

WIFI CONTROLLED SMART FIRE EXTINGUISHING ROBOT

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in
Electronics and Communication Engineering

by

P. NAVEEN (37130282)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

**Accredited with Grade "A" by NAAC
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI-600119**

APRIL 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC
Jeppiaar Nagar, Rajiv Gandhi Salai,
Chennai – 600119.

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 P. NAVEEN (37130282) who carried out the project entitled WIFI CONTROLLED SMART FIRE EXTINGUISHING ROBOT Under my supervision from September 2020 to April 2021.

Internal Guide

Dr. R. M.JOANY, M.E., Ph.D.,

Head of the Department

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

Submitted for Viva voce Examination held on 19/04/2021

Internal Examiner

External Examiner

DECLARATION

We, **P. NAVEEN** (37130282) hereby declare that the Project Report entitled WIFI CONTROLLED SMART FIRE EXTINGUISHING ROBOT done by us under the guidance of Dr. R. M. JOANY is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in ELECTRONICS AND COMMUNICATION ENGINEERING.

DATE:

PLACE: CHENNAI

P. NAVEEN (37130282)

SIGNATURE OF CANDIDATES

ACKNOWLEDGEMENT

I am 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. I am grateful to them.

I convey my thanks to **Dr. N. M. NANDHITHA, M.E., Ph.D.**, Dean School of Electrical and Electronics and **Dr. T. RAVI, M.E., Ph.D.**, Head of the Department of Electronics and Communication Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. R. M JOANY, ECE.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

Abstract

Fire Accident will occur very rarely, but once it occurred its consequences will be devastating. So, at any cost fire accidents should be eliminated completely.

Through this project you are going to build for a unique fire protection system for the Homes and commercial buildings. You will need Nodemcu to interface the microcontroller with smoke sensor, temperature sensor sprinkler. You will program the microcontroller in such a way that say whenever the smoke sensor detects the smoke in the air, a sms will be sent to respective authorities. After sending a sms the microcontroller will immediately check the temperature in the room.

If the temperature is beyond certain level, immediately water sprinkler will be turned on. The sprinkler will be in on position till the temperature is reduced below than the prescribed value.

The data regarding Sprinkler status, how much time it was in on position, temperature status, smoke level etc. will be immediately stored into remote server. Thereby we can avoid loss of life.

CONTENTS

CHAPTER	TITLE	PAGE NO
1	INTRODUCTION	1
2	LITERATURE SURVEY	2
2.1	INTRODUCTION	3
2.2	FIRE FIGHTING SYSTEM	3
2.3	SENSORS	4
2.3.1	SENSORS	4
2.3.2	HEAT DETECTORS	4
2.3.3	FLAME DETECTORS	5
2.4	FIRE ALARM SYSTEM DESIGN	5
2.5	EMBEDDED AND REAL TIME SYSTEM	5
2.5.1	EMBEDDED SYSTEMS	6
2.5.2	REAL TIME SYSTEMS	6
2.6	MICROCONTROLLER	6
2.6.1	ARDUINO	7
2.6.2	RASPBERRY PI	7
3	EMBEDDED SYSTEMS	8
3.1	OVERVIEW OF EMBEDDED SYSTEMS	10
3.2	BLOCK DIAGRAM OF EMBEDDED SYSTEMS	11
3.2.1	CHARACTERISTICS OF EMBEDDED SYSTEMS	12
3.3	POWER SUPPLY	13
3.4	TRANSFORMERS	15
3.5	RECTIFIERS	16

	3.6	FILTERS	26
	3.7	REGISTERS	28
	3.8	REGULATORS	30
	3.9	FEATURES AND DESCRIPTION OF REGULATOR	32
4		ERNET OF THINGS	34
	4.1	i History	36
	4.2	Applications	37
	4.3	Media	43
	4.3	Environmental monitoring	48
5		Trends and characteristics	40
	5.1	Intelligence	53
	5.2	Architecture	58
	5.3	Network architecture	60
	5.4	Features:	74
	5.5	Applications:	80
	5.6	Problems & Concerns	80
	5.7	WATER SPRINKLER:	82

	5.8	Generating Ultrasonic Waves	83
	5.9	How Ultrasonic Sensors work?	84
	5.9.1	Ultrasonic Sensors	84
	5.10	ARDUINO SOFTWARE	84
6		CONCLUSION	84
		REFERENCES	85

CHAPTER 1

INTRODUCTION

Fire accidents is defined as an undesirable event which emits heat, smoke or flame. Fire accident is a major form of accident and can cause a huge number of casualties because of the danger and risk involved in rescuing victims out of the fire.

When fire fighting units engage in such situations there is a high possibility to loss the life of fire personnel's. In everyday life, it is not feasible to always rely on human patrol for detecting and extinguishing fire at a fire accident scene.

If an automated system is made to patrol the perimeter for fire accidents, then we can have an early warning system. This will be very effective in a fire accident in industries and residential areas where the fire possibilities are high.

In order to achieve this, we must come up with an idea which can detect a flame, locate it and extinguish the fire immediately before it poses a threat to anything around it. For risky situations, it would be idealistic to send a fire fighting robot that could quickly and efficiently find the fire and suppress it.

Effective monitoring, high speed recognition, and extinguishing of fire are problems to be dealt with immediately. To reduce the risk of losing life in such situations, firefighting robots can be used. The automatic robot is designed to avoid further spreading of the fire that could lead to possible human casualties or damage to property. Firefighting robot will help the fire fighters to do their job effectively.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction: This chapter overviews various technologies and techniques that have been employed for use in firefighting system. It also reviews the principles of sensors and the principles of web technologies. This was done with the aim of providing guidance to certain design decisions for later use throughout the project.

2.2 Firefighting System: This section discusses the main component of the firefighting system. Fire detection devices: As a rule, fire detection devices are divided into two basic types: Manually actuated and automatically actuated devices [8] [9]. Manually actuated devices also known as “Fire alarm boxes” are located near the exits and in many cases look like the red button on the wall. Somebody should push the button in a risk of a fire. But it will be late when somebody push the button after seeing the flame[9] . Modern automatically actuated fire alarms are used to detect fire at the earliest possible stage. They were produced for working 24 hours per day without any human intervention [9] .

2.3 Sensors: There are 4 basic types of automatic alarm-initiating devices are designed to detect, smoke, heat, fire gases, and flame [10] . 8

2.3.1 Smoke Alarm: Also Known as smoke detectors, these devices are one of the best early-warning devices of a fire that why we choose it as our main sensor in our design. It designed to sense low levels of smoke and sound an alarm [10]. There are two type of smoke alarm one has built in alarm which alerts people around it. Other connected to the building’s fire alarm system [10]. When this detector senses smoke, it may either sound an alarm in the room, or send a signal to the building fire alarm system. Smoke alarms are located in areas where they cannot be set off accidentally by steam from showers or from cooking smoke [10]. Smoke detectors have 2 main types: · Photoelectric Smoke Detectors. · IonizationSmoke Detectors [10] .

2.3.2 Heat detectors: Usually use in places where smoke detectors cannot be effective like kitchens. Heat detectors react at fixed temperatures or

when heat is rising at a certain rate to provide detection in these areas.

Smoke sensors have heat detectors as part of their design to provide dual protection [10]. It has 4 main types: · Fixed Temperature Heat Detector. · Rate of Rise Detector. 9 · Rate Compensation. · Line Type Detectors.

2.3.3 Fire Gases Detectors: When a fire burns, it changes the makeup of the atmosphere within the space [10]. Depending on the fuel, some of the gases released by the fire including the following: · Water vapor (H₂O). · Carbon dioxide (CO₂). · Carbon monoxide (CO). · Hydrogen chloride (HCL). · Hydrogen cyanide (HCN). · Hydrogen fluoride (HFL). · Hydrogen sulfide (H₂S) [10].

2.3.4 Flame detectors: The appearance of the flame is a stage after the smokes or gases and has the highest degree of dangerousness. There are 3 basic types of flame detectors also known as light detectors: · Detecting light in the ultraviolet wave spectrum (UV detectors). · Detecting light in the infrared wave spectrum (IR). · Detecting both types of light.

2.4 Fire Alarm System Structure Design: There are 3 main designs for the fire alarm system: · Conventional Analogue. 10 · Addressable Analogue. · Wireless Fire alarm system [10]. Conventional vs. Addressable Fire Alarm System: There are several differences between conventional & addressable fire alarm system: · Addressable give information's about individual detectors whereas conventional systems only give information about give information about specific circuits (zones). · Addressable allow text label to allow easy identification of any event. · Most addressable systems allow early warning · Addressable systems have a real time clock [10]. We choose addressable fire alarm system to be implemented in our system design because it's more effective.

2.5 Embedded and Real Time systems:

2.5.1 Embedded systems: An embedded system is a specialized computer system that is part of a larger system or machine. Embedded systems can also be thought of as information processing subsystems integrated in a larger system. Some embedded systems include an operating system [11] . Embedded systems functions: · Monitor the environment: · Embedded systems read data from input sensors. · Control the environment: 11 · 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 [12] . There are many categories of embedded systems for communication devices to home appliances to control systems. In our daily life we use many embedded systems like Digital alarm clock, cellular phone, microwave oven, coffee machine and refrigerator [12] .

2.5.2 Real-time systems: Real-time computing (RTC) or reactive computing describes hardware and software systems subject to a "real-time constraint", for example from event to system response. Real-time programs must guarantee response within specified time constraints, often referred to as "deadlines". The correctness of these types of systems depends on their temporal aspects as well as their functional aspects. Real-time responses are often understood to be in the order of milliseconds, and sometimes microseconds. A system not specified as operating in real time cannot usually guarantee a response within any timeframe, although typical or expected response times may be given [13]. There are two types of real-time systems: reactive and embedded. Reactive real-time system involves a system that has constant interaction with its environment. · An embedded real-time system is used to control specialized hardware that is installed within a larger system [13]. · A hard Real time system should always respond to an event with in the deadline or else the system fails and endangers human lives 12 but in soft real time system, failing to meet the deadline produces false output and does not endanger the human lives and our designed embedded system is a soft real time system [14] . The major part of this project is the hardware model consisting of a sufficient sensor with embedded system. Embedded systems are computer in the widest sense. Based on functionality and performance requirements, embedded systems can be categorized as, Stand-alone system, Real time system, Networked information appliances and Mobile devices. Every embedded System consists of custom-built hardware built around a central processing unit (CPU). This Hardware also contains memory chips onto which the software is loaded. The software residing on the memory chip is also called as the firmware [14] .

2.6 Microcontrollers: There are a lot of types of microcontrollers:

2.6.1 Arduino: Arduino is an open source electronics platform based on easy to use hardware and software. Arduino boards have ability to do many jobs like reading inputs light on a sensor, finger on a button, or a

Twitter and turn it into an output activating a motor, turning on an LED,

publishing something online. By changing the instructions the microcontroller board is being controlled to do actions as needed [15] [16]. Features of Arduino: · Inexpensive · Cross-platform 13 · Simple, clear programming environment · Open source and extensible software Open source and extensible hardware. Figure 2.1 shows the Arduino chip [17].

2.6.2 Raspberry pi: The Raspberry Pi chips and ports device looks like a motherboard with the mounted exposed but it has all the components you need to connect input, output, and storage devices and start computing

[15] Figure 2-4 shows the raspberry pi 2 model b+. 14 figure 2.2 Raspberry pi 2 model B+ board [18]. Raspberry Pi has two models of the device: Model A, Model B. The only differences are the addition of Ethernet and an extra USB port on the more expensive Model B [15]. Raspberry Pi Basic's: Here are the various components on the Raspberry Pi board shows in figure 2-5: 15 Figure 2.3 various components on the Raspberry Pi 2 board [19]. Some features that are missing, such as Wi-Fi and audio in, can be added using the USB port(s) or a USB hub as needed. The Raspberry pi's programmability and simplicity make it very like the computers of yore that spawned so many programmers and system hobbyists. To allow network connectivity for Raspberry Pi model B we attach Ethernet connector or an external Wi-Fi device

Wireless Automatic Fire Fighting Surveillance Robot: It's an autonomous fire proof rescuer robot. The robot designed in a way that it can traverse through fire and hazardous situation. It sense and communicate information regarding these situations in real time with the server. The robot is fixed with multi-sensors which carried a driver circuit has been integrated for communication in these hazardous situations through Zigbee and a data acquisition system (DAQ)

Autonomous Fire Fighting Mobile Platform It got its important in fire-prone area by implemented a mobile robot to perform this task. A mobile robot is equipped with the basic fighting equipment that can patrol through the hazardous site via a guiding track with the aim of early detection for fire. When the fire source is being identified, the flame will be promptly extinguished using the fire extinguishing system that is mounted on its platform. The patrolling movement is guided by a set of lines with the use of a conventional line [25]. To detect for fire source, the input from flame

sensors were finelytuned in relation to the surrounding area, external interference and the mobility of the AFFMP prior the deployment of the

platform. To monitor for hazardous site via patrolling process, it aids to share out the burden of fire-fighters in fire fighting tasks as the firefighters can safely delegate the fire fighting tasks to AFFMP.

Robotic fighting vehicles: It used in at some fire locations, like flammable or explosive material storage areas and nuclear power plants, are too hazardous for human firefighters to enter. FireRob is a firefighting vehicle that a single operator can direct on the ground by remote control. It extinguishes fires without intervention of firefighters without intervention of fighters with highpressure cannon on a hydraulic arm that pumps water up to 55 m away [26]. Other smaller, remote-controlled vehicles have been adapted to fight fires, such as Segway's water cannon prototype which is remotely-operated vehicle, and others that also contain cameras, high-pressure hoses, and remote operation. Fire-rob is the only that integrates hydraulic arm blade, grip, and other tool attachments for path clearing in difficult terrain or inaccessible areas, and carries its own waterand foam tanks.

Existing system:

- In existing system, we are going to build a Fire Alarm System using Arduino, LM35 Temperature Sensor and GSM Module.
- The objectives of this fire detector using Arduino is to sense the surroundings for occurrence of fire with help of LM35 temperature sensor, and send 3 SMS alerts to two mobile numbers stored inside the Arduino program if fire is detected (using GSM Module).

Proposed system:

- Automated mode, the robot is completely automated to search for the presence of possible flames and obstacles in the vicinity.
- The robot moves around and search for the signs of flame.
- The robot will search for flames using the three flame sensors

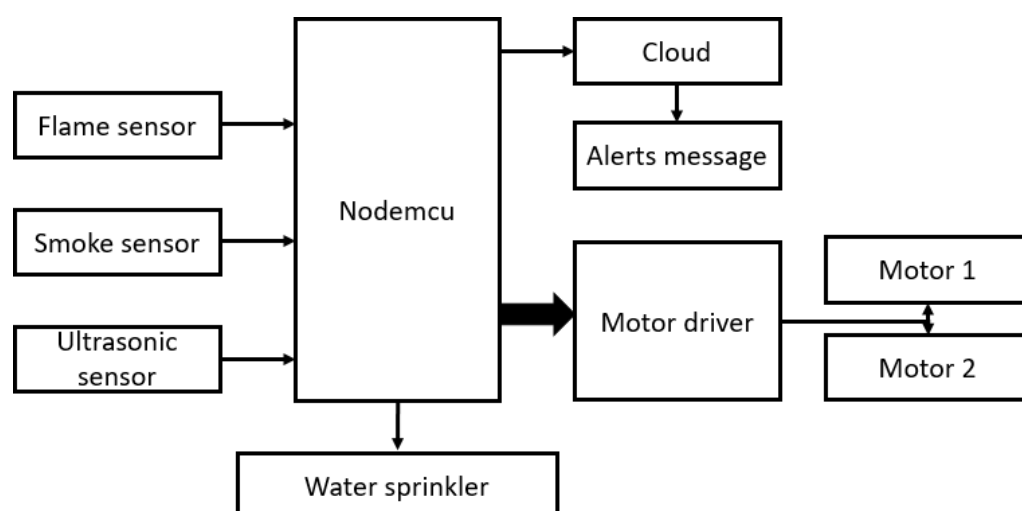
placed in front of the robot.

- Interface the Smoke sensor and temperature sensor with the Nodemcu .
- Now calibrate the Smoke sensor for specific smoke level.
- If the smoke level in the air is more than the prescribed limit, immediately a sms will be sent to the respective authorities.
- After sending the sms, the microcontroller will check the temperature value in that room. If temperature is higher than the prescribed limit, immediately the sprinkler will be turned on.
- The turning on and off of the sprinkler will be done by servo motor automatically.
- The present status of the smoke level, sprinkler status will be updated in remote server for further server.

Advantages:

- It is used to easy detect the fire and control the fire.

Block diagram:



Hardware required:

NodeMCU

Flame sensor

Smoke sensor

Ultrasonic sensor

GSM

Relay

Water motor

Software required:

Arduino ide

Embedded c

3. EMBEDDED SYSTEMS

3.1 Overview of 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, satellite control

3.2 Block diagram of an embedded system:

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 1.1

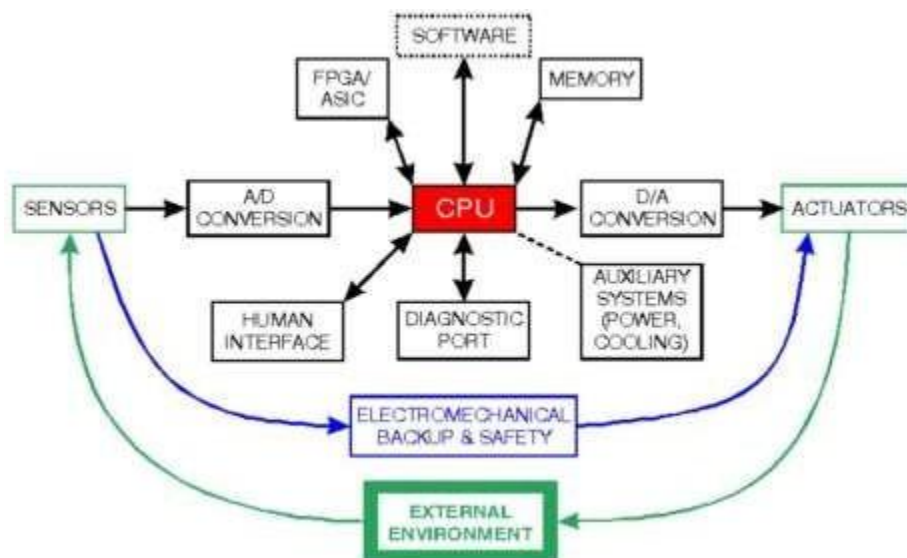


Fig 1.1 Block diagram of a typical embedded system

1.2.1 Characteristics of embedded systems

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.

Application Specific Systems:

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 reprogram ability. Some embedded systems, however, require the flexibility of reprogram ability. Programmable DSPs are common for such applications.

Reactive Systems

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.

Distributed 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.

Heterogeneous Architectures

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.

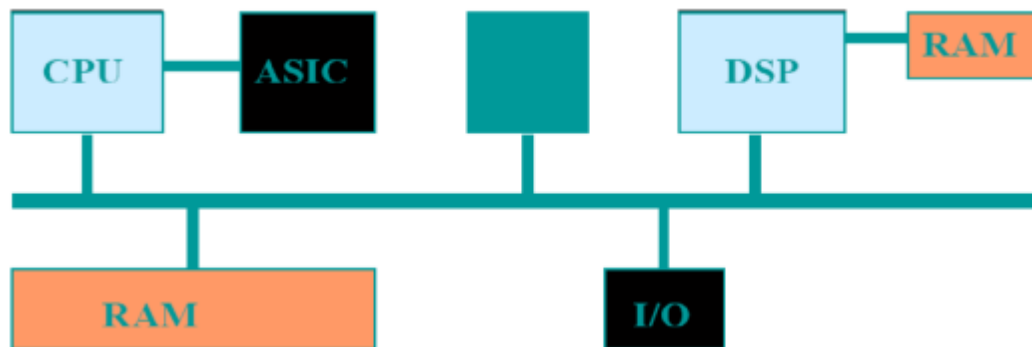


Fig 1.2 Embedded Systems having Heterogeneous Architectures

Harsh environment

Many embedded systems do not operate in a controlled environment. Excessive heat is often a problem, especially in applications involving combustion (e.g., many transportation applications). Additional problems can be caused for embedded computing by a need for protection from vibration, shock, lightning, power supply fluctuations, water, corrosion, fire, and general physical abuse.

System safety and reliability

As embedded system complexity and computing power continue to grow, they are starting to control more and more of the safety aspects of the overall system. These safety measures may be in the form of software as well as hardware control. Mechanical safety backups are normally activated when the computer system loses control in order to safely shut down system operation. Software safety and reliability is a bigger issue. Software doesn't normally "break" in the sense of hardware. However software may be so complex that a set of unexpected circumstances can cause software failures leading to unsafe situations. Discussion of this topic is outside the scope of this book, but the challenges for embedded designers include designing reliable software and building cheap, available systems using unreliable components. The main challenge for embedded system designers is to obtain low-cost reliability with minimal redundancy.

Control of physical systems

One of the main reasons for embedding a computer is to interact with the environment. This is often done by monitoring and controlling external machinery. Embedded computers transform the analog signals from sensors into digital form for processing. Outputs must be transformed back to analog signal levels. When controlling physical equipment, large current loads may need to be switched in order to operate motors and other actuators. To meet these needs, embedded systems may need large computer circuit boards with many non-digital components. Embedded system designers must carefully balance system tradeoffs among analog components, power, mechanical, network, and digital hardware with corresponding software.

Small and low weight

Many embedded computers are physically located within some larger system. The form factor for the embedded system may be dictated by aesthetics. For example, the form factor for a missile may have to fit inside the nose of the missile. One of the challenges for embedded systems designers is to develop non-rectangular geometries for certain solutions. Weight can also be a critical constraint. Embedded automobile control systems, for example, must be light weight for fuel economy. Portable CD players must be light weight for portability purposes.

Cost sensitivity

Cost is an issue in most systems, but the sensitivity to cost changes can vary dramatically in embedded systems. This is mainly due to the effect of computer costs have on profitability and is more a function of the proportion of cost changes compared to the total system cost.

Power management

Embedded systems have strict constraints on power. Given the portability requirements of many embedded systems, the need to conserve power is important to maintain battery life as long as possible. Minimization of heat production is another obvious concern for embedded systems.

1.3 POWER SUPPLY

All electronic circuits works 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 some what, or the load connected to the output dc voltages changes.

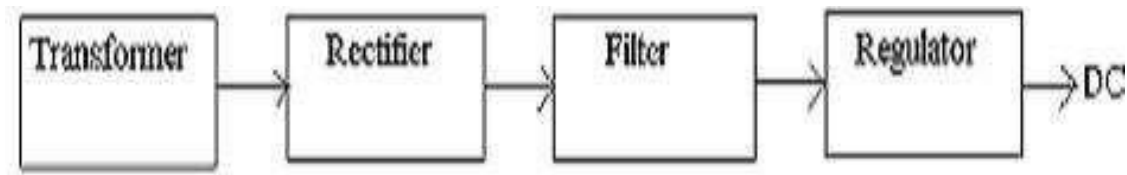


Fig 1.General Block Of Power Supply Unit

1.4 TRANSFORMER:

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.

1.5 RECTIFIER:

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.

1.6 FILTERS:

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.

1.7 REGISTERS:

The controller IC has two 8 bit registers, an instruction register (IR) and a data register (DR). The IR stores the instruction codes and address information for display data RAM (DD RAM) and character generator RAM (CG RAM). The IR can be written, but not read by the MPU.

The DR temporally stores data to be written to /read from the DD RAM or CG RAM. The data written to DR by the MPU, is automatically written to the DD RAM or CG RAM as an internal operation.

When an address code is written to IR, the data is automatically transferred from the DD RAM or CG RAM to the DR. data transfer between the MPU is then completed when the MPU reads the DR. likewise, for the next MPU read of the DR, data in DD RAM or CG RAM at the address is sent to the DR automatically. Similarly, for the MPU write of the DR, the next DD RAM or CG RAM address is selected for the write operation.

The dot-matrix liquid crystal display controller and driver LSI displays alphanumeric, Japanese kana characters, and symbols. It can be

configured to drive a dot-matrix liquid crystal display under the control of a

4- or 8-bit microprocessor. Since all the functions such as display RAM, character generator, and liquid crystal driver, required for driving a dot-matrix liquid crystal display are internally provided on one chip, a minimal system can be interfaced with this controller/driver

1.8 REGULATORS:

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.

1.9 FEATURES AND DESCRIPTION OF REGULATORS

- Output Current up to 1A
- Output Voltages of 5, 6, 8, 9, 10, 12, 15, 18, 24V
- Thermal Overload Protection
- Short Circuit Protection
- Output Transistor Safe Operating Area Protection

4 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.

History

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.

Applications

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.

Media

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.

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.

Infrastructure management

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.

Manufacturing Network

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.

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.

Medical and healthcare

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.

Building and home automation

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.

Transportation

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.

Metropolitan scale deployments

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.

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.

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.

Trends and characteristics

Intelligence

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.

Architecture

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.

Network architecture

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.

Complexity

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.

Size considerations

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.

Space considerations

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.

Sectors

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

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.

Frameworks

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 communication between a thing and an MQTT broker

Enabling technologies for IoT

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:

Short-range wireless

- 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 powerconsumption, low data rate, low cost, and high throughput.

Medium-range wireless

- HaLow – Variant of the Wi-Fi standard providing extended range forlow-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.

Long-range wireless

- 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.

Wired

- 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.

Simulation

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.

Politics and civic engagement

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.

Government regulation on IoT

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.

Criticism and controversies

Platform fragmentation

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.

Privacy, autonomy, and control

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.

Data storage and analytics

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.

Security:

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.

Design

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."

Environmental sustainability impact:

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.

Intentional obsolescence of devices:

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.

Confusing terminology:

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.

IoT adoption barriers

Complexity and unclear value propositions:

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.

Privacy and security concerns:

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.

Traditional governance structures:

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.

NODE MCU:

The ESP8266 is the name of a micro controller designed by Espressif Systems. The ESP8266 itself is a self-contained WiFi networking solution offering as a bridge from existing micro controller to WiFi and is also capable of running self-contained applications. This module comes with a built in USB connector and a rich assortment of pin-outs. With a micro USB cable, you can connect NodeMCU devkit to your laptop and flash it without any trouble, just like Arduino. It is also immediately breadboard friendly.

ESPlorer is an IDE (Integrated Development Environment) for ESP8266 devices. It's a multi platform IDE, can be used in any OS environment, this simply means that it runs on Windows, Mac OS X or Linux. Supported platforms: • Windows(x86, x86-64) • Linux(x86, x86-64, ARM soft & hard float) • Solaris(x86, x86-64) • Mac OS X(x86, x86-64, PPC, PPC64) This software allows you to establish a serial communications with your ESP8266 module, send commands, and upload code and much more. Requirements: • You need to have JAVA installed in your computer. If you don't have, go to this website: <http://java.com/download>, download and install the latest version. It requires JAVA (SE version 7 and above)

installed. • In order to complete the sample project presented in this Guide

you need to flash your ESP8266 with NodeMCU firmware. Refer to chapter-4 in this guide on how to flash the NodeMCU firmware. Main Resources: • ESPlorer Homepage: <http://esp8266.ru/esplorer/> • GitHub Repository: <https://github.com/4refr0nt/ESPlorer>

ESPlorer is an IDE (Integrated Development Environment) for ESP8266 devices. It's a multi platform IDE, can be used in any OS environment, this simply means that it runs on Windows, Mac OS X or Linux. Supported platforms: • Windows(x86, x86-64) • Linux(x86, x86-64, ARM soft & hard float) • Solaris(x86, x86-64) • Mac OS X(x86, x86-64, PPC, PPC64) This software allows you to establish a serial communications with your ESP8266 module, send commands, and upload code and much more. Requirements: • You need to have JAVA installed in your computer. If you don't have, go to this website: <http://java.com/download>, download and install the latest version. It requires JAVA (SE version 7 and above) installed. • In order to complete the sample project presented in this Guide you need to flash your ESP8266 with NodeMCU firmware. Refer to chapter-4 in this guide on how to flash the NodeMCU firmware. Main Resources: • ESPlorer Homepage: <http://esp8266.ru/esplorer/> • GitHub Repository: <https://github.com/4refr0nt/ESPlorer>

The GPIO(General Purpose Input/Output) allows us to access to pins of ESP8266 , all the pins of ESP8266 accessed using the command GPIO, all the access is based on the I/O index number on the NodeMCUdev kits, not the internal GPIO pin, for example, the pin 'D7' on the NodeMCU dev kit is mapped to the internal GPIO pin 13, if you want to turn 'High' or 'Low' that particular pin you need to called the pin number '7', not the internal GPIO of the pin. When you are programming with generic ESP8266 this confusion will arise which pin needs to be called during programming, if you are using NodeMCU devkit, it has come prepared for working with

Lua interpreter which can easily program by looking the pin names

associated on the Lua board. If you are using generic ESP8266 device or any other vendor boards please refer to the table below to know which IOindex is associated to the internal GPIO of ESP8266

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 dev 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.[9]

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^{[11][12][13]}). NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub.^[14] 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.^[15] Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform,^[16] 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^[17] to NodeMCU project,^[18] 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 but dedicated 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.

ESP8266 Arduino Core

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 tool chains to allow Arduino C/C++ to be compiled down to 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 down to the target MCU's machine language. Some creative ESP8266 enthusiasts have developed an Arduino core for the ESP8266 WiFi SoC that is available at the GitHub ESP8266 Core webpage. This is what is popularly called the "ESP8266 Core for the Arduino IDE" and it has become one of the leading software development platforms for the various ESP8266 based modules and development boards, including NodeMCUs.

The Button

The Button is a Wi-Fi connected push button designed by Peter R Jennings.[11] The Button is designed for single-purpose, internet-enabled functions. When the button is pressed, a connection is made to a web server which will perform the desired task. Applications include a doorbell or panic button.

NodeUSB

NodeUSB is an open IoT platform about the size of a standard USB

stick. It was designed to leverage NodeMCU (Lua) for easy programming and

has the extra feature of USB capability. It is ideal for Plug-n-Play solutions, allowing easy prototyping for developers.[12]

ijWatch

ijWatch is an open-hardware and open-source Wi-Fi smartwatch, using an OLED screen and running NodeMCU firmware.[13] The author believes it may be the first smartwatch. (As in, the watch itself is fully functional without the pairing of another bluetooth device such as a smartphone)

Smoke sensor:



A **gas detector** is a device that detects the presence of gases in an area, often as part of a safety system. This type of equipment is used to detect a gas leak or other emissions and can interface with a control system so a process can be automatically shut down. A gas detector can sound an alarm to operators in the area where the leak is occurring, giving them the opportunity to leave. This type of device is important because there are many gases that can be harmful to organic life, such as humans or animals.

Gas detectors can be used to detect combustible, flammable and toxic gases, and oxygen depletion. This type of device is used widely in industry and can be found in locations, such as on oil rigs, to monitor manufacture processes and emerging technologies such as photovoltaic. They may be used in firefighting.

Gas leak detection is the process of identifying potentially hazardous gas leaks by sensors. These sensors usually employ an audible alarm to alert people when a dangerous gas has been detected. Exposure to toxic gases can also occur in operations such as painting, fumigation, fuel filling, construction, excavation of contaminated soils, landfill operations, entering confined spaces, etc. Common sensors include combustible gas sensors, photoionization detectors, infrared point sensors, ultrasonic sensors, electrochemical gas sensors, and semiconductor sensors. More recently, infrared imaging sensors have come into use. All of these sensors are used for a wide range of applications and can be found in industrial plants, refineries, pharmaceutical manufacturing, fumigation facilities, paper pulp mills, aircraft and shipbuilding facilities, hazmat

operations, waste-water treatment facilities, vehicles, indoor air quality testing and homes.

Gas leak detection methods became a concern after the effects of harmful gases on human health were discovered. Before modern electronic sensors, early detection methods relied on less precise detectors. Through the 19th and early 20th centuries, coal miners would bring canaries down to the tunnels with them as an early detection system against life-threatening gases such as carbon dioxide, carbon monoxide and methane. The canary, normally a very songful bird, would stop singing and eventually die if not removed from these gases, signaling the miners to exit the mine quickly.

The first gas detector in the industrial age was the *flame safety lamp* (or Davy lamp) was invented by Sir Humphry Davy (of England) in 1815 to detect the presence of methane (firedamp) in underground coal mines. The flame safety lamp consisted of an oil flame adjusted to specific height in fresh air. To prevent ignition with the lamps flame was contained within a glass sleeve with a mesh flame arrestor. The flames height varied depending on the presence of methane (higher) or the lack of oxygen (lower). To this day, in certain parts of the world flame safety lamps are still in service.

The modern era of gas detection started in 1926-1927 with the development of the catalytic combustion (LEL) sensor by Dr. Oliver Johnson. Dr Johnson was an employee of Standard Oil Company in California (now Chevron), he begun research and development on a method to detect combustible mixtures in air to help prevent explosions in fuel storage tanks. A demonstration model was developed in 1926 and denoted as the Model A. The first practical "electric vapor indicator" meter begun production in 1927 with the release of the Model B.

The worlds first gas detection company, Johnson-Williams Instruments (or J-W Instruments) was formed in 1928 in Palo Alto, CA by Dr Oliver Johnston and Phil Williams. J-W Instruments is recognized as the first electronics company in Silicon Valley. Over the next 40 years J-W Instruments pioneered many "firsts" in the modern age of gas detection, including making instruments smaller and more portable, development of

a portable oxygen detector as well as the first combination instrument that could detect both combustible gases/vapors as well as oxygen.

Before the development of electronic household carbon monoxide detectors in the 1980s and 1990s, carbon monoxide presence was detected with a chemically infused paper that turned brown when exposed to the gas. Since then, many electronic technologies and devices have been developed to detect, monitor, and alert the leak of a wide array of gases.

As the cost and performance of electronic gas sensors improved, they have been incorporated into a wider range of systems. Their use in automobiles was initially for engine emissions control, but now gas sensors may also be used to ensure passenger comfort and safety. Carbon dioxide sensors are being installed into buildings as part of demand-controlled ventilation systems. Sophisticated gas sensor systems are being researched for use in medical diagnostic, monitoring, and treatment systems, well beyond their initial use in operating rooms. Gas monitors and alarms for carbon monoxide and other harmful gases are increasingly available for office and domestic use, and are becoming legally required in some jurisdictions.

Originally, detectors were produced to detect a single gas. Modern units may detect several toxic or combustible gases, or even a combination.^[1] Newer gas analyzers can break up the component signals from a complex aroma to identify several gases simultaneously.^[2]

Gas detectors can be classified according to the operation mechanism (semiconductors, oxidation, catalytic, photoionization, infrared, etc.). Gas detectors come packaged into two main form factors: portable devices and fixed gas detectors.

Portable detectors are used to monitor the atmosphere around personnel and are either hand-held or worn on clothing or on a belt/harness. These gas detectors are usually battery operated. They transmit warnings via audible and visible signals, such as alarms and flashing lights, when dangerous levels of gas vapors are detected.

Fixed type gas detectors may be used for detection of one or more gas types. Fixed type detectors are generally mounted near the process area of a plant or control room, or an area to be protected, such as a residential bedroom. Generally, industrial sensors are installed on fixed type mild steel structures and a cable connects the detectors to a SCADA system for continuous monitoring. A tripping interlock can be activated for an emergency situation.

Electrochemical gas detectors work by allowing gases to diffuse through a porous membrane to an electrode where it is either chemically oxidized or reduced. The amount of current produced is determined by how much of the gas is oxidized at the electrode,^[3] indicating the concentration of the gas. Manufacturers can customize electrochemical gas detectors by changing the porous barrier to allow for the detection of a certain gas concentration range. Also, since the diffusion barrier is a physical/mechanical barrier, the detector tended to be more stable and reliable over the sensor's duration and thus required less maintenance than other early detector technologies.

However, the sensors are subject to corrosive elements or chemical contamination and may last only 1–2 years before a replacement is required.^[4] Electrochemical gas detectors are used in a wide variety of environments such as refineries, gas turbines, chemical plants, underground gas storage facilities, and more.

Catalytic bead sensors are commonly used to measure combustible gases that present an explosion hazard when concentrations are between the lower explosion limit (LEL) and upper explosion limit (UEL). Active and reference beads containing platinum wire coils are situated on opposite arms of a Wheatstone bridge circuit and electrically heated, up to a few hundred degrees C. The active bead contains a catalyst that allows combustible compounds to oxidize, thereby heating the bead even further and changing its electrical resistance. The resulting voltage difference between the active and passive beads is proportional to the concentration of all combustible gases and vapors present. The sampled gas enters the sensor through a sintered metal frit, which provides a barrier to prevent an explosion when the instrument is carried into an atmosphere containing combustible gases. Pellistors measure essentially all combustible gases,

but they are more sensitive to smaller molecules that diffuse through the sinter more quickly. The measureable concentration ranges are typically from a few hundred ppm to a few volume percent. Such sensors are inexpensive and robust, but require a minimum of a few percent oxygen in the atmosphere to be tested and they can be poisoned or inhibited by compounds such as silicones, mineral acids, chlorinated organic compounds, and sulfur compounds.

Photoionization detectors (PIDs) use a high-photon-energy UV lamp to ionize chemicals in the sampled gas. If the compound has an ionization energy below that of the lamp photons, an electron will be ejected, and the resulting current is proportional to the concentration of the compound. Common lamp photon energies include 10.0 eV, 10.6 eV and 11.7 eV; the standard 10.6 eV lamp lasts for years, while the 11.7 eV lamp typically last only a few months and is used only when no other option is available. A broad range of compounds can be detected at levels ranging from a few ppb to several thousand ppm. Detectable compound classes in order of decreasing sensitivity include: aromatics and alkyl iodides; olefins, sulfur compounds, amines, ketones, ethers, alkyl bromides and silicate esters; organic esters, alcohols, aldehydes and alkanes; H₂S, NH₃, PH₃ and organic acids. There is no response to standard components of air or to mineral acids. Major advantages of PIDs are their excellent sensitivity and simplicity of use; the main limitation is that measurements are not compound-specific. Recently PIDs with pre-filter tubes have been introduced that enhance the specificity for such compounds as benzene or butadiene. Fixed, hand-held and miniature clothing-clipped PIDs are widely used for industrial hygiene, hazmat, and environmental monitoring.

Infrared (IR) point sensors use radiation passing through a known volume of gas; energy from the sensor beam is absorbed at certain wavelengths, depending on the properties of the specific gas. For example, carbon monoxide absorbs wavelengths of about 4.2-4.5 μm .^[5] The energy in this wavelength is compared to a wavelength outside of the absorption range; the difference in energy between these two wavelengths is proportional to the concentration of gas present.^[5]

This type of sensor is advantageous because it does not have to be

placed into the gas to detect it and can be used for remote sensing.
Infrared point

sensors can be used to detect hydrocarbons^[6] and other infrared active gases such as water vapor and carbon dioxide. IR sensors are commonly found in waste-water treatment facilities, refineries, gas turbines, chemical plants, and other facilities where flammable gases are present and the possibility of an explosion exists. The remote sensing capability allows large volumes of space to be monitored.

Engine emissions are another area where IR sensors are being researched. The sensor would detect high levels of carbon monoxide or other abnormal gases in vehicle exhaust and even be integrated with vehicle electronic systems to notify drivers.

Infrared image sensors include active and passive systems. For active sensing, IR imaging sensors typically scan a laser across the field of view of a scene and look for backscattered light at the absorption line wavelength of a specific target gas. Passive IR imaging sensors measure spectral changes at each pixel in an image and look for specific spectral signatures that indicate the presence of target gases.^[7] The types of compounds that can be imaged are the same as those that can be detected with infrared point detectors, but the images may be helpful in identifying the source of a gas.

Semiconductor sensors detect gases by a chemical reaction that takes place when the gas comes in direct contact with the sensor. Tin dioxide is the most common material used in semiconductor sensors,^[8] and the electrical resistance in the sensor is decreased when it comes in contact with the monitored gas. The resistance of the tin dioxide is typically around 50 k Ω in air but can drop to around 3.5 k Ω in the presence of 1% methane.^[9] This change in resistance is used to calculate the gas concentration. Semiconductor sensors are commonly used to detect hydrogen, oxygen, alcohol vapor, and harmful gases such as carbon monoxide.^[10] One of the most common uses for semiconductor sensors is in carbon monoxide sensors. They are also used in breathalyzers.^[9] Because the sensor must come in contact with the gas to detect it, semiconductor sensors work over a smaller distance than infrared point or ultrasonic detectors.

Ultrasonic gas leak detectors are not gas detectors per se. They detect the acoustic emission created when a pressured gas expands in a low pressure area through a small orifice (the leak). They use acoustic sensors to detect changes in the background noise of its environment. Since most high-pressure gas leaks generate sound in the ultrasonic range of 25 kHz to 10 MHz, the sensors are able to easily distinguish these frequencies from background acoustic noise which occurs in the audible range of 20 Hz to 20 kHz.^[11] The ultrasonic gas leak detector then produces an alarm when there is an ultrasonic deviation from the normal condition of background noise. Ultrasonic gas leak detectors cannot measure gas concentration, but the device is able to determine the leak rate of an escaping gas because the ultrasonic sound level depends on the gas pressure and size of the leak.^[11]

Ultrasonic gas detectors are mainly used for remote sensing in outdoor environments where weather conditions can easily dissipate escaping gas before allowing it to reach leak detectors that require contact with the gas to detect it and sound an alarm. These detectors are commonly found on offshore and onshore oil/gas platforms, gas compressor and metering stations, gas turbine power plants, and other facilities that house a lot of outdoor pipeline.

Relay:

A relay is an electrically operated switch. Current flowing through the coil of the relay creates a magnetic field which attracts a lever and changes the switch contacts. The coil current can be on or off so relays have two switch positions and they are doublethrow (changeover) switches. Relays allow one circuit to switch a second circuit which can be completely separate from the first. For example a low voltage battery circuit can use a relay to switch a 230V AC mains circuit. There is no

electrical connection inside the relay between the two circuits; the link is magnetic and mechanical.

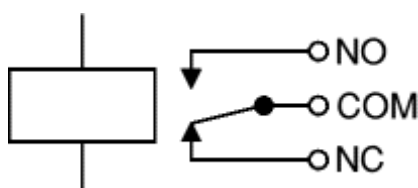
The coil of a relay current, typically 30mA for as much as 100mA for operate from lower cannot provide this current and a transistor is usually used to amplify the small IC current to the larger value required for the relay coil. The maximum output current for 200mA so these devices can without amplification.



passes a relatively large a 12V relay, but it can be relays designed to voltages. Most ICs (chips) the popular 555 timer IC is supply relay coils directly



Relays are usually SPDT or DPDT but they can have many more sets of switch contacts, for example relays with 4 sets of changeover contacts are readily available. Most relays are designed for PCB mounting but you can solder wires directly to the pins providing you take care to avoid melting the plastic case of the relay. The animated picture shows a working relay with its coil and switch contacts. You can see a lever on the left being attracted by magnetism when the coil is switched on. This lever moves the switch contacts. There is one set of contacts (SPDT) in the foreground and another behind them, making the relay DPDT.



The relay's switch connections are usually labeled COM, NC and NO:

- **COM** = Common, always connect to this, it is the moving part of the switch.
- **NC** = Normally Closed, COM is connected to this when the relay coil is **off**.
- **NO** = Normally Open, COM is connected to this when the relay coil is **on**.

Flame sensor:

A flame detector is a sensor designed to detect and respond to the presence of a flame or fire, allowing flame detection. Responses to a detected flame depend on the installation, but can include sounding an alarm, deactivating a fuel line (such as a propane or a natural gas line), and activating a fire suppression system. When used in applications such as industrial furnaces, their role is to provide confirmation that the furnace is working properly; it can be used to turn off the ignition system though in many cases they take no direct action beyond notifying the operator or control system. A flame detector can often respond faster and more accurately than a smoke or heat detector due to the mechanisms it uses to detect the flame.

Ultraviolet detector

Ultraviolet (UV) detectors work by detecting the UV radiation emitted at the instant of ignition. While capable of detecting fires and explosions within 3–4 milliseconds, a time delay of 2–3 seconds is often included to minimize false alarms which can be triggered by other UV sources such as lightning, arc welding, radiation, and sunlight. UV detectors typically operate with wavelengths shorter than 300 nm to minimize the effects of natural background radiation. The solar blind UV wavelength band is also easily blinded by oily contaminants.

Near IR array

Near infrared (IR) array flame detectors (0.7 to 1.1 μm), also known as visual flame detectors, employ flame recognition technology to confirm fire by analyzing near IR radiation using a charge-coupled device (CCD). A

near infrared (IR) sensor is especially able to monitor flame phenomena, without too much hindrance from water and water vapour. Pyroelectric sensors operating at this wavelength can be relatively cheap. Multiple channel or pixel array sensors monitoring flames in the near IR band are arguably the most reliable technologies available for detection of fires. Light emission from a fire forms an image of the flame at a particular instant. Digital image processing can be utilized to recognize flames through analysis of the video created from the near IR images.

Infrared

Infrared (IR) or wideband infrared (1.1 μm and higher) flame detectors monitor the infrared spectral band for specific patterns given off by hot gases. These are sensed using a specialized fire-fighting thermal imaging camera (TIC), a type of thermographic camera. False alarms can be caused by other hot surfaces and background thermal radiation in the area. Water on the detector's lens will greatly reduce the accuracy of the detector, as will exposure to direct sunlight. A special frequency range is 4.3 to 4.4 μm . This is a resonance frequency of CO_2 . During burning of a hydrocarbon (for example, wood or fossil fuels such as oil and natural gas) much heat and CO_2 is released. The hot CO_2 emits much energy at its resonance frequency of 4.3 μm . This causes a peak in the total radiation emission and can be well detected. Moreover, the "cold" CO_2 in the air is taking care that the sunlight and other IR radiation is filtered. This makes the sensor in this frequency "solar blind"; however, sensitivity is reduced by sunlight. By observing the flicker frequency of a fire (1 to 20 Hz) the detector is made less sensitive to false alarms caused by heatradiation, for example caused by hot machinery.

A severe disadvantage is that almost all radiation can be absorbed by water or water vapour; this is particularly valid for infrared flame detection in the 4.3 to 4.4 μm region. From approx. 3.5 μm and higher the absorption by water or ice is practically 100%. This makes infrared sensors for use in outdoor applications very unresponsive to fires. The biggest problem is our ignorance; some infrared detectors have an (automatic) detector window self test, but this self test only monitors the occurrence of water or ice on the detector window.

A salt film is also harmful, because salt absorbs water. However, water vapour, fog or light rain also makes the sensor almost blind, without the user knowing. The cause is similar to what a fire fighter does if he approaches a hot fire: he protects himself by means of a water vapour screen against the enormous infrared heat radiation. The presence of water vapor, fog, or light rain will then also "protect" the monitor causing it to not see the fire. Visible light will, however be transmitted through the water vapour screen, as can easily be seen by the fact that a human can still see the flames through the water vapour screen.

The usual response time of an IR detector is 3–5 seconds.

Infrared thermal cameras

MWIR infrared (IR) cameras can be used to detect heat and with particular algorithms can detect hot-spots within a scene as well as flames for both detection and prevention of fire and risks of fire. These cameras can be used in complete darkness and operate both inside and outside.

UV/IR

These detectors are sensitive to both UV and IR wavelengths, and detect flame by comparing the threshold signal of both ranges. This helps minimize false alarms.

IR/IR flame detection

Dual IR (IR/IR) flame detectors compare the threshold signal in two infrared ranges. Often one sensor looks at the 4.4 micrometer carbon dioxide (CO₂), while the other sensor looks at a reference frequency. Sensing the CO₂ emission is appropriate for hydrocarbon fuels; for non-carbon based fuels, e.g., hydrogen, the broadband water bands are sensed.

IR3 flame detection

Multi-infrared detectors make use of algorithms to suppress the effects of background radiation (blackbody radiation), again sensitivity is reduced by this radiation.

Triple-IR flame detectors compare three specific wavelength bands within the IR spectral region and their ratio to each other. In this case one sensor looks at the 4.4 micrometer range while the other sensors look at reference wavelengths both above and below 4.4. This allows the detector

to distinguish between non-flame IR sources and actual flames which emit hot CO₂ in the combustion process. As a result, both detection range and immunity to false alarms can be significantly increased. IR3 detectors can detect a 0.1m² (1 ft²) gasoline pan fire at up to 65 m (215 ft) in less than 5 seconds. Triple IRs, like other IR detector types, are susceptible to blinding by a layer of water on the detector's window.

Most IR detectors are designed to ignore constant background IR radiation, which is present in all environments. Instead they are designed to detect suddenly changing or increasing sources of the radiation. When exposed to changing patterns of non-flame IR radiation, IR and UV/IR detectors become more prone to false alarms, while IR3 detectors become somewhat less sensitive but are more immune to false alarms.

3IR+UV flame detection

Multi-Infrared (Multi-IR/3IR) detectors use algorithms to determine the presence of fire and tell them apart from background noise known to as "Black-body Radiation," which in generally reduce the range and accuracy of the detector. Black-body Radiation is constantly present in all environments , but is given off especially strongly by objects at high temperature. this makes high temperature environments, or areas where high temperature material is handled especially challenging for IR only detectors. Thus, one additional UV-C band sensor is sometimes included in flame detectors to add another layer of confirmation, as black body radiation does not impact UV sensors unless the temperature is extremely high, such as the plasma glow from an Arc welding machine.

Multi-wavelength detectors vary in sensor configuration. 1 IR+UV, or UVIR being the most common and low cost. 2 IR + UV being a compromise between cost and False alarm immunity and 3 IR + UV, which combines past 3IR technology with the additional layer of identification from the UV sensor.

Multi-Wavelength or Multi-spectral detectors such as 3IR+UV and UVIR are an improvement over their IR-only detectors counterparts which have been known to either false alarm or lose sensitivity and range in the presence of strong background noise such as direct or reflected light sources or even sun exposure. IR detectors have often relied on Infrared bulk energy growth to as their primary determining factor for fire detection, declaring an alarm when the sensors exceed a given range and ratio.

This

approach however is prone to trigger from non-fire noise. whether from blackbody radiation, high temperature environments, or simply changes in the ambient lighting. alternatively in another design approach, IR-only detectors may only alarm given perfect conditions and clear signal matches, which results in missing the fire when there is too much noise, such as looking into the sunset.

Modern Flame detectors may also make use of high speed sensors, which allow the capture of the flickering movement of flame, and monitor the pattern and ratios of the spectral output for patterns unique to fire. higher speed sensors allow for not only faster reaction times, but also more data per second, increasing the level of confidence in fire identification, or false alarm rejection.

Visible sensors

A visible light sensor (for example a camera: 0.4 to 0.7 μm) is able to present an image, which can be understood by a human being. Furthermore, complex image processing analysis can be executed by computers, which can recognize a flame or even smoke. Unfortunately, a camera can be blinded, like a human, by heavy smoke and by fog. It is also possible to mix visible light information (monitor) with UV or infrared information, in order to better discriminate against false alarms or to improve the detection range.^[3] The corona camera is an example of this equipment. In this equipment the information of an UV camera mixed with visible image information. It is used for tracing defects in high voltage equipment and fire detection over high distances.

In some detectors, a sensor for visible radiation (light) is added to the design.

The detection range:

The range of a flame detector is highly determined by the mounting location. In fact, when making a projection, one should imagine in what the flame detector "sees". A rule of thumb is, that the mounting height of the flame detector is twice as high as the highest object in the field of view. Also the accessibility of the flame detector must be taken into account, because of maintenance and/or repairs. A rigid light-mast with a pivot point is for this reason recommendable. A "roof" on top of the flame detector (30 x 30 cm, 1 x 1-foot) prevents quick pollution in

outdoor

applications. Also the shadow effect must be considered. The shadow effect can be minimized by mounting a second flame detector in the opposite of the first detector. A second advantage of this approach is, that the second flame detector is a redundant one, in case the first one is not working or is blinded. In general, when mounting several flame detectors, one should let them "look" to each other not let them look to the walls. Following this procedure blind spots (caused by the shadow effect) can be avoided and a better redundancy can be achieved than if the flame detectors would "look" from the central position into the area to be protected. The range of flame detectors to the 30 x 30 cm, 1 x 1- foot industry standard fire is stated within the manufacturers data sheets and manuals, this range can be affected by the previously stated de- sensitizing effects of sunlight, water, fog, steam and blackbody radiation.

WATER SPRINKLER:

An Irrigation sprinkler is a device used to irrigate agricultural crops, lawns, landscapes, golf courses, and other areas. They are also used for cooling and for the control of airborne dust. Sprinkler irrigation is a method of applying irrigation water which is similar to natural rainfall. Water is distributed through a system of pipes usually by pumping. It is then sprayed into the air through sprinklers so that it breaks up into small water drops which fall to the ground. The pump, valves, distribution pipes, and sprinklers are generally designed to apply water as uniformly as possible. Sprinklers that spray in a fixed pattern are generally called sprays or spray heads. Sprays are not usually designed to operate at pressures, due to misting problems that may develop.

Higher pressure sprinklers that themselves move in a circle are driven by a ball drive, gear drive, or impact mechanism (impact sprinklers). These can be designed to rotate in a full or partial circle.

Rainguns are similar to impact sprinkler, except that they generally operate at very high pressures of 40 to 130 lbf/in² (275 to 900 kPa) and flows of 50 to 1200 US gal/min (3 to 76 L/s), usually with nozzle diameters in the range of 0.5 to 1.9 inches (10 to 50 mm). In addition to irrigation, guns are used for industrial applications such as dust suppression and logging.

Many irrigation sprinklers are buried in the ground along with their supporting plumbing, although above ground and moving sprinklers are also common. Most irrigation sprinklers operate through electric and

hydraulic technology and are grouped together in zones that can be collectively turned on and off by actuating a solenoid-controlled valve.

Residential



An oscillating sprinkler is commonly used to water residential lawns, and is moved as needed.

Home lawn sprinklers vary widely in their size, cost, and complexity. They include impact sprinklers, oscillating sprinklers, drip sprinklers, and underground sprinkler systems. Small sprinklers are available at home and garden stores or hardware stores for small costs. These are often attached to an outdoor water faucet and are placed only temporarily. Other systems may be professionally installed permanently in the ground and are attached permanently to a home's plumbing system. An ingenious domestic sprinkler made by Nomad called a 'set-and-forget tractor sprinkler' was used in Australia in the 1950s. Water pressure ensured that the sprinkler slowly moved across a lawn.

Permanently installed systems may often operate on timers or other automated processes. They are occasionally installed with retractable heads for aesthetic and practical reasons (making damage during lawn mowing or other maintenance less likely). These often are programmed to operate at certain times of day or on some other schedule.

Underground Sprinkler[

Underground sprinklers function through means of basic electronic and hydraulic technology. This valve and all of the sprinklers that will be activated by this valve are known as a zone. Upon activation, the solenoid, which sits on top of the valve is magnetized lifting a small stainless steel plunger in its center. By doing this, the activated (or raised) plunger allows air to escape from the top of a rubber diaphragm located in the center of the valve. Water that has been charged and waiting on the bottom of this same diaphragm now has the higher pressure and lifts the diaphragm. This pressurized water is then allowed to escape down stream of the valve through a series of pipes, usually made of PVC (higher pressure commercial systems) or polyethylene pipe (for typically lower pressure residential systems). At the end of these pipes and flush to ground level

(typically) are pre measured and spaced out sprinklers. These sprinklers can be fixed spray heads that have a set pattern and generally spray between 1.5–2m (7–15 ft.), full rotating sprinklers that can spray a broken stream of water from 6–12m (20–40 ft.), or small drip emitters that release a slow, steady drip of water on more delicate plants such as flowers and shrubs. use of indigenous materials also recommended.^[2]

Agricultural Science[

Center pivot irrigation sprinkler nozzles, used in crop irrigation



Rotator style pivot applicator sprinkler



End Gun style pivot applicator sprinkler

The first use of sprinklers by farmers was some form of home and golf course type sprinklers. These ad hoc systems, while doing the job of the buried pipes and fixed sprinkler heads, interfered with cultivation and were expensive to maintain. In the 1950s a firm based in Portland, Oregon Stout-Wyss Irrigation System, developed the rolling pipe type irrigation system for farms that has become the most popular type for farmers irrigating large fields. With this system large wheels attached to the large pipes with sprinkler heads move slowly across the field.^[3]

Most irrigation sprinklers are used as part of a sprinkler system, consisting of various plumbing parts, pump unit,^[4] piping and control equipment. Outdoor sprinkler systems are sometimes used as a deterrent against homeless people. This sprinkler system was programmed to drench unsuspecting sleepers at random times during the night. Local businessmen soon copied this system in an effort to drive homeless people away from public sidewalks adjacent to their business

In 2014, it was reported that use of common garden hoses in combination with spray nozzles may generate aerosols containing droplets smaller than 10 μm , which can be inhaled by nearby people. Water stagnating in a hose between uses, especially when warmed by the sun, can host the growth and interaction of *Legionella* and free-living amoebae (FLA) as biofilms on the inner surface of the hose. Clinical cases of Legionnaires' disease or Pontiac fever have been found to be associated with inhalation

of garden hose aerosols containing Legionella bacteria. The report provides measured microbial densities resulting from controlled hose conditions in order to quantify the human health risks. The densities of Legionella spp. identified in two types of hoses were found to be similar to those reported during legionellosis outbreaks from other causes. It is proposed that the risk could be mitigated by draining hoses after use.



Features:

DC brushless motor with long lifetime

- Heavy duty work, can sustain continual 24 hours
- Sustain -40~125°C, suitable for extreme outdoor environment
- Durable permanent magnetic rotor/impeller & fine ceramic shaft
- Advanced magnetic drive technology for static-impeller, without any leakage for ever
- The motor with big machine movement optimization design, has very low temp rise
- Automatic polarity protection, overload protection, block protection special design to meet car vibration working condition, special design to meet car power supplying way which occur high peak voltage or unstable voltage
- Equipped with specializing car water-against connector
- Applied liquid: pure water, antifreeze solution
- IP protection level: IP 65
- Low or no maintenance
- Low power consumption

Protection functions:

·Automatic polarity protection ·Blocked protection

Typical Applications;

Car engine cooling circulation
Car engine pre-heating
Heating system (Car Auxiliary heaters & parking heaters)
Electric vehicles water circulation system
Normal Hot Water Circulation
Liquid Transfer
General Purpose Pumping

Applications:

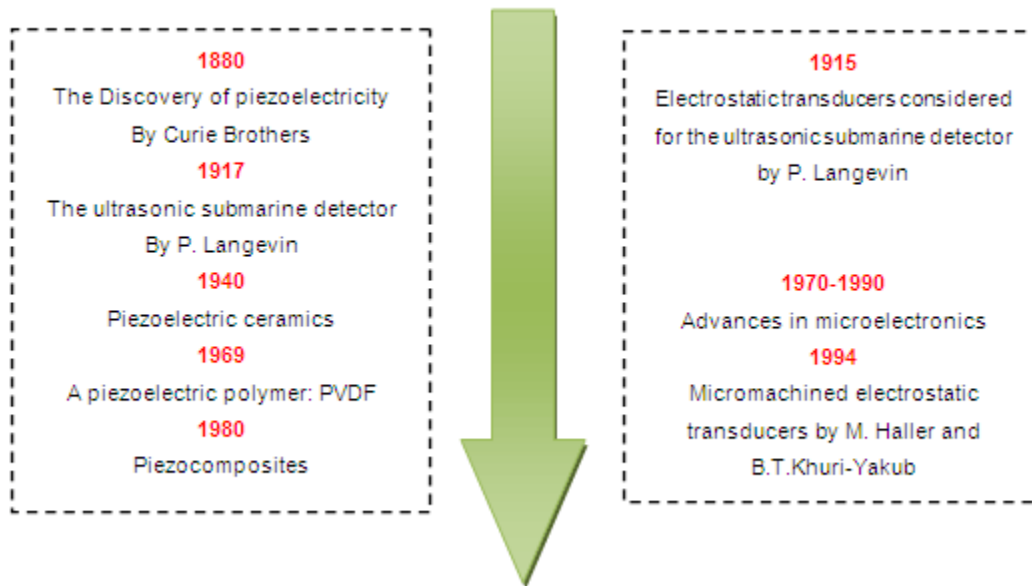
- Fire alerting system have a wide range of applications.
- Chemical Factories, Shopping Malls, local shops, Educational institutes, Parking Areas, Companies etc.

Ultrasonic (UV) Sensors or Ultrasound Sensors

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 extent.

History

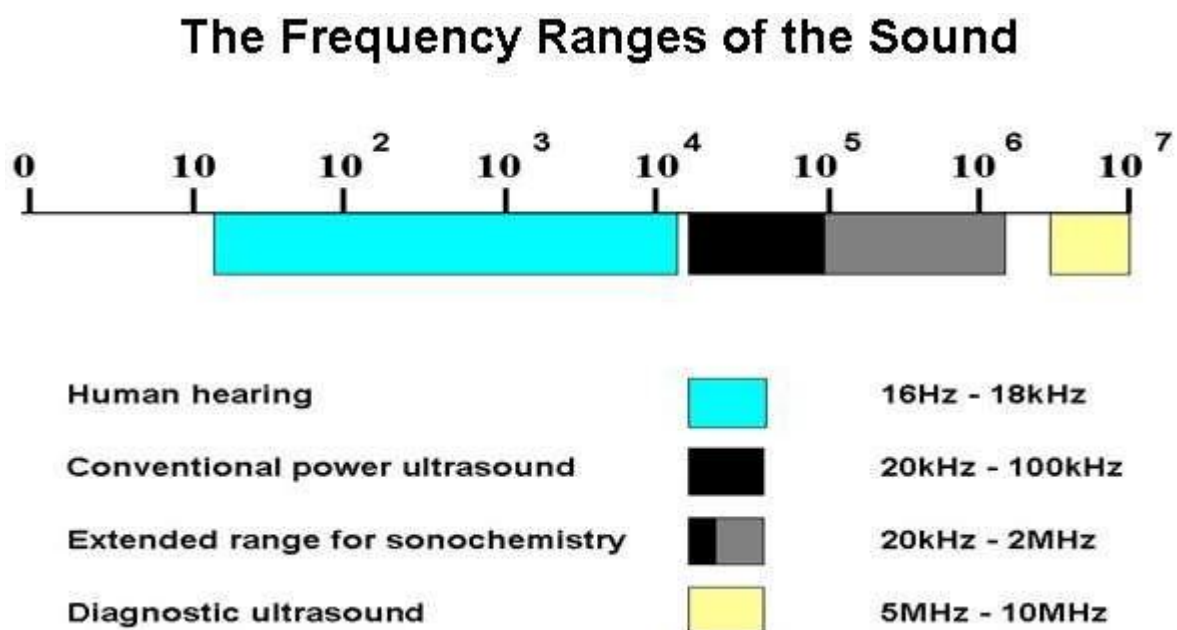
Ultrasonic Transducers: Historical Perspective



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.

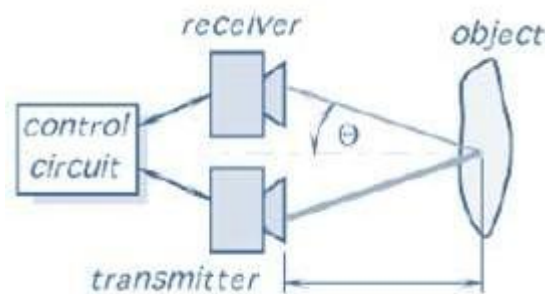
How Ultrasonic Sensors work?

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



$$L = \frac{v t \cos \theta}{2}$$

Where 't' is the time taken by the wave to reach back to the sensor and 'θ' is the angle between the horizontal and the path taken as shown in the figure. If the object is in motion, instruments based on Doppler shift are used. Get all the details about internal structure and working of an ultrasound sensor at [Insight-How Ultrasonic Sensors Work](#).

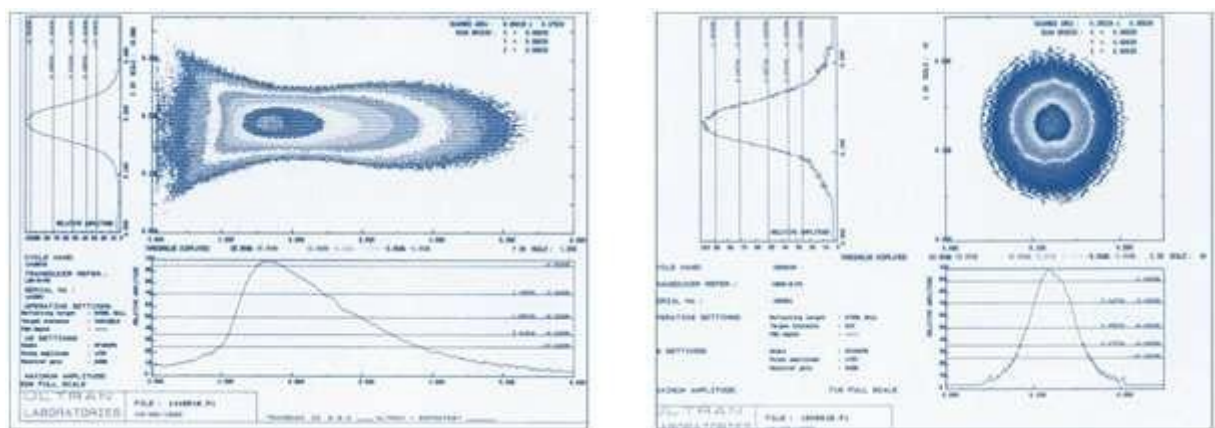
Generating Ultrasonic Waves

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:



Axial and Cross Sectional beam profiles

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).

Importance of Ultrasonic Sensors

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.

Problems & Concerns

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

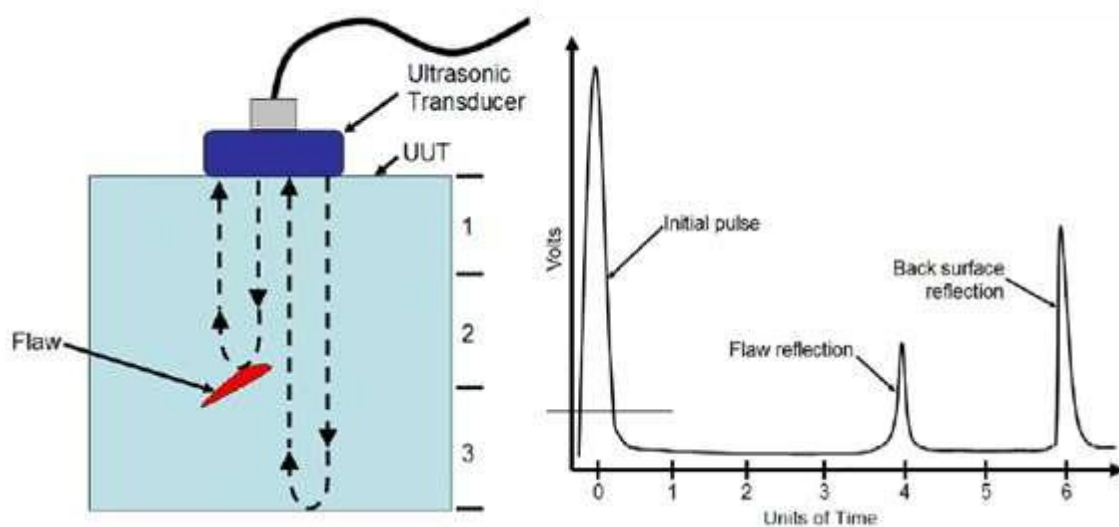
are not a true representation of the imaged object. Just like the vision starts to blur when the distance of the object from the eye gets too small for the eyes to see it, ultrasonic devices also have a 'dead zone' where the sensor cannot reliably make measurements. This happens due to a phenomenon called 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.

Applications

The applications of ultrasonic sensors can be classified on the basis of the property that they exploit. These can be summarized as:

Domain	Parameter	Applications
Time	Time-of-Flight, Velocity	Density, Thickness, Flaw Detection, Anisotropy, Robotics, Remote Sensing etc.
Attenuation	Fluctuations in reflected and Transmitted Signals	Defect characterization, microstructures, interface analysis
Frequency	Ultrasonic Spectroscopy	Microstructure, grain size, porosity, phase analysis.
Image	Time-of-Flight, velocity, attenuation mapping in Raster C-Scan or SARs	Surface and internal Defect imaging, density, velocity, 2D and 3D imaging.

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.



Flaw Detection Using Ultrasonic Sensors

Future

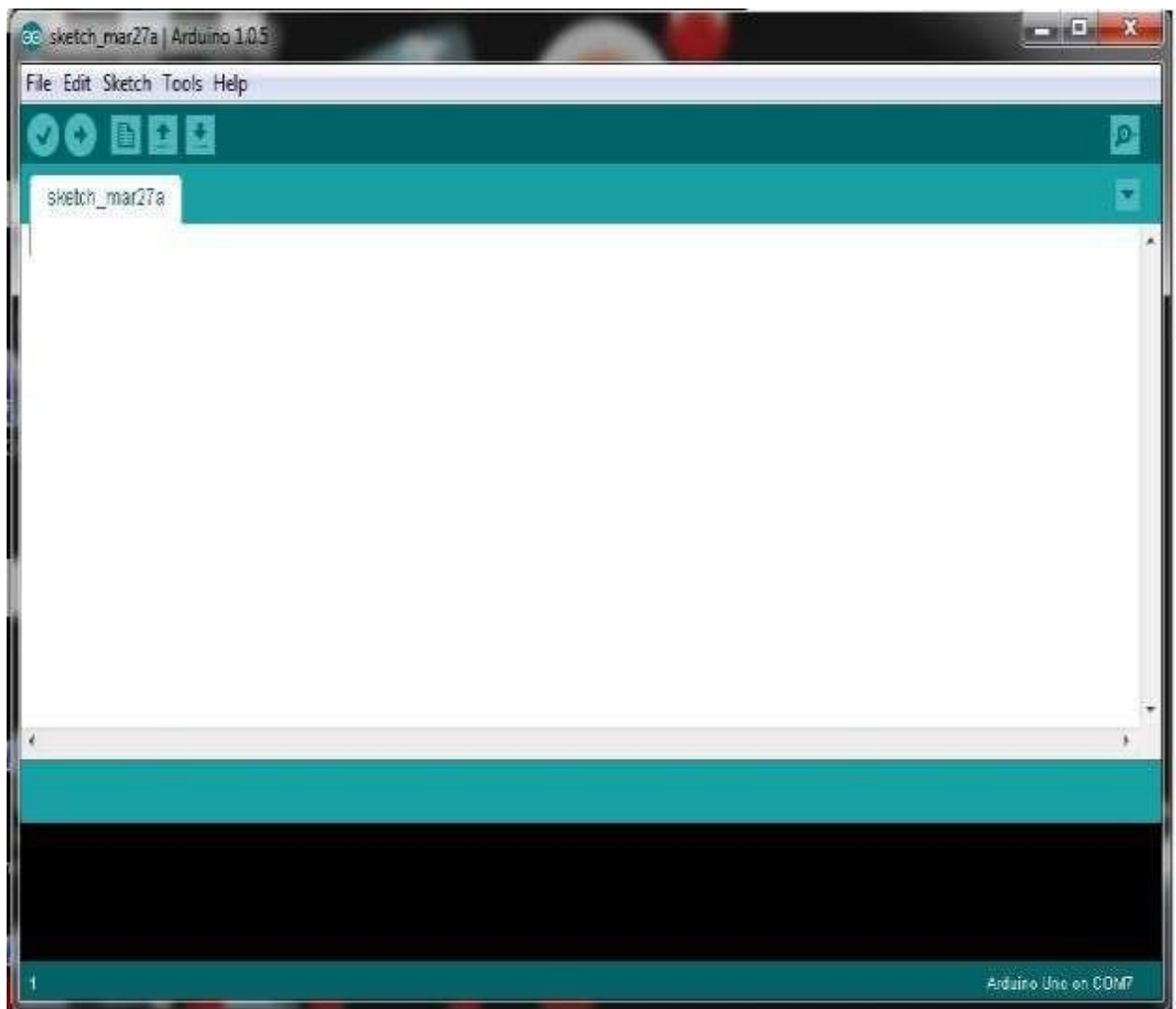
Non destructive testing and flaw detection uses ultrasonic waves in various modes like the Longitudinal (L-wave) mode and the Shear (S-wave) mode to detect flaws in materials. With the advances in Science, new materials offering increased performance at lower voltages like the capacitive micromachined 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

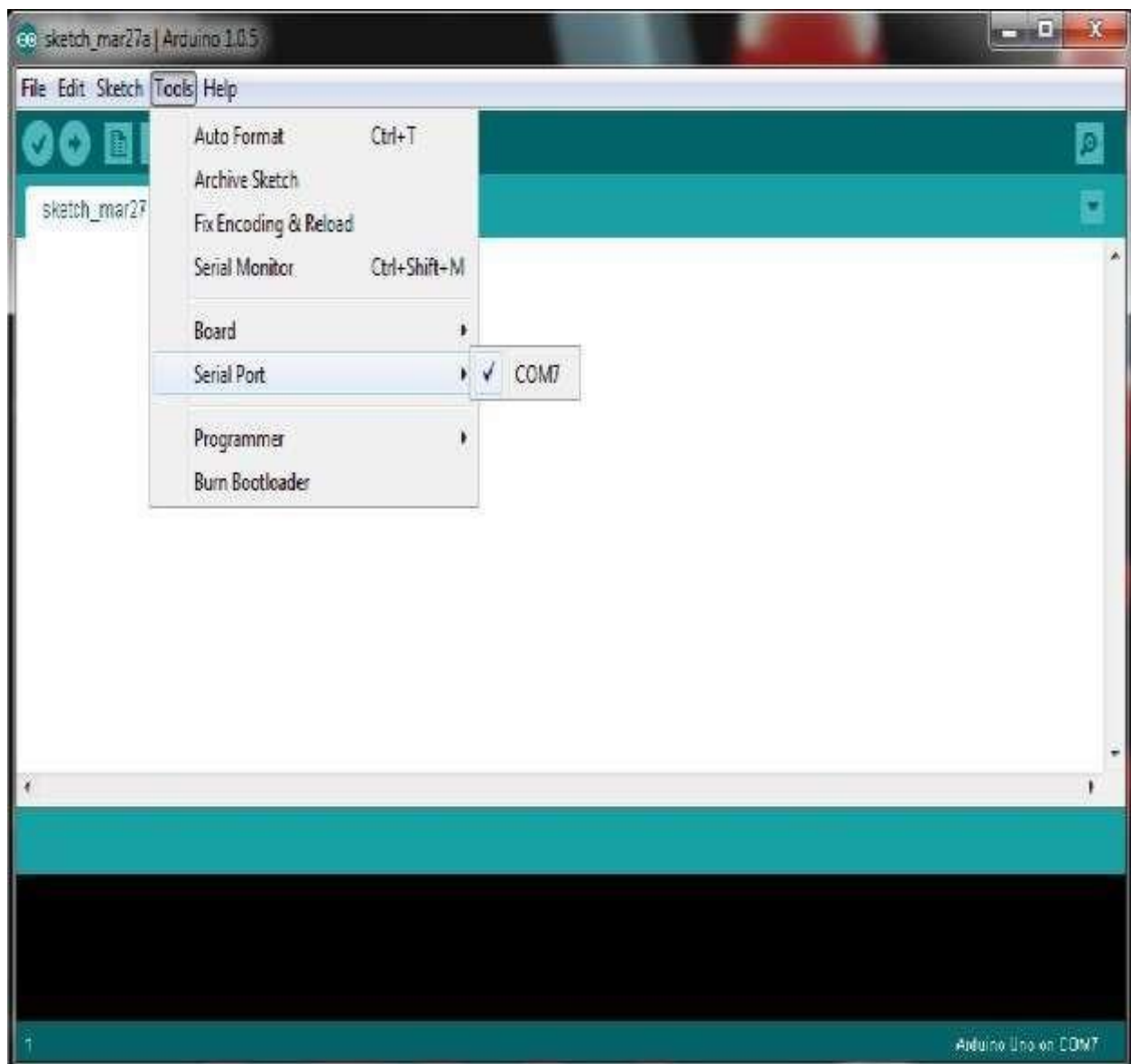
applications are expected to thrive and offer a substantial alternative to the contemporary technologies.

ARDUINO SOFTWARE:

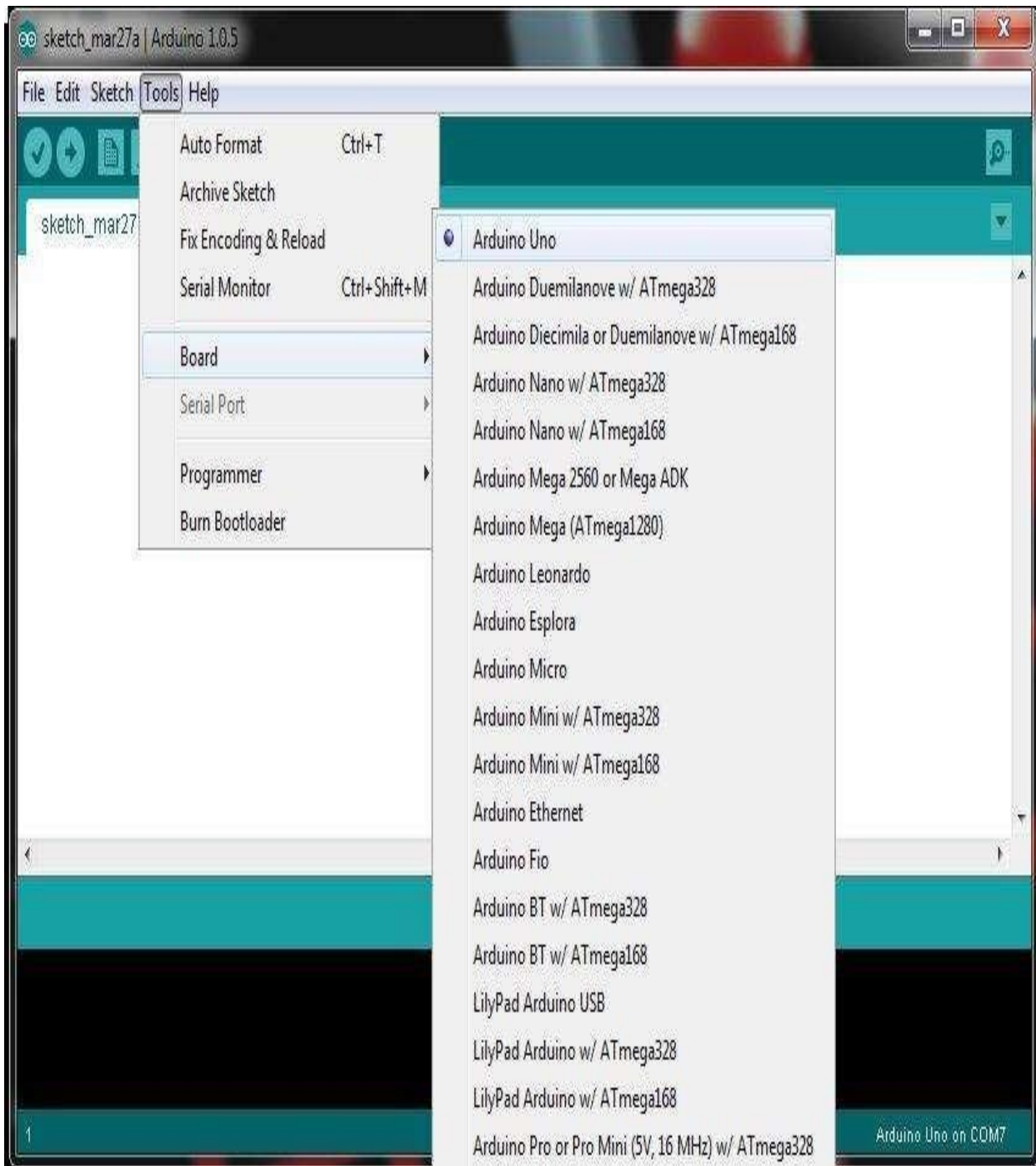
1. Open Arduino IDE as shown below
- Open Arduino IDE



2. Select the COM Port from tool
Select the COM Port



3. Select the required Arduino board from Tools as shown below
Select the required Arduino board



4. Write the sketch in Arduino IDE

Sketch in Arduino IDE



```
sketch_mar28a §
#include <Servo.h> //includes the servo library
int motor_pin1 = 4;
int motor_pin2 = 5;
int motor_pin3 = 6;
int motor_pin4 = 7;
int servopin = 8;
int sensorpin = 0;
int dist = 0;
int leftdist = 0;
int rightdist = 0;
int object = 500; //distance at which the robot should look for another route
const int RightSensor = 1; // This pin is used to read the value of the Right Sensor.
const int LeftSensor = 2; // This pin is used to read the value of the Left Sensor.
int SensorLeft; // This stores the value of the Left Sensor pin to use later on in the sketch
int SensorRight; // This stores the value of the Right Sensor pin to use later on in the sketch
int SensorDifference; // This value is used to determine the difference between the Left and Right
```

1

Arduino Uno on COM7

5. Compile and upload the Sketch to Arduino board upload the Sketch to Arduino board



Result



Conclusion

This fire extinguishing robot using IoT is introduced to help fire men to avoid the risk situations. This proposed work presents an outline about the fire extinguishing robot using IoT and also gives objectives and advantages of the proposed system. It provides better features that make it a more practically usable robot in real time. By introducing this system in industries and other factories, fire accident rates can be decreased

REFERENCES

- [1] Undug, J., Arabiran, M.P., Frades, J.R. Mazo, J., Teogangco, M., “Fire Locator, Detector and Extinguisher Robot with SMS Capability”, 8th IEEE International Conference Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)
- [2] TawfiquerRakib, M.A. Rashid Sarkar, “Design and Fabrication of Autonomous Fire Extinguisher Robot with Multisensor Fire Detection Using PID Controller”, 5th International Conference on Informatics, Electronics and Vision (ICIEV)
- [3] SanoberFarheen, Imtiaz H. Kalwar, Ian Grout, Elfred Lewis, Yasmeen NazPanhwar, “Prototype for Localization of Multiple Fire Detecting Mobile Robots in a Dynamic Environment”, International Conference on Computing for Sustainable Global Development (INDIACom)