar to Circuit City's failed DIVX.

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems will have widespread and beneficial effects by 2025. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the Exchequer George Osborne, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances. The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning. On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favourite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of things can provide is enabling

extended home security features and home automation. The concept of an "Internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. However, the application of the IoT is not only restricted to these areas. Other specialized use cases of the IoT may also exist. An overview of some of the most prominent application areas is provided here.

In order to hone the manner in which things, media and big data are interconnected, it is first necessary to provide some context into the mechanism used for media process. It has been suggested by Nick Couldry and Joseph Turow that practitioners in media approach big data as many actionable points of information about millions of individuals. The industry appears to be moving away from the traditional approach of using specific media environments such as newspapers, magazines, or television shows and instead tap into consumers with technologies that reach targeted people at optimal times in optimal locations. The ultimate aim is of course to serve, or convey, a message or content that is (statistically speaking) in line with the consumer's mind-set. For example, publishing environments are increasingly tailoring the messages (advertisements) and content (articles) to appeal to consumers that have been exclusively gleaned through various data-mining activities. The media industries process big data in a dual, interconnected manner: Targeting of consumers (for advertising by marketers) Data-capture Thus, the Internet of things creates an opportunity to measure, collect and analyse an ever-increasing variety of behavioural statistics. Cross-correlation of this data could revolutionise the targeted marketing of products and services. For example, as noted by Danny Meadows-Klue, the combination of analytics for conversion tracking with behavioural targeting has unlocked a new level of precision that enables display advertising to be focused on the devices of people with relevant interests. Big data and the IoT work in conjunction. From a media perspective, data is the key derivative of device interconnectivity, whilst being pivotal in allowing clearer accuracy in targeting. The Internet of things therefore transforms the media industry, companies and even governments, opening up a new era of economic growth and competitiveness. The wealth of data generated by this industry (i.e. big

data) will allow practitioners in advertising and media to gain an elaborate layer on the present targeting mechanisms used by the industry.

4.4 ENVIRONMENTAL MONITORING

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

Control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control

systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The National Science Foundation established an Industry/University Cooperative Research Center on intelligent maintenance systems (IMS) in 2001 with a research focus to use IoT-based predictive analytics technologies to monitor connected machines and to predict machine degradation, and further to prevent potential failures. The vision to achieve near-zero breakdown using IoT-based predictive analytics led the future development of e-manufacturing and maintenance activities. The term IIoT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate \$12 trillion of global GDP by 2030 while connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be

designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IoT-enabled intelligent system of such cases has been demonstrated by the NSF Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, so that users will know in near real time when is the best time to replace band saw. This will significantly improve user experience and operator safety, and save costs on replacing band saw belts before they actually break. The developed analytical algorithms were realized on a cloud server, and was made accessible via the Internet and on mobile devices.

4.5 ENERGY MANAGEMENT

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). Besides home based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using advanced metering infrastructure (AMI) devices

connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and reclosers.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature: The integration of the internet with building energy management systems in order to create energy efficient and IOT driven "smart buildings". The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviours. The integration of smart devices in the built environment and how they might be used in future applications.

The IoT can assist in integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the

driver or user). Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Song do, South Korea, the first of its kind fully equipped and wired smart city, is near completion. Nearly everything in this city is planned to be wired, connected and turned into a constant stream of data that would be monitored and analysed by an array of computers with little, or no human intervention. Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants, has already seen 18,000 city application downloads for their smartphones. This application is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda among others. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification. Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluid mesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able

to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.

4.13 Consumer application

A growing portion of IoT devices are created for consumer use. Examples of consumer applications include connected car, entertainment, residences and smart homes, wearable technology, quantified self, connected health, and smart retail. Consumer IoT provides new opportunities for user experience and interfaces. Some consumer applications have been criticized for their lack of redundancy and their inconsistency, leading to a popular parody known as the “Internet of Shit.” Companies have been criticized for their rush into IoT, creating devices of questionable value, and not setting up stringent security standards.

4.6 UNIQUE ADDRESSABILITY OF THINGS

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code however this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners.

Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet of things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be critical for the successful

development of the IoT in the future. A combination of these ideas can be found in the current GS1/EPCglobal EPC Information Services (EPCIS) specifications. This system is being used to identify objects in industries ranging from aerospace to fast moving consumer products and transportation logistics.

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research to integrate the concepts of the Internet of things and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. In the future the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components), virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments.

The system will likely be an example of event-driven architecture, bottom-up made (based on the context of processes and operations, in real-time) and will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (multi-agent systems, B-ADSc, etc.). In an Internet of things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web. Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components,

avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations). Building on top of the Internet of things, the web of things is an architecture for the application layer of the Internet of things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyse and process data, thus providing easy real time scalability.

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IoT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, Domestic Robotics (Domotics) running inside a smart home might only share data within and be available via a local network.

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important. The GeoWeb and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbour operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things.

There are three core sectors of the IoT: enterprise, home, and government, with the Enterprise Internet of Things (EIoT) being the largest of the three. By 2019, the EIoT sector is estimated to account for nearly 40% or 9.1 billion devices.

A Solution to "basket of remotes"

According to the CEO of Cisco, the commercial opportunity for "connected products ranging from cars to household goods" is expected to be a \$USD 19 trillion. Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one

another. There are multiple approaches to solve this problem, one of them called the "predictive interaction", where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. While AllJoyn alliance is composed of the top 20 World technology leaders, there are also big companies that promote their own protocol like CCF from Intel. Manufacturers are becoming more conscious of this problem, and many companies have begun releasing their devices with open APIs. Many of these APIs are used by smaller companies looking to take advantage of quick integration.

IoT frameworks might help support the interaction between "things" and allow for more complex structures like distributed computing and the development of distributed applications. Currently, some IoT frameworks seem to focus on real-time data logging solutions, offering some basis to work with many "things" and have them interact. Future developments might lead to specific software-development environments to create the software to work with the hardware used in the Internet of things. Companies are developing technology platforms to provide this type of functionality for the Internet of things. Newer platforms are being developed, which add more intelligence. REST is a scalable architecture that allows things to communicate over Hypertext Transfer Protocol and is easily adopted for IoT applications to provide communication from a thing to a central web server. MQTT is a publish-subscribe architecture on top of TCP/IP that allows bidirectional

There are many technologies that enable IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfil:

- Bluetooth low energy (BLE) – Specification providing a low power variant to classic Bluetooth with a comparable communication range.
- Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth.
- Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range.

- QR codes and barcodes – Machine-readable optical tags that store information about the item to which they are attached.
- Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
- Thread – Network protocol based on the IEEE 802.15.4 standard, similar to Zigbee, providing IPv6 addressing.
- Transport Layer Security (network protocol) TLS – Network security protocol.
- Wi-Fi – Widely used technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point.
- Wi-Fi Direct – Variant of the Wi-Fi standard for peer-to-peer communication, eliminating the need for an access point.
- Z-Wave – Communication protocol providing short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi. Used primarily for home automation.
- Zigbee – Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.
- HaLow – Variant of the Wi-Fi standard providing extended range for low-power communication at a lower data rate.
- LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.
- Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission.
- Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.
- Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.

- Multimedia over Coax Alliance (MoCA) – Specification enabling whole-home distribution of high definition video and content over existing coaxial cabling.
- Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as Home Plug utilize PLC for networking IoT devices.

IoT modeling and simulation (and emulation) is typically carried out at the design stage before deployment of the network. Network simulators like OPNET, NetSim and NS2 can be used to simulate IoT networks. Digital Twins may also be implemented to produce updates on the status and health of an asset, based upon sensor readings integrated with a computational model of the asset.

Some scholars and activists argue that the IoT can be used to create new models of civic engagement if device networks can be open to user control and interoperable platforms. Philip N. Howard, a professor and author, writes that political life in both democracies and authoritarian regimes will be shaped by the way the IoT will be used for civic engagement. For that to happen, he argues that any connected device should be able to divulge a list of the "ultimate beneficiaries" of its sensor data and that individual citizens should be able to add new organizations to the beneficiary list. In addition, he argues that civil society groups need to start developing their IoT strategy for making use of data and engaging with the public.

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used. Presently the regulators have shown more interest in protecting the first three issues identified above. Current regulatory environment: A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:

- Data security – At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a “defence in depth” approach and encrypt data at each stage.
- Data consent – users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.

Data minimization – IoT companies should collect only the data they need and retain the collected information only for a limited time.

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multistakeholder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights.

A resolution passed by the Senate in March 2015, is already being considered by the Congress. This resolution recognized the need for formulating a National Policy on IoT and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the IoT ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to connect IoT devices

Several standards for the IoT industry are actually being established relating to automobiles because most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cyber security guidelines and a database of best practices to make automotive computer systems more secure.

IoT suffers from platform fragmentation and lack of technical standards a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard. Customers may be hesitant to bet their IoT future on a proprietary

software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect. IoT's amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active devices vulnerable.

Philip N. Howard, a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening information access. Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation. Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and Data Mining are inherently incompatible with privacy. Writer Adam Greenfield claims that these technologies are not only an invasion of public space but are also being used to perpetuate normative behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passers-by who stopped to read the advertisement. The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century. The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In *Discipline and Punish: The Birth of the Prison* Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era. Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism. In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned into a control society, with the computer replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.

The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely

overcome such invasion of privacy. Peter-Paul Verbeek, a professor of philosophy of technology at the University of Twente, Netherlands, writes that technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent. Justin Brookman, of the Center for Democracy and Technology, expressed concern regarding the impact of IoT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big data — well, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.'" The question is whether we want to have some sort of policy framework in place to limit that." Tim O'Reilly believes that the way companies sell the IoT devices on consumers are misplaced, disputing the notion that the IoT is about gaining efficiency from putting all kinds of devices online and postulating that "IoT is really about human augmentation. The applications are profoundly different when you have sensors and data driving the decision-making." Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy, you're going to have to watch the very concept of privacy be rewritten under your nose." The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IoT to erode people's control over their own lives. The ACLU wrote that "There's simply no way to forecast how these immense powers – disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control – will be used. Chances are big data and the Internet of Things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us." In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program. The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately. However the British Computer Society is doubtful these principles were ever actually implemented. In 2009 the Dutch Parliament rejected a similar smart metering

program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011.

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are send to a distributed system for the analytics of the sensory data. Another challenge is the storage of this bulk data. Depending on the application there could be high data acquisition requirements which in turn lead to high storage requirements. Currently the internet is already responsible for 5% of the total energy generated and this consumption will increase significantly when we start utilizing applications with multiple embedded sensors.

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices. According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology. In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control

pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators. David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as the bug that allowed the hack having been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it. The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers... An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search." In general, the intelligence community views the Internet of things as a rich source of data. As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015. IoTSF has a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners. In addition, large IT companies are continuously developing innovative solutions to ensure the security for IoT devices. As per the estimates from KBV Research, the overall IoT security market would grow at 27.9% rate during 2016-2022 as a result of growing infrastructural concerns and diversified usage of Internet of things. In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites.

Given widespread recognition of the evolving nature of the design and management of the Internet of things, sustainable and secure deployment of IoT solutions must design for "anarchic scalability." Application of the concept of anarchic scalability can be extended to physical systems (i.e. controlled real-world objects), by virtue of those systems being designed to account for uncertain

management futures. This "hard anarchic scalability" thus provides a pathway forward to fully realize the potential of Internet of things solutions by selectively constraining physical systems to allow for all management regimes without risking physical failure. Brown University computer scientist Michael Littman has argued that successful execution of the Internet of things requires consideration of the interface's usability as well as the technology itself. These interfaces need to be not only more user-friendly but also better integrated: "If users need to learn different interfaces for their vacuums, their locks, their sprinklers, their lights, and their coffeemakers, it's tough to say that their lives have been made any easier."

A concern regarding Internet of things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. With production of electronic equipment growing globally yet little of the metals (from end-of-life equipment) are being recovered for reuse, the environmental impacts can be expected to increase. Also, because the concept of Internet of things entails adding electronics to mundane devices (for example, simple light switches), and because the major driver for replacement of electronic components is often technological obsolescence rather than actual failure to function, it is reasonable to expect that items that previously were kept in service for many decades would see an accelerated replacement cycle if they were part of the IoT. For example, a traditional house built with 30 light switches and 30 electrical outlets might stand for 50 years, with all those components still original at the end of that period. But a modern house built with the same number of switches and outlets set up for IoT might see each switch and outlet replaced at five-year intervals, in order to keep up to date with technological changes. This translates into a ten-fold increase in waste requiring disposal.

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety." Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States DMCA section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own. Examples of post-sale manipulations include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, and enforced EULA on Wii U.

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a "terminology zoo". The lack of clear terminology is not "useful from a practical point of view" and a "source of confusion for the end user". A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics. According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of Things (IoT), Internet of Everything (IoE), Industrial Internet, Pervasive Computing, Pervasive Sensing, Ubiquitous Computing, Cyber-Physical Systems (CPS), Wireless Sensor Networks (WSN), Smart Objects, Cooperating Objects, Machine-to-Machine (M2M), Ambient Intelligence (Aml), Operational Technology (OT), and Information Technology (IT). Regarding IIoT, an industrial sub-field of IoT, the Industrial Internet Consortium's

Vocabulary Task Group has created a "common and reusable vocabulary of terms" to ensure "consistent terminology" across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert to be notified when a new term is published. As of March 2017, this database aggregates 711 IoT-related terms, however, without any attempts to reduce terminological ambiguity and complexity.

Despite a shared belief in the potential of IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Dan Yarmoluk from ATEK Access Technologies has written that "the IoT industry appears heavily focused on gadgets and not making them relevant to the particular business verticals" and "can appear expensive and intimidating." Mike Farley has argued in Forbes that many IoT solutions are either too complex or lack a clear use case for end-users. "Instead of convincing consumers that they need complex systems to serve needs they don't have, we should fix real problems people struggle with every day." Many gadgets in the consumer IoT space have appealed to early adopters, yet failed to demonstrate relevance to ordinary people's lives. In order to overcome barriers, "we need to stop making toys no one cares about and instead work on building simple solutions to real, everyday problems for real people." A recent study by Ericsson regarding the adoption of IoT among Danish companies, has suggested that many are struggling "to pinpoint exactly where the value of IoT lies for them". A company must identify where the value of IoT lies in order to capture it, otherwise non-action is the consequence. This indicates that a major roadblock to IoT adoption is not technical but analytical in nature.

According to a recent study by Noura Aleisa and Karen Renaud at the University of Glasgow, "the Internet of Things' potential for major privacy invasion is a concern" with much of research "disproportionally focused on the security concerns of IoT." Among the "proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles", only very few turned out to be fully satisfactory. Louis Basenese, investment director at Wall Street Daily, has criticized the industry's lack of attention to security issues: "Despite

high-profile and alarming hacks, device manufacturers remain undeterred, focusing on profitability over security. Consumers need to have ultimate control over collected data, including the option to delete it if they choose...Without privacy assurances, wide-scale consumer adoption simply won't happen." In a post-Snowden world of global surveillance disclosures, consumers take a more active interest in protecting their privacy and demand IoT devices to be screened for potential security vulnerabilities and privacy violations before purchasing them. According to the 2016 Accenture Digital Consumer Survey, in which 28000 consumers in 28 countries were polled on their use of consumer technology, security "has moved from being a nagging problem to a top barrier as consumers are now choosing to abandon IoT devices and services over security concerns." The survey revealed that "out of the consumers aware of hacker attacks and owning or planning to own IoT devices in the next five years, 18 percent decided to terminate the use of the services and related services until they get safety guarantees." This suggests that consumers increasingly perceive privacy risks and security concerns to outweigh the value propositions of IoT devices and opt to postpone planned purchases or service subscriptions.

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies' traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence." Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity." This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements." Some of these companies risk being 'kodaked' - "Kodak was a market leader until digital disruption eclipsed film photography with digital photos" - failing to "see the disruptive forces

affecting their industry" and "to truly embrace the new business models the disruptive change opens up." Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online" but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business.

4.7 EMBEDDED SYSTEMS

An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, often with real-time computing constraints. It is usually embedded as part of a complete device including hardware and mechanical parts. In contrast, a general-purpose computer, such as a personal computer, can do many different tasks depending on programming. Embedded systems have become very important today as they control many of the common devices we use.

Since the embedded system is dedicated to specific tasks, design engineers can optimize it, reducing the size and cost of the product, or increasing the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale.

Physically, embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, or the systems controlling nuclear power plants. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure.

In general, "embedded system" is not an exactly defined term, as many systems have some element of programmability. For example, Handheld computers share some elements with embedded systems — such as the operating systems and microprocessors which power them — but are not truly embedded systems, because they allow different applications to be loaded and peripherals to be connected.

Embedded systems provide several functions

Monitor the environment; embedded systems read data from input sensors. This data is then processed and the results displayed in some format to a user or users

Control the environment; embedded systems generate and transmit commands for actuators.

Transform the information; embedded systems transform the data collected in some meaningful way, such as data compression/decompression

Although interaction with the external world via sensors and actuators is an important aspect of embedded systems, these systems also provide functionality specific to their applications. Embedded systems typically execute applications such as control laws, finite state machines, and signal processing algorithms. These systems must also detect and react to faults in both the internal computing environment as well as the surrounding electromechanical systems.

There are many categories of embedded systems, from communication devices to home appliances to control systems. Examples include;

Communication devices

e.g.: modems, cellular phones

Home Appliances

e.g.: CD player, VCR, microwave oven

Control Systems

e.g.: Automobile anti-lock braking systems, robotics, and satellite control

An embedded system usually contains an embedded processor. Many appliances that have a digital interface -- microwaves, VCRs, cars -- utilize embedded systems. Some embedded systems include an operating system. Others are very specialized resulting in the entire logic being implemented as a single program. These systems are embedded into some device for some specific purpose other than to provide general purpose computing . A typical embedded system is shown in Fig 5.1

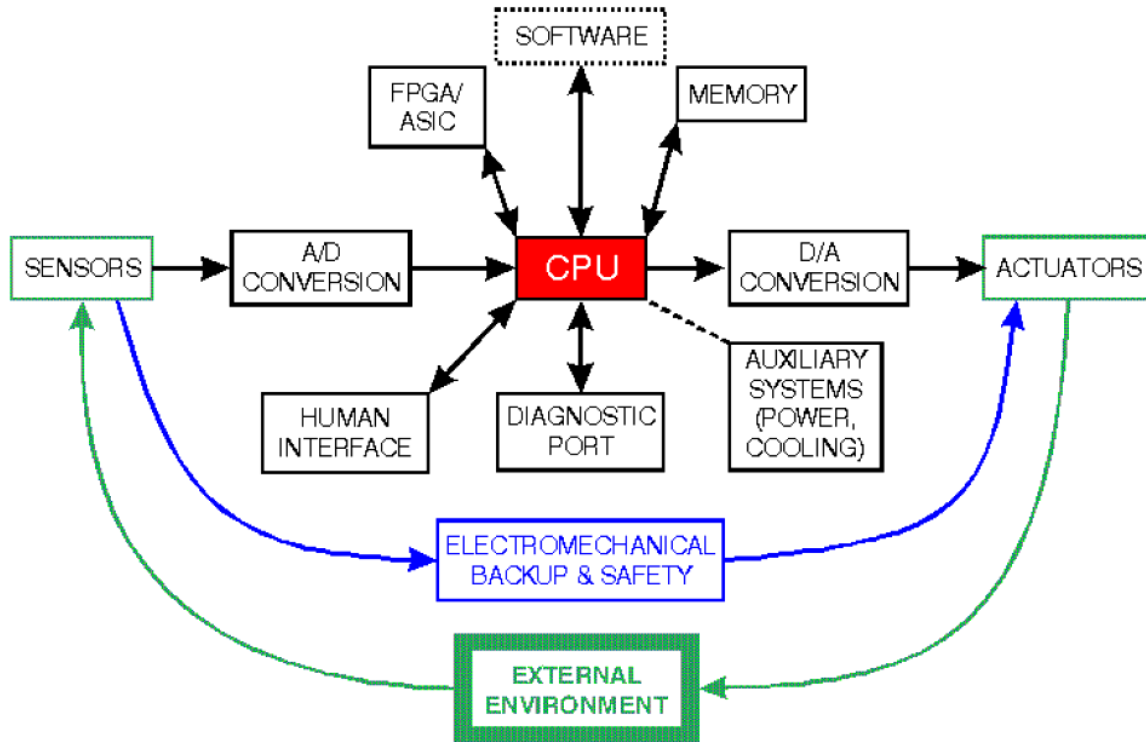


Fig 4.1 Block diagram of a typical embedded system

Embedded systems are characterized by a unique set of characteristics. Each of these characteristics imposed a specific set of design constraints on embedded systems designers. The challenge to designing embedded systems is to conform to the specific set of constraints for the application.

Embedded systems are not general-purpose computers. Embedded system designs are optimized for a specific application. Many of the job characteristics are known before the hardware is designed. This allows the designer to focus on the specific design constraints of a well-defined application. As such, there is limited user reprogrammability. Some embedded systems, however, require the flexibility of reprogrammability. Programmable DSPs are common for such applications.

As mentioned earlier, a typical embedded systems model responds to the environment via sensors and control the environment using actuators. This requires embedded systems to run at the speed of the environment. This characteristic of embedded system is called “reactive”. Reactive computation means that the system

(primarily the software component) executes in response to external events. External events can be either periodic or aperiodic. Periodic events make it easier to schedule processing to guarantee performance. Aperiodic events are harder to schedule. The maximum event arrival rate must be estimated in order to accommodate worst case situations. Most embedded systems have a significant reactive component. One of the biggest challenges for embedded system designers is performing an accurate worst case design analysis on systems with statistical performance characteristics (e.g., cache memory on a DSP or other embedded processor). Real time system operation means that the correctness of a computation depends, in part, on the time at which it is delivered. Systems with this requirement must often design to worst case performance. But accurately predicting the worst case may be difficult on complicated architectures. This often leads to overly pessimistic estimates erring on the side of caution. Many embedded systems have a significant requirement for real time operation in order to meet external I/O and control stability requirements. Many real-time systems are also reactive systems.

A common characteristic of an embedded system is one that consists of communicating processes executing on several CPUs or ASICs which are connected by communication links. The reason for this is economy. Economical 4 8-bit microcontrollers may be cheaper than a 32-bit processors. Even after adding the cost of the communication links, this approach may be preferable. In this approach, multiple processors are usually required to handle multiple time-critical tasks. Devices under control of embedded systems may also be physically distributed.

Embedded systems often are composed of heterogeneous architectures (Fig 1.2). They may contain different processors in the same system solution. They may also be mixed signal systems. The combination of I/O interfaces, local and remote memories, and sensors and actuators makes embedded system design truly unique. Embedded systems also have tight design constraints, and heterogeneity provides better design flexibility.

All electronic circuits work only in low DC voltage, so we need a power supply unit to provide the appropriate voltage supply for their proper functioning. This unit consists of transformer, rectifier, filter & regulator. AC voltage of typically 230volts rms is connected to a transformer voltage down to the level to the desired ac voltage. A diode rectifier that provides the full wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator circuit can use this dc input to provide dc voltage that not only has much less ripple voltage but also remains the same dc value even the dc voltage varies somewhat, or the load connected to the output dc voltages changes.

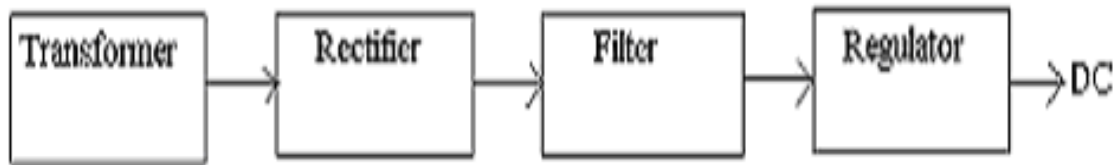


Fig 4.2 General Block of Power Supply Unit

A transformer is a static piece of which electric power in one circuit is transformed into electric power of same frequency in another circuit. It can raise or lower the voltage in the circuit, but with a corresponding decrease or increase in current. It works with the principle of mutual induction. In our project we are using a step down transformer to providing a necessary supply for the electronic circuits. Here we step down a 230volts ac into 12volts ac.

A dc level obtained from a sinusoidal input can be improved 100% using a process called full wave rectification. Here in our project for full wave rectification we use bridge rectifier. From the basic bridge configuration we see that two diodes(say D2 & D3) are conducting while the other two diodes (D1 & D4) are in off state during the period $t = 0$ to $T/2$. Accordingly for the negative cycle of the input the conducting diodes are D1 & D4. Thus the polarity across the load is the same.

In the bridge rectifier the diodes may be of variable types like 1N4001, 1N4003, 1N4004, 1N4005, 1N4007 etc... can be used. But here we use 1N4007, because it can withstand up to 1000v. In order to obtain a dc voltage of 0 Hz, we have to use a low pass filter. So that a capacitive filter circuit is used where a capacitor is connected at the rectifier output & a dc is obtained across it. The filtered waveform is essentially a dc voltage with negligible ripples & it is ultimately fed to the load. The output voltage from the capacitor is more filtered & finally regulated. The voltage regulator is a device, which maintains the output voltage constant irrespective of the change in supply variations, load variations & temperature changes. Here we use fixed voltage regulator namely LM7805. The IC LM7805 is a +5v regulator which is used for microcontroller.

NodeMCU is an open source IoT platform.^{[4][5]} It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module.^{[6][7]} The term "NodeMCU" by default refers to the firmware rather than the development kits. The firmware uses the Lua scripting language. It is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson^[8] and SPIFFS

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems^[6] began production of the ESP8266.^[10] The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core,^[citation needed] widely used in IoT applications (see related projects). NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub.^[11] Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9.^[12] Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform,^[13] and committed to NodeMCU project, then NodeMCU was able to support the MQTT IoT protocol, using Lua to access the MQTT broker. Another important update was made on 30 Jan 2015, when Devsaurus ported the u8glib^[14] to NodeMCU project,^[15] enabling NodeMCU to easily drive LCD, Screen, OLED, even VGA displays.

In summer 2015 the creators abandoned the firmware project and a group of independent contributors took over. By summer 2016 the NodeMCU included more than 40 different modules. Due to resource constraints users need to select the modules relevant for their project and build a firmware tailored to their needs.

As Arduino.cc began developing new MCU boards based on non-AVR processors like the ARM/SAM MCU and used in the Arduino Due, they needed to modify the Arduino IDE so that it would be relatively easy to change the IDE to support alternate toolchains to allow Arduino C/C++ to be compiled for these new processors. They did this with the introduction of the Board Manager and the SAM Core. A "core" is the collection of software components required by the Board Manager and the Arduino IDE to compile an Arduino C/C++ source file for the target MCU's machine language. Some ESP8266 enthusiasts developed an Arduino core for the ESP8266 WiFi SoC, popularly called the "ESP8266 Core for the Arduino IDE".^[16] This has become a leading software development platform for the various ESP8266-based modules and development boards, including NodeMCUs.

NodeMCU is an open source LUA based firmware developed for ESP8266 wifi chip. By exploring functionality with ESP8266 chip, NodeMCU firmware comes with ESP8266 Development board/kit i.e. NodeMCU Development board.

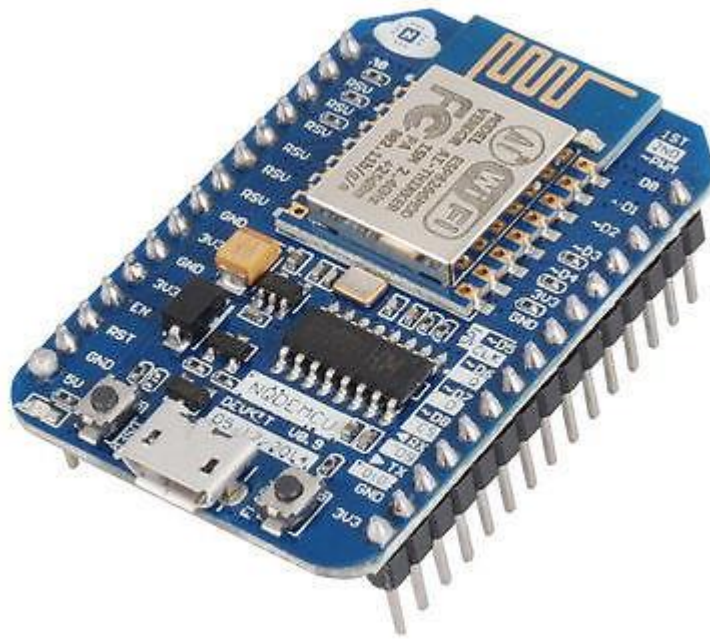


Fig 4.3 Node MCU

Since NodeMCU is open source platform, their hardware design is open for edit/modify/build..NodeMCU Dev Kit/board consist of ESP8266 wifi enabled chip. The ESP8266 is a low-cost Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. For more information about ESP8266, you can refer ESP8266 WiFi Module. There is Version2 (V2) available for NodeMCU Dev Kit i.e. NodeMCU Development Board v1.0 (Version2), which usually comes in black colored PCB.

We need to code in C\C++ programming language if we are using Arduino IDE for developing NodeMCU applications and Lua language if we are using ESPlorer IDE.

Basically, NodeMCU is Lua Interpreter, so it can understand Lua script easily. When we write Lua scripts for NodeMCU and send/upload it to NodeMCU, then they will get executes sequentially. It will not build binary firmware file of code for NodeMCU to write. It will send Lua script as it is to NodeMCU to get execute.

In Arduino IDE when we write and compile code, ESP8266 toolchain in background creates binary firmware file of code we wrote. And when we upload it to NodeMCU then it will flash all NodeMCU firmware with newly generated binary firmware code. In fact, it writes the complete firmware.

That's the reason why NodeMCU not accept further Lua scripts/code after it is getting flashed by Arduino IDE. After getting flashed by Arduino sketch/code it will be no more Lua interpreter and we got error if we try to upload Lua scripts. To again start with Lua script, we need to flash it with NodeMCU firmware. Since Arduino IDE compile and upload/writes complete firmware, it takes more time than ESPlorer IDE.

In current technology scenario, monitoring of gases produced is very important. From home appliances such as air conditioners to electric chimneys and safety systems at industries monitoring of gases is very crucial. Gas sensors are very important part of such systems. Small like a nose, gas sensors spontaneously react to the gas present, thus keeping the system updated about any alterations that occur in the concentration of molecules at gaseous state.

Gas sensors are available in wide specifications depending on the sensitivity levels, type of gas to be sensed, physical dimensions and numerous other factors. This Insight covers a methane gas sensor that can sense gases such as ammonia which might get produced from methane. When a gas interacts with this sensor, it is first ionized into its constituents and is then adsorbed by the sensing element. This adsorption creates a potential difference on the element which is conveyed to the processor unit through output pins in form of current. What is this sensing element? Is it kept in some chamber or is kept exposed? How does it get current and how it is taken out? Let's find out in this Insight!!!

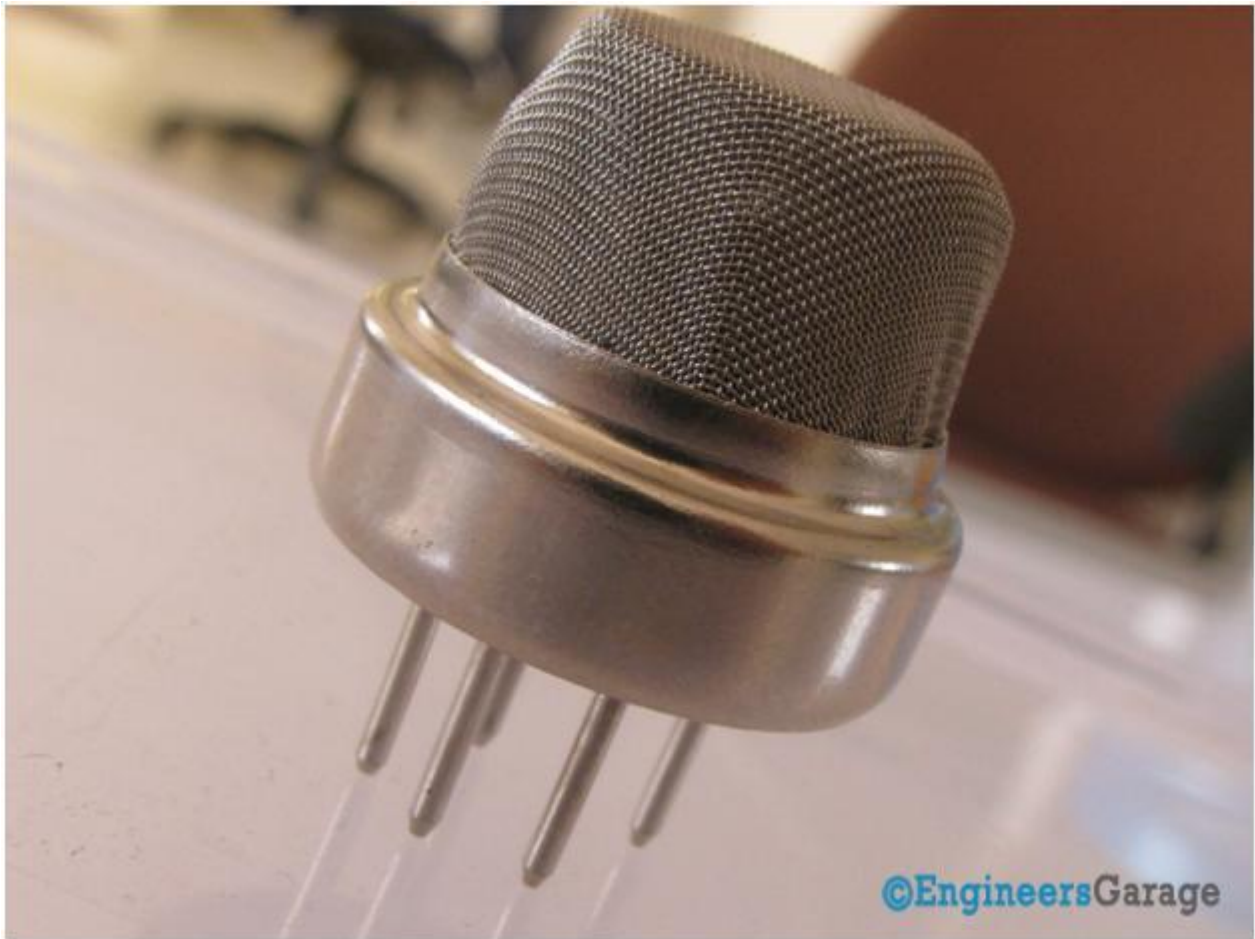


Fig 4.4 Gas Sensor

The gas sensor module consists of a steel exoskeleton under which a sensing element is housed. This sensing element is subjected to current through connecting leads. This current is known as heating current through it, the gases coming close to the sensing element get ionized and are absorbed by the sensing element. This changes the resistance of the sensing element which alters the value of the current going out of it. Image shows externals of a standard gas sensor module: a steel mesh, copper clamping ring and connecting leads. The top part is a stainless steel mesh which takes care of the following:

Bats are wonderful creatures. Blind from the eyes and yet a vision so precise that could distinguish between a moth and a broken leaf even when flying at full speed. No doubt the vision is sharper than ours and is much beyond human capabilities of seeing, but is certainly not beyond our understanding. Ultrasonic ranging is the technique used by bats and many other creatures of the animal

kingdom for navigational purposes. In a bid to imitate the ways of nature to obtain an edge over everything, we humans have not only understood it but have successfully imitated some of these manifestations and harnessed their potential to the greatest

The history dates back to 1790, when Lazzaro Spallanzani first discovered that bats maneuvered in flight using their hearing rather than sight. Jean-Daniel Colladon in 1826 discovered sonography using an underwater bell, successfully and accurately determining the speed of sound in water. Thereafter, the study and research work in this field went on slowly until 1881 when Pierre Curie's discovery set the stage for modern ultrasound transducers. He found out the relationship between electrical voltage and pressure on crystalline material. The unfortunate Titanic accident spurred rigorous interest into this field as a result of which Paul Langevin invented the hydrophone to detect icebergs. It was the first ultrasonic transducer. The hydrophone could send and receive low frequency sound waves and was later used in the detection of submarines in the World War 1.

On a note parallel to the SONAR, medical research also started taking interest in ultrasonics. In late 1930's Dr. Karl Dussik used a technique called hyperphonography which recorded echoes of ultrasonic waves on a sensitive paper. This technique was used to produce ultrasound pictures of the brain to help detect tumors and marked the birth of ultrasound imaging. After that, many scientists like Ian Donald, Douglas Howry, Joseph Holmes, John Wild and John Reid improved upon the various aspects of ultrasonic sensors in the medical field which enabled diagnosis of stomach cancers, ovarian cysts, detection of twin pregnancies, tumors etc. Industry too did not waste time in jumping on to the bandwagon and soon developed techniques like ultrasonic welding and non destructive testing at the outset of the 1960s.

Ultrasonic sensors are devices that use electrical-mechanical energy transformation, the mechanical energy being in the form of ultrasonic waves, to measure distance from the sensor to the target object. Ultrasonic waves are longitudinal mechanical waves which travel as a succession of compressions and rarefactions along the direction of wave propagation through the medium. Any sound wave above the human auditory range of 20,000 Hz is called ultrasound. Depending

on the type of application, the range of frequencies has been broadly categorized as shown in the figure below:

When ultrasonic waves are incident on an object, diffused reflection of the energy takes place over a wide solid angle which might be as high as 180 degrees. Thus some fraction of the incident energy is reflected back to the transducer in the form of echoes and is detected. The distance to the object (L) can then be calculated through the speed of ultrasonic waves (v) in the medium by the relation

For the generation of such mechanical waves, movement of some surface like a diaphragm is required which can then induce the motion to the medium in front of it in the form of compression and rarefaction. Piezoelectric materials operating in the motor mode and magnetostrictive materials have been widely employed in the generation of ultrasonic waves at frequency ranges of 1-20 MHz and 20-40 kHz respectively. The sensors employ piezoelectric ceramic transducers which flex when an electric signal is applied to them. These are connected to an electronic oscillator whose output generates the oscillating voltages at the required frequency. Materials like Lead Zirconate Titanate are popular piezoelectric materials used in medical ultrasound imaging. For best results, the frequency of the applied oscillations must be equal to the natural frequency of the ceramic, which produces oscillations readily through resonance. It offers maximum sensitivity and efficiency when operated at resonance.

Piezoelectricity being a reversible phenomenon produces electrical voltages when ultrasonic waves reflect back from the target and impinge upon the ceramic structure. In this way, a transducer may work both as a transmitter and a receiver in pulsed mode. When continuous measurement of distances is required, separate transducers may be used for transmission and reception. The sensors when used in industry are generally employed in arrays which may be mechanical arrays consisting of oscillating or rotating sensors, or electronic arrays which may be linear, curved or phased. To visualize the output of an ultrasonic sensor, displays of different kind are used whose shape depends on the type of transducer array used and the function. A sectorized Field of View is produced by mechanical arrays and curved and phased electronic arrays, while a linear field is generated by linear

arrays. The display modes may be linear graphical plotting with amplitude on y-axis and time on x-axis called Amplitude mode or A-mode, or intensity modulated B-scans where the brightness of a spot indicates the amplitude of reflected waves. Other modes include M-mode, Doppler (D) Mode etc.

The parameterization of these sensors is generally done by monitoring the reflected and transmitted signals from the lateral and axial motion of transducer while keeping the target fixed in a specific medium (water in general). The sound beam diverges rapidly, hence care is taken that the transducer produces the smallest possible beams. The narrower the beam pattern, the more sensitive the sensor is. However, the angle possible between the transducer and the surface increases with the beam width. The beam patterns of the kind shown below are observed:

The parameters on which the performance of an ultrasonic sensor is measured include bandwidth, attenuation, dynamic range and resolution like grayscale, axial and lateral resolution. Other parameters are Nominal Frequency, Peak Frequency, Bandwidth center Frequency, Pulse Width, sensitivity and Signal to Noise Ratio (SNR).

There are a variety of sensors based on other physical transduction principles like the optical range finding sensors and the microwave based devices too. Then why should one use ultrasonic transducers in the first place, given that the speed of sound is very slow than the speed of electromagnetic waves? The answer lies in the question itself. Because the EM waves based devices are too fast. Being slower than the EM waves, the time taken by ultrasonic waves is much longer than that taken by the latter and hence its measurement can be done more easily and less expensively. Because these are based on sound waves rather than EM waves, these would work in places where the latter would not.

For example, in the case of clear object detection and measurement of liquid levels or high glare environments, light based sensors would suffer greatly because of the transmittance of the target or the translucence of the propagating media. Ultrasonic devices being based upon sound propagation would remain practically unaffected. These also function well in wet environments where optical beams may suffer from refraction from the water droplets in the environment. On account of

range and accuracy, the ultrasonic sensors may lie in between two EM wave based sensors, the Infrared rangefinders on the lower end and the LIDARs on the upper end. Not as accurate or long distance as the LIDARs, the Ultrasonic rangefinders fare better than the IR rangefinders which are highly susceptible to ambient conditions and require recalibration when environment changes. Further these devices offer advantage in medical imaging as compared to MRI or X-Ray scans due to inexpensiveness and portability. No harmful effects of ultrasonic waves at the intensity levels used have been detected in contrast to X-rays or radioactivity based methods and is particularly suited for imaging soft tissues.

However, Ultrasonic sensors too aren't free of all the problems. The speed of sound in a medium increases as the temperature of the medium increases. Thus even when the target has remained in the same place, it may now seem that it has shifted to a place closer to the sensor. Air currents due to varied reasons may disturb the path of the wave which could lead to 'Missed Detection' or a wrong measurement.

Acoustic noise like high pitched sounds created due to whistling or hissing of valves and pneumatic devices at the frequency close to the operating frequency may interfere with the output of the sensor. Electrical noise also affects the performance of the sensor. These may generate artifacts which are not a true representation of the imaged object. Just like the vision starts to blur when the distance of the object from the eye gets too small for the eyes to see it, ultrasonic devices also have a 'dead zone' where the sensor cannot reliably make measurements. This happens due to a phenomenon called ringing which is the continuous vibration of the transducer after emitting the pulse. Thus when the distance is too small, the transducer has not yet come to rest to be able to differentiate between the vibration due to the incident radiation or the oscillation from the electrical excitation. The dangers of Ultrasonic waves are also well founded. If the intensity is too high, it can cause human tissues to heat and may cause ruptures in people exposed to it. Ethical issues like fetus identification and resulting abortions in medical field are also a widespread concern.

Research has been going on to overcome the problems of ultrasonic sensors, particularly in medical imaging where it is known as ultrasound. The artifacts of ultrasonic sensors like Acoustic shadowing and Acoustic Enhancement are being exploited to characterize tissues which allow the differentiation between solid and cystic tissues. The industry too has reaped the benefits from ultrasonic sensors in applications like plastic welding, jewelry cleaning, remote sensing and telemetry, assisted parking systems etc. Robotics has been known to use ultrasonic rangefinders as a favorite tool for distance ranging and mapping. Even the fashion industry is using ultrasonic sensors in hair styling like hair extension implants.

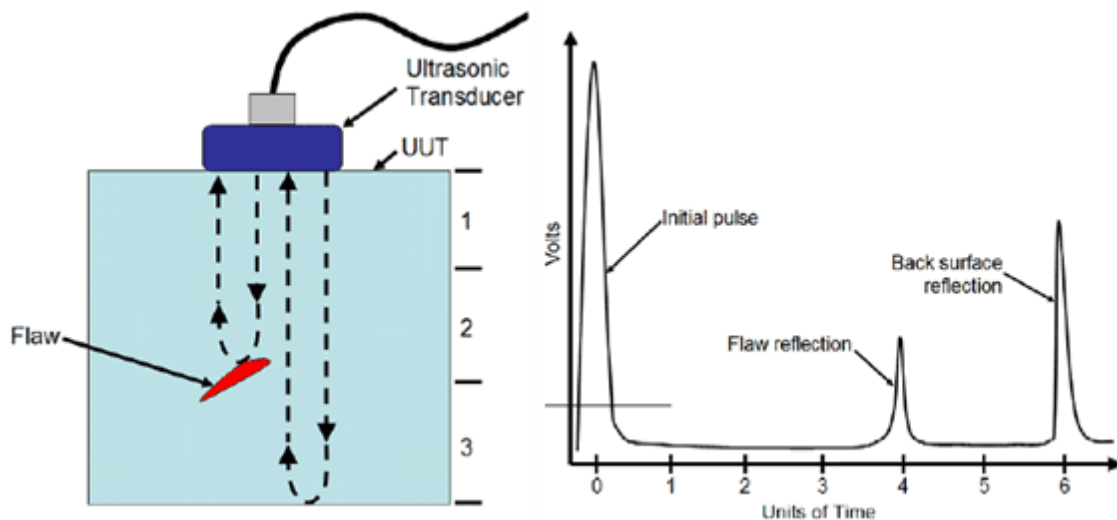


Fig4.5 Flaw Detection Using Ultrasonic Sensors

Non destructive testing and flaw detection uses ultrasonic waves in various modes like the Longitudinal (L-wave) mode and the Shear (S-wave) mode to detect flaws in materials. With the advances in Science, new materials offering increased performance at lower voltages like the capacitive micromachined ultrasonic transducers (CMUTs) are being developed which are expected to have higher bandwidth and greater potential for integration with electronic circuits.

These devices provide non-invasive measures for the detection of problems in all kinds of materials, be it a living tissue or non-living manufactured goods. With a healthy history of being able to detect many problems which otherwise left the doctors dazed and the problem untreated, ultrasonic sensors do offer a lot of promise even in the coming times. The environmental and psychological effects of

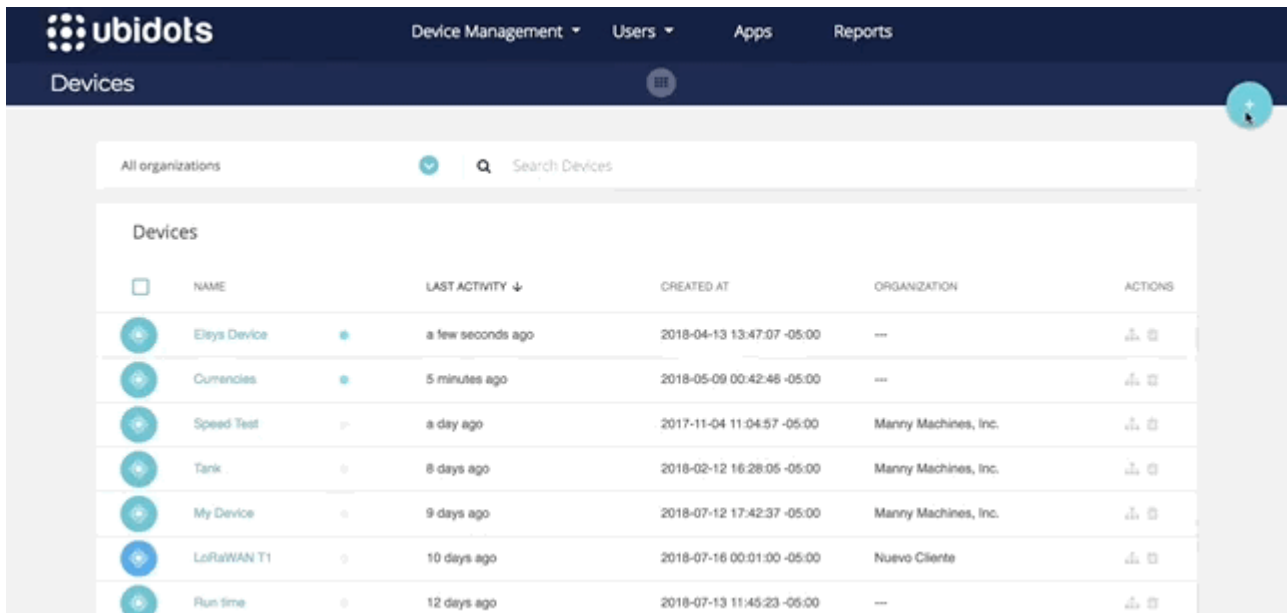
exposure to EM-radiation being rigorously being put under the scanner, ultrasonic applications are expected to thrive and offer a substantial alternative to the contemporary technologies.



Fig 4.6 ultra sonic sensor

The basics components of any Internet of Things application powered by Ubidots are: Devices, Variables, Synthetic Variables Engine, Dashboards, and Events. Within this article we will address each of these concepts as they relate to Ubidots IoT Development and Deployment Platform and how you can better organize your Ubidots Apps to best connect with the users.

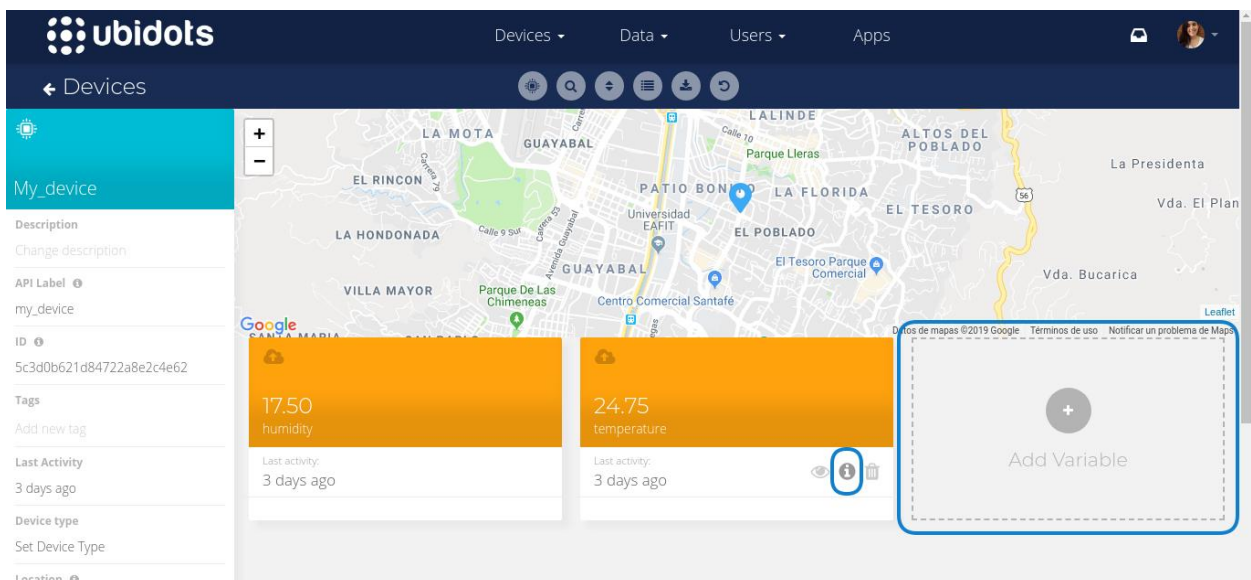
Once your devices, variables, and general Application is assembled, give your App some layers with Ubidots Device Management to learn more about Ubidots internal architecture and how you can use Apps, Organizations, and Users to efficiently connect your data with those who should be using it.



	NAME	LAST ACTIVITY ↓	CREATED AT	ORGANIZATION	ACTIONS
	Eleys Device	a few seconds ago	2018-04-13 13:47:07 -05:00	---	
	Currencias	5 minutes ago	2018-05-09 00:42:48 -05:00	---	
	Speed Test	a day ago	2017-11-04 11:04:57 -05:00	Manny Machines, Inc.	
	Tank	8 days ago	2018-02-12 16:28:05 -05:00	Manny Machines, Inc.	
	My Device	9 days ago	2018-07-12 17:42:37 -05:00	Manny Machines, Inc.	
	LoRaWAN T1	10 days ago	2018-07-16 00:01:00 -05:00	Nuevo Cliente	
	Run time	12 days ago	2018-07-13 11:45:23 -05:00	---	

Fig 4.7. Variables

1. Assigning a label as a variable within your hardware's code.
2. Clicking the "+" icon found in any single device screen and assign a name which will also correspond to the variable's label. By default, Ubidots assigns an additional unique identifier to the variable called Variable ID. To find both the variable's ID and variable's label, select the "i" icon from the variables card.



The screenshot shows the 'My_device' page in Ubidots. On the left is a sidebar with device details. The main area features a map of Santa Fe, Argentina, with two variable cards overlaid: '17.50 humidity' and '24.75 temperature'. Both cards show 'Last activity: 3 days ago'. A blue dashed box highlights the 'Add Variable' button (a circle with a plus sign) and the information icon (an 'i' in a circle) on the temperature card.

Fig 4.8 Synthetic Variables Engine

Ubidots Synthetic Variables (SV) Engine is a simple and effective way to create insights from the raw data stored in Ubidots' Cloud. Using Ubidots SV Engine, users can create Synthetic Variables that calculate and enhance data to give data-driven decision to user of an Ubidots powered application.

For example, to calculate Average (mean) Energy consumed this week, we will need to create a synthetic variable called Energy to calculate the product of Current and Voltage ($P=C*V$): the default variable Current is multiplied by Voltage. Then average the product every week with built-in function `mean()`.

Here is a complete list of available functions, such as `cos(x)` or `ceil(x)` functions, and more!

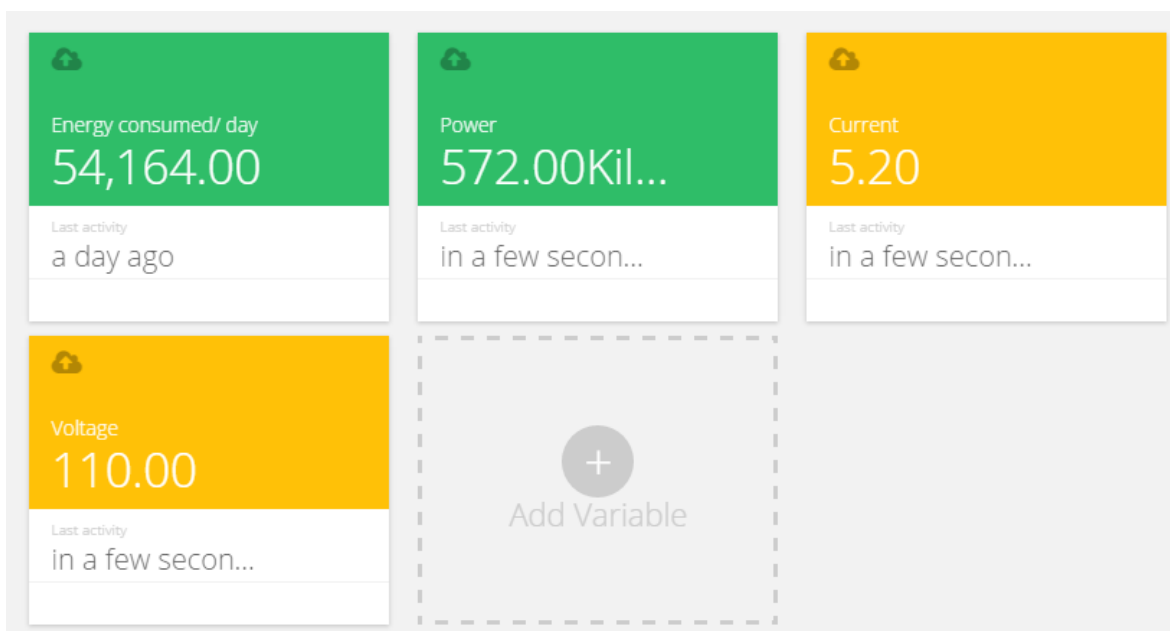


Fig 4.9 Note that default variables are yellow, and Synthetic Variables are green.

Dashboards are the human-machine interfaces where data is easily visualized. Your Ubidots account will let you create as many dashboards as needed, containing widgets and data-visualizations to comprehend your data at a glance. For additional details on your dashboard's construction, check out this tutorial.

In Ubidots, Events are messages triggered and delivered through Email, SMS, Telegrams, Slack, Voice Call or webhook messages based on a customized design rule created in the application. If you wish to create alerts for your IoT application, check out this tutorial for additional support.

- When sensor readings reach a specific value

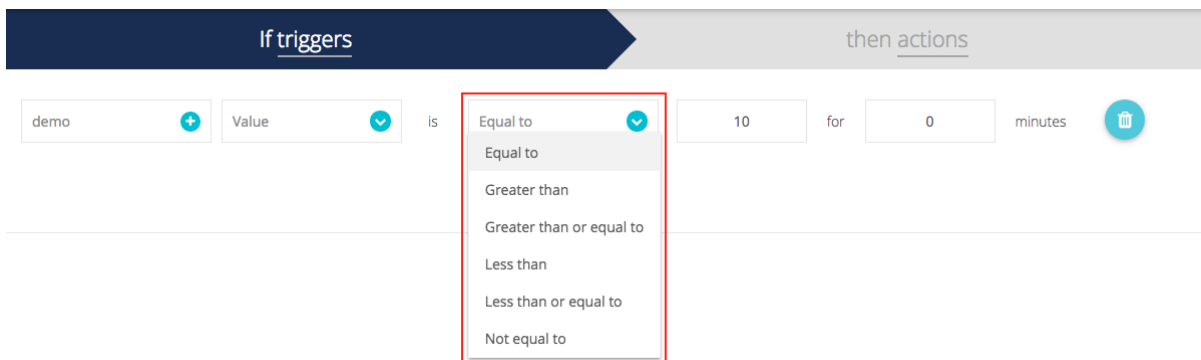


Fig 4.10 Variable is inactive during a specific amount of time

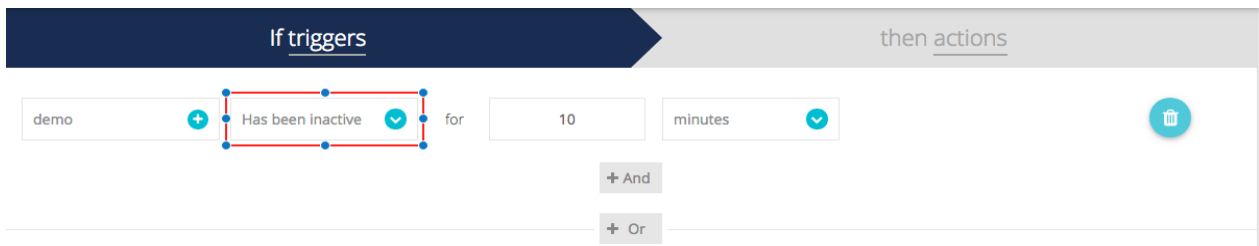


Fig 4.11 When a device enters or exits a specific area (geofence)

CHAPTER 5

RESULT AND DISCUSSION

This Project presents an automatic vehicle accident detection system using GPS and GSM modems which is inbuilt in Arduino ide. This detection and messaging system is composed of a GPS receiver, LPC 2148 Microcontroller and a GSM Modem. GPS Receiver gets the location information from satellites in the form of latitude and longitude. The Microcontroller processes this information and this processed information is sent to the user/owner using ubdots could modem A GSM modem is interfaced to the MCU. The ubdots could modem sends an SMS to the mobile and informs about this accident. This enable it to monitor the accident situations and it can immediately alerts the police/ambulance service with the location of accident.

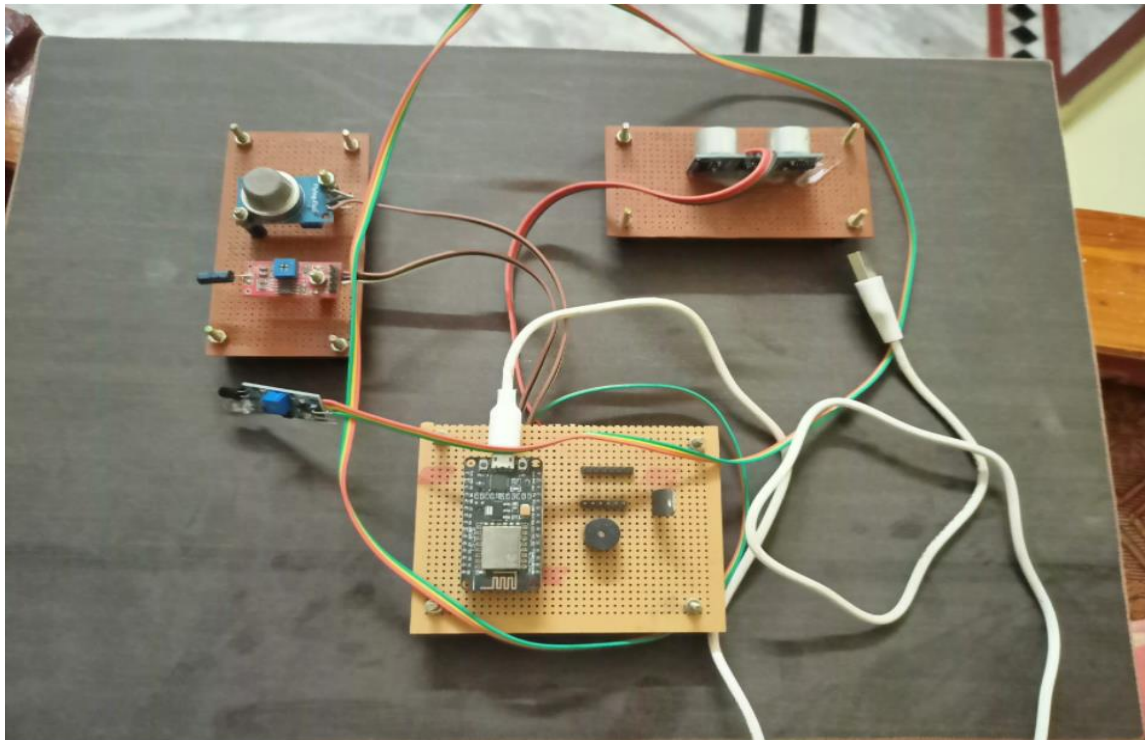


Fig 5.1 circuit connection view

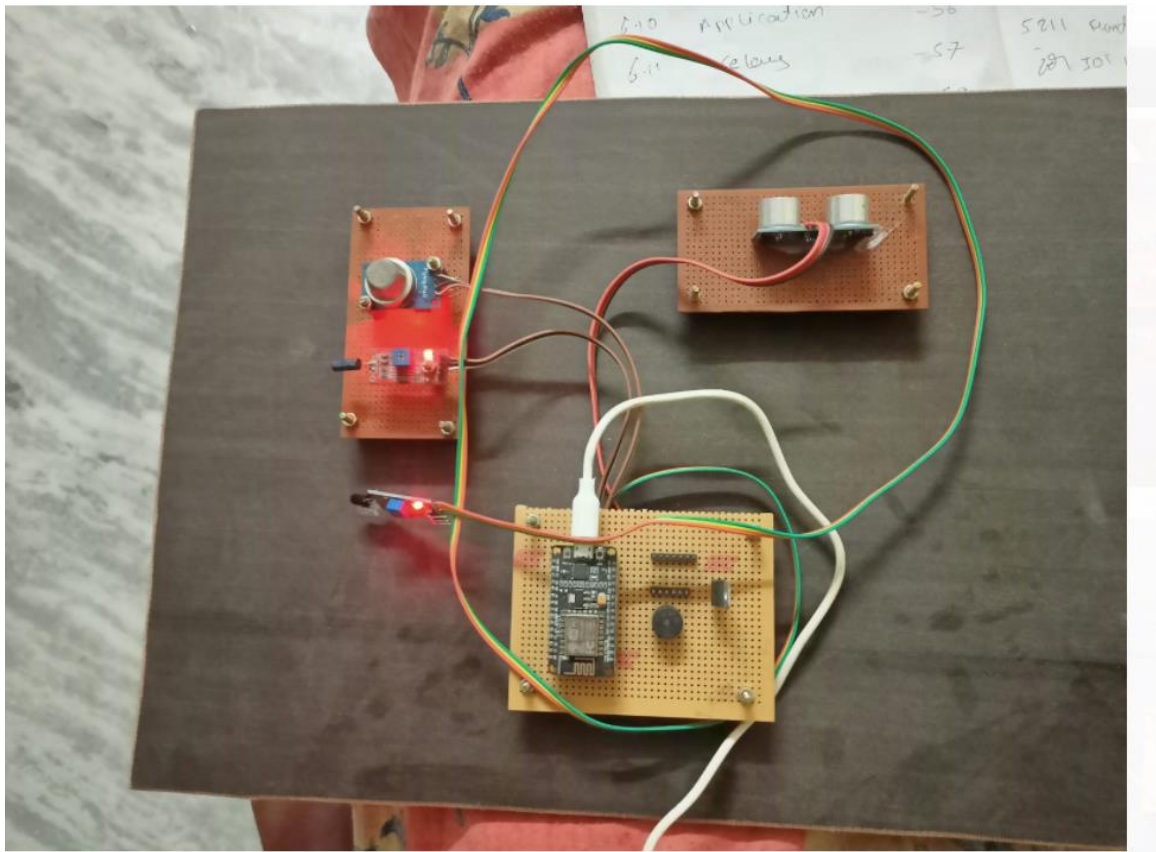


Fig 5.2 circuit connections view 2

CHAPTER 6

SUMMARY AND CONCLUSION

We additionally needed to execute a mishap anticipation plan. By utilizing this framework, we can stay away from numerous mishaps brought about by the accompanying frameworks. The framework is all around as costly as a ultrasonic sensor. The framework enjoys many benefits, like knowing the distance of the following vehicle. Later on, we will decrease the speed of a similar vehicle to the following distance of the other vehicle. With this framework, we can forestall numerous mishaps and mishaps in a little nation like India. Use to decide the distance to the following vehicle. Later on, the speed of one vehicle will be diminished in accordance with the following mile of different vehicles. 0m) between the vehicle and different vehicles. The proposed framework incorporates security contemplations while supplanting a vehicle, recognizing anything in the accompanying position, and showing the distance between the vehicle and different vehicles.

REFERENCES

- [1]. M. Milera, F. Todic, and M. Ševrović, "Extracting accurate location information from a highly inaccurate traffic accident dataset: A methodology based on a string-matching technique", Elsevier Transportation Research Part C, 68(2016), 185–193, 2016.
- [2]. R. K. Kodali, and S. Sahu, "MQTT based vehicle accident detection and alert system", IEEE 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 186-189, 2017.
- [3]. M. Virant, and M. Ambrož, "Universal safety distance alert device for road vehicles, MDPI Electronics, 5(19), 1-17, 2016.
- [4]. M. Sanathra, A. Parmar, K. Parmar, D. Patel, and M. Darji, "Car accident detection and notification: an analytical survey", International Research Journal of Engineering and Technology, 6(8), 1465-1468, 2019.

- [5]. L. A. Ajao, J. Agajo, O. M. Olaniyi, I. Z. Jibril, A. E. Sebiotimo, "A secure tracking automobile system for oil and gas distribution using telematics and blockchain techniques", *Balkan Journal of Electrical & Computer Engineering*, 7(3), 257-268, 2019.
- [6]. J. Agajo, J. G. Kolo, L. A. Ajao, K. Y. Olusola, and A. Prince, "Equipment and security personnel tracking and localization using GPS/GSM geo-location technique incorporating ublox Neo 6 GPS module", *Journal of Engineering and Technology (JET)*, 7(2), 87-102, 2016.
- [7]. L. A. Ajao, J. G. Kolo, E. A. Adedokun, O. M. Olaniyi, O. C. Inalegwu, and S. K. Abolade, "A smart door security-based home automation system: An internet of things", *Scifed Journal of Telecommunication*, 2(2), 1-9, 2018.