An industry-oriented mini project report
on

AUTOMATIC INTRUDER DETECTION AND ALERTING SYSTEM VIA MAIL

submitted in partial fulfillment of the
academic requirement for the award of
Degree of

BACHELOR OF TECHNOLOGY
in
Electronics &Communication Engineering

Submitted by:
S.SRIKANTH SAI VARMA (20R01A04A8)

under the esteemed guidance of

Dr.Rajender

CMR INSTITUTE OF TECHNOLOGY
(UGCAUTONOMOUS)
Approved by AICTE,Permanent Affiliationto JNTUH, Accredited byNBA and NAAC
Kandlakoya(V),MedchalDist-501 401
www.cmrithyderabad.edu.in

2023-24

CMR INSTITUTE OF TECHNOLOGY

(UGCAUTONOMOUS)

ApprovedbyAICTE,PermanentAffiliationto JNTUH,AccreditedbyNBAandNAAC

Kandlakoya(V),MedchalDist-501 401

www.cmrithyderabad.edu.in

CERTIFICATE

This is to certify that an Industry oriented Mini Project entitled with "AUTOMATIC INTRUDER DETECTION AND ALERTING SYSTEM VIA MAIL"
is being submitted by:

S.SRIKANTH SAI VARMA (20R01A04A8)

to JNTUH, Hyderabad, in partial fulfillment of the requirement for award of the degree of B.Tech in Electronics &Communication Engineering and is a record of a bonafide work carried out under our guidance and supervision. The results in this project have been verified and are found to be satisfactory. The results embodied in this work have not been submitted to have any other University forward of another degree or diploma.

Signature of Guide	Signature of Project Coordinator	Signature of HOD
Dr.Rajender	**MRS.V.sumathi**	**Dr.K.Niranjan Reddy**

EXAMINER

ACKNOWLEDGEMENT

I am extremely grateful to **Dr. M Janga Reddy**, Director, **Dr. B. Satyanarayana**, Principal and **Dr.K.Niranjan Reddy**, Head of Department, Dept of Electronics & Communication Engineering, CMR Institute of Technology for their inspiration and valuable guidance during entire duration.

I am extremely thankful to **MRS. V.sumathi,** Mini Project Coordinator and internal guide **Dr.Rajender**, Dept of Dept of Electronics &Communication Engineering, CMR Institute of Technology for their constant guidance, encouragement and moral support throughout the project.

I will be failing in duty if we do not acknowledge with grateful thanks to the authors of their references and other literatures referred in this Project.

I express our thanks to all staff members and friends for all the help and coordination extended in bringing out this Project successfully in time.

Finally, I am very much thankful to my parents and relatives who guided directly o in directly for every step towards success.

S.SRIKANTH SAI VARMA (20R01A04A8)

Declaration

I S.SRIKANTH SAI VARMA (2 0 R 0 1 A 0 4 A 8) of the Mini-Project entitled as "***Automatic Intruder Detection And Alerting system Via Mail"*** hereby declared that the matter embodied in this project is the genuine work doneby us only and has not been submitted either to the university or to any university/institute for the fulfillmentof the requirement of any course of study.

S.SRIKANTH SAI VARMA (20R01A04A8)

ABSTRACT

The main problem in this research is the increasing prevalence of theft and burglary cases. This incident was caused by the busyness of every person in his daily life so that he forgot the security of his house. The IoT-based home security system that utilizes the PIR sensor as a human motion detector and then sends a notification in the form of notification via SMS or e-mail is one solution to overcome the problem that was previously proposed in previous research. However, to further clarify the warnings sent from the system, a home security system is needed that can attach images in the notification. In this study developed an IoT-based home security system. The IoT security system developed, can automatically send email alerts by attaching images when the PIR sensor detects human presence. The IoT system requires a Raspberry Pi as a microcontroller that has been connected to the internet, a PIR sensor to detect human movement and Pi Camera to win images when there are human encounters that are within the range of PIR sensors. Experiments in the study show that the IoT system can automatically send email alerts by attaching images when PIR sensors detect human presence in various light conditions with a range of 0-5 meters and the speed of sending email alerts affected by conditions of internet network connections and files size of image sent.

INDEX

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

This incident can be caused by everyone's daily activities, which result in neglected home security.The solution to addressing home security issues has been done in previous studies, namely the creation of IoT-based security systems. Research explains the detection of human movement with the help of PIR sensors, IP cameras, and smart cam applications based on auto motion detect then sends an alarm in the form of an alarm, SMS notification and notification real-time e-mail to homeowners. It is just that the lack of an existing security system IP Camera is not used to take pictures when human movement is detected by the PIR sensor which is then attached to the email notification as an alert email. Another disadvantage is that there are no images sent to the SMS or e-mail notification. Homeowners cannot see or distinguish the notification from people who do not know or known people. In IoT, everything is expected to be able to interact and communicate with each other, such as exchanging data and information related to environmental conditions.The development of IoT-based home security systems is a solution to address the shortcomings of previous research. The IoT security system makes it possible to control and monitor home conditions remotely in real time over the internet network One of the challenges that will be solved is related to the development of IoT-based security systems, namely the process of automating sending email alerts by attaching images captured by Pi Camera when the PIR sensor detects human presence and knowing the things that affect the sending of email alerts that attach the image. Raspberry Pi (Raspy) is a microcontroller used in this security system and also a server for sending alert emails . Utilizing email services in sending notifications is currently felt to be the most effective compared to the use of SMS services because users of SMS services are decreasing especially at Indosat providers .The Raspy used is equipped with a Wi-Fi module, and another module is added, namely, the PIR sensor to detect human movement. As with the human senses, sensors can sense the environment .This PIR sensor can filter the wavelengths of passive infrared light between 8 to 14 micrometers, waves of passive infrared light produced from the human body range from 9 to 10 micrometers. Raspy is also equipped with a Pi Camera module to capture images when human movement is within the range of a PIR sensor at a distance of 0 to 5 meters

1.1 Existing System:

Before the implementation of the proposed automatic intruder detection and alerting system via email, let's consider the typical components and features of an existing security system that may or may not include email alerting capabilities.

1. Security Cameras: The existing system may consist of security cameras strategically placed to monitor specific areas or premises.
2. Video Recording: The security cameras may be connected to a video recording system that stores the captured footage for later review if needed.
3. Motion Sensors: Motion sensors may be incorporated into the security system to detect any movement within the monitored areas. When motion is detected, an alarm may be triggered.

4. Alarm System: The existing system might include an alarm system that activates when an intrusion is detected. The alarm could be a loud siren or a silent alarm that notifies a central monitoring station.
5. Security Personnel: In some cases, the existing system may rely on security personnel who manually monitor the camera feeds and respond to potential intrusions.

DISADVANTAGES:

The existing system might have certain limitations, which can be addressed by the proposed automatic intruder detection and alerting system via email. Some common limitations include:
1. Delayed Response: Depending on the availability and attentiveness of security personnel, the response time to an intrusion may be delayed, potentially allowing intruders to escape or cause damage.
2. Manual Monitoring: The reliance on security personnel for continuous monitoring of camera feeds is labor-intensive and subject to human errors or fatigue, leading to potential oversight of suspicious activities.
3. Lack of Timely Notifications: The existing system may not have an automated alerting mechanism, such as email notifications, to promptly inform relevant individuals about detected intrusions.
4. Limited Analysis Capabilities: The existing system may lack advanced video analytics and intrusion detection algorithms, limiting its ability to accurately distinguish between normal activities and suspicious behavior.

1.2 Proposed System:

Automatic Intruder Detection and Alerting System via Email

The proposed system aims to enhance the existing security infrastructure by incorporating advanced technologies and features for automatic intruder detection and timely email alerting. Here is an outline of the proposed system:
1. Hardware Components:
Security Cameras: Install surveillance cameras at strategic locations to capture video footage of the monitored areas.
Motion Sensors: Utilize motion sensors to detect any movement or unusual activity within specific zones.
Network-Connected Devices: Connect the cameras, motion sensors, and other relevant components to a local network or centralized control system.
2. Software Components:
Video Analytics Software: Implement advanced video analytics algorithms to analyze the live video feed from the security cameras in real-time. This software can detect human figures, recognize faces, and identify suspicious activities.
Intrusion Detection Algorithm: Develop a robust intrusion detection algorithm that processes the video analytics data and motion sensor inputs to de
termine potential intrusions. This algorithm should take into account factors such as movement patterns, duration, and location of detected motion.
Email Alerting System: Integrate an email notification system into the software that can automatically generate and send email alerts when an intrusion is detected. The system should allow for customization of email recipients and provide relevant information about the intrusion, such as time, location, and captured images or videos.

3. System Workflow:

Real-time Monitoring: The system continuously monitors the video feeds and motion sensor inputs in real-time, analyzing the data for potential intrusions.

Intrusion Detection: The intrusion detection algorithm processes the video analytics data and motion sensor inputs to identify and classify potential intrusions accurately.

Email Alert Generation: When an intrusion is detected, the system generates an email alert containing details about the intrusion, including timestamp, location, and supporting visual evidence (images or video clips).

Email Notification: The email alerting system sends the generated email notifications to designated recipients, such as security personnel, property owners, or authorized individuals, who can take appropriate actions upon receiving the alerts.

4. Customization and Configuration:

Sensitivity Settings: Users can customize the sensitivity of the intrusion detection algorithm to adjust the system's responsiveness to different environments and minimize false positives or false negatives.

Zone Configuration: The system allows users to define specific areas or zones within the camera coverage for focused monitoring and intrusion detection.

5. Secure Access and Authentication:

User Authentication: Implement secure user authentication mechanisms to ensure that only authorized individuals can access the system, view the video feeds, and manage system settings.

Encryption: Apply encryption techniques to secure communication channels, ensuring the privacy and integrity of email notifications and other sensitive data.

6. Logging and Reporting:

System Logs: Maintain comprehensive logs of detected intrusions, email alerts sent, system events, and user activities for auditing, analysis, and reporting purposes.

Reporting Interface: Provide a user-friendly interface for accessing and generating reports based on the system's log data, facilitating post-incident analysis and security assessment.

By implementing the proposed system, it aims to enhance the existing securityinfrastructure by automating intruder detection, reducing response times, and providing timely email notifications to designated recipients. The system's advanced video analytics capabilities, customization options, and secure communication ensure improved security and peace of mind for users.

ADVANTAGES:

Advantages of the Proposed Automatic Intruder Detection and Alerting System via Email:

1.Real-time Intruder Detection: The system provides real-time monitoring and analysis of video feeds and motion sensor data, enabling prompt detection of potential intrusions.

2. Timely Email Notifications: By integrating an email alerting system, the proposed system ensures that relevant individuals receive immediate notifications about detected intrusions. Email notifications provide a quick and convenient method of communication, allowing recipients to take appropriate actions prompt

3. Improved Security Responsiveness: With automated intruder detection and email alerts, the system enhances the overall security responsiveness.

4. Customizable Alerting Parameters: The system allows users to customize intrusion detection sensitivity and define specific areas or zones for monitoring..

5. Enhanced Accuracy with Video Analytics: By utilizing advanced video analytics algorithms, the system can accurately distinguish between normal activities and suspicious behavior. This reduces false alarms and increases the system's overall accuracy, minimizing unnecessary disruptions.

6. Scalability and Integration: The proposed system is designed to be scalable, accommodating varying numbers of security cameras, motion sensors, and email recipients.

Chapter 2

EMBEDDED SYSTEM

2.1 Introduction:

Many embedded systems have substantially different design constraints than desktop computing applications. No single characterization applies to the diverse spectrum of embedded systems. However, some combination of cost pressure, long life-cycle, real-time requirements, reliability requirements, and design culture dysfunction can make it difficult to be successful applying traditional computer design methodologies and tools to embedded applications. Embedded systems in many cases must be optimized for life-cycle and business-driven factors rather than for maximum computing throughput. There is currently little *tool* support for expanding embedded computer design to the scope of holistic embedded system design. However, knowing the strengths and weaknesses of current approaches can set expectations appropriately, identify risk areas to tool adopters, and suggest ways in which tool builders can meet industrial needs. If we look around us, today we see numerous appliances which we use daily, be it our refrigerator, the microwave oven, cars, PDAs etc. Most appliances today are powered by something beneath the sheath that makes them do what they do. These are tiny microprocessors, which respond to various keystrokes or inputs. These tiny microprocessors, working on basic assembly languages, are the heart of the appliances. We call them embedded systems. Of all the semiconductor industries, the embedded systems market place is the most conservative, and engineering decisions here usually lean towards established, low risk solutions. Welcome to the world of embedded systems, of computers that will not look like computers and won't function like anything we are familiar with.

2.2 CLASSIFICATION

Embedded systems are divided into autonomous, realtime, networked & mobile categories.

They function in standalone mode. Many embedded systems used for process control in manufacturing units& automobiles fall under this category.

Networked embedded systems

They monitor plant parameters such as temperature, pressure and humidity and send the data over the network to a centralized system for on line monitoring.

Mobile gadgets

Mobile gadgets need to store databases locally in their memory. These gadgets imbibe powerful computing & communication capabilities to perform realtime as well as nonrealtime tasks and handle multimedia applications. The embedded system is a combination of computer hardware, software, firmware and perhaps additional mechanical parts, designed to perform a specific function. A good example is an automatic washing machine or a microwave oven. Such a system is in direct contrast to a personal computer, which is not designed to do only a specific task. But an embedded system is designed to do a specific task with in a given timeframe, repeatedly, endlessly, with or without human interaction.

Hardware

Good software design in embedded systems stems from a good understanding of the hardware behind it. All embedded systems need a microprocessor, and the kinds of microprocessors used in them are quite varied. A list of some of the common microprocessors families are: ARM family, The Zilog Z8 family, Intel 8051/X86 family, Motorola 68K family and the power PC family. For processing of information and execution of programs, embedded system incorporates microprocessor or micro- controller. In an embedded system the microprocessor is a part of final product and is not available for reprogramming to the end user. An embedded system also needs memory for two purposes, to store its program and to store its data. Unlike normal desktops in which data and programs are stored at the same place, embedded systems store data and programs in different memories. This is simply because the embedded system does not have a hard drive and the program must be stored in memory even when the power is turned off. This type of memory is called ROM. Embedded applications commonly employ a special type of ROM that can be programmed or reprogrammed with the help of special devices.

2.3 OTHER COMMON PARTS FOUND ON MANY EMBEDDED SYSTEMS

- UART& RS232
- PLD
- ASIC's& FPGA's

2.4 DESIGN PROCESS

Embedded system design is a quantitative job. The pillars of the system design methodology are the separation between function and architecture, is an essential step from conception to implementation. In recent past, the search and industrial community has paid significant attention to the topic of hardware-software (HW/SW) codesign and has tackled the problem of coordinating the design of the parts to be implemented as software and the parts to be implemented as hardware avoiding the HW/SW integration problem marred the electronics system industry so long. In any large scale embedded systems design methodology, concurrency must be considered as a first class citizen at all levels of abstraction and in both hardware and software. Formal models & transformations in system design are used so that verification and synthesis can be applied to advantage in the design methodology. Simulation tools are used for exploring the design space for validating the functional and timing behaviors of embedded systems.

2.3.1 SPECIFICATION

During this part of the design process, the informal requirements of the analysis are transformed to formal specification using SDL.

2.3.2 SYSTEM-SYNTHESIS

For performing an automatic HW/SW partitioning, the system synthesis step translates the SDL specification to an internal system model switch contains problem graph& architecture graph. After system synthesis, the resulting system model is translated back to SDL.

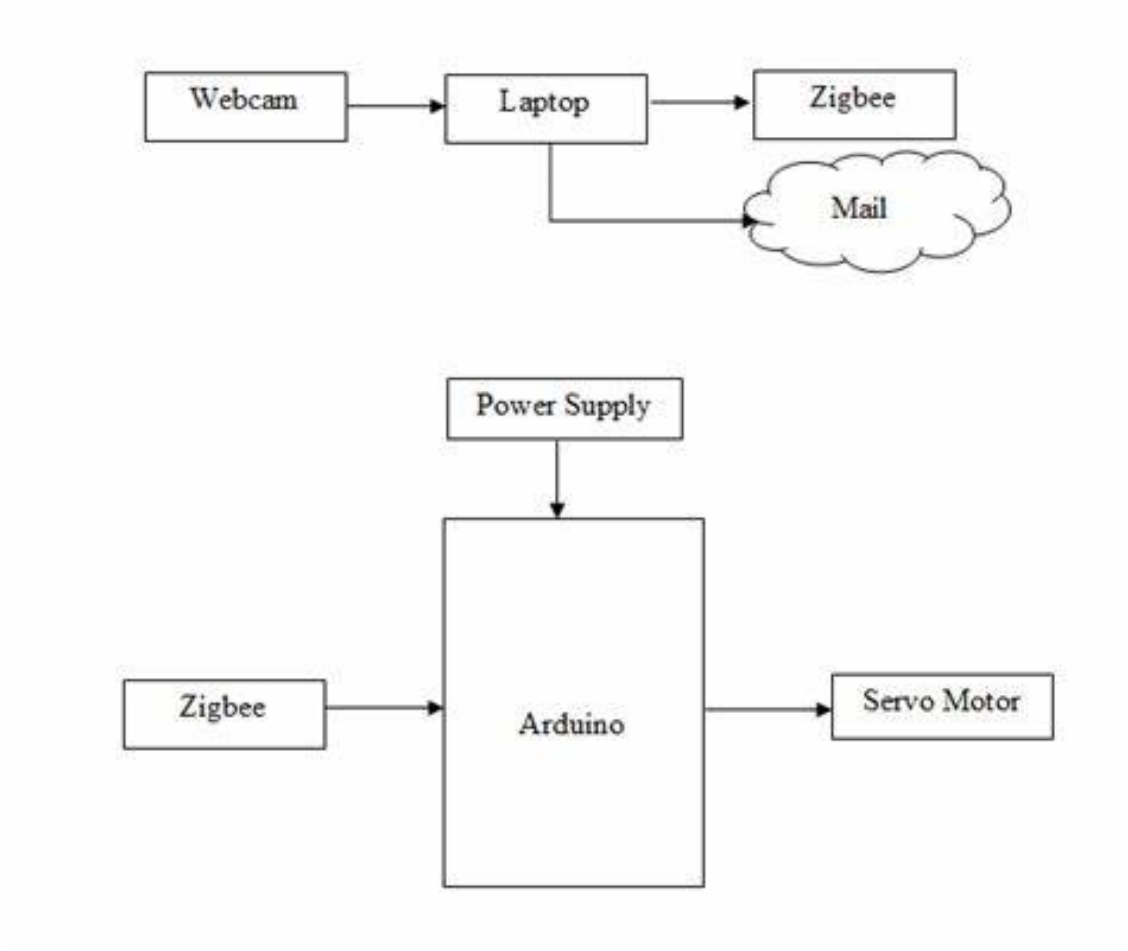
2.3.3 IMPLEMENTATION-SYNTHESIS

SDL specification is then translated into conventional implementation languages such as VHDL for hardware modules and C for software parts of the system.

2.3.4 PROTOTYPING

On a prototyping platform, the implementation of the system under development is executed with the software parts running on multiprocessor unit and the hardware part running on a FPGA board known as phoenix, prototype hardware for Embedded Network Interconnect Accelerators.

Block diagram



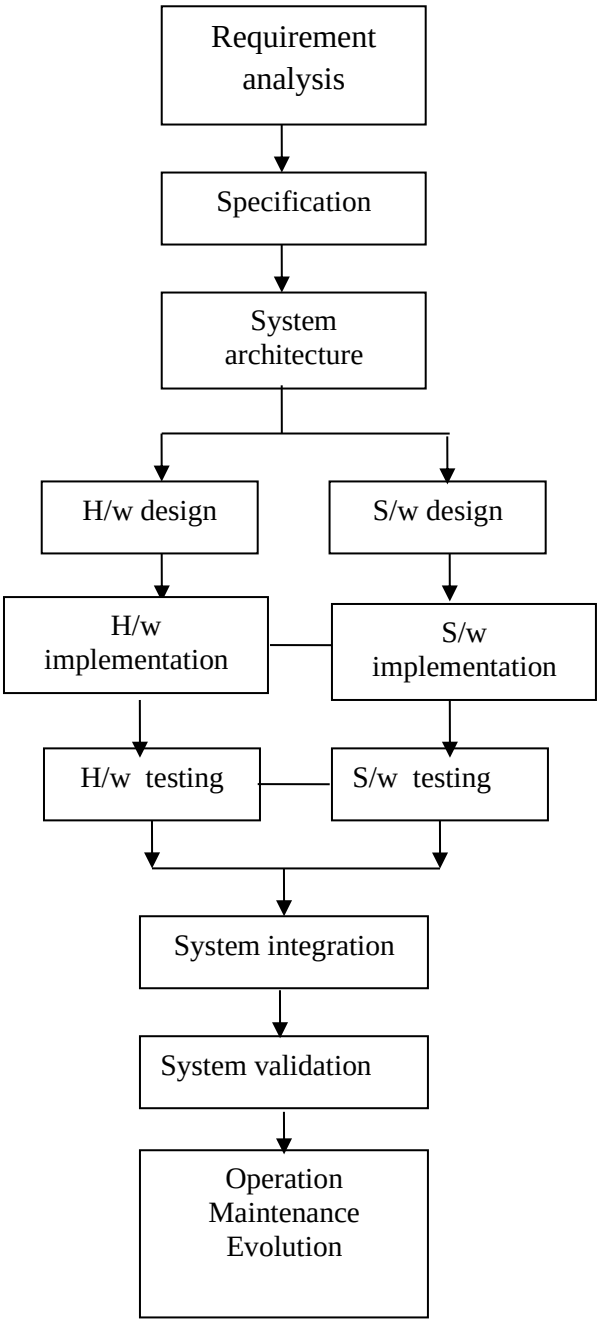


Fig 2.1: Embedded Development Life Cycle

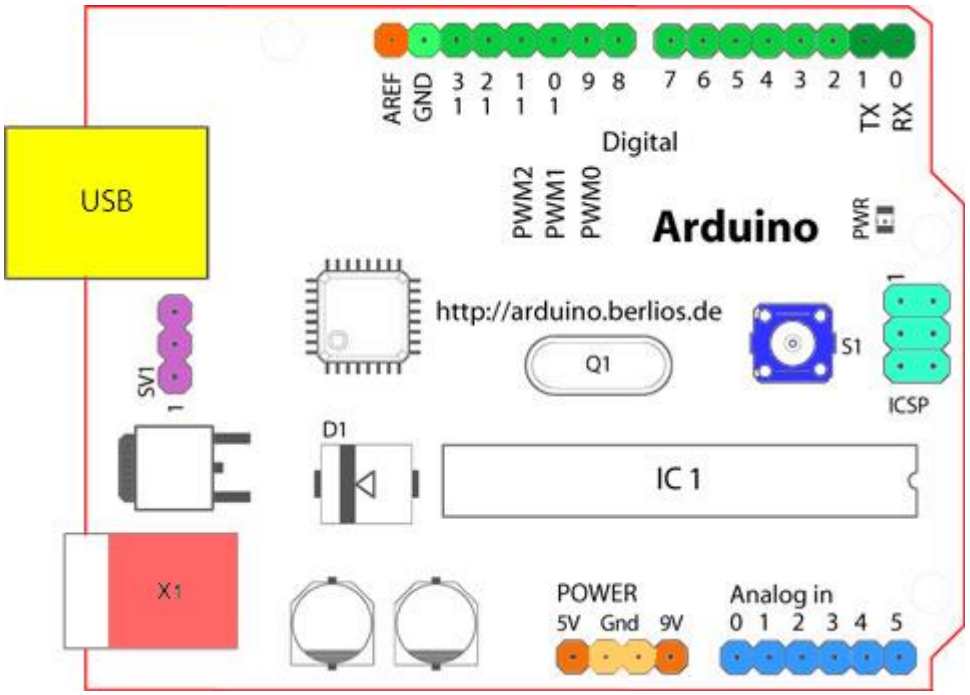
- **Aerospace and defence electronics**: Fire control, radar, robotics/sensors, sonar.
- **Automotive**: Autobody electronics, auto power train, auto safety, car information systems.
- **Broadcast & entertainment**: Analog and digital sound products, camaras, DVDs, Set top boxes, virtual reality systems, graphic products.
- **Consumer/internet appliances**: Business handheld computers, business network computers/terminals, electronic books, internet smart handheld devices, PDAs.
- **Data communications:** Analog modems, ATM switches, cable modems, XDSL modems, Ethernet switches, concentrators.
- **Digital imaging**: Copiers, digital still cameras, Fax machines, printers, scanners.
- **Industrial measurement and control:** Hydro electric utility research & management traffic management systems, train marine vessel management systems.
- **Medical electronics:** Diagnostic devices, real time medical imaging systems, surgical devices, critical care systems.
- **Server I/O:** Embedded servers, enterprise PC servers, PCI LAN/NIC controllers, RAID devices, SCSI devices.
- **Telecommunications**: ATM communication products, base stations, networking switches, SONET/SDH cross connect, multiplexer.
- **Mobile data infrastructures**: Mobile data terminals, pagers, VSATs, Wireless LANs, Wireless phones.

Chapter.3

ARDUINO

Arduino:

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmega microcontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output pins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs, small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploading your compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power.



Structure of Arduino Board

DIGITAL PINS

In addition to the specific functions listed below, the digital pins on an Arduino board can be used for general purpose input and output via the pin Mode(), Digital Read(), and Digital Write() commands. Each pin has an internal pull-up resistor which can be turned on and off using digital Write() (w/ a value of HIGH or LOW, respectively) when the pin is configured as an input. The maximum current per pin is 40mA.

Serial: 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. On the Arduino Diecimila, these pins are connected to the corresponding pins of the FTDI USB-to-TTL Serial chip. On the Arduino BT, they are connected to the corresponding pins of the WT11 Bluetooth module. On the Arduino Mini and LilyPad Arduino, they are intended for use with an external TTL serial module (e.g. the Mini-USB Adapter).

External Interrupts: 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attach Interrupt() function for details.

PWM: 3, 5, 6, 9, 10, and 11 Provide 8-bit PWM output with the analog Write() function. On boards with an ATmega8, PWM output is available only on pins 9, 10, and 11.

BT Reset: 7. (Arduino BT-only) Connected to the reset line of the bluetooth module.

SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication, which, although provided by the underlying hardware, is not currently included in the Arduino language.

LED: 13. On the Diecimila and LilyPad, there is a built-in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off.

ANALOG PINS

In addition to the specific functions listed below, the analog input pins support 10-bit analog-to-digital conversion (ADC) using the analog Read() function. Most of the analog inputs can also be used as digital

pins: analog input 0 as digital pin 14 through analog input 5 as digital pin 19. Analog inputs 6 and 7 (present on the Mini and BT) cannot be used as digital pins.

I^2C: 4 (SDA) and 5 (SCL). Support I^2C (TWI) communication using the Wire library (documentation on the Wiring website).

POWER PINS

VIN (sometimes labeled "9V"): The input voltage to the Arduino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin. Also note that the Lily Pad has no VIN pin and accepts only a regulated input.

5V: The regulated power supply used to power the microcontroller and other components on the board. This can come either from VIN via an on-board regulator, or be supplied by USB or another regulated 5V supply.

3V3 (Diecimila-only) : A 3.3 volt supply generated by the on-board FTDI chip.

GND: Ground pins.

OTHER PINS

AREF: Reference voltage for the analog inputs. Used with analog Reference().

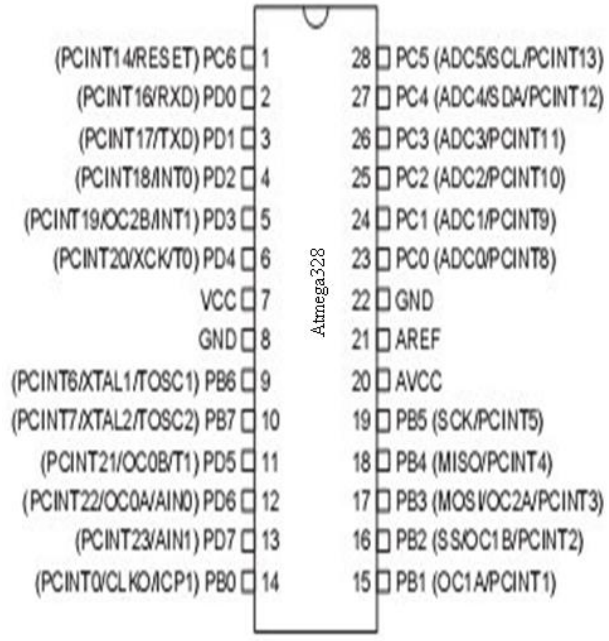
Reset: (Diecimila-only) Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board.

Chapter 4
HARDWARE COMPONENTS

4.1.1 Controller (ATMEGA328)

Controller is heart of our system. This controller following features: 32Kbytes of in-system programmable flash with read-whilewrite capabilities, two 8-bit Timer/Counters, 23 programmable I/O Lines, and operating Voltage is 1.8 - 5.5V, Temperature Range
-40°C to 105°C, three flexible Timer/Counters.Pin configuration of ATmega328 IC consists of 28 pins. There is Port B, Port C &
Port D an 8-bit bi-directional I/O port with internal pull-up resistors.

Pin diagram



Pin Configuration of Atmega328

Pin Description

VCC: Digital supply voltage.

GND: Ground.

Port A (PA7-PA0): Port A serves as the analog inputs to the A/D Converter. Port A also serves as an 8-bit bi-directional I/O port, if the A/D Converter is not used. Port pins can provide internal pull-up resistors

(selected for each bit). The Port A output buffers have symmetrical drive characteristics with both high sink and source capability. When pins PA0 to PA7 are used as inputs and are externally pulled low, they will source current if the internal pull-up resistors are activated. The Port A pins are tri-stated when a reset condition becomes active, even if the clock is not running.

Port B (PB7-PB0): Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running. Port B also serves the functions of various special features of the ATmega32.

Port C (PC7-PC0): Port C is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port C output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running. If the JTAG interface is enabled, the pull-up resistors on pins PC5(TDI), PC3(TMS) and PC2(TCK) will be activated even if a reset occurs. The TD0 pin is tri-stated unless TAP states that shift out data are entered. Port C also serves the functions of the JTAG interface.

Port D (PD7-PD0): Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running. Port D also serves the functions of various special features of the ATmega32.

Reset (Reset Input): A low level on this pin for longer than the minimum pulse length will generate a reset, even if the clock is not running. Shorter pulses are not guaranteed to generate a reset.

XTAL1: Input to the inverting Oscillator amplifier and input to the internal clock operating circuit.

XTAL2:Output from the inverting Oscillator amplifier.

AVCC: AVCC is the supply voltage pin for Port A and the A/D Converter. It should be externally connected to VCC, even if the ADC is not used. If the ADC is used, it should be connected to VCC through a low-pass filter.

AREF: AREF is the analog reference pin for the A/D Converter

4.2 Servo motor

A servo motor is a type of motor that can rotate with great precision. Normally this type of motor consists of a control circuit that provides feedback on the current position of the motor shaft, this feedback allows the servo motors to rotate with great precision. If you want to rotate an object at some specific angles or distance, then you use a servo motor.

Servo motor

Servo Motor Working Mechanism

It consists of three parts:

Controlled device

1. Output sensor
2. Feedback system

It is a closed-loop system where it uses a positive feedback system to control motion and the final position of the shaft. Here the device is controlled by a feedback signal generated by comparing output signal and reference input signal.Here reference input signal is compared to the reference output signal and the third signal is produced by the feedback system. And this third signal acts as an input signal to the control the

device. This signal is present as long as the feedback signal is generated or there is a difference between the reference input signal and reference output signal. So the main task of servomechanism is to maintain the output of a system at the desired value at presence of noises.

Servo Motor Working Principle

A servo consists of a Motor (DC or AC), a potentiometer, gear assembly, and a controlling circuit. First of all, we use gear assembly to reduce RPM and to increase torque of the motor. Say at initial position of servo motor shaft, the position of the potentiometer knob is such that there is no electrical signal generated at the output port of the potentiometer. Now an electrical signal is given to another input terminal of the error detector amplifier. Now the difference between these two signals, one comes from the potentiometer and another comes from other sources, will be processed in a feedback mechanism and output will be provided in terms of error signal. This error signal acts as the input for motor and motor starts rotating. Now motor shaft is connected with the potentiometer and as the motor rotates so the potentiometer and it will generate a signal.

Interfacing Servo Motors with Microcontrollers: Interfacing hobby Servo motors like s90 servo motor with MCU is very easy. **Servos have three wires coming out of them**. Out of which two will be used for Supply (positive and negative) and one will be used for the signal that is to be sent from the MCU. An **MG995 Metal Gear Servo Motor** which is most commonly used for RC cars humanoid bots etc. The picture of MG995 is shown below:

Controlling Servo Motor: All motors have three wires coming out of them. Out of which two will be used for Supply (positive and negative) and one will be used for the signal that is to be sent from the MCU.Servo motor is controlled by PWM (Pulse with Modulation) which is provided by the control wires. There is a minimum pulse, a maximum pulse and a repetition rate. Servo motor can turn 90 degree from either direction form its neutral position. The servo motor expects to see a pulse every 20 milliseconds (ms) and the length of the pulse will determine how far the motor turns. For example, a 1.5ms pulse will make the motor turn to the 90° position, such as if pulse is shorter than 1.5ms shaft moves to 0° and if it is longer than 1.5ms than it will turn the servo to 180°.

4.3.1 Web cam

A webcam is a video camera which is designed to record or stream to a computer or computer network. They are primarily used in video telephony, live streaming and social media, and security. Webcams can be built-in computer hardware or peripheral devices, and are commonly connected to a device using USB or wireless protocols.

Web cam

4.3.2 Image sensor

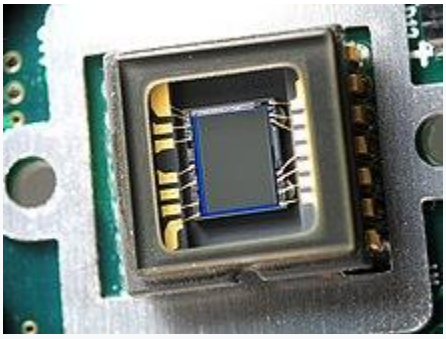


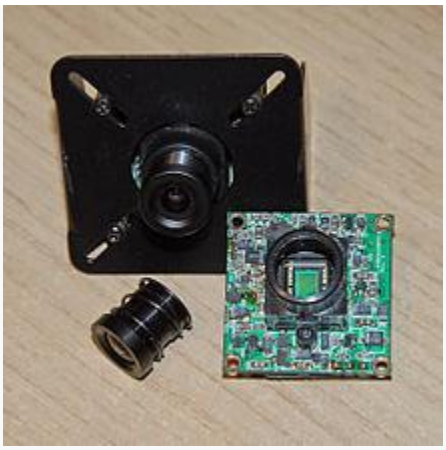
Image sensor

Charge-coupled device (CCD) image sensor of a webcam

Image sensors can be CMOS or CCD, the former being dominant for low-cost cameras, but CCD cameras do not necessarily outperform CMOS-based cameras in the low-price range. Most consumer webcams are capable of providing VGA-resolution video at a frame rate of 30 frames per second. Many newer devices can produce video in multi-megapixel resolutions, and a few can run at high frame rates such as the PlayStation Eye, which can produce 320×240 video at 120 frames per second.[22] Most image sensors are sourced from Omnivision or Sony.

As webcams evolved simultaneously with display technologies, USB interface speeds and broadband internet speeds, the resolution went up from gradually from 320×240, to 640×480, and some now even offer 1280×720 (aka 720p) or 1920×1080 (aka 1080p) resolution.[23][24][25] Despite the low cost, the resolution offered as of 2019 is impressive, with now the low-end webcams offering resolutions of 720p, mid-range webcams offering 1080p resolution, and high-end webcams offering 4K resolution at 60 fps.

4.3.3 Optics



optics

Various lenses are available, the most common in consumer-grade webcams being a plastic lens that can be manually moved in and out to focus the camera. Fixed-focus lenses, which have no provision for adjustment, are also available. As a camera system's depth of field is greater for small image formats and is greater for lenses with a large f-number (small aperture), the systems used in webcams have a

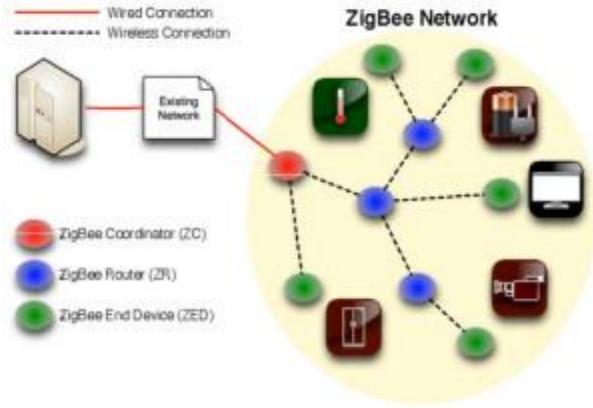
sufficiently large depth of field that the use of a fixed-focus lens does not impact image sharpness to a great extent.Most models use simple, focal-free optics (fixed focus, factory-set for the usual distance from the monitor to which it is fastened to the user) or manual focus.Webcams can come with different presets and fields of view. Individual users can make use of less than 90° horizontal FOV for home offices and live streaming. Webcams with as much as 360° horizontal FOV can be used for small- to medium-sized rooms (sometimes even large rooms). Depending on the users' purposes, webcams in the market can display the whole room or just the general vicinity.

4.4.1 Zig Bee

Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz and 2.4 GHz frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.

Zigbee

4.4.2 Zigbee Architecture



Zigbee system structure

Zigbee system structure consists of three different types of devices such as Zigbee coordinator, Router and End device. Every Zigbee network must consist of at least one coordinator which acts as a root and bridge

of the network. The coordinator is responsible for handling and storing the information while performing receiving and transmitting data operations. Zigbee routers act as intermediary devices that permit data to pass to and fro through them to other devices. End devices have limited functionality to communicate with the parent nodes such that the battery power is saved as shown in the figure. The number of routers, coordinators and end devices depends on the type of network such as star, tree and mesh networks.

Zigbee protocol architecture consists of a stack of various layers where IEEE 802.15.4 is defined by physical and MAC layers while this protocol is completed by accumulating Zigbee's own network and application layers.

Physical Layer: This layer does modulation and demodulation operations up on transmitting and receiving signals respectively. This layer's frequency, date rate and number of channels are given below.

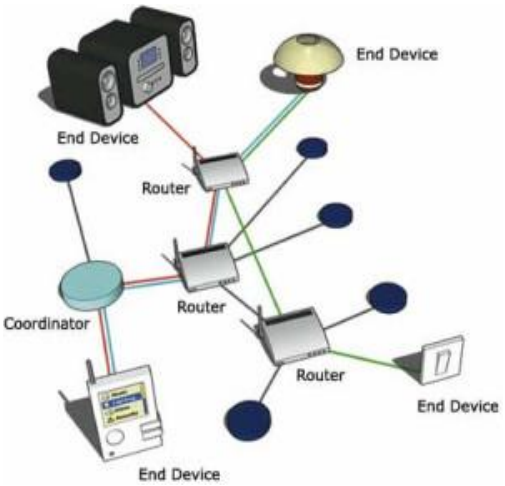
MAC Layer: This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance (CSMA). This also transmits the beacon frames for synchronizing communication.

Network Layer: This layer takes care of all network related operations such as network setup, end device connection and disconnection to network, routing, device configurations, etc.

Application Support Sub-Layer: This layer enables the services necessary for Zigbee device object and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

Application Framework: It provides two types of data services as key value pair and generic message services. Generic message is a developer defined structure, whereas the key value pair is used for getting attributes within the application objects. ZDO provides an interface between application objects and APS layer in Zigbee devices. It is responsible for detecting, initiating and binding other devices to the network.

4.4.3 Zigbee Operating Modes and Its Topologies

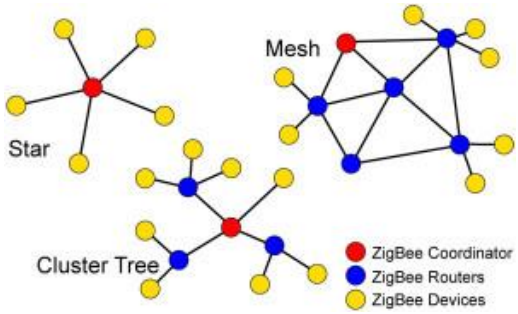


Zigbee Communication Operation

Zigbee two way data is transferred in two modes: Non-beacon mode and Beacon mode. In a beacon mode,

the coordinators and routers continuously monitor active state of incoming data hence more power is consumed. In this mode, the routers and coordinators do not sleep because at any time any node can wake up and communicate. However, it requires more power supply and its overall power consumption is low because most of the devices are in an inactive state for over long periods in the network.In a beacon mode, when there is no data communication from end devices, then the routers and coordinators enter into sleep state. Periodically this coordinator wakes up and transmits the beacons to the routers in the network

4.4.4 Zigbee Topologies



Zigbee Topologies

Zigbee supports several network topologies; however, the most commonly used configurations are star, mesh and cluster tree topologies. Any topology consists of one or more coordinator. In a star topology, the network consists of one coordinator which is responsible for initiating and managing the devices over the network. All other devices are called end devices that directly communicate with coordinator. This is used in industries where all the end point devices are needed to communicate with the central controller, and this topology is simple and easy to deploy.In mesh and tree topologies, the Zigbee network is extended with several routers where coordinator is responsible for staring them. These structures allow any device to communicate with any other adjacent node for providing redundancy to the data. If any node fails, the information is routed automatically to other device by these topologies. As the redundancy is the main factor in industries, hence mesh topology is mostly used. are given below.

	Zigbee	Sub-GHz	Wi-Fi	Bluetooth
Physical Layer Standard	802.15.4	Proprietary / 802.15.4g	802.11	802.15.1
Application Focus	Monitoring & control	Monitoring & control	Web, email, video	Cable replacement
Battery Life (days)	100 – 1,000+	1,000+	0.5 - 5	1 - 7
Network Size	100s to 1,000s	10s to 100s	32	7
Bandwidth (Kbits/s)	20 - 250	0.5 – 1,000	11,000+	720
Range (meters)	1 – 100+	1 – 7,000+	1 – 30+	1 – 10+
Network Architecture	Mesh	Point-to-point, star	Star	Star
Optimized For	Reliability, low power, low cost, scalability	Long range, low power, low cost	Speed	Low cost, convenience
Silicon Labs Products	Ember® ZigBee® EM35x Series	EZRadio®, EZRadioPRO®, Si10xx wireless MCUs	N/A	N/A

Comparison Table of Zigbee

4.4.5 Applications of Zigbee Technology

Applications of Zigbee Technology

Industrial Automation: In manufacturing and production industries, a communication link continually monitors various parameters and critical equipments. Hence Zigbee considerably reduce this communication cost as well as optimizes the control process for greater reliability.

Home Automation: Zigbee is perfectly suited for controlling home appliances remotely as a lighting system control, appliance control, heating and cooling system control, safety equipment operations and control, surveillance, and so on.

Smart Metering: Zigbee remote operations in smart metering include energy consumption response, pricing support, security over power theft, etc.

Smart Grid monitoring: Zigbee operations in this smart grid involve remote temperature monitoring, fault locating, reactive power management, and so on.

This is all about a brief description of Zigbee technology's architecture, operations modes, configurations and applications. We hope that we have given you enough content on this title, for you to understand it better. We are pioneers in developing Zigbee based projects.

4.5 POWER SUPPLY:

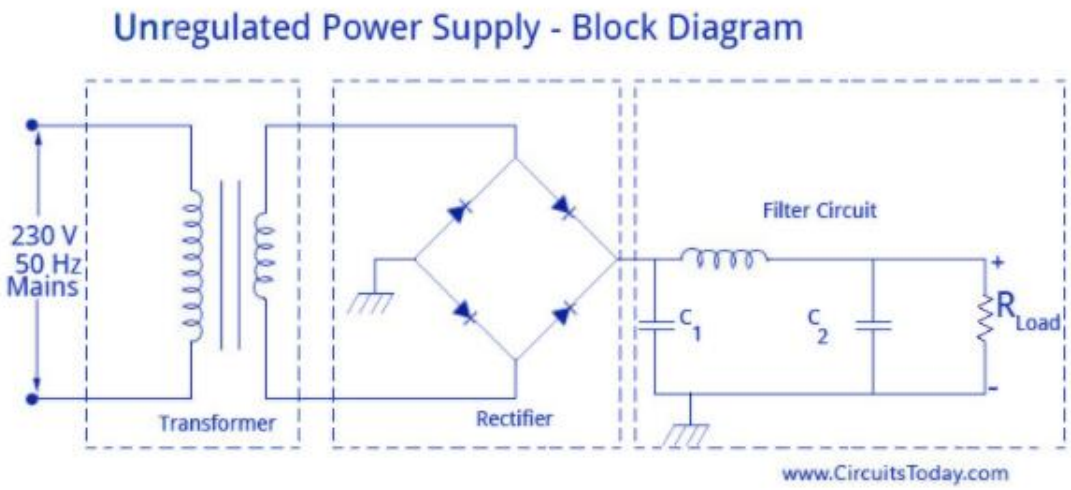
Almost all basic household electronic circuits need an unregulated AC to be converted to constant DC, in order to operate the electronic device. All devices will have a certain power supply limit and the electronic circuits inside these devices must be able to supply a constant DC voltage within this limit. This DC supply

is regulated and limited in terms of voltage and current. But the supply provided from mains may be fluctuating and could easily break down the electronic equipment, if not properly limited. This work of converting an unregulated alternating current (AC) or voltage to a limited Direct current (DC) or voltage to make the output constant regardless of the fluctuations in input, is done by a regulated power supply circuit.

All the active and passive electronic devices will have a certain DC operating point (Q-point or Quiescent point), and this point must be achieved by the source of DC power.

The DC power supply is practically converted to each and every stage in an electronic system. Thus a common requirement for all these phases will be the DC power supply. All low power system can be run with a battery. But, for a long time operating devices, batteries could prove to be costly and complicated. The best method used is in the form of an unregulated power supply –a combination of a transformer, rectifier and a filter. The diagram is shown below.

4.5.1 unregulated power supply



As shown in the figure above, a small step down transformer is used to reduce the voltage level to the devices needs. In India, a 1 Ø supply is available at 230 volts. The output of the transformer is a pulsating sinusoidal AC voltage, which is converted to pulsating DC with the help of a rectifier. This output is given to a filter circuit which reduces the AC ripples, and passes the DC components. But here are certain disadvantages in using an unregulated power supply.

Disadvantages of unregulated power supply

1. Poor Regulation – When the load varies, the output does not appear constant. The output voltage changes by a great value due to the huge change in the current drawn from the supply. This is mainly due to the high internal resistance of the power supply (>30 Ohms).

2. AC Supply Main Variations – The maximum variations in AC supply mains is give or take 6% of its rated value. But this value may go higher in some countries (180-280 volts). When the value is higher it's DC voltage output will differ largely.

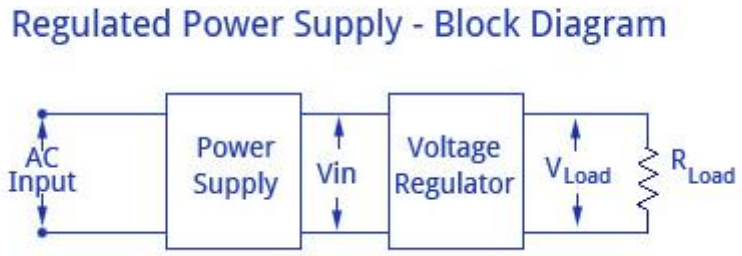
3. Temperature Variation – The use of semiconductor devices in electronic devices may cause variation in temperature.

These variations in dc output voltage may cause an inaccurate or erratic operation or even malfunctioning of many electronic circuits. For instance, in oscillators the frequency will shift, in transmitters output will get distorted, and in amplifiers, the operating point will shift causing bias instability.

All the above-listed problems are overcome with the help of a **voltage regulator** which is employed in conjunction with an unregulated power supply. Thus, the ripple voltage is largely reduced. Thus, the supply becomes a regulated power supply.

4.5.2 REGULATED POWER SUPPLY

Regulated power supply is an electronic circuit that is designed to provide a constant dc voltage of predetermined value across load terminals irrespective of ac mains fluctuations or load variations.



A regulated power supply essentially consists of an ordinary power supply and a voltage regulating device, as illustrated in the figure. The output from an ordinary power supply is fed to the voltage regulating device

that provides the final output. The output voltage remains constant irrespective of variations in the ac input voltage or variations in output (or load) current.

Figure given below shows the complete circuit of a regulated power supply with a transistor series regulator as a regulating device. Each part of the circuit is explained in detail.

5.TESTING AND RESULT

Testingmethods

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input	: identified classes of valid input must be accepted.
Invalid Input	: identified classes of invalid input must be rejected.
Functions	: identified functions must be exercised.
Output	: identified classes of application outputs must be exercised.
Systems/Procedures	: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

Unit Testing

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle,

although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

Integration Testing:

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing:

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered

6 . Result:

The proposed automatic intruder detection and email alert system enhances security by integrating advanced video analytics, motion sensors, and real-time monitoring.It ensures rapid intrusion detection, reducing the risk of security breaches going unnoticed, and offers immediate email notifications for swift response.Customizable parameters tailor the system to different environments, minimizing false alarms, and prioritizing security.

Prototype of Automatic Intruder Detection And Alerting Via Mail

7. Conclusion:

The proposed automatic intruder detection and email alert system enhances security by integrating advanced video analytics, motion sensors, and real-time monitoring.It ensures rapid intrusion detection, reducing the risk of security breaches going unnoticed, and offers immediate email notifications for swift response.Customizable parameters tailor the system to different environments, minimizing false alarms, and prioritizing security.The system is scalable, integrates seamlessly with existing security infrastructure, and offers improved responsiveness, accuracy, and overall security.

8. References:

[1] Subdirektorat Statistik Politik dan Keamanan, "Statistik Kriminal 2018," Badan Pusat Statistik, Indonesia, 2018.
[2] S. Tanwar, P. Pately, K. Patelz, S. Tyagix, N. Kumar and M. Obaidat, "An Advanced Internet of Thing based Security Alert System for Smart Home," IEEE, 2017.
[3] D. Yendri and R. E. Putri, "Sistem Pengontrolan Dan Keamanan Rumah Pintar (Smart Home) Berbasis Android," pp. 1-6, 2018.
[4] R. Khana and U. Usnul, "Rancang Bangun Sistem Keamanan Rumah Berbasis IoT dengan Platform Android," Ejournal Kajian Teknik Elektro Vol.3 No.1, pp. 18-31, 2018.
[5] Budianingsih and A. Riyanto, "Prototipe Sistem Keamanan cerdas pada komplek perumahan," Jurnal Pendidikan Informatika dan Sains, pp. 146-154, 2018.
[6] P. A. Dhobi and N. Tevar, "IoT Based Home Appliances Control," Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication, pp. 648- 651, 2017.
[7] A. N. Ansari, M. Sedky, N. Sharma and A. Tyagi, "An Internet of things approach for motion detection using Raspberry Pi," in Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, Harbin, China, 2015.
[8] M. Al-Kuwari, A. Ramadan, Y. Ismael, L. Al-Sughair and A. Gastli, "Smart-Home Automation using IoT-based Sensing and Monitoring Platform," IEEE, 2018

[9] P. B. Patel, V. M. Choksi, S. Jadhav and M. Potdar, "Smart Motion Detection System using Raspberry Pi," International Journal of Applied Information Systems (IJAIS), vol. 10, no. 5, 2016.
[10] A. Rusli, "Pengguna SMS dan Telepon di Indonesia, Beralih ke Data Internet," Cendana News, 24 Mei 2017. [Online]. Available: https://www.cendananews.com/2017/05/pengguna-sms-dantelepon-di-indonesia-beralih-ke-data-internet.html. [Accessed 25 April 2019].
[11] S. S. K. d. T. Informasi, "Statistik Telekomunikasi Indonesia," Badan Pusat Statistik, Indonesia, 2017.
[12] F. S. Perilla, G. R. V. Jr. and N. M. Cacanindin, "Fire Safety and Alert System Using Arduino Sensors with IoT Integration," ICSCA, 2018.
[13] Dakhi, Herlina and Rini, "Sistem Pemantau Ruang Jarak Jauh Menggunakan Sensor PIR (Passive Infrared) Berbasis Atmega 8535," Repositori Institusi USU, pp. 5-7, 2017.
[14] J.Chandramohan, R.Nagarajan, K.Satheeshkumar, N.Ajithkumar, P.A.Gopinath and S.Ranjithkumar, "Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi," International Journal Of Engineering And Computer Science, vol. 6, no. 3, 2015.
[15] D. Herdiwijaya, "Pengukuran Kecerahan Langit Malam arah Zenith untuk Penentuan Awal," pp. 95-102, 2016.