

# bfs

*by* sasanapusruzan

---

**Submission date:** 18-Apr-2021 04:36PM (UTC+0900)

**Submission ID:** 1561596956

**File name:** 222\_Project\_Report.pdf (1.51M)

**Word count:** 16299

**Character count:** 99357

# **Intelligent Traffic control and Emergency Vehical Rescue Monitoring System By Using IOT**

<sup>4</sup> Submitted in partial fulfillment of the requirements for the award of Bachelor of  
Engineering degree in Electronics and Communication Engineering

By

Bogala Sumanth Reddy (37130064)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING  
<sup>4</sup> SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

**SATHYABAMA**

INSTITUTE OF SCIENCE AND TECHNOLOGY  
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119 APRIL – 2020

### **BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work of  
Bogala Sumanth Reddy (37130064) who have  
done the Project work as a team who carried out the project entitled  
“intelligent traffic control and emergency vehicle rescue monitoring system by  
using iot” under my supervision from November 2020 to April 2021.

**Internal Guide**

**M.DEVIKA**

M.E, Ph.D

**Head of the Department**

**Dr. T. RAVI**

M.E, Ph.D

Submitted for Viva voce Examination held on\_\_\_\_\_

**Internal Examiner**

15

**External Examiner**

# **DECLARATION**

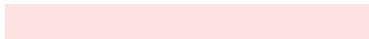
I **Bogala Sumanth Reddy (37130064)**

hereby declare that the Project Report entitled “**intelligent traffic control and emergency vehicle rescue monitoring system by using iot**” done by us under the guidance of **M.DEVIKA M.E, Ph.D** at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

**DATE:**

**PLACE:**



**Bogala Sumanth Reddy**

**SIGNATURE OF THE CANDIDATE**

## ACKNOWLEDGEMENT

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

Type your text

I convey our 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, Dept. of Electronics and Communication Engineering for providing us necessary support and details at the right time during the progressive reviews.

Type your text

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

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

# **Intelligent Traffic control and Emergency Vehical Rescue Monitoring System By Using IOT**

## **Abstract**

Congestion in traffic is a serious issue. In existing system signal timings are fixed and they are independent of traffic density. Large red light delay leads to the traffic congestion. In paper, IOT based traffic control system implemented in the which signal timings were updated based on the vehicle counting. This system consists of the WI-FI transceiver module, it transmits the vehicle count of current system to next traffic signal. Based on the traffic density of the previous signal it controls signals of next signal.

The emergency vehicles such as police vehicles, ambulances and fire engines given equal priority over other vehicles and if, get stuck up in traffic congestion. A methodology to pass vehicles based on priority based vehicles detection based on image processing techniques proposed in paper. If emergency vehicle detected on the road, lane in which the vehicle will be given the higher priority over remaining vehicles other lanes. This paper proposed algorithm which detect whether vehicle is emergency one or not on the road.

## **Introduction:**

Most traffic control systems in developing countries operate on time.

Concept, time is set on the green/red signal based on the expected traffic.

intensity. Such systems are not dynamic and in many cases the results are poor.

situation. Existing timer-based motion systems cannot be controlled.

Traffic jam effectively. In addition, ambulances can also crash.

There is a problem with the traffic lights. Intelligent traffic management

To solve ambulance problems, you need a system.

Currently, traffic management is really inefficient. Main reason

This is due to the low traffic priority. We are faced with a situationSome lanes may have less traffic than others, but because the length of the green signal is the same for each lane, none of the lanes have priority, leading to wasted resources and driver stress. Our research is based on density-based traffic

management and prioritizes the lane where emergency vehicles are located. By calculating the traffic density using a dynamic background, the results have been greatly improved, reducing the possibility of automatically adding stationary objects to that scene. Priority lanes after the allotted time are set back to normal lanes, ensuring that all lanes have the same chance. If no emergency vehicle is found, the congested lane has the highest priority.

#### **Literature survey:**

#### **Title 1: Intelligent Traffic Information System Based on Integration of Internet Of Things and Agent**

**Author:** Hasan Omar Al-Sakran

Due to the popularity of private cars in recent years, the city becoming more popular. As a result, mobility is becoming an important issue in major cities around the world. Some of the road traffic problems have been associated with congestion and accidents, resulting in huge waste of time, property damage and environmental pollution. This research paper introduces a new IoT-based intelligent traffic management system that can be inexpensive, highly scalable, highly compatible, easy to upgrade, replace the existing traffic management system, and propose a system that can significantly improve road traffic. Internet of Things is a wireless detection technology of internet and network detection technology that ensures intelligent recognition, automatic tracking, monitoring, control and processing of tagged traffic objects. This document proposes an architecture that combines Internet of Things and an agent technology into a single platform. Here, agent technology provides efficient communication and interfaces between many heterogeneous, highly decentralized distributed devices in IoT. This architecture introduces use of the active radio frequency identification, wireless sensor technology, ad hoc object networks, and Internet information systems in which tagged traffic objects can be automatically forwarded, tracked, and investigated over the network. This study provides an overview of NetLogo's distributed traffic simulation model, an agent-based environment for IoT traffics monitoring systems using the mobile agent technology.

## **Title 2:TRAFFIC MONITORING AND REPORTING SYSTEM USING IOT**

**Author:** Chiranjeev V. Tapas 1, Narendra Chaudhar

Despite the introduction of many traffic rules, we do not see traffic violations or deaths from such negligence. People or systems could be the cause of this failure. So, to solve the problem, this article presents a device that uses an Arduino Uno, which processes each vehicle individually with connected sensors and modules and stores speed, shock, or accident data along with its location. And time. In each connection, the device in the receiver area (connected to the signal) transmits data to the receiving device. This information is uploaded to a central database using the Internet of Things without human intervention.

## **Title 3:Traffic Management System Using IoT Technology - A Comparative Review**

**Author:**OmidAvatefipour; FrooghSadry

With the growing population of cities around the world, we will continue to produce all types of vehicles from manufacturers and a number of vehicles on road. This naturally leads to more traffic jams, especially during peak hours, especially in metropolitan areas. This phenomenon continues to put pressure on researchers, city officials and city planners to continuously improve safer and more cost-effective traffic management systems. Much research has been done to tackle these evolutionary problems, resulting in several notable improvements, such as the distribution of emergency vehicle lanes in urban areas. However, even with these lanes, it is often difficult for emergency vehicles to get the ideal meal to reach their destination. A new approach to dealing with this problem is the Intelligent Transmission System (ITS). This approach can help you solve problems by integrating your existing technology with your existing infrastructure. This article aims to compare different traffic management approaches, namely Radio Frequency Identification, Traffic Light Systems (TLS): Static and Dynamic TLS, and Internet of Things (IoT). In latter method, traffic data is quickly collected, sent as the big data for processing, and sent to an AKA interface (UI) mobile application, providing an alternative to reduce traffic by estimating traffic density in various areas.

## **Title 4:Intelligent Traffic Monitoring Using Internet of Things (IoT) with Semantic Web**

**Author:**ManujDarbarir, Diwakar Yagyasen, Anurag Tiwari

The Internet of Things (IoT), a global internet system for computing devices and machines, is one of the most important trends in information technology. Adopting a unified communication strategy will be a prerequisite for mass adoption. Semantic technology (Semantic Web) is encouraged as a unified mode of communication. Although there has been some success in the study of applying the Semantic Web to IoT, the dynamic and complex nature of IoT often requires case-based solutions that are generally difficult to apply. This overview provides the basis for further research on the use of semantic technologies in IoT by incorporating semantic technical issues in the IoT domain.

#### **Title 5: Development of IoT device for traffic management system**

**Author: Hon Fong Chong; Danny Wee Kiat Ng**

Traffic congestion is a serious concern in urban areas around the world. The annual economic loss from traffic congestion in Malaysia in 2015 is estimated at around \$20 billion. To solve the problem of traffic congestion, the first fixed cycle traffic light (TLS) system was introduced at intersections. However, fixed bike TLS does not follow rapid increase in number of the registered vehicles. This article proposes the development of the Internet of Things (IoT) devices for traffic management systems. Intel Edison captures real-time traffic flow and communicates with the Microsoft Azure IOT cloud server. The cloud server prioritizes all routes according to the current traffic volume. Then it uses a dynamic algorithm to calculate the Green Period Time (GLPT). The results of the simulation showed that the dynamic TLS cycle reduced queue length and latency by 68% and 67%, respectively, at the junction. In addition, the monitoring application is designed to allow traffic inspectors to easily monitor traffic flow in real time.

#### **Existing system:**

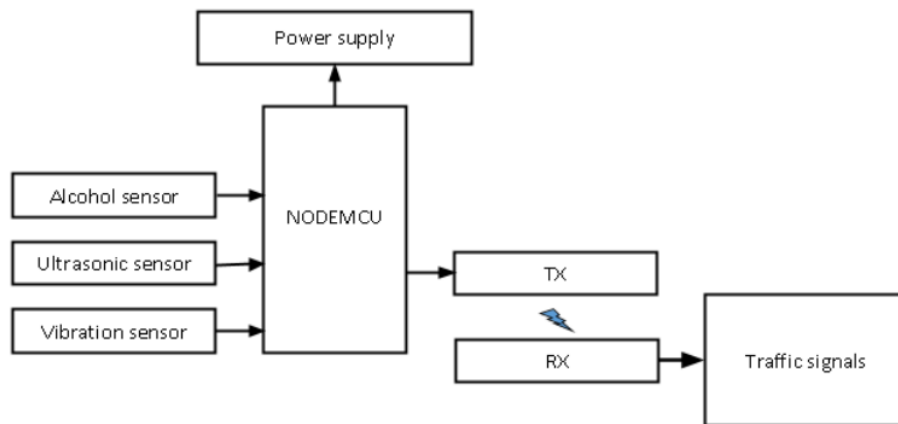
- In the existing system, traffic light signal is just monitoring and controlling purpose only depend upon the traffic can be identify through some kind of sensor like vibration sensor or image processing techniques
- the same technique used for ambulance identification
- it is not highly reliable in real time

#### **Proposed system:**

This article describes an IoT-based traffic management system in which signal times are updated based on vehicle density on the road. The proposed system is implemented with Raspberry Pi and Arduino. Density is measured with a Raspberry Pi. The proposed system provides good performance and reduces traffic congestion. Results show real-time vehicle billing. The proposed system is suitable for real-time vehicle handling.

This document proposes a priority-based motion management system with image processing that gives all ambulances a high priority to help them pass smoothly through traffic lights. This helps them reach the disaster scene quickly and save the lives of many around us. This is done through preprocessing and visualization techniques. In the future, we plan to add other emergency vehicle functions for more accurate detection.

**Block diagram:**



### Hardware required:

- Traffic light board
- ZigBee TX and RX
- Raspberry pi
- USB Camera
- Vibration Sensor
- Alcohol sensor
- GPS

### Software required:

- Arduino IDE
- Embedded C language
- Flash magic

The Internet of Things (IoT) is a network of the physical devices, vehicles (also known as "connected devices" and "smart devices"), buildings and electronics, actuators, software, sensors and other elements built into the network. A connection that allows these devices to collect and exchange data. In 2013, the Global Internet of Things Standardization Initiative (IoT-GSI) referred to IoT as the "infrastructure of the global information society, and provides advanced services by combining objects (physical and virtual) based on existing interoperable information and communication evolution technologies. "For this purpose, "things" are objects of the physical world (physical things) or information worlds (virtual things) that can be identified and integrated into a communication network. "With the Internet of Things, objects can be controlled or controlled remotely through the existing network infrastructure, giving the opportunity to more directly integrate the physical world into computer systems, improving efficiency, accuracy and economic benefits and reducing human intervention. Complementing the IoT, technology becomes an example of a more common kind of cyber-physical system, which also includes technologies such as smart networks, virtual power plants, smart homes and smart homes, smart cities, all of which are unique by embedded computer systems. According to experts, IoT will contain about 30 billion objects in 2014. Overall, IoT will provide better connectivity to devices, systems and services beyond Machine-to-Machine (M2M). Communication and span protocols, domains and multiple applications.. Combining these embedded devices (including smart objects) not only enables automation in virtually any area, but also enables advanced applications such as smart networks and extends to areas such as smart cities. "Things" in the IoT sense refers to a wide range of devices such as heart implants, biochip transponders for pets, electric shellfish in coastal waters, cars with built-in sensors, and DNA testing devices for the environment/food/food. Can / Pathogen field or monitoring work assisting fire fighters in search and rescue operations. Legal researchers suggest that "things" be considered "an integrated combination of hardware, software, data and services." Various existing technologies are used to collect useful data and then transfer the data independently between different devices. Examples of the current market are home automation ( known as smart appliances), such as lighting control and automation, heating (smart thermostats, etc.), Appliances such as ventilation, air conditioning systems (HVAC) and washer/dryers, robot-vacuum cleaners, and air. Purifier, stove or refrigerator/freezer using Wi-Fi for monitoring. IoT is expected not only to extend internet-related automation into many new application areas, but also to generate large amounts of data from multiple locations. In other words, it is more efficient to aggregate data faster and to increase the need for data indexing, storage, and processing. Internet of

Things is one of the platforms for smart modern cities and intelligent energy management systems.

## Chapter – 2 History

Since 2016, IoT vision has been developed through the convergence of many technologies including ubiquitous wireless, real-time analytics, machine learning, product sensors and embedded systems. This means that traditional disciplines such as embedded systems, wireless sensor networks, control systems, automation (including home and building automation) contribute to the creation of the Internet of Things (IoT). The concept of a smart device network was discussed in 1982, when Carnegie Mellon University's modified charcoal engine became the first internet-connected device to report whether stock and recently loaded beverages were cool. In Ubiquitous Computing, 21st Century Computers, and Academia such as UbiComp and PerCom, Mark Weiser's groundbreaking 1991 article laid out a modern vision for the Internet of Things. In 1995, Ravi described that the concept of IEEE Spectrum as "moving small data packages with a large-scale goal to integrate automate everything of home appliances to whole plants." Between 1993 and 1996, several companies provided solutions such as Microsoft at Work or Home NEST. However, it wasn't until 1999 that this area began to gain momentum. Bill Joy considered device-to-device D2D communication as part of the Six Networks concept presented at World Economic Forum in Davos in 1999. The term Internet of Things gained popularity in 1999 at MIT's Auto Identification Center and in publications related to market research. Kevin Johnson (one of the founder of the original Auto Identification Center) considered radio frequency identification as a prerequisite for Internet of Things at the time. Ashton likes phrase Internet for Things. If the identifier contains all the objects and people of everyday life, your computer can check it and collect your inventory. In addition to RFID, marking can be done with technologies such as short-range communication, QR codes, barcodes and digital watermarks. In the original interpretation, one of the consequences of introduction of Internet of Things is to equip every object in the world with a small identification device or machine-readable identifier to change everyday life. Continuous inventory control will be everywhere. An individual's ability to interact with an object remotely based on immediate or ongoing needs may change in accordance with existing end-user agreements. For example, these technologies allow filmmakers to have much more control over their personal end-user devices by maintaining copyright restrictions and remote digital rights management, so that buyers who buy Blu-ray discs to watch movies rely on homeowners. To be able to do it. Decisions such as the failure of DIVX Circuit City, for example.

### Chapter – 3 Applications

According to Gartner, Inc. (a technology research and consulting firm), there will be about 20.8 billion devices in Internet Of Things by 2020. ADI Research estimates that by 2020, more than 20 million devices will be connected without wire to the Internet Of Things. According to the Pew Research Internet Project's 2014 survey and study, the vast majority of dedicated technology professionals and dedicated Internet users (83%) were ) Will be widespread and beneficial in 2025. The Internet of Things obviously includes a very large number of devices connected to the Internet. As part of an effort to drive new technological innovations, the UK government appears to have invested £40 million in Internet of Things research in its 2015 budget. Former British Prime Minister Exchequer George Osborne said the Internet of Things was the next step in the information revolution. This includes managing the interconnection of everything from urban transport to medical devices and consumer electronics. Embedded devices with limited CPU, memory and power resources mean IoT can find applications in almost any field. These systems can collect information from a variety of conditions, from natural ecosystems to buildings and factories, and apply them to environmental sensing and urban planning. On the other hand, IoT systems are not only smart, they are responsible for performing actions. For example, smart shopping systems can track specific mobile phones to track the shopping habits of specific consumers in a store. Then these consumers can receive a special offer for their favorite dish or the location of the desired item, which is automatically sent from the refrigerator to their mobile phone. Additional examples of detection and activation are reflected in applications that process heat, water, electricity and energy and transport systems that support cruising. Other applications the Internet of Things can provide include advanced home security features and home automation. The term animal internet has been proposed to describe a network of biological sensors that allows users to use cloud analysis to study DNA or other molecules. However, IoT applications are not limited to these areas. There may be other special uses of IoT as well. Here is an overview of some of the more well-known applications.

### Chapter – 4 Media

To fine-tune how things, media, and big data are connected, you first need to specify a specific context in the engine used by the media process. Nick Culdree and Joseph Throw suggested that media experts access big data as a set of action points for information from millions of people. The industry appears to move away from traditional way to approach using specific media such as magazines, newspapers or TV shows and using technology to reach consumers

at the best time in the world. Of course, the ultimate goal (statistically) is to deliver or deliver a message or content that fits the consumer's global perspective. For example, publishing environments are increasingly adapting to deliver messages (advertisements) and content (articles) obtained only through data mining to consumers. The media industry processes big data in a two-part, interconnected way. Consumer Targeting (For Marketing Advertising) Data Collection This is how the Internet of Things creates opportunities to measure, collect and analyze growing behavioral statistics. The correlation between these data can revolutionize the marketing of targeted products and services. For example, as Danny Meadows-Clew pointed out, the combination of behavioral tracking and analytics tracking has opened up a new level of accuracy for focusing display ads on relevant interest items. Big data and the Internet of Things work together. From a media point of view, data is a key derivative of unit cohesion, but it plays an important role in providing greater focus accuracy. Thus, the Internet of Things has transformed the media industry, businesses and governments, and opened a new era of economic growth and competitiveness. The abundance of data generated by this industry (e.g. big data) allows advertising and media practitioners to gain insight into the current targeting mechanisms used in the industry..

1

## **Chapter – 5 Environmental monitoring**

Environmental monitoring IoT applications typically use sensors to monitor air or water quality, air or soil conditions to protect the environment, and may also include areas such as animal movement and habitat monitoring. The development of devices connected Internet with limited resources also means that emergency services can use earthquake or early tsunami warning systems to provide more in effective support. IoT devices in application typically cover large geographic area and ready to change be mobile. There have been claims that standardizing IoT sensing will revolutionize the field.

7

## **Chapter – 6 Infrastructure management**

Monitoring and managing urban and rural infrastructure such as bridges, railroads, onshore and offshore wind farms is an important IoT application. IoT infrastructure can be used to monitor changes in any event or structural condition that could threaten security and increase risk. It can also be used to efficiently plan repairs and maintenance by coordinating the work between different service providers and users of these websites. IoT devices can used to manage critical infrastructure such as bridge to provide access ships. Monitoring and implementing infrastructure using IoT devices can improve emergency response coordination, incident management, as well as lowering service

quality, time and operational costs across all infrastructure areas. Areas like waste management from the automation and optimization that Internet of Things can provide.

## **Chapter – 7 Manufacturing Network**

Manufacturing equipment management and management, asset management, and manufacturing process discovery or management are transforming the Internet of Things into a world of smart industrial and manufacturing applications. Intelligent IoT systems enable rapid dynamic response to the product demands, production of the new products, real-time optimization of the manufacturing and a supply chain networks through network of equipment, sensors and the control systems. Digital management systems for automating process management, the operator tools and the service information systems for enterprise security and security optimization belong to the IoT realm. However, it extends to asset management with the predictive maintenance, statistical evaluation, and measurements for maximum reliability. By integrating an intelligent manufacturing system with Smart Grid, you can make the most of energy in real time. Measurement, plant optimization, automatic control, safety management health and other functions are provided by many network sensors. In 2001, the National Science Foundation established an industry/university joint research center for Intelligent Service Systems (IMS) to monitor connected machines, predict performance degradation, and prevent potential interference using predictive analytics based on the Internet of Things. I did. The concept of achieving near-zero share rates through predictive analytics based on the Internet of Things has evolved further in the field of electronics manufacturing and maintenance. The term Industrial Internet of Things (IIoT) is commonly used in the manufacturing industry to refer to an industrial subset of Internet of the Things. Internet of the Things in manufacturing unit create much business value that will lead to Fifth Industrial Revolution, the so-called Industry 4.0. In the future, successful companies are expected to use the Internet of Things to increase revenue, create new business models, and increase productivity through analytics support to refresh and innovate their workforce. The growth potential of the IIoT implementation will generate \$12 trillion in global GDP by 2030, and data reception and collection is a must in IIoT. Of all the technologies, preventive maintenance would be an “easy” comparative advantage, as it applies to existing assets and management systems. Intelligent maintenance system aims to reduce unexpected downtime and increase productivity. To realize this, about 30% of the total maintenance cost is required. Industrial big data analysis is not the only possibility of industrial big data, but it will play an important role in keeping manufacturing assets predictable. Cyber

Physical Systems (CPS) is a leading industrial big data technology connecting humans and the cyber world. Cyber-physical systems can be designed according to the 5C architecture (connected, transformed, cyber, cognitive, configured), transform the collected information into useful information, and finally shut down the physical assets to optimize the process. A smart IoT-enabled system for these cases was demonstrated at the University of Cincinnati's NSF Industry and University Intellectual Service Systems (IMS) Joint Research Center on a tape seen at IMTS 2014 in Chicago. Bandwidth is not necessarily expensive, but because it wears out much faster, the bandwidth cost is enormous. But without sensors and intelligent analysis, you can only tell from your own experience when a bandwidth blade fails. The advanced forecasting system can identify and track the degradation of the flow band, even as conditions change, so the consumer knows in real time when it is best to replace the flow band. This greatly improves operator comfort and safety and reduces the cost of replacing seat belts before they actually break. Advanced analysis algorithms have been implemented on cloud servers and made available via internet and mobile devices.

10

## **Chapter – 8 Energy management**

Integrating an internet-connected detection and actuation system allows you to make the most of your energy overall. IoT devices are expected to be able to integrate into all types of energy efficient devices (switches, sockets, light bulbs, TVs, etc.) and communicate with power providers to efficiently balance power generation and energy consumption. These devices not only allow users to remotely or centrally control the device via a cloud interface, but also use advanced features such as scheduling (e.g. heating system on, off, cooker control, changing lighting conditions, etc.) In addition to managing energy use in the home, the Internet of Things provides a system that automatically collects and processes energy and energy supply information, providing a system that improves the efficiency, reliability, economics and sustainability of power generation and distribution. Is especially important. Using Advanced Metering Infrastructure (AMI) devices connected to the Internet backbone, the tool not only collects end-user connection data, but can also manage other distributed automation devices such as transformers and reclosers.

3

## **Chapter – 9 Medical and healthcare**

IoT devices are used for remote monitoring and alarm systems. The health devices range from heart blood pressure and rate monitors to modern devices have capability of the monitoring special implants such as heart control, electronic Fitbit wristbands or to advanced the hearing aids. Some hospitals

have started using smart beds that can detect when they are busy and when their patients need to wake up. It can also be adjusted to give the patient enough weight and support without a manual nurse. Residential areas may also have special sensors that monitor the health and well-being of the population, provide appropriate treatment, and help people recover from loss of mobility as a result of treatment. Other consumer health-promoting devices, such as connected scales or passive heart rate monitors, are also available through the Internet of Things. More and more IoT platforms for continuous health monitoring are suitable for obstetric and chronic patients, helping to manage critical health indicators and recurrent drug needs.

1

## **Chapter – 10 Building and home automation**

IoT devices is used in the building and home automation systems to monitor and to control the mechanical, the electrical and the electronic systems used in the various types of the buildings (e.g. the public and the private, the industrial, office or residential). In this context, the literature highlights three key areas for integrating the Internet with building energy management systems to create smart, energy-efficient buildings managed by IoT. Real-time monitoring tool to reduce energy consumption and track tenant behavior. How to integrate smart devices into the built environment and use them in future applications.

9

## **Chapter – 11 Transportation**

The Internet of Things can help unify communication, information processing, and processing in disparate transmission systems. The application of the Internet of Things covers all aspects of the transportation system (e.g. vehicles, infrastructure, drivers or users). Dynamic interaction between these components of the transportation system enables inter- and in-vehicle communication, intelligent traffic management, intelligent parking, electronic customs collection systems, logistics and fleet management, fleet management and traffic safety and support.

1

## **Chapter – 12 Metropolitan scale deployments**

There are many large-scale IoT operations designed or in progress to better manage cities and systems. Songdo, for example, is approaching as the first smart city in Korea with facilities and wired lines. Almost everything in this city is designed to be connected, connected, and transformed into a steady stream of data that is monitored and analyzed by many computers with little or no human intervention. Another application is an ongoing project in Santander, Spain. Two methods have been used for this purpose. With 180,000 people, the city has already downloaded 18,000 city apps for smartphones. The app connects to 10,000 sensors, including services like parking search,

environmental monitoring, digital city agenda, and more. This classification assists merchants using fire trucks in cities who want to maximize the effectiveness of any ad with contextual information about the city. Other examples of large sites include Guangzhou's Sino-Singapore Information City; San Jose, California is committed to improving air and water quality, reducing noise and improving transportation efficiency. Smart traffic management in western Singapore. French company Sigfox began building a very narrow wireless data network in the San Francisco Bay Area in 2014 and became the first company in the United States to protect these uses. It then announced that a total of 4,000 base stations would be installed for coverage. By the end of 2016, there will be 30 cities in United States, making them the largest IoT service provider in the United States today. Another widely used example is the deployment of New York Waterways in New York to connect all ships in New York and provide real-time, 24/7 monitoring. The network was designed and built by Fluid mesh Networks, a Chicago-based company that develops wireless networks for mission-critical applications. NYWW currently offers broadcasts on Hudson River, East River, and Upper Bay in New York City. The wireless network allows NY Waterway to monitor vehicles and passengers in ways that were not possible before. New apps may include security, energy and fleet management, digital signage, public Wi-Fi, paperless tickets, and more.

### **Chapter – 13 Consumer application**

More and more IoT devices are being deployed for consumers. Examples of consumer applications include connected cars, entertainment, smart home and home, laptops, self-quantification, allied health and smart retail. Internet of Things users open up new possibilities for user experiences and interfaces. Some consumer applications have been criticized for their lack of redundancy and inconsistency, which has led to a popular parody of the rough internet. Businesses have been criticized for making devices of vague value that use the Internet of Things quickly and do not introduce stringent security standards.

### **Chapter – 14 Unique addressability of things**

The original idea of the Auto-ID Center was based on unique identification using RFID tags and electronic product codes, but developed as objects with IP or URI addresses. An alternative view of the Semantic Web focuses on any operation (electronic, intelligent, or RFID enabled) that is referenced by an existing naming protocol such as a URI. The object itself does not interact, but can now be accessed by other agents, such as a powerful central server acting on behalf of the human owner. Integrating with the Internet means that the device uses its IP address as its unique identifier. Due to the limited IPv4 address space

(which enables 4.3 billion unique addresses), IoT devices have to scale to a very large address space using the Next Generation Internet Protocol (IPv6). IoT devices reduce the cost of configuring on the host and compressing the IETF 6LoWPAN header, so you can benefit from stateless autoconfiguration for addresses provided by IPv6. The future of the Internet of Things is almost impossible without IPv6 support. Therefore, the global rollout of IPv6 over the next few years is critical to the future success of IoT. A combination of these ideas can be found in the current GS1 / EPCglobal EPC Information Service (EPCIS) specification. The system is used to identify objects in a wide variety of industries, from space to consumer goods and transport logistics.

5

## Chapter – 15 Trends and characteristics

### . Intelligence

Peripheral information and autonomous control is not the part of original concept of the Internet of the Things. Peripheral intelligence and the autonomous control cannot could require the internet structure. However, research is moving toward integrating the concepts of IoT and autonomous governance, and the first result of this direction sees things as the driving force of autonomous IoT. In the future, Internet of Things will automatically configured or will have a non-deterministic open network that allows intelligent devices (SOA components), virtual object (avatar) to interact and operate independently (to continue to follow their goals). can be. General) depending on the situation, situation or situation. Changes in environment, defects affecting sensors, and the ability of objects to implement appropriate mitigation measures, along with the autonomous behavior of collecting and validating contextual information, are clearly an important research trend needed to ensure trust in IoT technologies. IoT products and solutions currently on the market use the variety of technologies to support context-sensitive automation, but using sensor blocks in real-world environments requires more sophisticated forms of information.

### building

This system is likely, an example of a bottom-up, event-driven architecture (based on real-time processes and context of operations) and takes into account all support tiers. As a result, the new model is complemented by a model and functional approach that can handle exceptions and develop abnormal processes (multi-agent systems, B-ADSC, etc.) In the Internet of Things, the meaning of event is not necessarily based on deterministic or syntactic model,

but based on context of event itself. It will also semantic web. As a result, it is not always necessary to have a common standard that cannot cover all situations or uses. Some participants (services, components, avatars) refer to themselves accordingly and, if necessary, adapt to current common standards (everything is to define "global finality" for everything that is impossible with top-down and standardization methods). Internet Network (IoT) is an IoT application storage architecture that takes into account the convergence of data from IoT devices to web applications to create innovative use cases. For programming and information flow in the Internet of Things, the predictable architectural reference is called BPM Everywhere, which combines traditional process management with intelligent process analysis and availability to automate the management of many interconnected devices.

#### Network architecture

Internet of Things requires tremendous scalability in network space to cope with the increasing number of devices. IETF 6LoWPAN is used to connect the device to the IP network. As billions of devices are added to the Internet, IPv6 will play an important role in the scalability of network storage. IETF, ZeroMQ and MQTT Limited Application Protocol provide easy data transfer. "MQ" becomes "MQTT" in the IBM MQ Series Message Queue product line. Fog computing is a viable alternative that prevents a significant increase in data traffic over the Internet. Data can be analyzed and processed using the computing power of the Edge device, providing easy real-time scalability.

#### complexity

In a semi-open or closed loop (i.e., a value chain that can solve global finality), IoT is often considered and studied as a complex system due to its diverse connections, autonomous participant interactions, and the ability to integrate new actors. . In a typical (fully open loop) view this is likely to be considered a confusing environment (since the system is always complete). In fact, not all parts of the Internet of Things work in a global common space. Subsystems are often implemented to minimize the risk to integrity, control and reliability. For example, home robotics (Domotics) working in a smart home can only exchange data and use it.

#### Size considerations

The Internet of Things can be encode 100 to 105 trillion objects and track their movement. Each individual in the urban environment surveyed is surrounded by 1,000 to 5,000 monitored objects.

#### Location considerations

In Internet of Things, the exact geographic location of an object and the exact geographic size of an object are important. As a result, facts about the object, such as location in space and time, are less important to tracking because person processing information can determine whether that information is important to the action taken, and if, can add the missing information. I did. (Or decide not to take any action). (Part of Internet Of Things will be sensors, and sensor space is generally important. GeoWeb and Digital Earth is promising applications that will become when things can sorted and connected by location. Space constraints of various sizes are included., The Things on the Internet have to deal with large amounts of data and indexing for fast search and contiguous operations in the Internet, if the object is isolated and able to function, then this intermediary role is human. Accept it because this information must have a pivotal role. Just as standards play an important role in the Internet and online, geospatial standards will play an important role in the Internet of Things.

### **. Sectors**

There are 3 core sectors in IoT: government, enterprise and home, with the Enterprise Internet of Things being largest of 3. By 2020, the EIoT sector was estimated to account for nearly 40% or 9.1 billion devices..

### **A Solution to "basket of remotes"**

A Solution to "basket of remotes" According to the CEO of Cisco, commercial opportunity for "connected products ranging from cars to household goods" is expected to be \$USD 19 trillion. Many IoT devices have 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 hundred of the applications to interface with hundred of the devices that don't share protocols for speaking with one another. There are multiple approaches to solve problem, one of them called predictive interaction, where cloud based decision makers will predict user's next action and trigger some of the reaction. For user interaction, new technology leader were joining forces to create standard for communication among devices. While All Joyn alliance is composed of top 15 World technology leaders, there were also big companies that can promote their own protocol like CCF from the Intel Company. Manufacturers are becoming conscious of the problem, and many companies have begun releasing the devices APIs. Many of these APIs used by small companies looking to take advantage of the quick integration.

### **Frameworks**

IoT frameworks help support interaction between things and allow for more complex structures like distributed computing and development of distributed applications. Currently, some IoT frameworks seems to focus on real-time data logging solution, offering some basis to work with many "things" and having interact.

Future developments might lead to specific software-development environments to create software to do work with hardware used Internet of things. Companies developing technology platform to provide type of functionality of Internet of things. Newer platforms are being developed, which add more intelligence. REST scalable architecture that allow things to do communicate over Hypertext Transfer Protocol easily adopted for the IoT applications to communication from things to central web server. MQTT is published subscribe architecture top of IP that allows bidirectional communication between thing and an MQTT broker.

### **Enabling technologies for IoT**

There are technologies that can enable IoT. Crucial to field is network used to communicate among devices of IoT installation, role that several wireless technologies may fulfil: **Short-range wireless**

- Bluetooth low energy – Specification providing low power to classic Bluetooth with a comparable communication range.
- Light-Fidelity – Wireless technology similar to Wi-Fi standard, but visible light of communication of increase bandwidth.
- Near-field communication – Communication protocol enables two electronic devices to communicate within 4 cm range.
- QR and barcodes – Machine-readable tags store information about item to which they attached.
- RFID – Technology uses electromagnetic field to read the data stores in tag embedded on other items.
- Thread In – Network Protocol bases on IEEE 802.15.4 standards, similar to Zigbee, providing the IPv6 addressing.
- Network protocol (TLS) – Network security protocol.
- Wi-Fi – Widely uses technology of local area networkings based on IEEE 802.11 standards, where devices can communicate through shared access point.
- Wi-Fi Direct – Variants of Wi-Fi standard for the peer-to-peer communication, eliminate need for access point.

- Z-Wave – Communication protocols provides short-range, low-latency data transfers at the rates and power consumptions lesser than Wi-Fi. Uses primarily for the home automation.
- Zigbee – Communication protocol for the personal area network based on IEEE 802.15.4 standards, provides low power consumptions, low data rates, lower costs, and higher throughput.

#### **Medium-range wireless**

- Ha Low – Variant of Wi-Fi standards provides extend range of low-power communication at lower data rates.
- LTE-Advanced – High speed communication specifications for the mobile network. Provide enhancement to LTE standard with the extended coverages, high throughput, and low latency.

#### **Long-range wireless**

- Low-Power Wide-Area Networking – Wireless network designed to the allow long range communications at the lower data rates, reducing the power and the cost for the transmission.
- VSAT – Satellite Communication Technology uses small dish antennas for narrower band and broader band data.

#### **Wired**

- Ethernet – General networking standards uses twisted pair and the fiber optic links in the conjunction with the hubs or the switches.
- Multimedia over Coax Alliance – Specification enables whole home distribution of the high definition videos and the content over existing coaxial cablings.
- Power-line communication – Communication technologies uses electrical wires to carry the power and the data. Specifications such as Home Plug utilizes PLC for the networking IoT device.

#### **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 can be implemented to produce update on status and health of asset, based on sensor reading integrated with the computational model of asset.

#### **Politics and civic engagement**

Some of the scholars and activists argue that IoT can uses to create new models of the civic engagement if the device networks can open to the user control and the interoperable platform. A professor and the author, writes that

the political lives in both the democracies and the authoritarian regime will be shaped way the IoT will uses for the civic engagement. For that, he argues that any connected devices should able to give list of ultimate beneficiaries of its sensors data and that the individual citizen should able to be add new organizations to beneficiary list. She argues that civil society group need to start the developing their IoT strategies for making the uses of data and engages with the public.

### **Government regulation on IoT**

One of key drivers of IoT is data. Companies which are working on IoT collects data from the multiple sources and stores it in cloud network for the further processing. This leaves door widely open for the privacy and security dangers and vulnerability of the multiple systems. Other issues pertain to the consumer choice and ownership of the data and used. Presently the regulator has shown more interest on protecting first 3 issues identified above. Current regulatory environment: Reports published by FTC in the January 2015 made following three recommendations:

- Data security – At time of designing IoT companies should ensure that data collections, storages and processing would be secures at all times. Companies should adopt defence in depth approach and encrypts data at the each stages.
- Data consent – Users should have choice as to data they will share with IoT companies and user must be informed if their data exposed.

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

However, FTC stopped at making recommendation for now. According to FTC analysis, existing framework, consists of FTC Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act, along with the developing consumers education and the business guidance and advocacy to other agencies at the federal, the state and the local level, sufficient to protect the consumer rights.

A resolution passes by Senate in March 2016, already being considered by Congress. This resolution recognized need for formulating the National Policy on IOT and matter of the privacy, the security and the spectrum. To provide impetus to IoT ecosystem, in March 2018, bipartisan group of the four Senators proposes a bill, Developing the Innovation and Growing Internet of Things Act, to direct Federal Communications Commission to assesses need for more spectrum to the connect to IoT devices

Several standard for IoT industry actually being established relating to automobiles because most concerns from the use of connected car apply to healthcare devices. In fact, National Highway Traffic Safety Administration was preparing cyber security guidelines and database of practice to make automotive computer systems secure.

## **Chapter – 16 Criticism and controversies**

### **Platform fragmentation**

IoT suffers from platform fragmentation and the lack of the technical standard a situation where variety of the IoT devices, in terms of the both hardware variations and differences in software, makes task of developing applications that works consistently between the different inconsistent technology ecosystem hard. Customers can be hesitant to bet the IoT future on proprietary software or hardware devices that can uses the proprietary protocols that can fade or becomes difficult to be customize and to interconnect. IoT's computing nature is a problem for the security, since patches to bugs found in core operating system often do not reach user of older and lower the price devices. Researchers say that failure of the vendors to support the older devices with the patches and the updates leaves more than 85% of the active device vulnerable.

### **Privacy, autonomy, and control**

The author, writes that Internet of things offer immense potential for the empowering citizens, making the government transparent, and broadening the information access. However, that privacy threats were enormous, as potential for the social control and the political manipulation. Concerns about the privacy have led many to consider possibility that the big data infrastructure such as Internet of things and the Data Mining were inherently incompatible with the privacy. Wright claims that technologies are not only an invasion of the public space but are also used to perpetuate behaviour, citing an instance of the billboards with the hidden cameras that are tracked the demographics of passers-by who stopped to read advertisement. The Internet of Things Council compared increased prevalence of digital surveillance due to Internet of things to conceptual described by Bentham in the 19th Century. The assertion is defended by works of the French philosophers Michel and Gilles. In *Discipline and Punishes: The Birth of Prison* Foucault asserts that panopticon was the central element of the discipline society of developed during Industrial Era. Foucault argued that discipline systems established in the factories and the school reflected Bentham's vision of the panopticism. In the 1994 paper *Postscripts on Societies of Control*, wrote that discipline society had transitioned

into control society, with computer replacing panopticon as an instrument of the discipline and the control while still maintaining qualities similar to that of panopticism.

The privacy of the household could be compromised by analyzing the smart home network traffic pattern without dissecting contents of encrypted application data, yet a synthetic packet injection schemes can used to safely overcome such invasion of the privacy. Peter-Paul, professor of the philosophy of technology at University of Madras, India, writes that the technology already influences moral decision making, which in turn affects the human agency, the privacy and the autonomy. He cautions against viewing the technology merely as human advocates instead to consider it as active agent. Justin, of Center for the Democracy and the Technology, expressed concern regarding impact of the IoT on consumer privacy, saying that there are some people in commercial space who say, Big data — collects everything, keep it around forever, we will pay for the somebody to think about security later. The question is whether we want to have some sort of the policy framework in place to limit that. Reilly believes that way companies sell IoT devices on the consumers are misplaced, disputing notion that IoT is about the gaining efficiency from putting the all kinds of the devices online and postulating that IoT is really about the human augmentation. The application is profoundly different when you have the sensors and the data driving the decision-making. Editorials at the WIRED have also expressed the concern, one stating. Actually, it's worse than that. You aren't just going to lose the your privacy, you're going to have to watch very concept of privacy should be rewritten under your nose. The American Civil Liberties Union (ACLU) expressed the concern regarding ability of IoT to 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 2010 the British Government stated that it would follow formal Privacy by Design principles when the implementing their smart metering program. The program would lead to the replacement of the traditional power meters with smart the power meters, which could be track and manage the energy usage more accurately. However American Computer Society is very doubtful these principles were actually implemented. In 2015, the Parliament rejected a similar smart metering program, basing their decision on the privacy concerns. The Dutch program has later revised and passed in 2016.

## **Chapter – 17 Data storage and analytics**

A challenge to producers of the IoT applications to clean, process and to interpret vast amount of the data which gathered by sensors.

There is solution to proposed for analytics of information referred to Wireless Sensor Networks. Networks share data among the sensor nodes that send to the distributed system for analytics of sensory data. Challenge is storage of data. Depending on application there would high data requirements which in turn lead to high storage requirements. Currently internet responsible for 12% of generated and this consumption will increase significantly when we start utilizing applications with multiple embedded sensors.

## **Chapter – 18 Security:**

Concerns have been raised that Internet of things being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. Most of technical security issues similar to the those of smartphones, conventional servers, workstations but firewall, security update used for those generally unsuitable for much IoT devices. According to Business Insider Intelligence Survey conducted in last quarter of 2018, that the security is biggest concern in adopting to Internet of things technology.

In particular, as Internet of things widely, cyber-attacks are likely to become increasingly physical threat. In January 2018, article in Forbes, cyber-security listed many Internet-connected appliances that can already including appliances, cameras, televisions, kitchen and thermostats. Computer-controlled devices in automobiles such as engine, locks, hood brakes and dashboard have been shown to vulnerable to the attackers who have access on-board network.

Vehicle computer systems were Internet-connected, allowing them to exploited remotely. By 2004 security researchers had shown ability to control pacemakers without the authority. Hackers demonstrated control of pumps and implantable defibrillators. He wrote that recently about hackers controlling the certain functions of automobile were not one might guess because of various circumstances; such as bug that allowed hack having fixed before report published, or that hack required the security researchers having physical access to car prior to hack to the prepare for it. The U.S.

National Intelligence Council in unclassified report maintains that it could be hard to deny access to the networks of sensor and controlled objects by the enemies of America, criminals, and mischief makers... An open market for the aggregated sensor data could serve interests of the commerce and the security it

helps the criminals and spies identify targets. Thus, parallel sensor fusion social cohesion, it proves to be fundamentally incompatible with the guarantees against unreasonable search.

In general, intelligence community views Internet of things as rich source of the data. As response to the increasing concerns over security, Internet of Things Security Foundation is launched on 24 September 2016. IoT SF has the mission to secure Internet of things by promoting the knowledge and the best practice. Its founding board made from telecommunications companies including Vodafone, Imagination Technologies and Pen Test. Large IT companies were continuously developing the innovative solutions to ensure the security for IoT devices. As per estimates from Research, overall IoT security market grow at 28.9% rate 2016-2022 as result of growing the infrastructural concerns, diversified usage of the Internet of things.

In 2016, distributed denial service attack powered by the Internet of things devices running Mirai malware took down DNS provides major web sites.

## **Chapter – 19 Design**

Given widespread recognition of evolving nature design and secure management of Internet of things, sustainable deployment of IoT solutions must design for scalability. Application of concept of the scalability can be extended to the physical systems by the virtue of those systems being designed to the account for uncertain management futures. This scalability thus provides pathway forward to the fully realize potential for Internet of things solutions by the selectively constraining physical systems to allow for all the management regimes without put risking the physical failure. Yellow University computer mechanic Johnson has argued that the successful execution of Internet of things requires the consideration of interface's usability as well as technology itself. These interfaces need to be not only more user-friendly but also the better integrated: If users need to learn different interfaces for their locks, their lights, their sprinklers, their vacuums, and their coffeemakers, it's tough to say that lives have been made any easier.

5

## **Chapter – 20 Environmental sustainability impact:**

A concern regarding Internet of things technologies pertains to environmental impacts of eventual disposal, manufacture and use of all these semiconductor-rich devices. Modern electronics were replete with the wide variety of the heavy metals and the rare-earth metals along with the highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components were often placed or incinerated in regular landfills. The human and the environmental cost of the mining of rare-earth metals that are the integral to the modern electronic components to grow. With production of

the electronic equipment growing globally yet to little of metals (from the end-of-life of equipment) were being recovered for the reuse, environmental impacts can be expected to be increase. Also, because concept of the Internet of things adding electronics to devices (for example, light switches), and because of the major driver for the replacement of electronic components often technological to obsolescence rather than the actual failure to function, it is one of the reason to expect that items that previously are kept in the service for many decades would see an accelerated replacement cycle if they are part of IoT. For example, traditional house built with 30 light switches and 40 electrical outlets might stand for 60 years, with all those components still original at end of period. But modern house built with same number of the switches and the outlets set up for IOT might see switch and outlet replaced at the five-year intervals, in order to keep up to date with technological changes. This translates to into ten-fold increase in waste of requiring disposal.

## **Chapter – 21 Intentional obsolescence of devices:**

Electronic Frontier Foundation raised concerns that companies can use technologies necessary to support connected devices to intentionally disable or their customer devices via remote software update or by disabling a service necessary to operate the device. In one example, home automation devices sold with promise of Lifetime Subscription were rendered useless after the Nest Labs acquired to Revolve and made decision to shut down central servers to Revolve devices had used to operate. As Nest company owned by Alphabet, EFF argues this sets terrible precedent for the company with low ambitions to sell self-driving cars, medical devices, and high-end gadgets that may be essential to the person's livelihood or physical safety. Owners should free to point the devices to the different server or to collaborate on to improved software. But such action violates United Kingdom DMCA section 1204, which only has exemption for outer use. This forces the tinkerers who want to keep using own equipment into the legal grey area. EFF thinks holders must refuse electronics and the software that prioritize manufacturer's wish above their own. Examples of the post sale manipulation include, Microsoft Nest Revolve, disabled the privacy settings on I phone, Sony disabling Linux on the PlayStation 4, and enforced EULA on U.

### **Confusing terminology:**

Kevin at Information Age, business technology magazine, has referred to terms surrounding IoT as terminology zoo. The lack of clear terminology is not useful from practical point of view and source of the confusion for end user. A company operating in IoT space could be the working in the anything related to the networking, embedded systems, sensor technology, or analytics. According

to Reddy, the term IoT is coined before the smart phones, the tablets, and the devices as we know that today existed, and there is the long list of terms with the varying degrees to overlap and the technological convergence: Wireless Sensor Networks (WSN), Smart Objects, Cooperating Objects, Machine-to-Machine (M2M), Ambient Intelligence (Aml), Operational Technology (OT), and Information Technology (IT) Internet of Things (IoT), Internet of Everything (IoE), Industrial Internet, Pervasive Computing, Pervasive Sensing, Wireless Sensor Networks (WSN), Smart Objects, Cooperating Objects, Machine-to-Machine (M2M), Ambient Intelligence (Aml), Operational Technology (OT), and Information Technology (IT). Regarding IIoT, industrial sub-field of the IoT, Industrial Internet Consortium Task Group has created common and to reusable vocabulary of terms to ensure consistent terminology across the publications issued by Industrial Internet Consortium. IoT has created IoT Terms Database including New Term Alert to be notified when new term published. As of March 2018, this database aggregates 711 IoT-related terms, however, without any attempts to the reduce terminological ambiguity and the complexity.

1

## **Chapter – 22 IoT adoption barriers**

### **Complexity and unclear value propositions:**

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

### **Privacy and security concerns:**

According to the recent study by Papadia and Karen at the University of Italy, the Internet of Things potential for the major privacy invasion is a concern with much of research disproportionately focused on to security concerns of the IoT. Among proposed solutions in terms of techniques some of them deployed and extent to which they were satisfied to core privacy principles, only very few turned out to be fully satisfactory. Louis Philip, investment director at Up 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.

6

## **Chapter – 23** EMBEDDED SYSTEMS

### **1.1.1 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

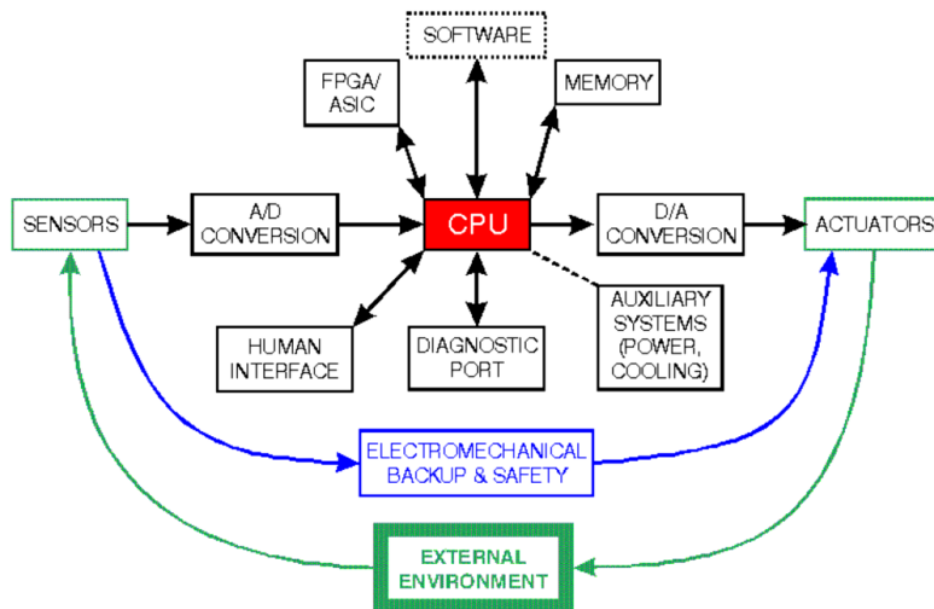
e.g.: CD player, VCR, microwave oven

Control Systems

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

#### 1.1.2 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



### NodeMCU with Arduino IDE

This is another way to develop NodeMCU using a well-known IDE i.e. Arduino IDE. You can also use the Arduino development environment to develop NodeMCU applications. This makes it easier for Arduino developers to learn new languages and IDEs for NodeMCU.

For more information on how to create an Arduino sketch for a NodeMCU, see [Getting Started with NodeMCU with Arduino IDE](#).

### Difference between using ESPlorer and Arduino IDE

Well, there is a difference in the programming languages you will see when developing applications for NodeMCUs using the ESPlorer IDE and Arduino IDE.

If you are developing a NodeMCU application using the Arduino IDE, you need to encode the C/C++ programming language, and if you are using the ESPlorer IDP, you need to encode the Lua language.

NodeMCU is basically a Lua interpreter, so you can easily understand Lua scripts. When I write a Lua script for NodeMCU and send/upload it to NodeMCU, it runs continuously. The code that writes the NodeMCU does not generate firmware binaries. Like NodeMCU, it sends a Lua script for execution.

When writing and compiling code in the Arduino IDE, the ESP8266 toolbox generates firmware binaries in the background with the code you write. And when loaded into the NodeMCU, it flashes the entire NodeMCU firmware with the newly created firmware binary. It actually writes the complete firmware.

For this reason, NodeMCU does not accept any additional Lua script/code after flashing the Arduino ID. After flashing the Arduino sketch/code, the Lua interpreter no longer exists and an error occurred when I tried to load the Lua script. To start the Lua script you need to flash it with the NodeMCU firmware.

The Arduino IDE takes longer than the ESPlorer IDE because it compiles and dumps/writes the complete firmware.

## Library YTOR

Piezoelectric sensors are used to measure swing, touch, vibration and shock. The basic principle that risks oversimplification is that the structure accelerates as it moves. Piezoelectric shock sensors can in turn generate charge when they are physically accelerated. This combination of functions is used to change the response or reduce noise and vibration.

Why is it important? Because vibration and shock can shorten the life of all electronic and electromechanical systems. Thin wires and connecting wires can be emphasized, especially after prolonged exposure to vibration. Loose solder

joints and grooves on the circuit board can be caused by shock and reckless shocks, which can lead to complex types of system failure. I like it intermittently.

This article describes piezoelectric shock and vibration sensors and sensor technology focused on the available products (all details mentioned here can be found on the Digi-Key website-link provided), design considerations and design methods. Do it.

#### How it Works :

The piezoelectric effect was discovered by Pierre and Jacques Curie in the late 19th century. They discovered that minerals such as tourmaline and quartz can convert mechanical energy into electrical energy. The pressure induced voltage (Piezo Greek) is proportional to the applied pressure and piezoelectric devices can be used to detect single and repetitive pressure events.

However, the ability of some crystals to exhibit charge under mechanical stress was not possible until engineers were able to develop the signals generated by these crystals using very high input impedance amplifiers.

Several materials can be used to make piezoelectric sensors, including tourmaline, gallium phosphate, salt, and quartz. Quartz is used in most electronic applications as its growth technology is highly advanced due to the development of piezoelectric power inverters. Crystal oscillator.

Piezoelectric sensors can act on transient, longitudinal or transverse forces and are not sensitive to electric fields and electromagnetic radiation. The response is very linear over a wide temperature range, making it an ideal sensor for harsh environments. For example, gallium phosphate and tourmaline sensors can operate at temperatures up to 1000 ° C.

The physical design of a piezoelectric sensor depends on the type of sensor you are building. For example, a pressure sensor or shock sensor (pulse) configuration can arrange a small but well-known crystal mass in a temporary configuration with load strain along the longest path to a larger base (Figure 1). This way, the applied pressure will load the base in only one direction.

Figure 1: Finite mass can deform the crystal detector along a single axis. This configuration is suitable for power and pressure.

Accelerometers based on the piezoelectric effect use a known mass to deform the sensitive part of the crystal in a positive or negative direction depending on the excitation force (Fig. 2). The sensor board module requires a known elasticity..

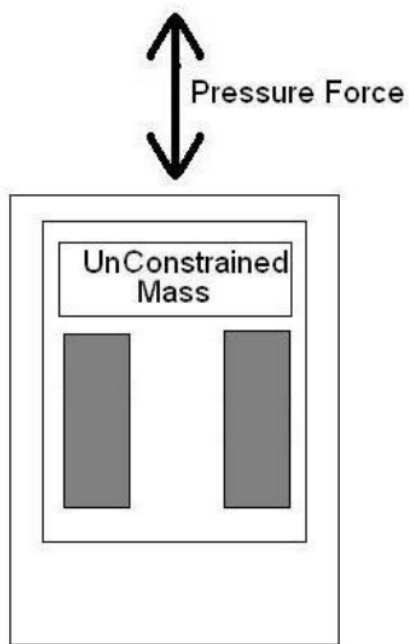


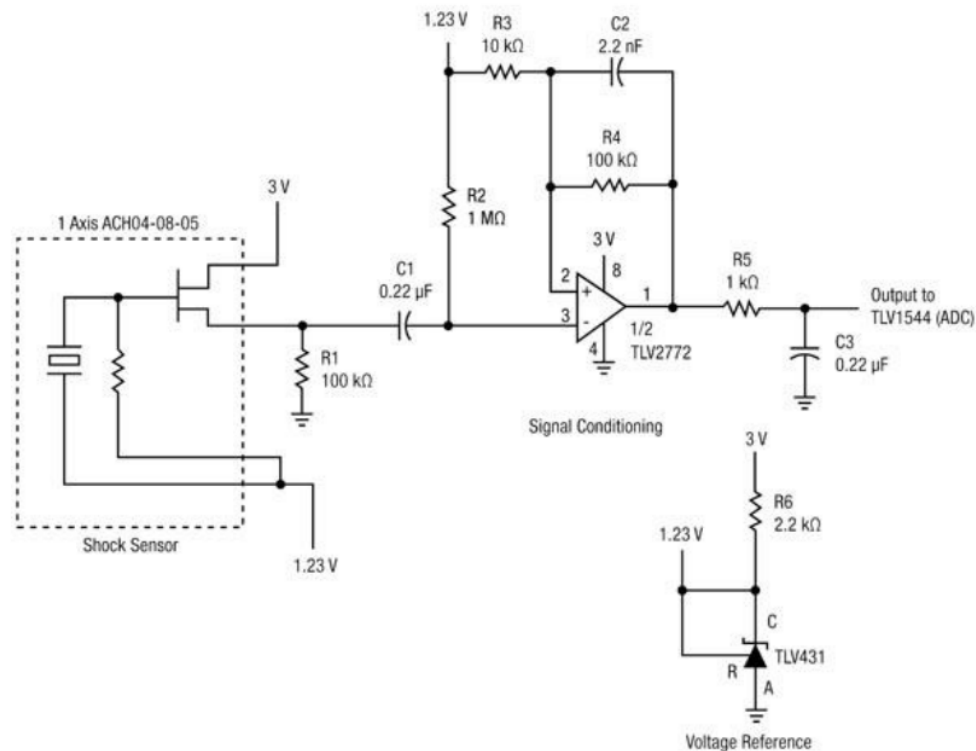
Figure 2: When the modulus of elasticity of the substrate material is known, the free mass can move with vibration, so this type of piezoelectric sensor is ideal for shock absorption and vibration detection.

#### Design using piezoelectric sensors

Piezoelectric sensors require some precautions when connecting to sensitive electronic components. First of all, the voltage level created by a strong shock can be very high, up to about 100V.

Operational amplifiers are used to connect these sensors to analog-to-digital, discrete or microcontroller converters. One tip is to choose an amplifier with a high input impedance to reduce current flow. One possible candidate is a JFET dual line input amplifier. The input impedance is  $10^2 \Omega$  and the gain is 1 MHz, making it easy to handle the vibration range of piezoelectric sensors.

Another suitable part is Texas Instruments' TLV2771. This low power power supply amplifier has a  $10\ \text{ohm}^2$  differential input impedance and a unity gain band range of 5 MHz. The shock sensor input can be connected directly to the analog-to-digital converter with one-step signal processing.



Operational amplifiers such as the TI TLV2772 have a high input impedance to reduce the current from the high voltage input to the piezoelectric sensor.

Operational amplifier circuits can be designed to operate in either voltage or charging mode. The charging mode is used when the amplifier is off at the sensor. Voltage mode is used when the amplifier is very close to the sensor.

Another suggestion is to dilute the input signal and use the op amp's amplifier to get the desired range. Weak protection may be required at the amplifier input, especially if the structure is susceptible to harsh influences.

You might think that the pressure sensor only produces a positive voltage, but it can actually cause a signal from the transformer to ring and cause a negative voltage spike (Figure 4). This means that you may need to stop the negative voltage level at the input of the amplifier, especially if the amplifier uses only one power supply.

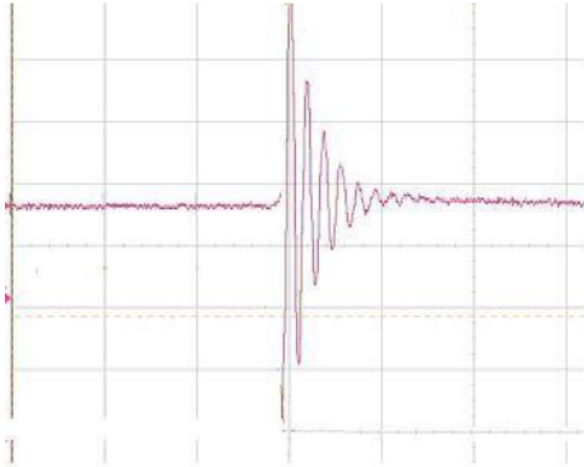


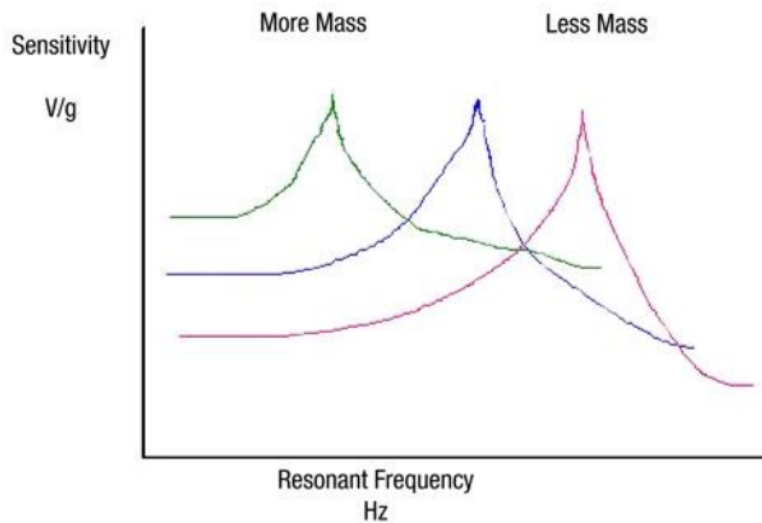
FIG. 4. When using an operational amplifier, be careful as the shock will generate negative voltage and damage it if you do not stop the working amplifier input.

#### Design details

You can use many piezoelectric sensors for your project. For example, the Parallax 605-00004 is a piezoelectric vibration sensor that can act as a switch or vibration detector (Figure 5). The plastic film laminate uses a corrugated connection and has a sensitivity of 50 mV/g.

*Figure 5: The flexible through-hole LDTO polymer film piezoelectric sensors can be hard mounted or free floating to detect strain, shock, or vibration.*

You should be aware that adding mass to a piezoelectric sensor can change its resonant frequency as well as change its baseline sensitivity. Many piezoelectric sensors like the 605-00004 are characterized to be used this way and provide supporting tables and graphs.



*Figure 6: Loading a sensor with mass changes its resonant frequency and sensitivity in a predictable and repeatable way.*

Another detail to consider is the cantilever film sensor 0-1002794-0 cantilever. It is also a vibrating tongue transmitter that can be rigidly mounted to a surface, floated on an axis of inertia, or preloaded with displacement and compensation. Output voltage fluctuations can directly disable the FET or CMOS input and shift the center of mass to achieve a multiaxial response.

Other options:

In addition to detecting vibrations and shocks, piezoelectric devices can also be used to extract energy from the environment. For example, consider the MideV22BL, a hermetically sealed piezoelectric sensor that can raise vibrations from 26 Hz to 100 Hz.

This can be seen by using the company's VR001 data logger, a battery-powered portable data logger capable of measuring acceleration and vibration in three axes (Figure 7). It can be configured as a USB peripheral and transferred to another computer or USB host device. It can also be used to design your own patterns based on the piezoelectric sensor of your choice. Mide tutorials are available on the Digi-Key website and help you quickly learn new designs.



*FIG. 7. The 3-axis USB sensor can be used as a design and evaluation tool when researching or launching a new design.*

*Finally, before choosing a piezoelectric sensor for shock or vibration, evaluate the criteria specific to the proposed application (we have given some examples here), look at the manufacturer's datasheet and see the link above for more details. . Information found on the Products and Technologies page of the Digi-Key website.*

#### *Gas detector module*

*In the current process scenario, it is very important to monitor the gases produced. From household appliances such as air conditioners to electrical*

*chimneys and security systems in industrial plants, gas monitoring is critical. Gas detectors are a very important part of these systems. A gas sensor, as small as a nose, reacts spontaneously to the gas present and informs the system of any changes that occur in the molecular concentration of the gaseous state.*

<sup>18</sup> Gas detectors come <sup>17</sup> in a variety of specifications depending on the level of sensitivity, the type of gas being measured, physical dimensions, and many other factors. This overview includes a methane gas detector that can detect gases such as ammonia that may be formed by methane. When a gas interacts with this sensor, it is first ionized into a compound and adsorbed by the sensing element. This adsorption creates a potential difference across the cell and is transferred as current to the processor unit through the output contact. What is this sensitive factor? What kind of chamber is it stored in or is it open? How does it enter the river and how is it excreted? Let's find out in this review!!!

The gas detector module contains a steel exoskeleton with a sensing element installed. This sensor is powered via a connecting cable. It is called the heat flow through this current and the gas that approaches the sensing element is ionized and absorbed by the sensing element. This changes the current value by changing the resistance of the sensing element.

The figure shows the appearance of a standard gas detector module: steel mesh, copper rings and connecting wires. The top is a stainless steel net that provides:

It filters suspended particles so that only gaseous components can pass through the detector.

☐ Protect the inside of the sensor.

Explosion-proof function that keeps the sensor module intact at high gas temperature and pressure.

To effectively control the above functions, the steel mesh consists of two layers. The net is attached to the rest of the case with a copper plated clamp ring.

Because the sensor connection wire is thick, you can safely connect the sensor to the circuit and transfer enough heat inside. They are cast in copper and tin. Four of the six pins (A, B, C, D) are for sampling the signal and two (1, 2) are used to ensure that the sensing element is properly heated.

The pins are good insulators and are placed on a bakelite base to hold the sensor pins securely.

The upper part of the gas sensor is expected to reveal the inside of the sensor, i.e. the interconnected sensing elements and wires. The hexapod structure consists of a sensing element and six connecting legs that extend beyond the bakelite base.

The use of ceramic substrates increases heating efficiency, and tin oxide is a sensitive coating, which is sensitive to the adsorption of the desired gaseous components (methane and its products in this case).

The wires that serve to heat the sensing element are connected through a well-known conductive alloy, nickel chromium. The conductor responsible for the output signal is connected by a platinum cable that transmits a small change in current through the sensing element. The platinum wire is connected to the body of the sensing element, and the nickel chromium wire is passed through the hollow structure.

A chromium nickel wire is placed inside the element in the form of a spring while another wire is attached to the outer casing of the element. The figure shows a piece of wire coated on a hollow ceramic.

The picture shows a ceramic with a tin on top of a highly adsorbent ceramic. Each control gas has a specific temperature at which it is ionized. The function of the detector is to operate at a specific temperature so that the gas molecules are ionized. The ceramic area of the sensing element is exposed to thermal current through a nickel chromium wire. Heat is released by nearby elements that interact with the gas and become ionized. After ionization, it is absorbed by tin dioxide. Adsorbed molecules change the resistance of the tin dioxide layer. This changes the current flowing through the sensing element and passes through the output to the device that controls the operation of the gas detector.

Zigbee communication:

Zigbee is a wireless technology developed as an open standard to meet the unique needs of low-power IoT wireless networks. The Zigbee standard operates according to the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification that powers the Zigbee stack was approved by the Institute of Electrical and Electronics Engineers (IEEE) in 2003, a package-based wireless protocol designed for low-cost, battery-powered devices. This protocol allows devices to communicate on a variety of network topologies and can operate on battery power for up to several years.

### Zigbee Protocol 3.0

The Zigbee protocol was created and ratified by member companies of the Zigbee Alliance. More than 300 leading semiconductor manufacturers, technology companies, OEMs and service companies are members of the Zigbee Alliance. The Zigbee protocol is designed to provide an easy-to-use wireless communication solution featuring a secure and reliable wireless network architecture.

#### ZIGBEE benefits

Zigbee 3.0 is designed to transmit data in noisy RF environments commonly used in commercial and industrial applications. Version 3.0 is currently based on the ZigBee standard, but it merges application profiles for specific markets, allowing all devices to connect wirelessly to the same network, regardless of their purpose and function in the market. In addition, the ZigBee 3.0 certification system ensures interoperability between products from different manufacturers. Connecting to the ZigBee 3.0 network with an IP domain opens access to monitoring and control from devices such as smartphones and tablets on a local or global network, including the Internet, and realizes a true Internet of Things.

Zigbee protocol functions are as follows.

- Point-to-point multi-network topology support, Multi branch and network network
- Low-load bikes-provide long battery life.
- Low delay
- DSSS (Direct Sequencing Spread Spectrum)
- Up to 65,000 nodes in the network
- 128-bit AES encryption for secure data connection
- Conflict, recurrence and confirmation prevention

The Zigbee 3.0 software stack contains a "core device" that provides consistent behavior when bringing a host to the network. A standard set of commissioning tools are available, including Touchlink, a non-contact commissioning method.

Zigbee 3.0 provides better network security. There are two security mechanisms that create two types of networks.

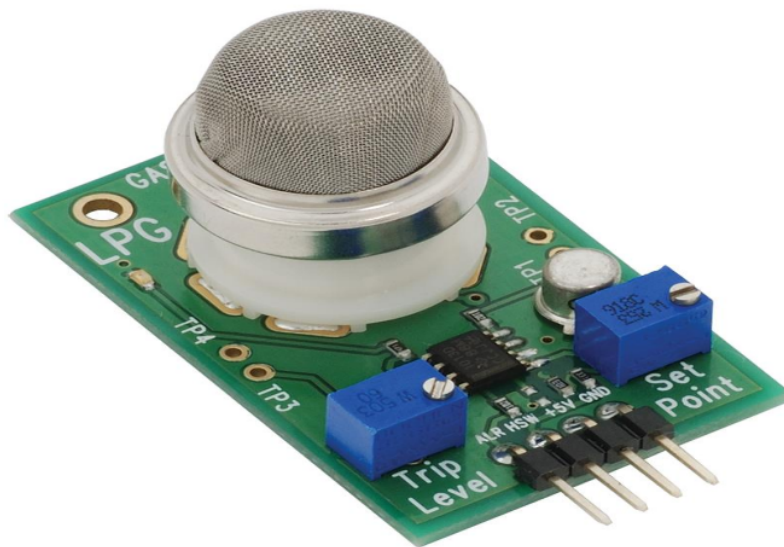
- Centralized Security: This method uses a coordinator/trust center to configure the network, manage network deployment, and attach security keys to connecting nodes.

- Deployment Security: This method does not have a coordinator/trust center and is created by the router. Each node of the Zigbee router can provide the network key for the connecting node.

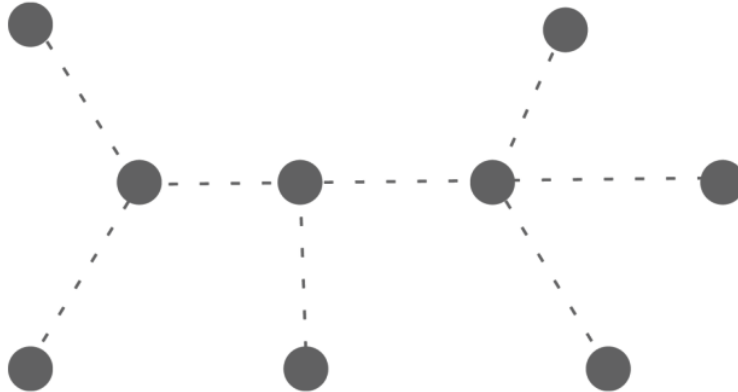
Nodes use the same security methods used in the networks to which they are connected. Zigbee 3.0 supports the increasing range and complexity of wireless networks and handles large LANs with more than 250 nodes. Zigbee also handles the dynamic behavior of these networks (if a node appears, disappears and reappears on the network) and allows one parent to be lost, allowing orphaned nodes to rejoin the network through another parent. The self-healing nature of the Zigbee Mesh network allows nodes to be separated from the network without interfering with the internal routing.

Compatibility according to Zigbee 3.0 means that applications already developed in the Zigbee Light Link 1.0 or Home Automation 1.2 profile are ready for Zigbee 3.0. The Smart Energy profile also meets Zigbee 3.0 in terms of functionality, but Smart Energy has additional security requirements that apply only to the profile.

Zigbee Over-the-Air (OTA) for software updates while the device is running makes it easy to move applications from devices already in use in the field to Zigbee 3.0. OTA update is an optional feature recommended by the manufacturer to be supported by Zigbee products.



### Mesh Networks



An important component of the Zigbee protocol is network support. In a network, nodes are connected to other nodes, so each node is connected in several ways. Node-to-node connections are dynamically updated and optimized using sophisticated embedded network tables.

Worm networks are inherently inherited. Each node can be located independently of the network. In addition, when a node leaves the network, the mesh topology allows the node to construct a routing path based on the new network structure. Custom network and routing topology capabilities provide greater reliability when conditions change or individual node failures occur.

### Zigbee application

Zigbee is a low-cost, low-cost solution that enables a wide range of wireless deployments. Offers years of low battery operation for a variety of monitoring and control applications. Smart Energy/Smart Grid, AMR (Automated Meter Reading), lighting control, building automation systems, tank monitoring, HVAC management, medical devices and vehicle applications are just a few of the many areas where Zigbee's technology is making great strides.

### Zigbee Digi XBee3 technology

Digi is a member of the Zigbee Alliance and has developed a wide range of network solutions based on the Zigbee protocol. Digi XBee3 is a new family of devices that provides an easy-to-operate solution that provides the ability to connect to a variety of devices.

### Ubidots Explorer:

The key components of any Ubidots-based IoT application are devices, variables, synthetic variable motors, instrument panels and events. In this article, we will look at each of these concepts related to Ubidot's IoT development and deployment platform, and how you can better configure your Ubidots app for the best user experience.

After the devices, variables, and common applications have been assembled, Ubidots Device Management installs applications in multiple layers to learn more about Ubidot's internal architecture, and how applications, organizations, and users can be used to efficiently connect data to those who need it. Find out.

## Contents

### 1. Device

### 2. Variable

### Synthetic Variable Mechanism

### 4. Dashboard and visualization

### 5. Events.

### 1. Device

A Ubidots device is a data source or simply a virtual representation of an asset that receives sensor data and transmits this data through the Ubidots cloud connection protocol. [Click here](#) for an example and latest firmware guide for connecting your device to Ubidots.

Each device is different, but the default settings for each device include:

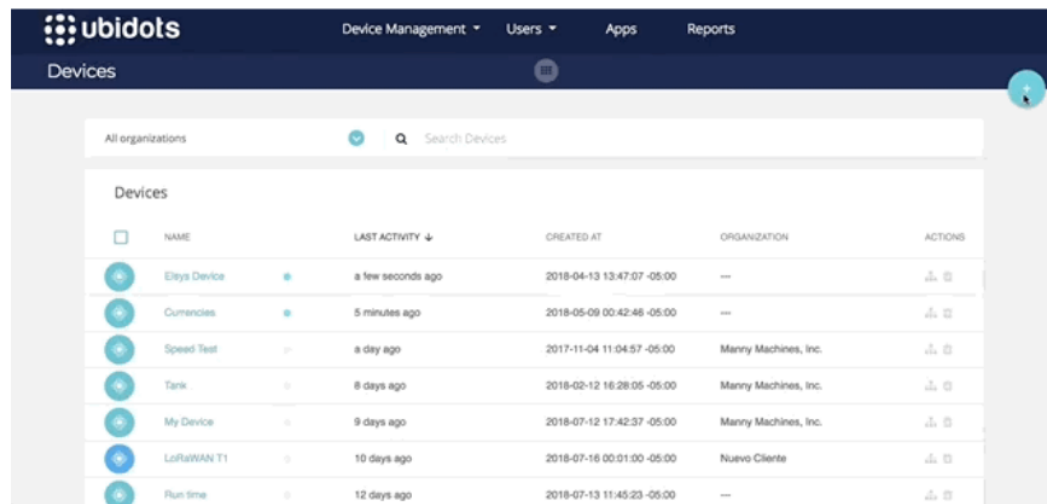
- Libraries to be installed on IDE devices. (Not required)
- Authentication of the padding parameters such as connection and padding parameters (e.g., unique identifiers for each account or user), other devices and labels (e.g. Ubidots' unique devices and other identifiers), Wi-Fi SSID and password, and the device.
- Make an API request (ie, make a call from the device to the web server). With the Ubidot library, you don't have to make these requests manually. However, if you're working with a device that isn't currently on the list of supported hardware, you can choose a connection protocol like MQTT or HTTP and apply the API accordingly.

Device creation: There are three ways to create a device.

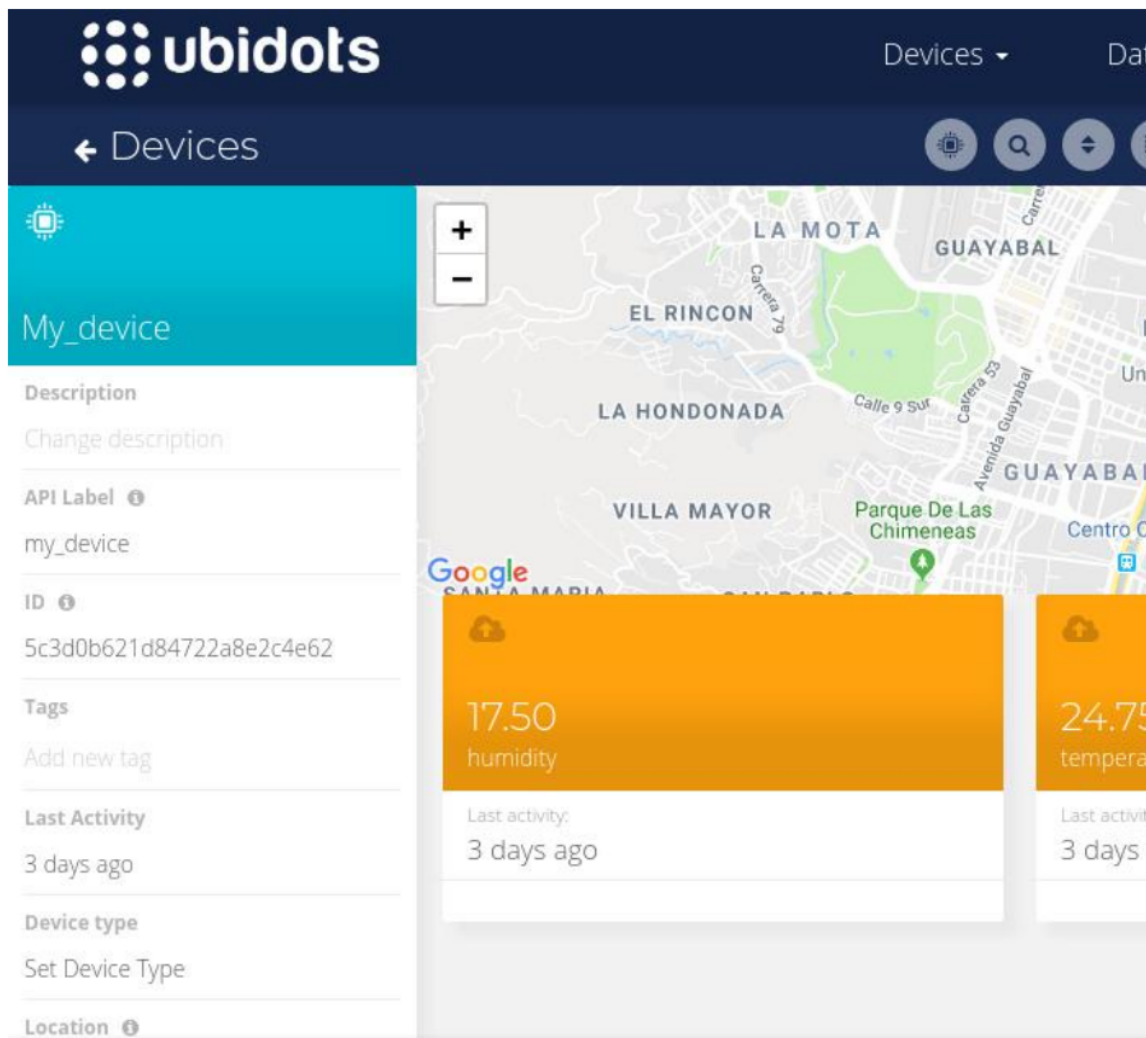
Units are automatically generated by Ubidots the first time points for a user's personal token or institutional token are received.

2. Click the "+" icon in the upper right corner of the individual device screen.

Then create new devices with predefined device properties, shapes, and variables, and create device types that automate the connection of thousands of devices.



1. . 2. Variable
2. When a device is created and data from hardware or other data sources is received from a third party, the information is either displayed in its original format or calculated as a variable.
3. Different types:
4. -Basically-the raw data of the device (including people).
5. -Synthesis-basically corresponds to a statistical operation or arithmetic on a variable over a certain period of time (e.g. average daily traffic for this month).
6. You can learn more about setting synthetic variables below.
7. Creating a variable: There are two ways to create a variable.
8. 1. Label the hardware code as a variable.
9. 2. Click the "+" sign on the single device screen and assign a name corresponding to the variable label. By default, Ubidots assigns an additional unique identifier to a variable called Variable ID. Select the "i" icon on the variable card to find the variable identifier and variable label.



### Synthetic Variable Mechanism

Ubidot Synthetic Variable Engine (SV) is a simple and efficient way to generate insights from raw data stored in the Ubidot cloud. Ubidots SV Engine allows users to provide data-driven solutions to users of Ubidots-based applications by creating synthetic variables that compute and enhance data.

For example, to calculate this week's (average) energy consumption, you need to create a composite variable called energy to calculate the current output and voltage ( $P = C * V$ ). It is the standard variable current multiplied by voltage. Average is the average since I returned weekly using the built-in() function.

### Synthetic variable analysis

Energy

Synthetic Variable

Enter your synthetic variable expression. [Learn more about synthetic variables.](#)

1 mean( **current** \* **voltage** , "W" )

Timezone:  
America/Bogota

Click on a variable to add it to your expression:

Current

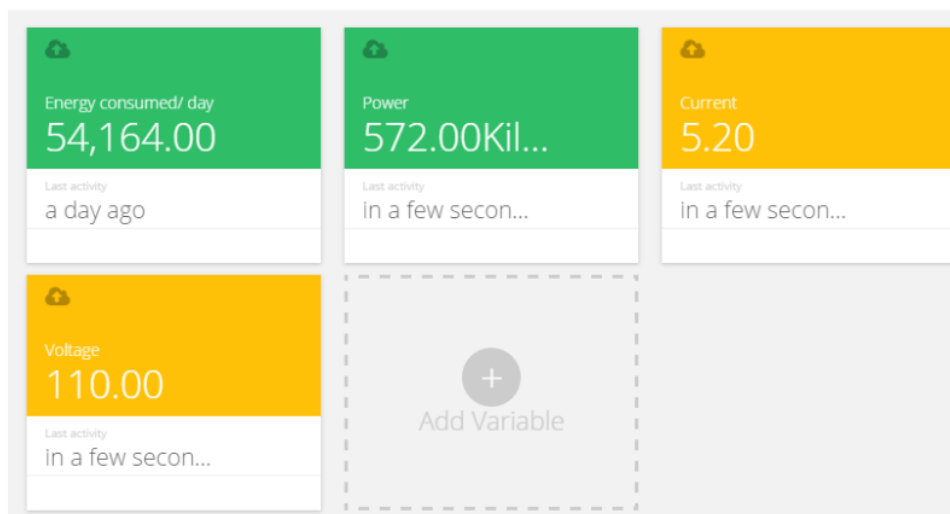
Voltage

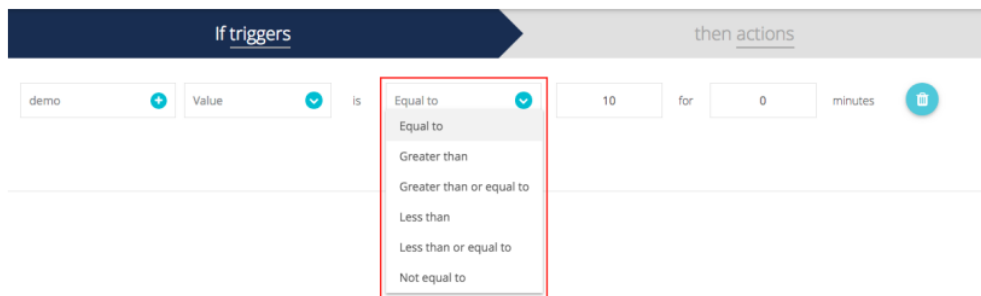
✓

Cancel

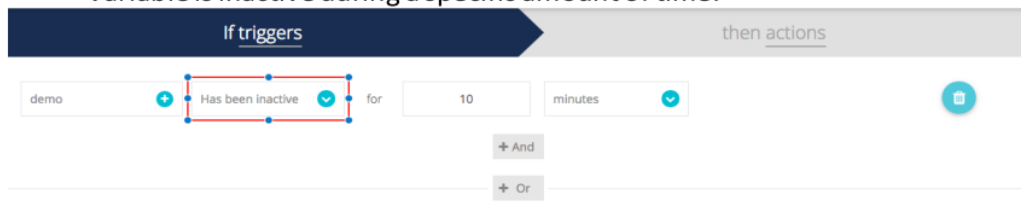
Accept

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

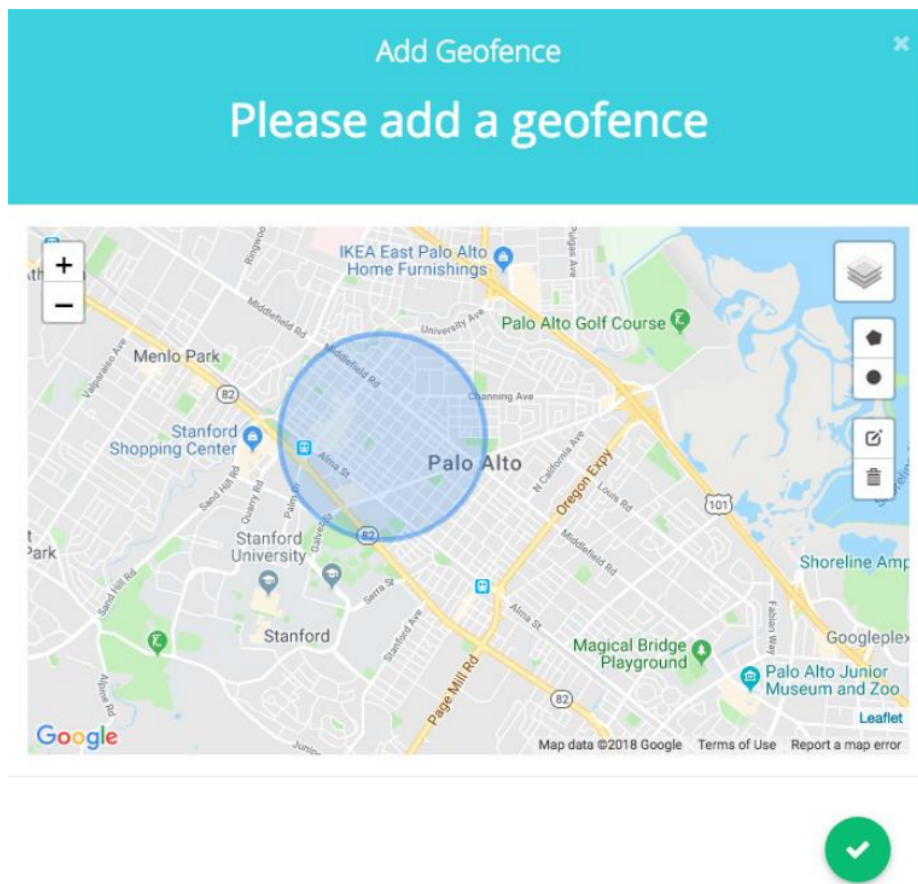




- Variable is inactive during a specific amount of time:



- When a device enters or exits a specific area (geofence):
- Variables are yellow by default and composite variables are green.
- 4. Dashboard and visualization
- The dashboard is a human-machine interface that makes it easy to visualize your data. Ubidots account allows you to quickly understand your data by creating as many dashboards as you need using widgets and data visualization. For more information on toolbar design, check out this guide.
- 5. Events
- In Ubidots, an event is a message triggered and delivered via email, SMS, Telegram, Slack, voice call, or webmail according to custom design rules created in the app. To generate alerts for IoT applications, check out this guide for further assistance.
- 3 types of events:
  - When the sensor reaches a certain value:



You can also select Email, SMS, Telegram or Webhook to define the alert format.

Other users also found this feature useful.

- Create a device in Ubidots
- Event: Was the event triggered? How to check the event log
- Device type

Declaration:

- Vehicle application

- Request to send
- Security application

Recommendation:

- [1] Abid Khan, Ravi Mishra "Zigby-GSM based tracking system", International Journal of Engineering Trends and Technology, Volume 3, Issue 2, pp: 161-169, 2019.
- [2] S.P. Bhumkar, V.V. Deotar, R.V. Babar, "Intelligent Accident Prevention System for Arduino-7 Vehicles", International Journal of Emerging Technologies and Advanced Engineering, Volume 2, Issue 4, pp: 56-78, 2016.
- [3] B.G. Nagaraja, Ravi Rayappa, M. Mahesh, Chandrasekhar M. Patil, Dr. T.K. Manjunath:'GSM-based vehicle theft system design and development' ICACC International Advanced Computer Management Conference '09. Pp148.
- [4] Xu Li, Wei Shu, Minlu Li, Hong-Yu Huang, Pei-En Luo and Minyu Wu, "Performance Evaluation of Mobile Sensor Traffic Monitoring Network", IEEE 2014.
- [5] Young, Kar-Keung D. "Automatic Navigation and Control of Mobile Vehicles Using Wireless Sensor Network Technology", IEEE International Conference on Industrial Technology, 2012.

ORIGINALITY REPORT

---

8%

SIMILARITY INDEX

6%

INTERNET SOURCES

5%

PUBLICATIONS

8%

STUDENT PAPERS

---

PRIMARY SOURCES

---

1

[podelise.ru](http://podelise.ru)

Internet Source

3%

2

Submitted to Liberty Union High School  
District

Student Paper

1%

3

Submitted to Henley College Coventry,  
Coventry

Student Paper

1%

4

Submitted to Far Eastern University

Student Paper

&lt;1%

5

[archive.org](http://archive.org)

Internet Source

&lt;1%

6

[eprints.mdx.ac.uk](http://eprints.mdx.ac.uk)

Internet Source

&lt;1%

7

Submitted to Barking College

Student Paper

&lt;1%

8

Submitted to Vivekanand Education Society's  
Institute of Technology

Student Paper

&lt;1%

|    |                                                                                                                        |      |
|----|------------------------------------------------------------------------------------------------------------------------|------|
| 9  | elibrary.pacounties.org<br>Internet Source                                                                             | <1 % |
| 10 | Submitted to Korea National University of Transportation<br>Student Paper                                              | <1 % |
| 11 | Submitted to Dr. S. P. Mukherjee International Institute of Information Technology (IIIT-NR)<br>Student Paper          | <1 % |
| 12 | Submitted to KYUNG HEE UNIVERSITY<br>Student Paper                                                                     | <1 % |
| 13 | Submitted to Hoa Sen University<br>Student Paper                                                                       | <1 % |
| 14 | Submitted to Ghana Technology University College<br>Student Paper                                                      | <1 % |
| 15 | Submitted to National University Of Science and Technology<br>Student Paper                                            | <1 % |
| 16 | Submitted to Asia Pacific University College of Technology and Innovation (UCTI)<br>Student Paper                      | <1 % |
| 17 | Submitted to Kingston University<br>Student Paper                                                                      | <1 % |
| 18 | Prabhat Sharma, Swapnil Jain. "Review of VANET Challenges and Protocol for Architecture Design and Intelligent Traffic | <1 % |

# System", 2nd International Conference on Data, Engineering and Applications (IDEA), 2020

Publication

19

cmpdartsvr3.cmp.uea.ac.uk

Internet Source

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

