RFID BASED SECURED TRANSFORMER CONTROL SYSTEM

PROJECT REPORT

submitted by

DINESHKUMAR P	**422520106011**
JAYASURIYA S	**422520106017**
KESAVAN V	**422520106024**
SARATHY D	**422520106036**

In partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING IN

ELECTRONICS AND COMMUNICATION ENGINEERING

UNIVERSITY COLLEGE OF ENGINEERING VILLUPURAM

ANNA UNIVERSITY:: CHENNAI 600025

MAY 2024

BONAFIDE CERTIFICATE

Certified that this project report "**RFID BASED SECURED TRANSFORMER CONTROL SYSTEM**" is the bonafide work of **DINESHKUMAR P** (422520106011), **JAYASURIYA S** (422520106017)**, KESAVAN V** (422520106024), **SARATHY D (**422520106036) who carried out the project under my supervision.

SIGNATURE	**SIGNATURE**
Dr.M.PHEMINA SELVI,	Dr.R.THAMARAISELVI,
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Department of Electronics and	Department of Electronics and
Communication Engineering	Communication Engineering
University College of Engineering	University College of Engineering
Villupuram.	Villupuram.

Submitted for Project Viva Examination held at University College of Engineering Villupuram on ……

INTERNAL EXAMINER	**EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We have completed the project successfully, due to the valuable guidance of certain outstanding persons. They have helped us to realize this achievement and hereby we express our gratitude to them.

We wish to express our sincere thanks and gratitude to our Dean **Dr.R.SENTHIL** for offering us all the facilities to do the project.

We also express our sincere thanks to Head of the Department **Dr.M.PHEMINA SELVI** Department of Electronics and Communication for his support and guidance to do this project work.

We express our heartfelt gratitude to our guide **Dr.R.THAMARAISELVI** her priceless guidance and motivation which helped us to bring this project to a perfect shape. And we thank to **Dr.M.PHEMINA SELVI** our internal project guide and Project Coordinator, Department of Electronics and Communication who encouraged us in each and every step of this project to complete it successfully

We would like to thank all the faculty members in our department for their guidance to finish this project successfully. We also like to thank all our friends for their willing assistance.

This project consumed huge amount of work, research, and dedication. Still, implementation would not have been possible if we did not have a support of many individuals and organizations. We would like to extend our sincere gratitude to all of them.

DECLARATION

We hereby declare that the work entitled **" RFID BASED SECURED TRANSFORMER CONTROL SYSTEM "** submitted in partial fulfilment of the requirement for the award of the degree in B.E., University College of Engineering - Villupuram, Anna University, Villupuram is a record of our work carried out by us during the academic year 2023- 2024 under the supervision of **Dr.R.THAMARAISELVI,** Department of Electronics and Communication Engineering, University College of Engineering, Anna University, Villupuram. The extent and source of information are derived from the existing literature and have been indicated through the dissertation at the appropriate places. The matter embodied in this work is original and has not been submitted for the award of any other degree or diploma, either in this or any other university.

(Signature of the Candidate)	(Signature of the Candidate)	(Signature of the Candidate)	(Signature of candidate)
Dineshkumar P	Jayasuriya S	Kesavan V	Sarathi V

I certify that the declaration made by the above candidate is true.

(Signature of the Guide)

Dr.R.THAMARAISELVI,

Teaching Fellow,

Department of Electronics and Communication Engineering,

University College of Engineering, Villupuram,

ABSTRACT

This project focuses on the safety of the lineman while working so they do not feel the sudden electric shock. As a lineman must deal with live wires very often, the chances of critical accidents are already very high. However, with the right amount of coordination among lineman and substation, a lot of these accidents can be avoided. The project aimed at providing the solution that ensures the safety of maintenance staff. Hence to avoid this we are implementing a password-based circuit breaker. Our system reads the lineman RFID tag information with help of RFID reader and then this system generates passwords and a relay switch to turn ON or OFF the circuit breaker using GSM module. OTP plays a major role in this system. The one time passwords mean the generated passwords are different at each time. These passwords provide total control to the system to turn on or off the supply to each line. The maintenance staff e.g. line man has the control to turn ON/OFF the line, because the line man has to put a request to the system to its working. If there is a problem in any particular section of the supply line, then staff wants to turn off that line and repair it. For that the system generates a onetime password and sends it to his phone. Using a matrix keypad, he can enter it in the system. Then the system compares entered password with the generated password. If the passwords are matched, then the supply to that line will be made OFF and the password is expired. No w he can repair the line more safely and after it is over he can turn on that line by u sing another password. This ensures security of the worker because no one can turn on the line without his permission. The activation or deactivation of the circuit breaker is indicating by a lamp (ON/OFF).

Keywords: Lineman, Security, OTP, Microcontroller, GSM module, RFID Tag , RFID Reader

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	**iv**
	LIST OF FIGURES	**v**
	LIST OF TABLES	x
1	**INTRODUCTION**	
	1.1 OVERVIEW	01
	1.1.1 Project Aim	02
	1.1.2 Importance	02
	1.1.3 Approach	02
	1.2 CHALLENGES	03
	1.2.1 Integration and Compatibility	03
	1.2.2 Regulatory Compliance	03
	1.2.3 Emergency Protocols	03
	1.2.4 Data Privacy	03
	1.3 PROBLEM STATEMENT	04
2	**LITERATURE SURVEY**	
	2.1 OVERVIEW OF THE PROJECT	05
	2.2 RELATED WORK	05
	2.3 SUMMARY OF THE LITERATURE SURVEY	05
3	**SYSTEM DESIGN**	
	3.1 Existing System	11
	3.1.1Disadvantages	11
	3.2 Proposed System	11
	3.2.1 Block diagram of Proposed system	13

3.2.2 Flow chart of proposed system 14

3.2.3 Advantages of proposed system 14

4 HARDWARE DESCRIPTION

4.1 POWER SUPPLY 15

4.1.1 Linear Power Supply 15

4.1.2 Transformer 16

4.1.3 Rectifier 18

4.2 RFID TAG 19

4.2.1 Active RFID Tag 20

4.2.2 Passive RFID Tag 22

4.3 RFID READ ER 23

4.3.1 Principle of Operation 23

4.3.2 Weigand Output Format Description 24

4.4 ARDUINO CONTROLLER 25

4.4.1 Introduction 25

4.4.2 History of Arduino 26

4.4.3 Hardware of Arduino controller 27

4.4.4 Power supply 29

4.4.5 PIN Diagram of Arduino 31

4.4.6 ATMEGA 328P 32

4.4.7 Architecture of ATMEGA328P 33

4.4.8 PIN diagram of ATMEGA328P 34

4.5 RELAY DRIVER 36
4.5.1 Relay Driver using Single Transistor 37
4.6 RELAYS 38
4.6.1 Electromagnetic relay working 38
4.7 LAMP LOAD 39
4.8 GSM MODULE 42
4.8.1 GSM Carrier Frequency 43
4.8.2 Voice Codecs 43
4.8.3 Network Structure 44
4.8.4 Subscriber Identity Module 44
4.8.5 Phone Locking 45
4.8.6 GSM Service Security 45
4.8.7 GSM Modem 47
4.9 LCD DISPLAY 50
4.9.1 Introduction 50
4.9.2 Types 50
4.9.3 Construction 51
4.9.4 Working 52
4.9.5 PIN Description 54
4.9.6 Registers 55
4.9.7 LCD Interfacing 56
4.9.8 Advantages 56
4.9.9 Disadvantages 57
4.9.10 Applications 57

	4.10 KEYPAD	57
	4.11 NODEMCU V3	58
	4.11.1 Introduction	59
	4.11.2 NodeMCU V3 PINout	60
5	**SOFTWARE DESCRIPTION**	
	5.1 Arduino IDE introduction	62
	5.2Features	63
	5.3 Arduino Software (IDE)	64
	5.4 Proteus 8 Professional	65
6	**RESULT AND OUTPUT**	
	6.1 RESULT AND DISCUSSION	71
7	**CONCLUSION AND FUTURE SCOPE**	
	7.1 FUTURE ENHANCEMENT	75
	7.2 CONCLUSION	75
	REFERENCES	76
	APPENDIX	77

LIST OF FIGURES

FIG NO	TITLE	PAGE NO
3.1	Block Diagram of Proposed System	13
3.2	Flow Chart of Proposed System	14
4.1	Block Diagram of Power Supply	16
4.2	Transformer	17
4.3	Step-Down Transformer	17
4.4	Rectifier	18
4.5	Bridge Rectifier	19
4.6	Single Diode Rectifier	19
4.7	RFID Tag	20
4.8	RFID Reader	23
4.9	Weigand Output Format Description	25
4.10	Hardware of Arduino controller	27
4.11	circuit diagram of Power supply	29
4.12	Block diagram of Power supply	30
4.13	PIN Diagram of Arduino	31
4.14	ATMEGA328P	32
4.15	Architecture of Atmega328P	33
4.16	Pin Diagram of ATMEGA328P	34
4.17	Relay Driver	37
4.18	Relay Driver Using Single Transistor	37

4.19	Relay module	39
4.20	GSM Module	50
4.21	LCD Display	54
4.22	LCD Interfacing	56
4.23	Keypad	57
4.24	NodeMCU V3	58
4.25	NodeMCU V3 PINout	60
5.1	Arduino IDE	64
5.2	Circuit design using components	67
5.3	Initial stage of simulation running process	68
5.4	OTP generation and sending process	69
5.5	Turning ON Transformer after entering Correct password	70
6.1	Initial Stage	71
6.2	After Scanning the RFID Tag	72
6.3	Turn ON Stage of Transformer	72
6.4	Turn OFF stage of Transformer	74

LIST OF TABLE TABLE

TABLE NO.	TITLE	PAGE NO
4.1	Details of PIN diagram	35
4.2	Key parameters of ATMEGA328P	36
4.3	PIN Description for LCD	54

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Security is the prime concern in our day-to-day life. Everyone needs to be securing as much as possible. The electric lineman safety system is designed to control a circuit breaker by using a password for the safety of electric man. Critical electrical accidents to line men are on the rise during electric line repair due to lack of communication and co-ordination between the maintenance staff and electric substation staff. This proposed system provides a solution that ensures safety of maintenance staff, i.e., line man. The control to turn on or off the line will be maintained by the line man only because this system has an arrangement such that a password is required to operate the circuit breaker (on/off).

The system is fully controlled by a microcontroller from Arduino family. A matrix keypad is interfaced to the microcontroller to enter the password. The entered password is compared with the password generated. If the password entered is correct, only then the line can be turned ON/OFF. To repair a particular section of the electric supply line, the lineman wants to turn off the supply to that line. Again he has to do the same process to the system. Then the system responds to him using the LCD display to enter the password.

The electric lineman safety system is designed to enhance the security of maintenance staff, particularly linemen, by implementing a password-based circuit breaker. This system, controlled by a microcontroller from the Arduino family, requires a password to operate the circuit breaker, ensuring only authorized personnel can turn on or off the supply to each line. By using a matrix keypad to enter the password, staff members can safely repair sections of the electric supply line, as the system generates a unique one-time password for each request. The proposed system also utilizes RFID technology and a GSM

module to further enhance security, providing linemen with total control over the circuit breaker while preventing unauthorized access. Activation or deactivation of the circuit breaker is indicated by a lamp, simplifying monitoring. Overall, this project aims to prevent critical accidents and ensure the safety of maintenance staff working with live wires.The system generates a password and it will be sent to the phone number which is stored in the program.

Overall, this project provides a solution that ensures the safety of maintenance staff by giving them total control to turn on or off the supply to each line while preventing unauthorized personnel from accessing the circuit breaker.

1.1.1 Project Aim

The primary objective of the project is to improve the safety measures for electric linemen working with live wires. By implementing a password-based circuit breaker system, the project aims to empower linemen with total control over the electric lines they are repairing, thereby minimizing the occurrence of accidents and ensuring their safety.

1.1.2 Importance

Electric linemen face considerable risks while conducting repairs on live wires. Accidents due to lack of communication and coordination between maintenance and substation staff are on the rise. Therefore, it is crucial to implement systems like the proposed password-based circuit breaker to enhance safety measures, safeguarding the lives of maintenance staff, particularly linemen.

1.1.3 Approach

The project utilizes RFID technology and a GSM module to generate unique one-time passwords for activating or deactivating electric lines. Linemen initiate the process by requesting access to the system. Upon receiving the request, the system generates a password and sends it to the lineman's

phone. The lineman then enters the password using a matrix keypad. If the entered password matches the generated one, the circuit breaker is activated or deactivated accordingly.

1.2 CHALLENGES

1.2.1 Integration and Compatibility

Ensure seamless integration of the RFID technology and GSM module with the microcontroller. Compatibility issues may arise between different components, so thorough testing and debugging are necessary.

1.2.2 Regulatory Compliance

Ensure that the system complies with relevant safety standards and regulations in the electrical industry. This may involve certification processes and adherence to specific guidelines for equipment used in electrical installations.

1.2.3 Emergency Protocols

Develop protocols for handling emergencies, such as power outages or system failures, to ensure the safety of both linemen and the public. Consider backup mechanisms for manual intervention in case of system malfunction.

1.2.4 Data Privacy

Address concerns regarding the collection, storage, and transmission of personal data, such as phone numbers associated with staff members. Implement robust data protection measures to safeguard sensitive information.

1.3 PROBLEM STATEMENT

The critical issue addressed by this project is the rising number of accidents involving electric linemen during repairs due to inadequate safety measures and lack of coordination between maintenance and substation staff. The project aims to mitigate this problem by providing linemen with exclusive control over electric lines through a password-based circuit breaker system, thereby enhancing their safety and preventing unauthorized access to the circuit breaker.

.

CHAPTER 2

LITERATURE SURVEY

2.1 OVERVIEW OF THE PROJECT

This project aims to improve lineman safety by implementing a password-controlled circuit breaker system. Linemen face a significant risk of electrical accidents due to miscommunication and lack of coordination during repairs. This system addresses this concern by requiring authorized personnel to use a password to turn the power on or off for maintenance work. The proposed approach utilizes RFID technology and a GSM module for enhanced security. When a lineman needs to work on a specific section, they request access through the system. The system then generates a unique one-time password (OTP) that is sent via SMS to the lineman's phone for verification. Only if the entered OTP matches the generated password does the circuit breaker activate or deactivate. This approach eliminates the security risks associated with static passwords and ensures only authorized personnel can control the power supply. Additionally, a lamp provides real-time status indication of the circuit breaker. Overall, this project offers a secure and reliable solution to improve lineman safety by preventing unauthorized access and accidental energization during power line maintenance.

2.2 RELATED WORK

Smith J, Johnson T et al.[1] "RFID-Based Secure Transformer Control System for Smart Grid Applications" - IEEE Transactions on Power Systems, 2023. This paper proposes a secure transformer control system utilizing RFID technology for smart grid applications. The system integrates RFID tags with transformer monitoring devices to enhance security and control measures within the power grid infrastructure. The authors demonstrate the effectiveness of the system through experimental validation in real-world grid environments.

Gupta A, Patel R et al.[2] "Enhanced Security Framework for Power Transformer Monitoring using RFID Technology" - International Journal of Electrical Power & Energy Systems, 2022.

This study presents an enhanced security framework for power transformer monitoring leveraging RFID technology. The framework incorporates advanced encryption techniques and authentication mechanisms to ensure data integrity and confidentiality in transformer control systems. Experimental results demonstrate the feasibility and effectiveness of the proposed framework in real-world scenarios.

Chen L, Wang Y et al.[3] "RFID-Based Secure Control System for Distribution Transformers in Smart Grid" - IEEE Access, 2021.

In this research, a RFID-based secure control system is proposed for distribution transformers in smart grid environments. The system utilizes RFID tags for device authentication and access control, enhancing the security of transformer control operations. The authors evaluate the performance of the system through simulation studies and practical implementations, highlighting its effectiveness in mitigating potential security threats.

Parveen Taj et al. [4]“Linemen Safety and Power line Broken Detection System” 2020 The proposed system ensures lineman safety by requiring a password for accessing control panel doors and circuit breakers. Linemen request and receive a secure password from the control room via GSM, entered through a keypad connected to an Arduino Uno. Unauthorized attempts trigger alerts to the control room after three incorrect entries, enhancing system security**.**

Kumar S, Sharma P et al. [5] "Design and Implementation of RFID-Based Secure Transformer Monitoring System" - International Conference on Power Systems, 2020. This paper presents the design and implementation of an RFID-based secure transformer monitoring system. The system integrates RFID technology with advanced monitoring sensors to provide real-time data on transformer performance and security status. Experimental results demonstrate the feasibility and reliability of the system in detecting and mitigating security breaches in transformer control environments.

Praveen et al [6] "Electric Line Man Safety using Android based Circuit Breaker" – IJRTER, 2019. They have used QR code as a password based circuit breaker to control the powerlines. When the electric linemen spotting the fault in the power transmission system then he power lines can be switched OFF by scanning the QR code with the help of Android APP. The APP check the password 1 and send password 2 to the microcontroller through Bluetooth. Then the microcontroller verifies the password 2 and opens out the relay to switch OFF the powerline. The linemen can rescan the same QR code to switch ON the powerline.

Wang X, Li M et al.[7] "Secure Transformer Control System Based on RFID and Blockchain Technology" - IEEE Transactions on Industrial Informatics, 2019. This research proposes a secure transformer control system based on RFID and blockchain technology. The system utilizes RFID tags for device identification and blockchain for secure data recording and transaction validation. Experimental results.

Rajesh Kumar, Singh A, et al.[8] "Enhancing Lineman Safety in Transformer Control Systems Using RFID Technology" - IEEE Transactions on Power Delivery, 2019.

This paper presents a solution for enhancing lineman safety in transformer control systems by employing RFID technology. The system restricts access to control panels and circuit breakers, ensuring that only authorized personnel can operate them using RFID authentication. Linemen receive unique RFID tags to enable access, minimizing the risk of unauthorized operation and potential accidents.

Jain A, Sharma S et al[9]"RFID-Based Secure Transformer Control System for Lineman Safety" - International Journal of Electrical Engineering, 2019. This paper presents a RFID-based secure transformer control system designed to ensure lineman safety during maintenance operations. The system utilizes RFID technology for authentication and access control, allowing only authorized personnel to operate the transformer. Linemen receive dynamic passwords via SMS through GSM modem integration, enhancing security measures and minimizing potential hazards.

Reddy V, Kumar A et al[10] "Enhanced Lineman Safety in Power Grids Using RFID-Based Transformer Control Systems" - IEEE Transactions on Power Systems, 2018. In this study, an enhanced lineman safety system is proposed for power grids, leveraging RFID-based transformer control systems. The system employs RFID tags for authentication and access management, with passwords dynamically generated and transmitted to linemen via SMS for operation. Experimental validation demonstrates the effectiveness of the system in minimizing risks and ensuring lineman safety.

Zhang H, Liu Q et al.[11] "RFID-Based Secure Control and Monitoring System for Power Transformers in Smart Grid" - IEEE Transactions on Smart Grid, 2018. In this study, a RFID-based secure control and monitoring system for power transformers in smart grid environments is proposed. The system integrates RFID technology with advanced monitoring algorithms to detect and mitigate security threats in transformer control operations.

Experimental results demonstrate the effectiveness of the system in enhancing the security and reliability of power grid infrastructure.

Sowmiya M, Siberian R.S et al.[12] "Security and Monitoring System by using RFID Tags and multiple sensors" - IEEE, 2017. This paper introduces a security and monitoring system utilizing RFID tags and multiple sensors for various applications including transformer control. The system employs RFID technology along with gas sensors, weight sensors, and RFID readers to detect and mitigate potential security threats in transformer control operations. Experimental results demonstrate the effectiveness of the system in ensuring the security and reliability of power grid infrastructure.

Pramod McMurray et al[13] “Electric Line Man Safety with Password Based Circuit Breaker and Intimation of HT Wire Sag using GSM” - 2017.The breaker system, governed by an 8051 microcontroller, prioritizes worker safety through password-protected operation. Password flexibility, stored in EEPROM, enables dynamic adjustments. Keypad inputs activate relays for breaker control, while LED indicators convey operational status and unauthorized access attempts, ensuring robust security measures.

Singh N, Gupta R et al.[14] "RFID-Based Transformer Control System for Ensuring Lineman Safety in Indian Electrical Networks" - Journal of Power Systems, 2016. This paper introduces a RFID-based transformer control system aimed at ensuring lineman safety in Indian electrical networks. The system employs RFID tags for authentication and access control, with dynamic password generation and transmission via GSM modem to authorized personnel. Experimental results demonstrate the efficacy of the system in mitigating hazards and enhancing worker safety.

Sharma V, Mishra S et al.[15] "Secure Transformer Control System for Lineman Safety in Indian Power Infrastructure" - International Journal of Electrical Engineering and Technology, 2015.In this study, a secure

transformer control system is proposed to ensure lineman safety in Indian power infrastructure. The system utilizes RFID technology for authentication and access management, with dynamic password distribution via GSM modem integration. Evaluation of the system's performance demonstrates its effectiveness in minimizing risks and enhancing worker safety in power grid environments.

2.3 SUMMARY OF THE LITERATURE SURVEY

The literature survey conducted for this report encompasses a comprehensive exploration of various technological solutions aimed at enhancing lineman safety in power grid environments. The primary focus revolves around implementing secure control systems for transformer monitoring and power line maintenance. These systems predominantly utilize RFID technology coupled with GSM modules to ensure authentication, access control, and dynamic password generation. Additionally, advanced encryption techniques and authentication mechanisms are integrated to uphold data integrity and confidentiality. From QR code-based circuit breakers to blockchain-enabled secure data recording, a multitude of innovative approaches are examined, all with the overarching goal of mitigating security threats and safeguarding lineman during maintenance operations. Through experimental validations and practical implementations, these studies underscore the efficacy of technological interventions in fortifying power grid infrastructure, ultimately contributing to the overarching objective of improved lineman safety.

CHAPTER 3

SYSTEM DESIGN

3.1 EXISTING SYSTEM

- Circuit breakers play a vital role in maintaining system security. Since their malfunctioning could results in further component outages and may lead to the insecure operating conditions.
- During maintenance of distribution lines there is a chance of communication gap between the electric line and sub-station operator or staff.
- This communication gap may risk life of electric line man.
- The control to turn ON/OFF the line lies with the line man only. During maintenance the entire line is turned off this cause inconvenience to the consumers.

3.1.1 Disadvantages of Existing System

- During maintenance the entire line is turned off this cause inconvenience to the consumers.
- Improper communication between maintenance staff and substation causes the electrical accidents.

3.2 PROPOSED SYSTEM

- The electric line man safety system provides a control to turn on or off the line and thereby ensures the safety of the staff. It consists of only an embedded section. The major component is a micro controller from PIC family.
- This system is designed for line man to avoiding accidents.

- The authorized person should show the ID proof in RFID reader. when ID proof is scanned then OTP will be sent to mobile though mobile using GSM module.
- Arduino is used to control and monitor the entire system.
- Then that authorized person should enter that OTP in keypad. That will be displayed in LCD Then the load will be turned off /on through driver relay.
- This ensures security of the worker because no one can turn on the line without his permission.
- Separate OTP will be send during load ON and OFF.

Based on the program done in the microcontroller a relay switches to turn on or off the circuit breaker. The system comprised of a RFID READER & TAG, GSM module, LCD display, buzzer, matrix keypad, and a relay. The main attraction of this project is the OTP generation. The generated passwords will be different at each time and after the use of this password it will be expired. From the AVR family ATmega328 microcontroller is used. It is an 8-bit micro- controller with 32KB memory. Normally the supply to the line is always on and it is indicated by using a lamp which is always on. If there is any problem in any section of the supply line, then the line man wants to turn off the supply to that section and repair it.

The LCD display provided along with the system gives visual Assistance of “LINE MAN SAFETY SYSTEM WITH OTP GENERATION” for easy operation of the system. The first lineman should scan their ID card (RFID TAG) using RFID reader and our system batches with database. Then the system generates a 4-bit length onetime password.

And also gives an indication of “OTPGENERATED”. Then it will be send to his phone (the number of which is stored in the program) gives an indication of “OTP SEND” and “ENTER OTP”.

3.2.1 Block Diagram of Proposed System

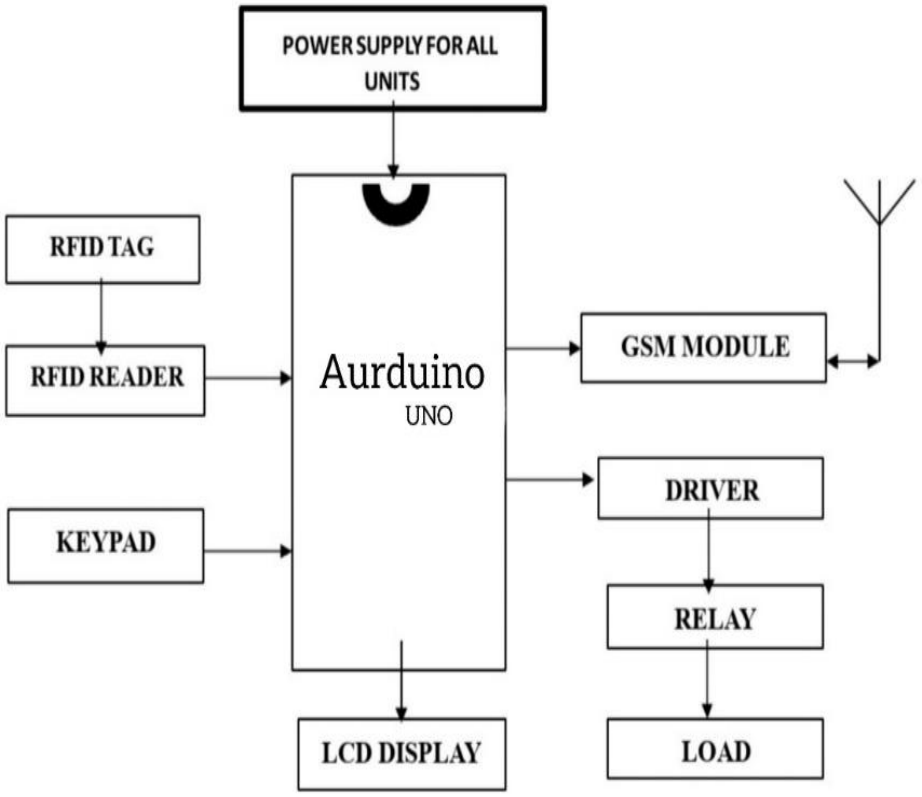


Figure 3.1 Block Diagram of the Proposed System

After enter it using the keypad, it will be compared with the generated password (which is stored in the ROM). If the passwords are matched, then the LCD displays “OTP MATCHED” and turn off the supply to the line i.e, the lamp will be turned off. Therefore, the line man can safely work on the line and repair it. When repair is over, he will reach the substation and again put a request to turn on the supply by RFID tag. Then system generates another password and using it he can turn on the line.

If the passwords are not matched up to or more than three times, an alarm will be activates. The GSM modem provides the communication between the system and the line man. The number of the phone in to which the OTP is send is stored in the program. This number may be either of the sub engineer's number or of the line man's number. It is possible to send the number to more people. But it will be based on the security only. It is also possible to use each password for a particular line. And also wireless communication can also use depends on the distance.

3.2.2 Flow Chart of Proposed System

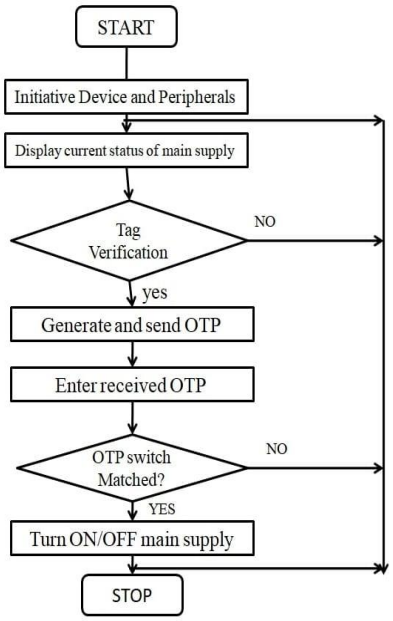


Figure 3.2 Flow Chart of the Proposed System

3.2.3 Advantages of Proposed System

- Save the life of line man and avoids accidental death in the transmission line
- User friendly operation of main line.
- Easy to install and operate.
- Cost effective.
- Easy to maintain and repair.

CHAPTER 4

HARDWARE DESCRIPTION

4.1 POWER SUPPLY

Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others. Power supplies for electronic devices can be broadly divided into linear and switching power supplies. The linear supply is a relatively simple design that becomes increasingly bulky and heavy for high current devices; voltage regulation in a linear supply can result in low efficiency. A switched-mode supply of the same rating as a linear supply will be smaller, is usually more efficient, but will be more complex.

4.1.1 Linear Power Supply

An AC powered linear power supply usually uses a transformer to convert the voltage from the wall outlet (mains) to a different, usually a lower voltage. If it is used to produce DC, a rectifier is used. A capacitor is used to smooth the pulsating current from the rectifier. Some small periodic deviations from smooth direct current will remain, which is known as ripple. These pulsations occur at a frequency related to the AC power frequency (for example, a multiple of 50 or 60 Hz).

The voltage produced by an unregulated power supply will vary depending on the load and on variations in the AC supply voltage. For critical electronics applications a linear regulator will be used to stabilize and adjust the voltage.

This regulator will also greatly reduce the ripple and noise in the output direct current. Linear regulators often provide current limiting, protecting the power supply and attached circuit from over current.

Adjustable linear power supplies are common laboratory and service shop test equipment, allowing the output voltage to be set over a wide range. For example, a bench power supply used by circuit designers may be adjustable up to 30 volts and up to 5 amperes output. Some can be driven by an external signal, for example, for applications requiring a pulsed output.

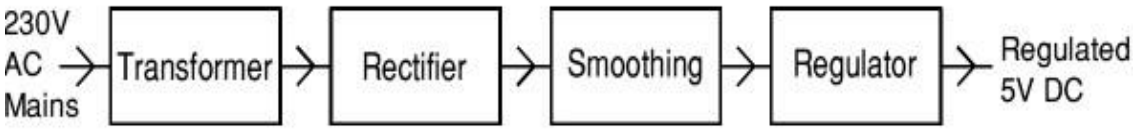


Figure 4.1 Block Diagram of a Regulated Power Supply System

4.1.2 Transformer

Transformers convert AC electricity from one voltage to another with little loss of power. Transformers work only with AC and this is one of the reasons why mains electricity is AC.

Step-up transformers increase voltage, step-down transformers reduce voltage. Most power supplies use a step-down transformer to reduce the dangerously high mains voltage (230V in UK) to a safer low voltage.

The input coil is called the primary and the output coil is called the secondary. There is no electrical connection between the two coils; instead they are linked by an alternating magnetic field created in the soft-iron core of the transformer. The two lines in the middle of the circuit symbol represent the core.

Transformers waste very little power so the power out is (almost) equal to the power in. Note that as voltage is stepped down current is stepped up.

The ratio of the number of turns on each coil, called the turn's ratio, determines the ratio of the voltages. A step-down transformer has a large number of turns on its primary (input) coil which is connected to the high voltage mains supply, and a small number of turns on its secondary (output) coil to give a low output voltage.

Turns ratio=Vp/Vs=Nn/Ns and Power out=Power in

Vs*Is=Vp * Ip

Vp = primary (input) voltage

Vs = secondary (output) voltage

Np = number of turns on primary coil

Ns = number of turns on secondary coil

Ip = primary (input) current

Is = secondary (output) current

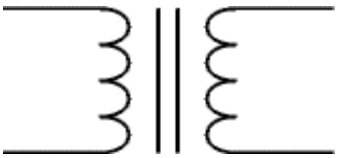


Figure 4.2 Transformer

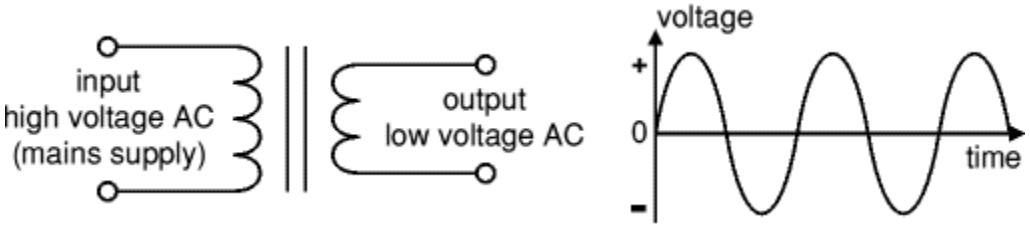


Figure 4.3 Step-Down Transformer and its Output

The low voltage AC output is suitable for lamps, heaters and special AC motors. It is not suitable for electronic circuits unless they include a rectifier.

4.1.3 Rectifier

There are several ways of connecting diodes to make a rectifier to convert AC to DC. The bridge rectifier is the most important and it produces full-wave varying DC. A full-wave rectifier can also be made from just two diodes if a Centre-tap transformer is used, but this method is rarely used now that diodes are cheaper. A single diode can be used as a rectifier but it only uses the positive (+) parts of the AC wave to produce half-wave varying DC.

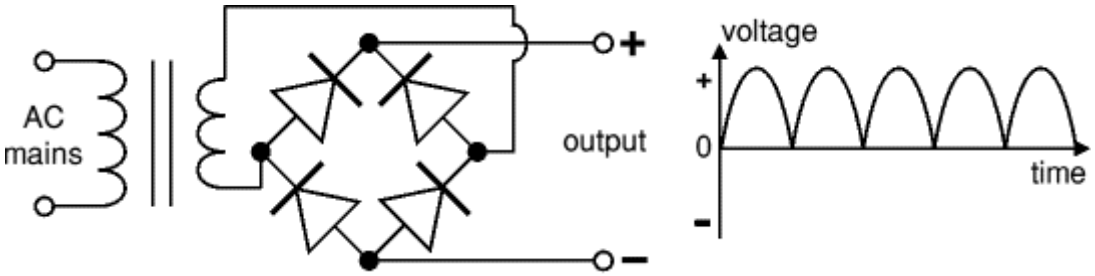


Figure 4.4 Rectifier and its Output

The varying DC output is suitable for lamps, heaters and standard motors. It is not suitable for electronic circuits unless they include a smoothing capacitor.

[a] Bridge Rectifier

A bridge rectifier can be made using four individual diodes, but it is also available in special packages containing the four diodes required. It is called a full-wave rectifier because it uses the entire AC wave (both positive and negative sections). 1.4V is used up in the bridge rectifier because each diode uses 0.7V when conducting and there are always two diodes conducting.

Bridge rectifiers are rated by the maximum current they can pass and the maximum reverse voltage they can withstand (this must be at least three times the supply RMS voltage so the rectifier can withstand the peak voltages).

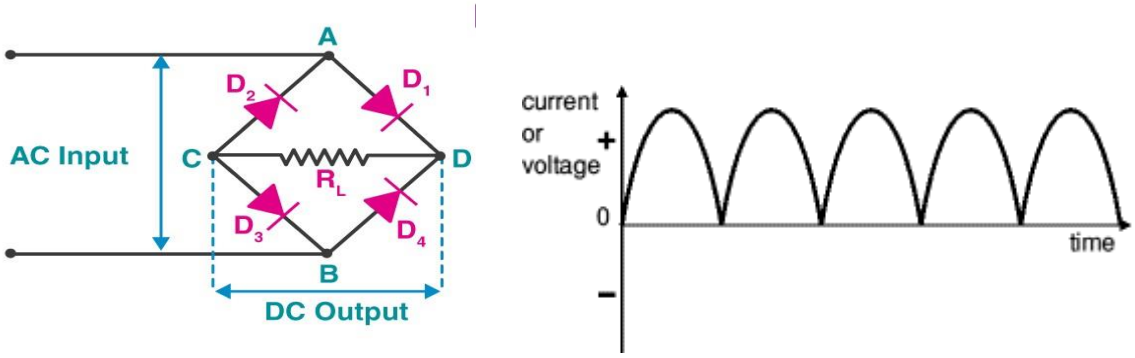


Figure 4.5 Bridge Rectifier and its Output

Alternate pairs of diodes conduct, changing over the connections so the alternating directions of AC are converted to the one direction of DC**.**

[b] Single-Diode Rectifier

A single diode can be used as a rectifier but this produces half-wave varying DC which has gaps when the AC is negative. It is hard to smooth this sufficiently well to supply electronic circuits unless they require a very small current so the smoothing capacitor does not significantly discharge during the gaps. Please see the Diodes page for some examples of rectifier diodes.

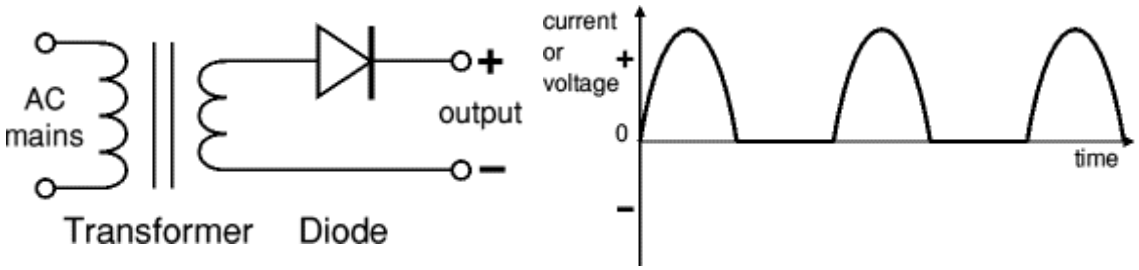


Figure 4.6 Single Diode Rectifier and its Output

4.2 RFID TAG

An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification. The

tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information).RFID tags can be very small - the size of a large rice grain. Others may be the size of a small paperback book.

Figure 4.7 RFID Tag

4.2.1 Active RFID Tag (Active Tag)

An RFID tag is an active tag when it is equipped with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna. Some active tags contain replaceable batteries for years of use; others are sealed units. (Note that It is also possible to connect the tag to an external power source.)

Advantages of active RFID tags

- Problems and Disadvantages with active RFID tags
- Features of active RFID tags

The major advantages of an active RFID tag are:

- It can be read at distances of one hundred feet or more, greatly improving the utility of the device
- It may have other sensors that can use electricity for power.

The problems and disadvantages of an active RFID tag are:

- The tag cannot function without battery power, which limits the lifetime of the tag.
- The tag is typically more expensive, often costing $20 or more each
- The tag is physically larger, which may limit applications.
- The long-term maintenance costs for an active RFID tag can be greater than those of a passive tag if the batteries are replaced.
- Battery outages in an active tag can result in expensive misreads.

Active RFID tags may have all or some of the following features:

- Longest communication range of any tag.
- The capability to perform independent monitoring and control.
- The capability of initiating communications.
- The capability of performing diagnostics.
- The highest data bandwidth.
- Active RFID tags may even be equipped with autonomous networking; the tags autonomously determine the best communication path.

4.2.2 Passive RFID Tag (Passive Tag)

A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory.

The major disadvantages of a passive tag are:

- The tag can be read only at very short distances, typically a few feet at most.

This greatly limits the device for certain applications.

- It may not be possible to include sensors that can use electricity for power.
- The tag remains readable for a very long time, even after the product to which the tag is attached has been sold and is no longer being tracked.

The advantages of a passive tag are:

- The tag functions without a battery; these tags have a useful life of twenty years or more.
- The tag is typically much less expensive to manufacture

The tag is much smaller (some tags are the size of a grain of rice). These tags have almost unlimited applications in consumer goods and other areas.

4.3 RFID READER

An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. A few factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have an impact on the RFID system's read range.

Figure 4.8 RFID Reader

4.3.1 Principle of Operation

The reader generates a magnetic field through its integrated antenna at 125 kHz. Passive RFID transponders also have an integrated antenna that is tuned to the same frequency. When they are within range of the reader unit they are able to draw sufficient power from the electromagnetic field to power their own internal electronics. Once powered they can modulate the incident magnetic field which is detected by the reader. In this way the Transponders can transmit their data to the reader.

There are many different types of transponders designed to operate at various frequencies, and their functions and the amount of information they carry can also vary. In general operation the reader will continually scan for any transponders that come within range and transmit their data to the reader. As EM4100 compatible transponders do not have collision avoidance algorithms only one card can be scanned within the range of the reader at any one time. When a transponder is read the reader will decode and transmit the received data via ASCII coded serial output, or standard Weigand output for the Weigand version of the reader unit.

4.3.2 Weigand Output Format Description

When using the Weigand output version the reader will scan for a valid transponder. When a read occurs the unit will transmit 40 bits of user data contained in the transponder in standard Weigand protocol. The output lines for the Weigand output are the DATA0, and DATA1 lines as described in line interface. Weigand protocol provides 2 lines for data transfer. A pulsed transition on the DATA1 line indicates logic 1 bit, while a pulsed transition on the DATA0 line indicates a logic 0 bit.

In their idle state both lines are held high. During data transfer the appropriate logic line will pulse low for 50uS followed by a period of 2ms where both lines are held high. In this fashion each bit is transmitted in sequence until all 40 bits are sent. The end of the transmission is signal led by both lines being held high for more than 50mS. Figure shows an example of the timing sequence for Weigand protocol.

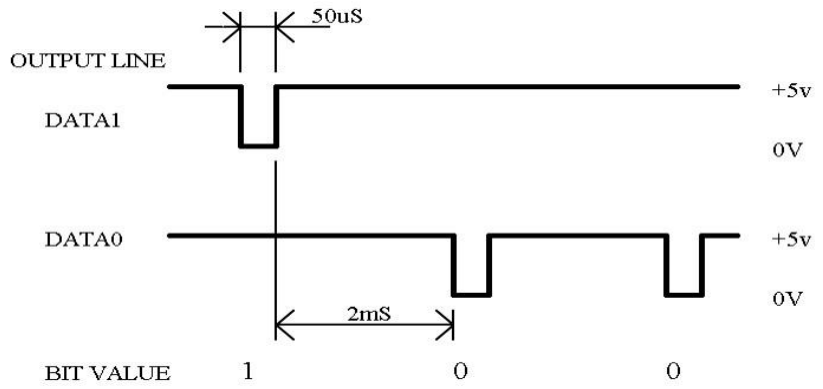


Figure 4.9 Weigand Output Format Description

4.4 ARDUINO CONTROLLER

4.4.1 Introduction

Arduino is a common term for a software company, project, and user community that designs and manufactures computer open-source hardware, open-source software, and microcontroller-based kits for building digital devices and interactive objects that can sense and control physical devices.

The project is based on microcontroller board designs, produced by several vendors, using various microcontrollers. These systems provide sets of digitals and analog I/O pins that can interface to various expansion boards (termed shields) and other circuits. The boards feature serial communication interfaces, including Universal Serial Bus (USB) on some models, for loading programs from personal computers. For programming the microcontrollers, the Arduino project provides an integrated development environment (IDE) based on a programming language named processing, which supports the languages C and C++.

The first Arduino was introduced in 2005,aiming to provide a low cost, easy way for novices and professionals to create devices the interact with their environment using sensors and actuators.

Common examples of such devices intended for beginner hobbyists include simple robots, thermostats, and motion detectors. Arduino boards are available commercially in preassembled form, or as do-it-yourself kits. The hardware design specifications are openly available, allowing the Arduino boards to be produced by anyone. Adafruit industries estimated in mid-2011 over 300,000 official Arduinos had been commercially produced, and in 2013, 700,000 official boards were in users' hands.

4.4.2 History Of Arduino

Colombian student Heman do Barragan created the development platform wiring as his Master's thesis project in 2004 at the Interaction Design Institute Ivrea in Ivrea, Italy. Massimo Banzi and Casey Reas (known for his work on processing) were supervisors for his thesis. The goal was to create low cost, simple tools for non-engineers to create digital projects.

The Wiring platform consisted of a hardware PCB with an ATmega128 microcontroller, an integrated development environment (IDE) based on processing and library functions to easily program the microcontroller. In 2005, Massimo Banzi, with David Mellis (then an IDII student) and David Cuartillas, added support for the cheaper ATmega8 microcontroller to Wiring. But instead of continuing the work on Wiring, they forked (or copied) the Wiring source code and started running it as a separate project, called Arduino

The Arduino's initial core team consist of Massimo Banzi David Cuartillas, Tom Igoe, Gianluca Martino, and David Mellis. The name Arduino comes from a bar in Ivrea, where some of the founders of the project used to meet. The bar was named after Arduino of Ivrea, who was the margrave of the March of Ivrea and King of Italy from 1002 to 1014. Following the completion of the Wiring platform, its lighter, lower cost versions were created and made available to the open-source community.

Associated researchers, including David Cuartillas, promoted the idea. Arduino's initial core team consisted of Massimo Banzi, David cuartillas, Tom Igoe, Gianluca Martino, and David Mellis.

4.4.3 Hardware Of Arduino Controller

Figure 4.10 Hardware of Arduino controller

An early Arduino board with an RS-232 serial communication interface (upper left) and an Atmel ATmega8 microcontroller chip (black, lower right); the 14 digital I/O pins are located at the top and the six analog input pins at the lower right. An Arduino board historically consists of an Atmel 8-, 16- and 32-bit AVR microcontroller (although since 2015 others makers' microcontrollers have been used) with complementary components that facilitate programming and incorporation into other circuits.

An important aspect of the Arduino is its standard connectors, which let users connect the CPU board to a variety of interchangeable add-on modules termed shields can be stacked and used in parallel. Before 2015, Official Arduino's had the Atmel meager series of chips, specifically the ATmega8, ATmega168, ATmega328, ATmega1280 and ATmega2560. In 2015, units by other produces were added. A handful of other processors have also been used by Arduino compatible devices.

Most boards include a 5V linear regulator and a 16 MHz crystal oscillator (or ceramic resonator in some variants), although some designs such as the Lilypad run at a 8 MHz and dispense with the onboard voltage regulator due to specific form-factor restrictions.

An Arduino's microcontroller is also pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory, compared with other devices that typically need an external programmer.

This makes using an Arduino more straightforward by allowing the use of an ordinary computer as the programmer. Currently, Opti boot loader is the default boot loader installed on Arduino UNO.

At a conceptual level, when using the Arduino integrated development environment, all boards are programmed over a serial connection. Its implementation varies with the hardware version. Some serial Arduino boards contain a level shifter circuit to convert between RS-232logic levels and transistor-transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header.

Other variants, such as the Arduino mini and the unofficial Boarding use a detachable USB-to-serial adapter board or cable, Bluetooth, or other methods, when used with traditional microcontroller tools instead of the Arduino IDE, standard AVR in-system programming (ISP) programming is used. The Arduino board exposes most of the microcontroller's I/O pins for use by other circuit. The Decimal(a), Demilune(b), and current Uno(c) provide 14 digital I/O pins, six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commonly available.

The Arduino Nano, and Arduino-compatible bare bones and boarding boards may provide male header pins on the underside of the board that can plug into solder less breadboards.

Many Arduino-compatible and Arduino-derived boards exist. Some are functionally equivalent to an Arduino and can be used interchangeably.

Many enhance the basic Arduino by adding output drivers, often for use in school-level education, to simplify making buggies and small robots.

Others are electrically equivalent but change the form factor, sometimes retaining compatibility with shields, sometimes not. Some variants use different processors, of varying compatibility.

4.4.4 Power Supply

A block diagram containing the parts of a typical power supply and the voltage at various points in the unit is shown. The AC voltage, typically 230V rms, is connected to a transformer, which steps that ac voltage down to the level for the desired DC output. A diode rectifier then provides a full-wave rectifier voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting DC voltage usually has some ripple or AC voltage variation.

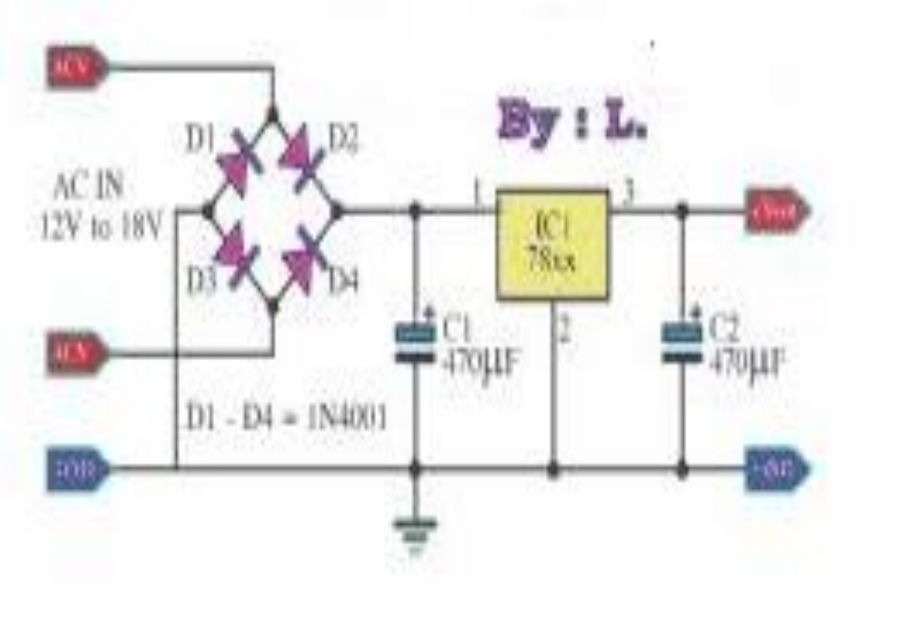


Figure 4.11 Circuit Diagram of Power Supply

Block Diagram

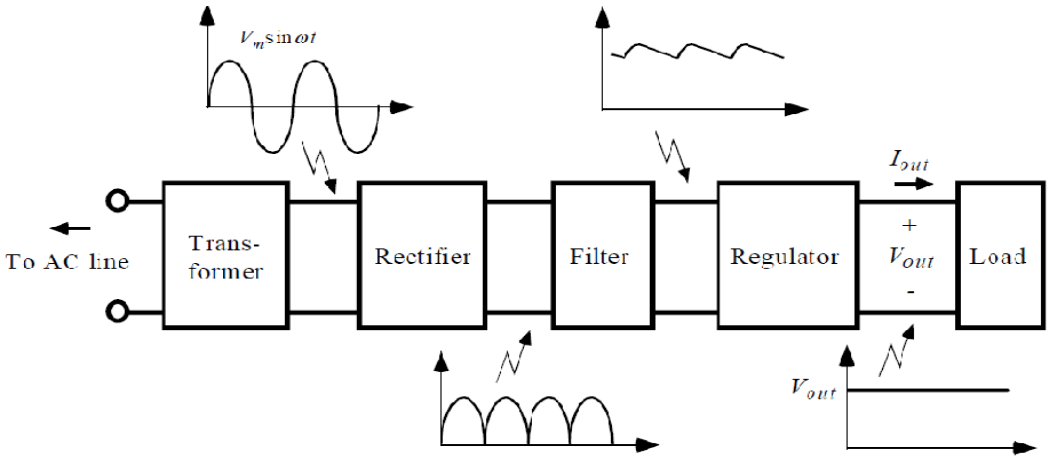


FIG 4.12 Block diagram of power supply

A regulator circuit can use this DC input to provide a DC voltage that not only has much less ripple voltage but also remains the same DC value even if the input DC voltage varies somewhat, or the load connected to the output DC voltage changes. This voltage regulation is usually obtained using one of several popular voltage regulator IC units.

(1) Transformer

A transformer is a static piece of which electric power in one circuit is transformed into electric power of the same frequency in another circuit. It can raise or lower the voltage in a circuit but with a corresponding decrease or increase in current. It works with the principles of mutual induction. In our project we are using a 12-0-12V center tapped step down transformer.

(2) Rectifier

A rectifier is an electrical device that converts alternating current (AC), which periodically reverse direction, to direct current (DC), current that flows in only one direction. A full-wave rectifier that whole of the input waveform to one of constant polarity (positive or negative) and its output.

We use single phase silicon bridge rectifier (BR1010) which has 4pins, two for input supply and two for output.

(3) Filter

The filtered waveform is essentially a DC voltage with negligible ripples, which is ultimately fed to the load.

(4) Regulator

The output voltage from the capacitor is more filtered and finally regulated. The regulator is a device, which maintains the output voltage constant irrespective of the change in supply variations, load variation and temperature changes. Here we use three fixed voltage regulators namely LM7812, LM7805 and LM7912. The IC7812 is a +12V regulator, IC7912 is a -12V regulator andIC7805 is a +5V regulator. For obtaining +10V and -10V, 5K potentiometer is being added across +12V and -12V supply.

4.4.5 PIN Diagram Of Arduino

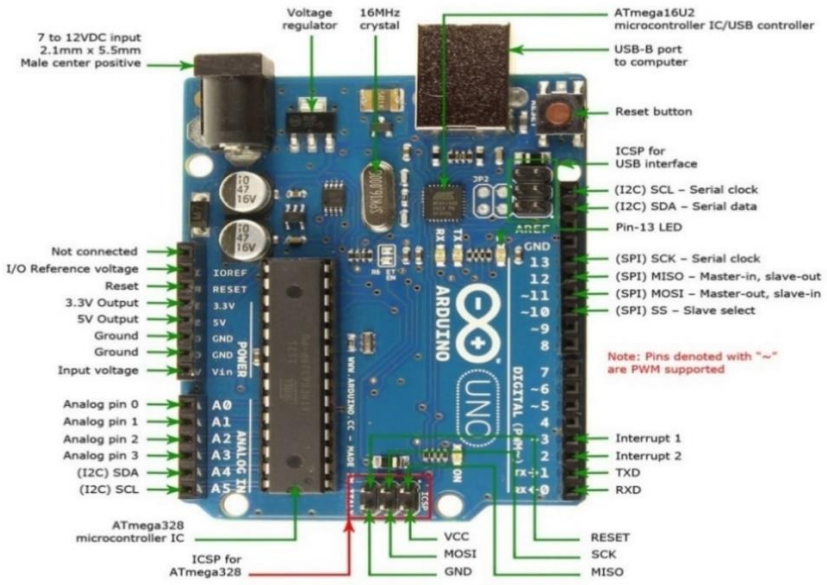


Figure 4.13 Pin Diagram of Arduino

Applications

- Oscillo, an open-source oscilloscope
- Scientific equipment such as the chemin

- Arduino me, a MIDI controller device that mimics the monomer
- Boudin, a trip computer that uses the on-board diagnostics interface found in most modern cars
- Ard pilot, drone software and hardware
- Arduino Phone, a do-it-yourself cellphone
- Get Duino, an Arduino mate for the Raspberry Pi
- Water quality testing platform
- Homemade CNC using Arduino and DC motors with close loop control by humifactions

4.4.6 ATMEGA328P

Today's microcontrollers are much different from what it were in the initial stage, and the number of manufactures are much more in count than it was a decade or two ago. At present some of the major manufactures are Microchip (PIC microcontrollers), Atmel (AVR microcontrollers), Hitachi, Phillips, Maxim, NXP, Intel, etc. ATmega328p belongs to Atmel's AVR series microcontroller family.

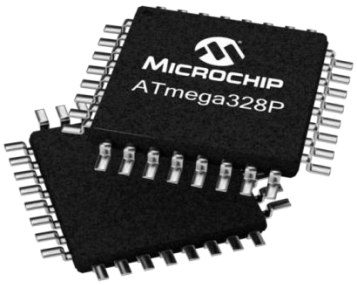


FIG 4.14 ATmega328P

Specifications Of ATMEGA328P

The Atmel 8-bit AVR RISC-based microcontroller combines 32KB ISP flash memory with read-while-write capabilities, 1KB EEPROM,2KB SRAM,23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5V. The device achieves throughputs approaching 1MIPS per MHz's

4.4.7 Architecture Of ATMEGA328P

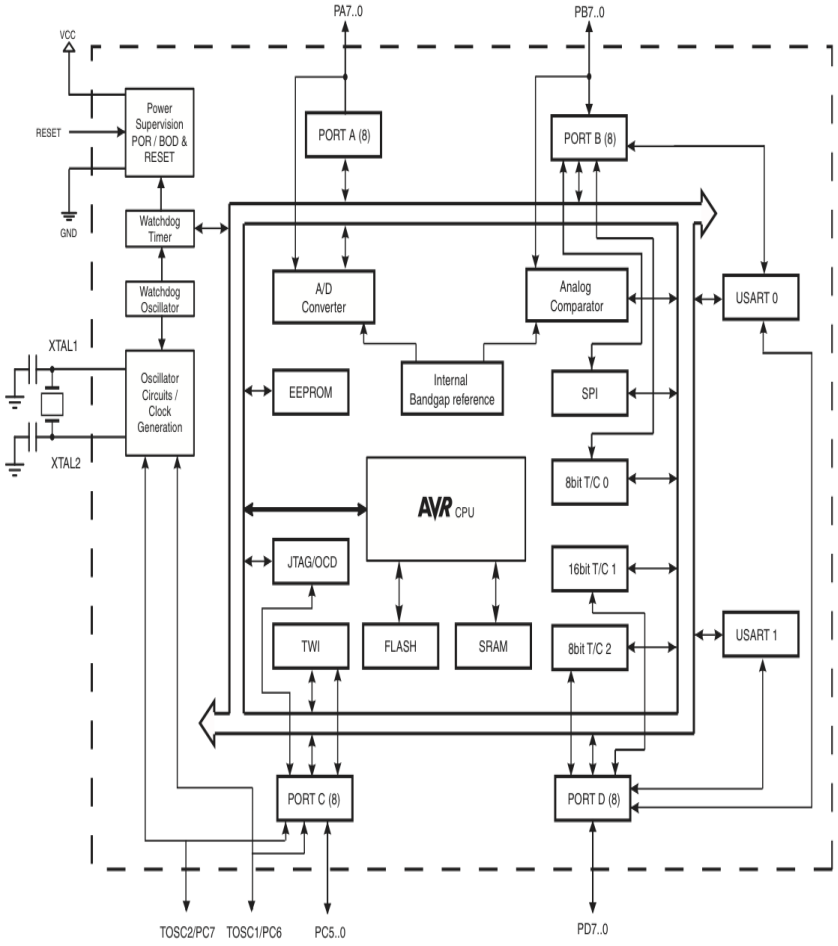


Figure 4.15 Architecture of ATmega328P

4.4.8 PIN Diagram Of ATMEGA328P

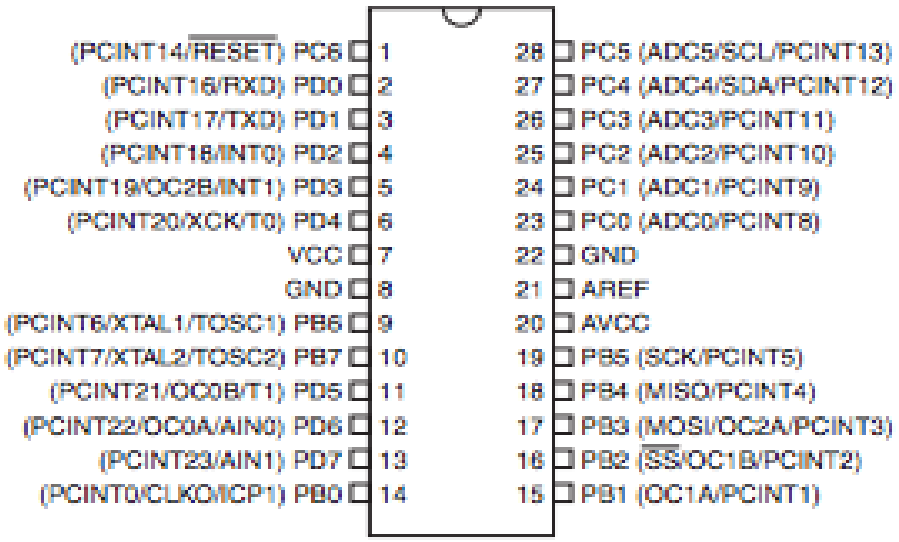


Figure 4.16 Pin Diagram of ATmega328P

The table below gives a description for each of the pins, along with their function.

Pin Number	Description	Function
1	PC6	Reset
2	PD0	Digital Pin (RX)
3	PD1	Digital Pin (TX)
4	PD2	Digital Pin
5	PD3	Digital Pin (PWM)
6	PD4	Digital Pin
7	Vcc	Positive Voltage (Power)
8	GND	Ground
9	XTAL 1	Crystal Oscillator
10	XTAL 2	Crystal Oscillator

11	PD5	Digital Pin (PWM)
12	PD6	Digital Pin (PWM)
13	PD7	Digital Pin
14	PB0	Digital Pin
15	PB1	Digital Pin (PWM)
16	PB2	Digital Pin (PWM)
17	PB3	Digital Pin (PWM)
18	PB4	Digital Pin
19	PB5	Digital Pin
20	AVCC	Positive voltage for ADC (power)
21	AREF	Reference Voltage
22	GND	Ground
23	PC0	Analog Input
24	PC1	Analog Input
25	PC2	Analog Input
26	PC3	Analog Input
27	PC4	Analog Input
28	PC5	Analog Input

TABLE 4.1 Details of pin diagram

Key Parameters Of ATMEGA328P

PARAMETERS	VALUE
Flash	32K bytes
RAM	2K bytes
Pin count	32
Max. operating frequency	20 MHZ
CPU	8-bit AVR
# of touch channels	16
Hardware and touch acquisition	No
Max I/O pins	26
Ext interrupts	24
USB interface	No
USB speed	No

TABLE 4.2 KEY PARAMETERS OF ATMEGA328P

Applications Of ATMEGA328P

Today the ATmega328 is commonly used in many projects and autonomous systems where a simple, low-powered, low-cost microcontroller is needed. Perhaps the most common implementations of this chip is on the popular Arduino development platform, namely the Arduino Uno and Arduino Nano models.

4.5 RELAY DRIVER

A relay is an electro-magnetic switch which is useful if you want to use a low voltage circuit to switch on and off a light bulb (or anything else) connected to the 220v mains supply.

The diagram below shows a typical relay (with “normally-open” contacts).

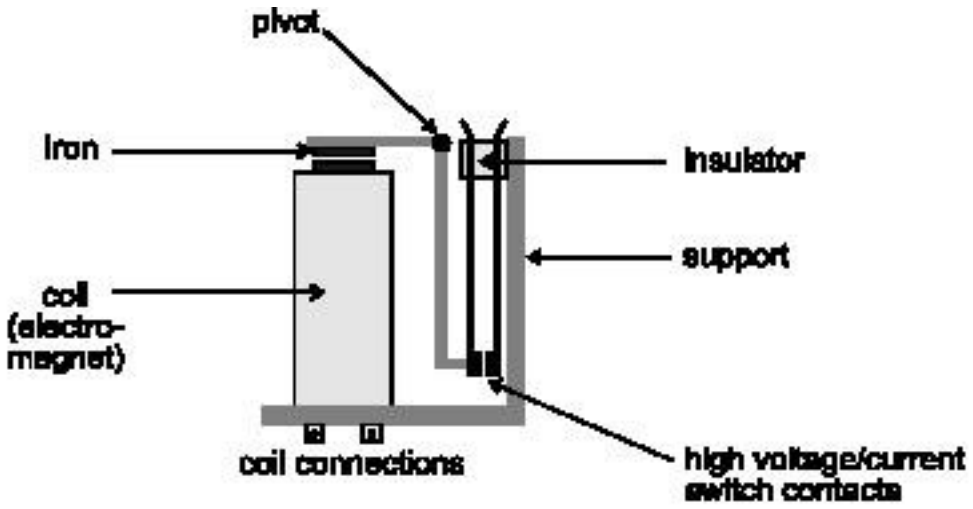


Figure 4.17 Relay Driver

The current needed to operate the relay coil is more than can be supplied by most chips (op. amps etc.), so a transistor is usually needed.

4.5.1 Relay Driver using Single Transistor

This circuit will drive a relay coil from a low power output, usually from an IC like 555 or a TTL/CMOS. It is used to switch high loads or loads that needs AC current to operate. The relay will be actuated when the input of the circuit goes high. The protection diode Dp is used to protect the transistor from the reverse current generated from the coil of the relay during the switch off time. The values for Rb and Qs vary accordingly.

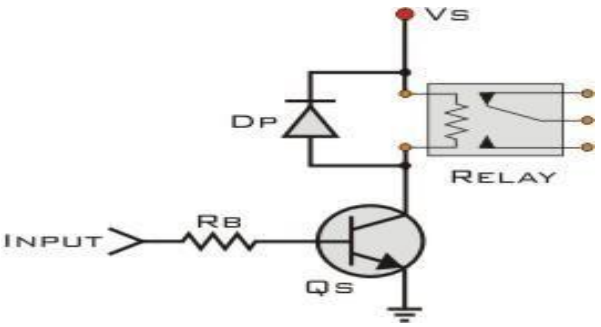


Figure 4.18 Relay Driver using Single Transistor

4.6 RELAYS

Definition Of Relay:

A relay is an electromagnetic switch operated by a relatively small electric current that can turn on or off a much larger electric current. The heart of a relay is an electromagnet (a coil of wire that becomes a temporary magnet when electricity flows through it) Electromagnetic relays are those relays which are operated by electromagnetic action. Modern electrical protection relays are mainly microprocessor based, but still electromagnetic relay holds its place.

It will take much longer time to be replaced the all-electromagnetic relays by microprocessor based static relays. So before going through detail of protection relay system we should review the various types of electromagnetic relays.

4.6.1 Electromagnetic Relay Working:

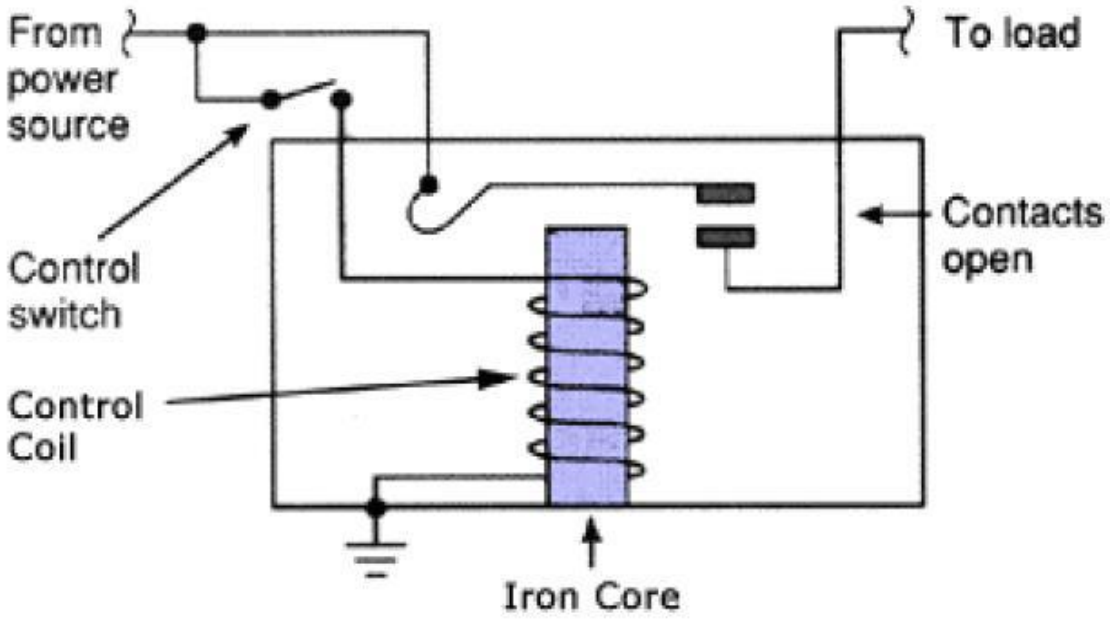
Practically all the relaying device is based on either one or more of the following **types of electromagnetic relays.**

1. Magnitude measurement,
2. Comparison,
3. Ratio measurement.

Principle of **electromagnetic relay working** is on some basic principles. Depending upon working principle the these can be divided into following **types of electromagnetic relays.**

1. Attracted Armature type relay,
2. Induction Disc type relay,
3. Induction Cup type relay,
4. Balanced Beam type relay,
5. Moving coil type relay,
6. Polarized Moving Iron type relay.

Figure 4.19 RELAY MODULE



4.7 LAMP LOAD

An **incandescent light bulb**, **incandescent lamp** or **incandescent light globe** is an electric light with a wire filament heated to such a high temperature that it glows with visible light (incandescence). The filament, heated by passing an electric current through it, is protected from oxidation and, to a lesser degree, from evaporation with a glass or fused quartz bulb that is filled with inert gas or more rarely is evacuated of all gases, such as those found in air.

In a halogen lamp, filament evaporation is slowed by a chemical process that redeposits metal vapor onto the filament, thereby extending its life.

The light bulb is supplied with electric current by feed-through terminals or wires embedded in the glass. Most bulbs are used in a socket which provides mechanical support and electrical connections.

Incandescent bulbs are manufactured in a wide range of sizes, light output, and voltage ratings, from 1.5 volts to about 300 volts. They require no external regulating equipment, have low manufacturing costs, and work equally well on either alternating current or direct current. As a result, the incandescent bulb is widely used in household and commercial lighting, for portable lighting such as table lamps, car headlamps, and flashlights, and for decorative and advertising lighting.

Incandescent bulbs are much less efficient than most other types of electric lighting; incandescent bulbs convert less than 5% of the energy they use into visible light, with standard light bulbs averaging about 2.2%. The remaining energy is converted into heat. The luminous efficacy of a typical incandescent bulb is 16 lumens per watt, compared with 60 lm/W for a compact fluorescent bulb or 150 lm/W for some white led lamps.

Some applications of the incandescent bulb (such as heat lamps) deliberately use the heat generated by the filament. Such applications include incubators, brooding boxes for poultry, heat lights for reptile tanks, infrared heating for industrial heating and drying processes, lava lamps, and the Easy-Bake Oven toy. Incandescent bulbs typically have short lifetimes compared with other types of lighting; around 1,000 hours for home light bulbs versus typically 10,000 hours for compact fluorescents and 30,000 hours for lighting LEDs.

The main source of light on Earth is the Sun. Sunlight provides the energy that green plants use to create sugars mostly in the form of starches, which release energy into the living things that digest them. This process of photosynthesis provides virtually all the energy used by living things. Historically, another important source of light for humans has been fire, from ancient campfires to modern kerosene lamps. With the development of electric lights and power systems, electric lighting has effectively replaced firelight. Some species of animals generate their own light, a process called bioluminescence. For example, fireflies use light to locate mates, and vampire squids use it to hide themselves from prey.

The primary properties of visible light are intensity, propagation direction, frequency or wavelength spectrum, and polarization, while its speed in a vacuum, 299,792,458 meters per second, is one of the fundamental constants of nature. Visible light, as with all types of electromagnetic radiation (EMR), is experimentally found to always move at this speed in a vacuum.

In physics, the term light sometimes refers to electromagnetic radiation of any wavelength, whether visible or not. In this sense, gamma rays, X-rays, microwaves and radio waves are also light. Like all types of EM radiation, visible light propagates as waves. However, the energy imparted by the waves is absorbed at single locations the way particles are absorbed. The absorbed energy of the EM waves is called a photon, and represents the quanta of light.

When a wave of light is transformed and absorbed as a photon, the energy of the wave instantly collapses to a single location, and this location is where the photon "arrives." This is what is called the wave function collapse. This dual wave-like and particle-like nature of light is known as the wave–particle duality. The study of light, known as optics, is an important research area in modern physics.

4.8 GSM MODULE

GSM, which stands for *G*lobal *S*ystem for *M*obile communications, reigns as the world's most widely used cell phone technology. Cell phones use a cell phone service carrier's GSM network by searching for cell phone towers in the nearby area.

The origins of GSM can be traced back to 1982 when the Groupie Special Mobile (GSM) was created by the European Conference of Postal and Telecommunications Administrations (CEPT) for the purpose of designing a pan-European mobile technology.

It is approximated that 80 percent of the world uses GSM technology when placing wireless calls, according to the GSM Association (GSMA), which represents the interests of the worldwide mobile communications industry. This amounts to nearly 3 billion global people.

For practical and everyday purposes, GSM offers users wider international roaming capabilities than other U.S. network technologies and can enable a cell phone to be a "world phone." More advanced GSM incorporates the earlier TDMA standard.

GSM carriers have roaming contracts with other GSM carriers and typically cover rural areas more completely than competing CDMA carriers (and often without roaming charges, too).

GSM also has the advantage of using SIM (*S*ubscriber *I*dentity *M*odule) cards in the U.S. The SIM card, which acts as your digital identity, is tied to your cell phone service carrier's network rather than to the handset itself. This allows for easy exchange from one phone to another without new cell phone service activation.

GSM uses digital technology and is a second-generation (2G) cell phone system. GSM, which predates CDMA, is especially strong in Europe. EDGE is faster than GSM and was built upon GSM.

4.8.1 GSM Carrier Frequency

GSM networks operate in a number of different carrier frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G), with most 2G GSM networks operating in the 900 MHz or 1800 MHz bands. Where these bands were already allocated, the 850 MHz and 1900 MHz bands were used instead (for example in Canada and the United States). In rare cases the 400 and 450 MHz frequency bands are assigned in some countries because they were previously used for first-generation systems. Most 3G networks in Europe operate in the 2100 MHz frequency band.

Regardless of the frequency selected by an operator, it is divided into timeslots for individual phones to use. This allows eight full-rate or sixteen half-rate speech channels per radio frequency. These eight radio timeslots (or eight burst periods) are grouped into a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate for all 8 channels is 270.833 kbit/s, and the frame duration is 4.615 ms .

The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900.

4.8.2 Voice Codecs

GSM has used a variety of voice codecs to squeeze 3.1 kHz audio into between 6.5 and 13 kbit/s. Originally, two codecs, named after the types of data channel they were allocated, were used, called Half Rate (6.5 kbit/s) and Full Rate (13 kbit/s). These used a system based upon linear predictive coding (LPC). In addition to being efficient with bitrates, these codecs also made it

easier to identify more important parts of the audio, allowing the air interface layer to prioritize and better protect these parts of the signal.

GSM was further enhanced in 1997 with the Enhanced Full Rate (EFR) codec,

12.2 kbit/s codec that uses a full rate channel. Finally, with the development of UMTS, EFR was refactored into a variable-rate codec called AMR-Narrowband, which is high quality and robust against interference when used on full rate channels, and less robust but still relatively high quality when used in good radio conditions on half-rate channels.

4.8.3 Network Structure

The structure of a GSM network The network is structured into several discrete sections:

- The Base Station Subsystem (the base stations and their controllers).
- the Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.
- The GPRS Core Network (the optional part which allows packet based Internet connections).
- The Operations support sys team (OSS) for maintenance of the network.

4.8.4 Subscriber Identity Module (SIM)

One of the key features of GSM is the Subscriber Identity Module, commonly known as a **SIM card**. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the

user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking and is illegal in some countries.

4.8.5 Phone Locking

Sometimes mobile network operators restrict handsets that they sell for use with their own network. This is called *locking* and is implemented by a software feature of the phone. Because the purchase price of the mobile phone to the consumer is typically subsidized with revenue from subscriptions, operators must recoup this investment before a subscriber terminates service (hence the *horrific* business model of wireless providers . A subscriber may usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or make use of free or fee based software and websites to unlock the handset themselves.

In some territories (e.g., Bangladesh, Belgium, Hong Kong, India, Malaysia, Pakistan, Singapore) all phones are sold unlocked.

In others (e.g., Finland, Germany, Singapore) it is unlawful for operators to offer any form of subsidy on a phone's price.

4.8.6 GSM Service Security

GSM was designed with a moderate level of service security. The system was designed to authenticate the subscriber using a pre-shared key and challenge response Communications between the subscriber and the base station can be encrypted. The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and

the user - whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.

GSM uses several cryptographic algorithms for security. The A5/1 and A5/2 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a ciphertext-only attack, and in February 2008, Pico Computing, Inc revealed its ability and plans to commercialize FPGAs that allow A5/1 to be broken with a rainbow table attack. The system supports multiple algorithms so operators may replace that cipher with a stronger one.

On 28 December 2009 German computer engineer Karsten Nohl announced that he had cracked the A5/1 cipher. According to Nohl, he developed a number of rainbow tables (static values which reduce the time needed to carry out an attack) and have found new sources for known plaintext attacks.

He also said that it is possible to build "a full GSM interceptor … from open-source components" but that they had not done so because of legal concerns.

In 2010, threatpost.com reported that "A group of cryptographers has developed a new attack that has broken Kasumi, the encryption algorithm used to secure traffic on 3G GSM wireless networks. The technique enables them to recover a full key by using a tactic known as a related-key attack, but experts say it is not the end of the world for Kasumi." Kasumi is the name for the A5/3 algorithm, used to secure most 3G traffic.

Although security issues remain for GSM newer standards and algorithms may address this. New attacks are growing in the wild which take advantage of poor security implementations, architecture, and development for smart phone applications.

Some wiretapping and eavesdropping techniques hijack the audio input and output providing an opportunity for a 3rd party to listen in to the conversation. Although this threat is mitigated by the fact the attack must come in the form of a Trojan, malware or a virus and might be detected by security software.

4.8.7 GSM Modem

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

A GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable. A GSM modem in the form of a PC Card / PCMCIA Card is designed for use with a laptop computer. It should be inserted into one of the PC Card / PCMCIA Card slots of a laptop computer.

A GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone.

A GSM modem can be a dedicated modem device with a serial, USB or Bluetooth connection, or it may be a mobile phone that provides GSM modem capabilities.

The term GSM modem is used as a generic term to refer to any modem that supports one or more of the protocols in the GSM evolutionary family, including the 2.5G technologies GPRS and EDGE, as well as the 3G technologies WCDMA, UMTS, HSDPA and HSUPA.

A GSM modem exposes an interface that allows applications such as Now SMS to send and receive messages over the modem interface. The mobile operator charges for this message sending and receiving as if it was performed directly on a mobile phone. To perform these tasks, a GSM modem must support an "extended AT command set" for sending/receiving SMS messages, as defined in the ETSI GSM 07.05 and 3GPP TS 27.005 specifications.

GSM modems can be a quick and efficient way to get started with SMS, because a special subscription to an SMS service provider is not required. The mobile operator charges for this message sending and receiving as if it was performed directly on a mobile phone.

In most parts of the world, GSM modems are a cost-effective solution for receiving SMS messages, because the sender is paying for the message delivery.

A GSM modem could also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on your computer. Any phone that supports the "extended AT command set" for sending/receiving SMS messages, as defined in ETSI GSM 07.05 and/or 3GPP TS 27.005, can be supported by the Now SMS/MMS Gateway. Note that not all mobile phones support this modem interface.

Due to some compatibility issues that can exist with mobile phones, using a dedicated GSM modem is usually preferable to a GSM mobile phone. This is more of an issue with MMS messaging, where if you wish to be able to receive inbound MMS messages with the gateway, the modem interface on most GSM phones will only allow you to send MMS messages. This is because the mobile phone automatically processes received MMS message notifications without forwarding them via the modem interface.

In computers use AT commands to control modems. Both GSM modems and dial-up modems support a common set of standard AT commands. You can use a GSM modem just like a dial-up modem.

In addition to the standard AT commands, GSM modems support an extended set of AT commands. These extended AT commands are defined in the GSM standards.
With the extended AT commands, you can do things like:

- Reading, writing and deleting SMS messages.
- Sending SMS messages.
- Monitoring the signal strength.
- Monitoring the charging status and charge level of the battery.
- Reading, writing and searching phone book entries.

The number of SMS messages that can be processed by a GSM modem per minute is very low -- only about six to ten SMS messages per minute.

Figure 4.20 GSM Module

4.9 LCD DISPLAY

LCD display is used for displaying the continually monitored values from the sensors. All the sensor values will be displayed on the LCD. Based on that user can observe all the temperature, humidity, and light intensity values. Without user involvement automatically controlling actions were performed whenever the present greenhouse values exceed the user predefined values.

In this project we use 16*2 LCD display. Based on our requirement we can select any type of LCDs.

4.9.1 Introduction

Liquid crystal cell displays (LCDs) are used in similar applications where LEDs are used. These applications are display of display of numeric and alphanumeric characters in dot matrix and segmental displays.

4.9.2 Types

- Dynamic Scattering Type
- Field Effect Type

4.9.3 Construction of A Dynamic Scattering Liquid Crystal Cell

The liquid crystal material may be one of the several components, which exhibit optical properties of a crystal though they remain in liquid form. Liquid crystal is layered between glass sheets with transparent electrodes deposited on the inside faces. When a potential is applied across the cell, charge carriers flowing through the liquid disrupt the molecular alignment and produce turbulence. When the liquid is not activated, it is transparent. When the liquid is activated, the molecular turbulence causes light to be scattered in all directions and the cell appear to be bright. This phenomenon is called dynamic scattering.

The construction of a field effect liquid crystal display is similar to that of the dynamic scattering type, with the exception that two thin polarizing optical filters are placed at the inside of each glass sheet.

The liquid crystal material in the field effect cell is also of different type from employed in the dynamic scattering cell.

The material used is twisted numeric type and actually twists the light passing through the cell when the latter is not energized.

A liquid crystal display (LCD) is an electronically-modulated optical device shaped into a thin, flat panel made up of any number of color or monochrome pixels filled with liquid crystals and arrayed in front of a light source (backlight) or reflector. It is often utilized in battery-powered electronic devices because it uses very small amounts of electric power.

LCD has material, which continues the properties of both liquids and crystals. Rather than having a melting point, they have a temperature range within which the molecules are almost as mobile as they would be in a liquid, but are grouped together in an ordered from similar to a crystal

. LCD consists of two glass panels, with the liquid crystal materials sandwiched in between them. The inner surface of the glass plates is coated with transparent electrodes which define in between the electrodes and the crystal, which makes the liquid crystal molecules to maintain a defined orientation angle. When a potential is applied across the cell, charge carriers flowing through the liquid will disrupt the molecular alignment and produce turbulence.

When the liquid is not activated, it is transparent. When the liquid is activated, the molecular turbulence causes light to be scattered in all directions and the cell appears to be bright. Thus, the required message is displayed. When the LCD is in the off state, the two polarizers and the liquid crystal rotate the light rays, such that they come out of the LCD without any orientation, and hence the LCD appears transparent.

4.9.4 Working

When sufficient voltage is applied to the electrodes the liquid crystal molecules would be aligned in a specific direction. The light rays passing through the LCD would be rotated by the polarizer, which would result in activating/highlighting the desired characters. The power supply should be of +5v, with maximum allowable transients of 10mv. To achieve a better/suitable contrast for the display the voltage (VL) at pin 3 should be adjusted properly. A module should not be removed from a live circuit.

The ground terminal of the power supply must be isolated properly so that voltage is induced in it. The module should be isolated properly so that stray voltages are not induced, which could cause a flicking display. LCD is lightweight with only a few, millimeters thickness since the LCD consumes less power, they are compatible with low power electronic circuits, and can be powered for long durations. LCD does not generate light and so light is needed

to read the display. By using backlighting, reading is possible in the dark. LCDs have long life and a wide operating temperature range. Before LCD is used for displaying proper initialization should be done.

LCDs with a small number of segments, such as those used in digital watches and pocket calculators, have individual electrical contacts for each segment. An external dedicated circuit supplies an electric charge to control each segment. This display structure is unwieldy for more than a few display elements.

Small monochrome displays such as those found in personal organizers, or older laptop screens have a passive-matrix structure employing super-twisted nematic (STN) or double-layer STN (DSTN) technology—the latter of which addresses a color-shifting problem with the former—and color -STN (CSTN)—wherein color is added by using an internal filter. Each row or column of the display has a single electrical circuit.

The pixels are addressed one at a time by row and column addresses. This type of display is called passive-matrix addressed because the pixel must retain its state between refreshes without the benefit of a steady electrical charge. As the number of pixels (and, correspondingly, columns and rows) increases, this type of display becomes less feasible.

Very slow response times and poor contrast are typical of passive matrix addressed LCDs. High-resolution color displays such as modern LCD computer monitors and televisions use an active-matrix structure. A matrix of thin-film transistors (TFTs) is added to the polarizing and color filters. Each pixel has its own dedicated transistor, allowing each column line to access one pixel. When a row line is activated, all the column lines are connected to a row of pixels and the correct voltage is driven onto all the column lines.

Figure 4.21 LCD Display

4.9.5 PIN Description for LCD

PIN NO	SYMBOL	FUNCTION
1	Vss	Ground terminal of Module
2	Vdd	Supply terminal of Module, + 5V
3	Vo	Power supply for liquid crystal drive
4	RS	Register select RS=0…Instruction register RS=1…Data register
5	R/W	Read/Write R/W=1…Read R/W=0…Write
6	EN	Enable
7-14	DB0-DB7	Bi-directional Data Bus. Data Transfer is performed once ,thru DB0-DB7,incase of interface data length is 8-bits;and twice, thru DB4-DB7 in the case of interface data length is 4-bits.Upper four bits first then lower four bits.
15	LAMP-(L-)	LED or EL lamp power supply terminals
16	LAMP+(L+) (E2)	Enable

TABLE 4.3 PIN Description for LCD

The function of each pins of LCD is described below **VCC, VSS and VEE** while v and v provide +5v and ground, respectively, v is used for controlling LCD contrast.

4.9.6 Registers

[a] RS, REGISTER SELECT

There are two very important registers inside the LCD. The RS pin is used for their selection as follows. If RS=0, the instruction code register is selected, allowing the user to send a command such as clear display, cursor at home,etc.if RS=1 the data register is selected, allowing the user to send data to be displayed on the LCD.

[b] R/W, READ/WRITE

R/W input allows the user to write information to the LCD or read information from it. R/W=1 when reading; R/W=0 when writing.

[c] E, ENABLE

The enable pin is used by the LCD to latch information presented on its data pins. When data is supplied to data pins, a high to low pulse must be applied to this pin for the LCD to latch in the data present at the data pins.

[d] D0 - D7

The 8-bit data pins, D0 – D7, are used to send information to the LCD or read contents of the LCD'S internal registers.

There are also instruction codes that can be sent to the LCD to clear the display or force the cursor to the home position or blink the cursor. RS=0 is used to check the busy flag bit to see if the LCD is ready to receive information.

The busy flag is D7 and can be read when R/W=1 and RS=0, as follows: if R/W=1, RS=0.when D7=1, the LCD is busy taking care of internal operation and will not accept any new information, when D7=0, the LCD is ready to receive new information.

4.9.7 LCD Interfacing with Microcontroller

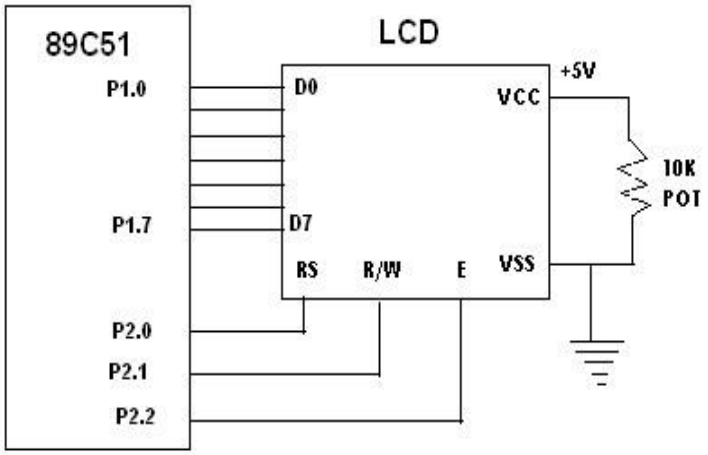


Figure 4.22 LCD Interfacing with Microcontroller

4.9.8 Advantages

- Consume much lesser energy (i.e. low power) when compared to LEDs.
- Utilizes the light available outside and no generation of light.
- Since very thin layer of liquid crystal is used, more suitable to act as display elements (in digital watches, pocket calculators, etc.)
- Since reflectivity is highly sensitive to temperature, used as temperature measuring sensor.
- Very cheap.

4.9.9 Disadvantages

- Angle of viewing is very limited.
- External light is a must for display.
- Since not generating its own light and makes use of external light for display, contrast is poor.
- Cannot be used under wide range of temperature.

4.9.10 Applications

- Watches
- Fax, Copy machines and Calculators

4.10 KEYPAD

The four rows of the keypad would be connected to the microcontroller pins directly, without any other connections. However, each of the 3 columns of the keypad would be connected into a pull-up resistor, which is connected into a voltage source and the microcontroller. The keypad is used as an input for the PIC16F877A microcontroller. Matrix Keypads are mostly used in calculators, mobile phones, telephones, ATMs, etc. It is used when several input switches are required. In this article, we will study how to interface a keypad with the PIC16F877A microcontroller.

Figure 4.23 Keypad

4.11 NODEMCU V3

The best way to develop quickly an IoT application with less Integrated circuits to add is to choose this circuit “NodeMCU”. It is an open-source firmware and development kit that plays a vital role in designing a proper IoT product using afew script lines.

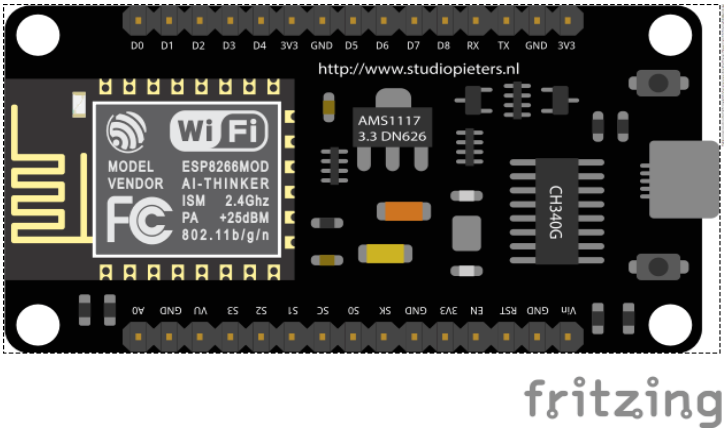


FIG 4.24 NODEMCUV3

The module is mainly based on ESP8266 that is a low-cost Wi-Fi microchip incorporating both a full TCP/IP stack and microcontroller capability. It is introduced by manufacturer Express if Systems. The ESP8266 NodeMcu is a complex device, which combines some features of the ordinary Arduino board with thepossibility of connecting to the internet.

Arduino Modules and Microcontrollers have always been a great choice to incorporate automation into the relevant project. But these modules come with a little drawback as they don’t feature a built-in WiFi capability, subsequently, we need to add external WiFi protocol into these devices to make them compatiblewith the internet channel.

This is the famous NodeMCU which is based on ESP8266 WiFi SoC. This is version 3 and it is based on ESP-12E (An ESP8266 based WiFi module). NodeMCU is also an open-source firmware and development kit

that helps you to prototype your IOT product within a few LUA script lines, and of course you can always program it with Arduino IDE.

4.11.1 Introduction NodeMCU V3

NodeMCU V3 is an open-source firmware and development kit that plays a vitalrole in designing an IoT product using a few script lines.

Multiple GPIO pins on the board allow us to connect the board with other peripherals and can generate PWM, I2C, SPI, and UART serial communications.

The interface of the module is mainly divided into two parts including both Firmware and Hardware where former runs on the ESP8266 Wi-Fi SoC and later is based on the ESP-12 module.

The firmware is based on Lua – A scripting language that is easy to learn, giving a simple programming environment layered with a fast-scripting language that connects you with a well-known developer community.the existing module and keep changing the entire interface until you succeed in optimizing the module as per your requirements.

- USB to UART converter is added on the module that helps in converting USB data to UART data which mainly understands the language of serial communication.

Instead of the regular USB port, MicroUSB port is included in the module that connects it with the computer for dual purposes: programming and powering upthe board.

The board incorporates status LED that blinks and turns off immediately, giving you the current status of the module if it is running properly when connected with the computer.

The ability of module to establish a flawless WiFi connection between two channels makes it an ideal choice for incorporating it with

other embedded devices like Raspberry Pi.

4.11.2 NodeMCU V3 Pinout

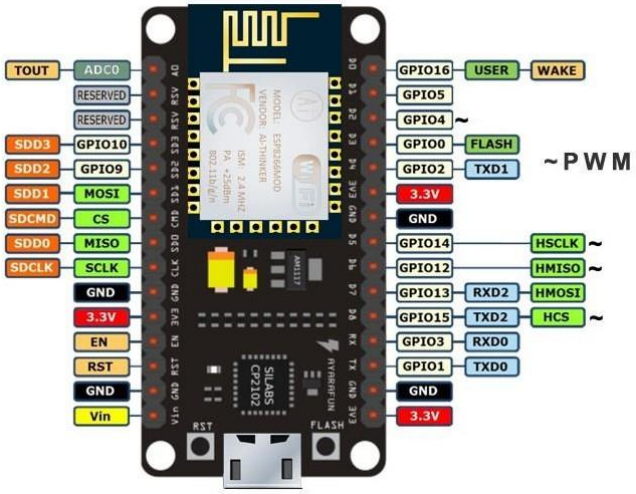


FIG **4.25 NODEMCU V3 PINOUT**

NodeMCU V3 comes with a number of GPIO Pins. Following figure shows the Pinout of the board. There is a candid difference between Vin and VU where former is the regulated voltage that may stand somewhere between 7 to 12 V while later isthe power voltage for USB that must be kept around 5 V.

Features

1. Open-source
2. Arduino-like hardware
3. Status LED
4. Micro USB port
5. Reset/Flash buttons
6. Interactive and Programmable
7. Low cost
8. ESP8266 with inbuilt wifi

9. USB to UART converter
10. GPIO pins
11. Arduino-like hardware IO
12. Advanced API for hardware IO, which can dramatically reduce the redundantwork for configuring and manipulating hardware.
13. Code like Arduino, but interactively in Lua script.
14. Nodejs style network API
15. Event-driven API for network applications, which facilitates developers writingcode running on a 5mm*5mm sized MCU in Nodejs style.
16. Greatly speed up your IOT application developing process.
17. Lowest cost WI-FI
18. Less than $2 WI-FI MCU ESP8266 integrated and easy to prototypingdevelopment kit.

As mentioned above, a cable supporting micro USB port is used to connect the board. As you connect the board with a computer, LED will flash. You may need some drivers to be installed on your computer if it fails to detect the NodeMCU board. You can download the driver from this page.

Note: We use Arduino IDE software for programming this module. It is important to note that the pin configuration appearing on the board is different from the configuration we use to program the board on the software i.e. when we write code for targeting pin 16 on the Arduino IDE, it will actually help is laying out thecommunication with the D0 pin on the module.

Following figure the shows the pin configuration to use in Arduino IDE.

CHAPTER 5

SOFTWARE DESCRIPTION

5.1 ARDUINO INTRODUCTION

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a twitter message - and turn it into an output - activating a motor, turning on an led, publishing

something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the arduino programming language (based on wiring), and the arduino software (ide), based on processing.

Over the years arduino has been the brain of thousands of projects, from everyday objects to complex scientific instruments. A worldwide community of makers - students, hobbyists, artists, programmers, and professionals - has gathered around this open-source platform, their contributions have added up to an incredible amount of accessible knowledge that can be of great help to novices and experts alike.

Arduino was born at the ivrea interaction design institute as an easy tool for fast prototyping, aimed at students without a background in electronics and programming. As soon as it reached a wider community, the arduino board started changing to adapt to new needs and challenges, differentiating its offer from simple 8-bit boards to products for IOT applications, wearable, 3d printing, and embedded environments. All arduino boards are completely open-source, empowering users to build them independently and eventually adapt them to their particular needs. The software, too, is open-source, and it is growing through thecontributions of users worldwide.

5.2 FEATURES

INEXPENSIVE - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the arduino module can be assembled by hand, and even the pre-assembled arduino modules cost less than 1000.

CROSS-PLATFORM - The arduino software (ide) runs on windows, macintosh osx, and linux operating systems. Most microcontroller systems are limited to windows.

SIMPLE, CLEAR PROGRAMMING ENVIRONMENT - The arduino software (ide) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the processing programming environment, so students learning to program in that environment will be familiar with how the arduino ide works.

OPEN SOURCE AND EXTENSIBLE SOFTWARE - The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through c++ libraries, and people wanting to understand the technical details can make the leap from arduino to the avr c programming language on which it's based. Similarly, you can add avr-c code directly into your arduino programs if you want to.

OPEN SOURCE AND EXTENSIBLE HARDWARE - The plans of the arduino boards are published under a creative commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. even relatively inexperienced

users can build the breadboard version of the module in order to understand how it works and save money

5.3 ARDUINO SOFTWARE (IDE)

The arduino integrated development environment - or arduino software (ide) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the arduino hardware to upload programs and communicate with them.

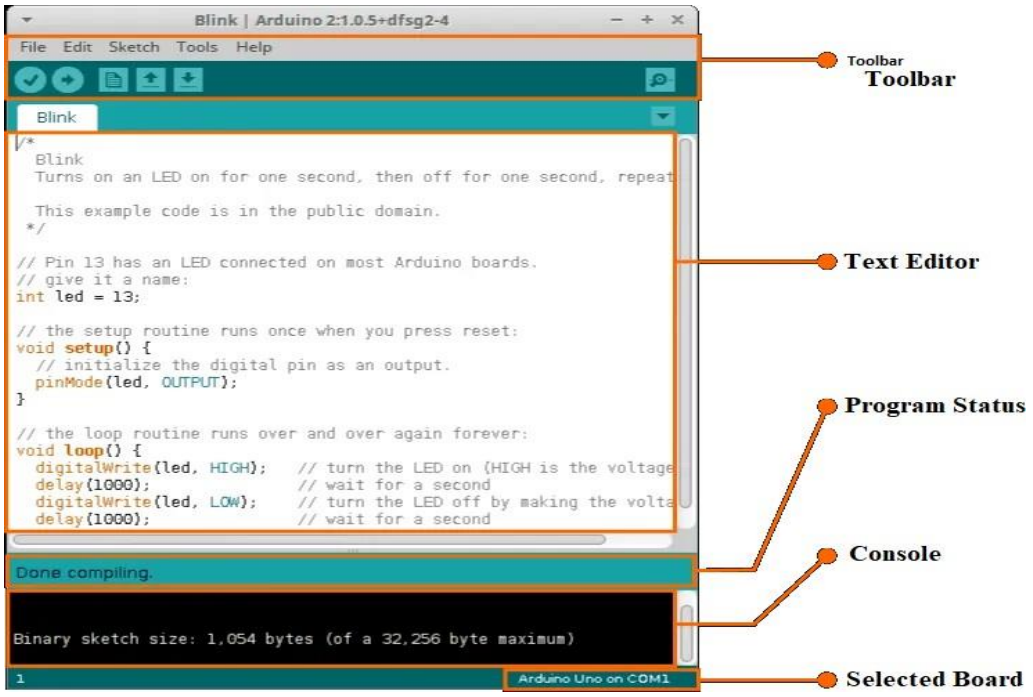


Figure 5.1 Arduino IDE

5.4 PROTEUS 8 PROFESSIONAL

Proteus 8 Professional is a software suite designed for electronic design automation, with a strong emphasis on simulation capabilities. While newer versions exist, Proteus 8 Professional still offers a robust set of tools for simulating electronic circuits before physical construction. Here's a detailed breakdown of its simulation features .

1. Mixed-Mode SPICE Simulation:

- Proteus 8 Professional utilizes SPICE (Simulation Program with Integrated Circuit Emphasis) for circuit analysis. This industry-standard method allows you to simulate various analog, digital, and mixed-signal circuits.
- You can define component models, including behavior and characteristics, to accurately represent real-world components in your simulation.
- Proteus offers a library of pre-defined models for common components like resistors, capacitors, transistors, and operational amplifiers. You can also import custom models for more specialized components.

2. Advanced Analysis Tools:

Proteus provides a wide range of analysis tools to examine various aspects of your circuit's behavior. These include:

Transient analysis: Simulates the circuit's response over time, allowing you to observe voltage, current, and power waveforms at different points.

AC analysis: Analyzes the circuit's behavior under varying AC (alternating current) frequencies, helping you determine frequency response, gain, and phase shift.

DC analysis: Analyses the circuit's behaviour under constant DC (direct current) conditions, providing information about voltages, currents, and power consumption.

Fourier analysis: Decomposes complex waveforms into their constituent frequencies, aiding in understanding signal behaviour.

Real-Time Visualization:

Proteus 8 Professional allows you to visualize the simulation results in real-time. You can view voltage and current waveforms on graphs, monitor component values numerically, and even animate the circuit's behaviour for a more intuitive understanding.

4. Model Creation and Libraries (Limitations to Consider):

- While Proteus 8 offers pre-defined models, creating custom models for specific components might be more limited compared to newer versions.
- The ability to import user-created model libraries might also be restricted.

5. Microcontroller Simulation (Potential Limitations):

- Proteus 8 Professional boasts the ability to simulate microcontrollers. This allows you to test the interaction between the microcontroller code and the surrounding circuitry.
- However, compared to newer versions, Proteus 8 might have a limited selection of microcontroller models and debugging features for firmware.

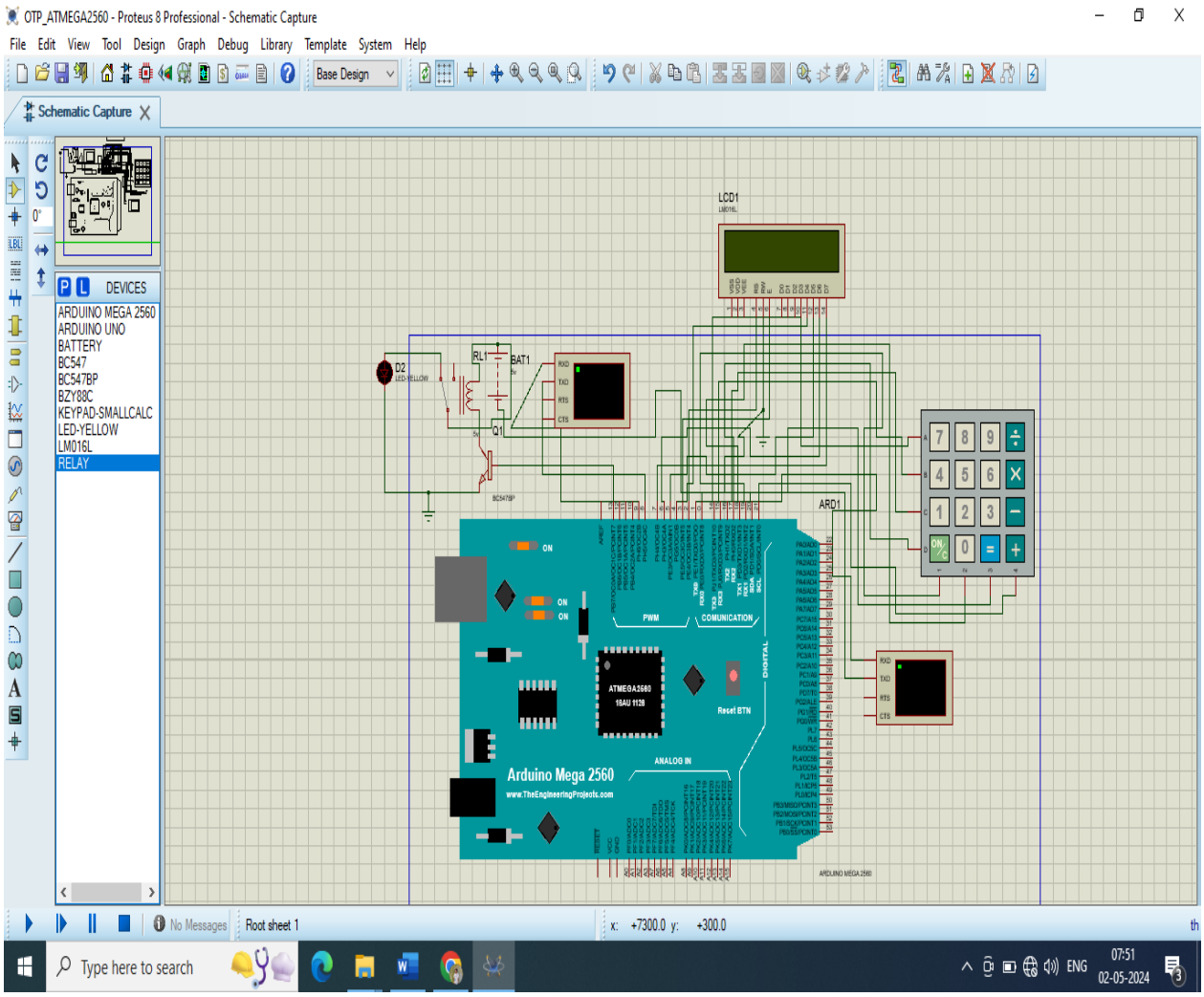
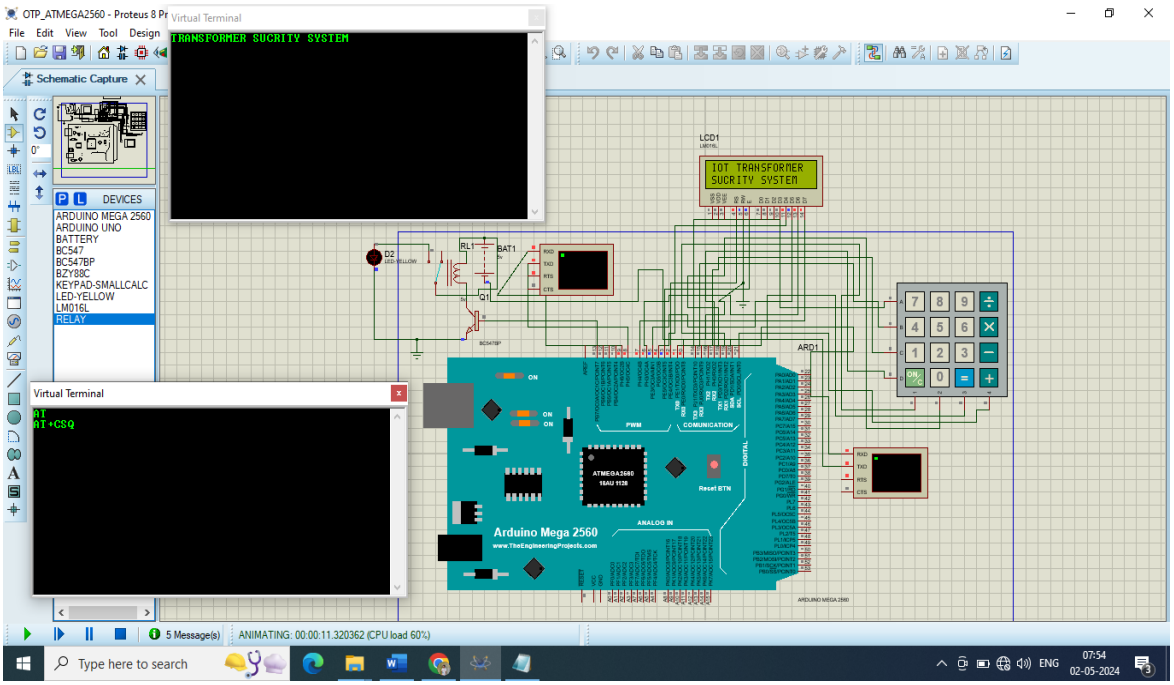


Figure 5.2 Circuit Design using Components

The above figure 5.1 shows the circuit connections between the components using proteus 8 professional software and this is the initial stage before running the simulation.



.

Figure 5.3 Initial stage of Simulation running process

Figure 5.3 shows the initial stage of simulation start running. when we start the simulation to run, the terminals will open on the windows.

The above first terminal is sender side likewise acts as Arduino and gsm interface. The second terminal acts as a receiver side as the OTP sends to mobile

The figure 5.3 represents the OTP that generated in the controller system is sent to the mobile as shown in terminal 2. Here the terminal 1 plays the role of both controller and GSM.

.

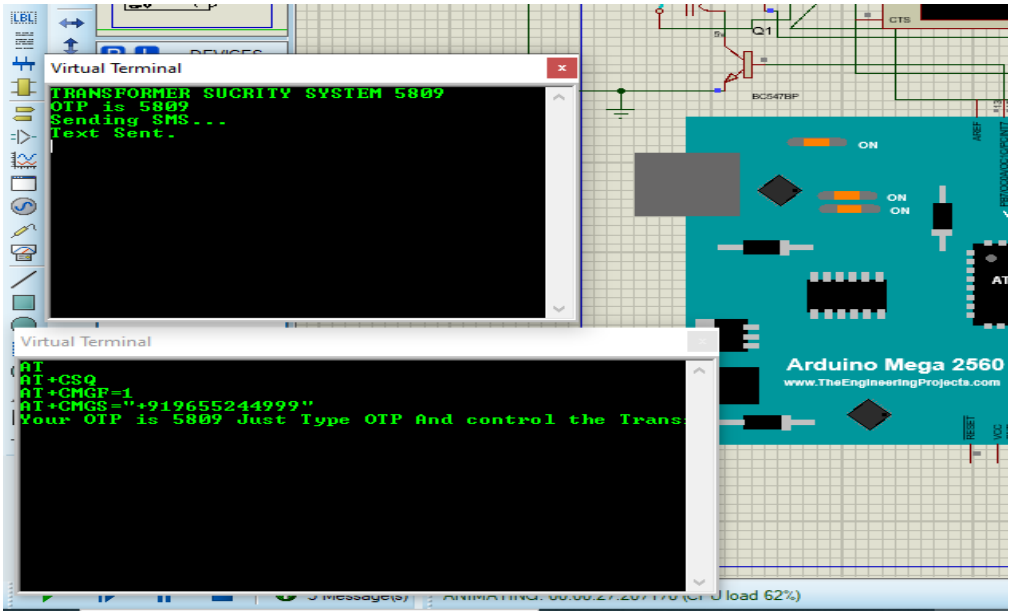


Figure 5.4 OTP Generation and sending process

After running the simulation you have to copy the identification number that you already coded to the Arduino mega 2560 and then you have to paste that authorised identification code in the first terminal.

Then the terminal verify the identification code that you have pasted is authorised or not. If the entered id is verified then the otp is generated and sent to the next terminal. At the next process the you have to enter that otp to the terminal using the matrix keyboard that you have designed using the proteus 8 software.

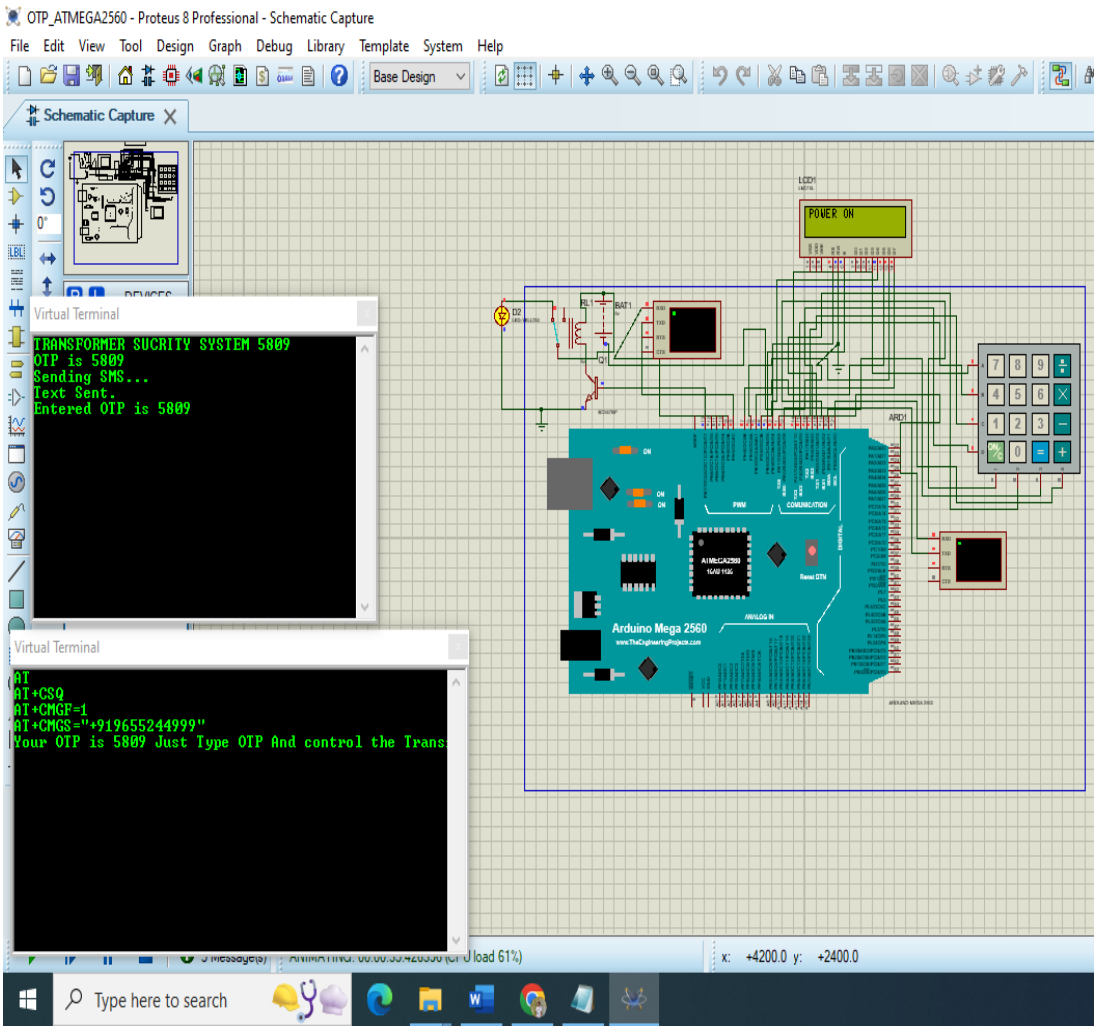


Figure 5.5 Turning ON Transformer after entering correct password

After entering the OTP through the keyboard as it is generated in the terminal. the controller that verifies the entered and sended OTP are same. If both are same. Then the transformer turned ON condition. In figure 4.14.4 LED that blinks shows the transformer that in ON condition.

CHAPTER 6
RESULT AND OUTPUT

6.1 RESULT AND DISCUSSION

The electric line man safety system is designed to control a switch gear with help of a password only. Password based switch gear generation and Password based switch gear verification are the major tasks involved in this system. Password based switch gear generation is the main attraction of this project. It provides a new approach to the security of the lineman and completely eliminates the accidents to the lineman due to electric shock during the electric line repair. This system can also implement in many other public areas also.

The electric line man safety system is designed to control a circuit breaker with help of a password only. OTP generation and OTP verification are the major tasks involved in this system. OTP generation is the main attraction of this project. It provides a new approach to the security of the lineman and completely eliminates the accidents to the lineman due to electric shock during the electric line repair.

6.2 OUTPUT

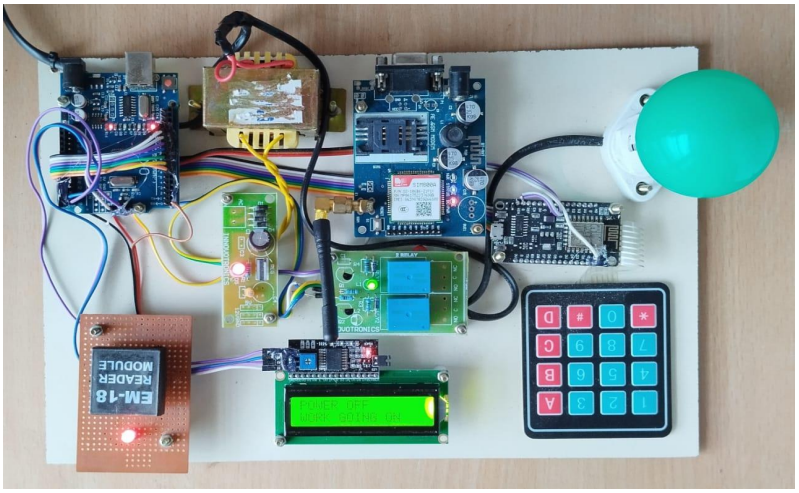


Figure 6.1 Initial Stage

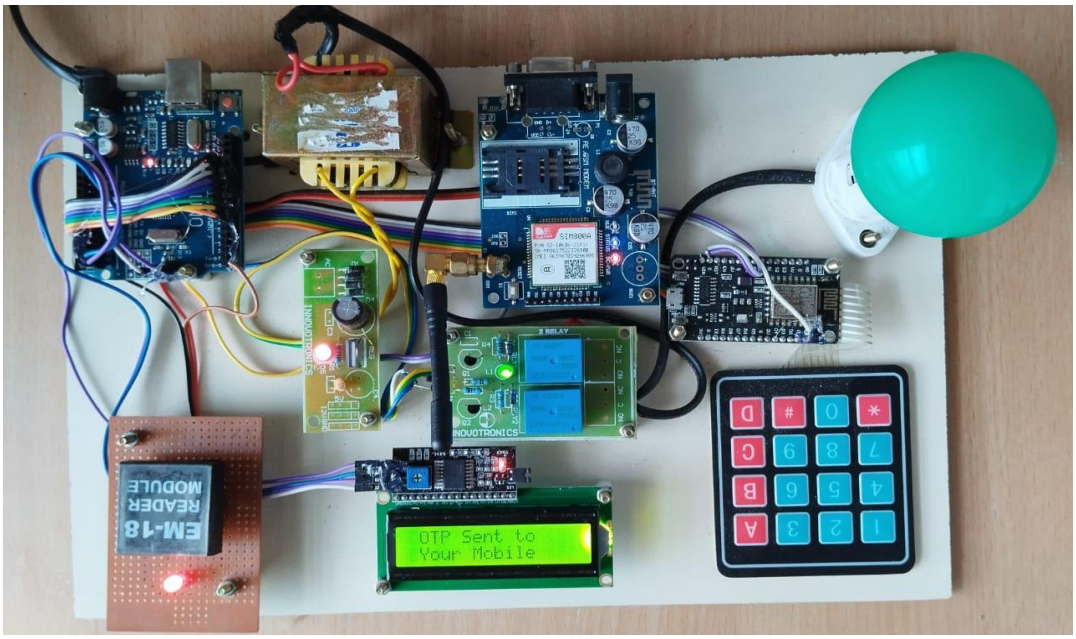


Figure 6.2 After Scanning The RFID Tag

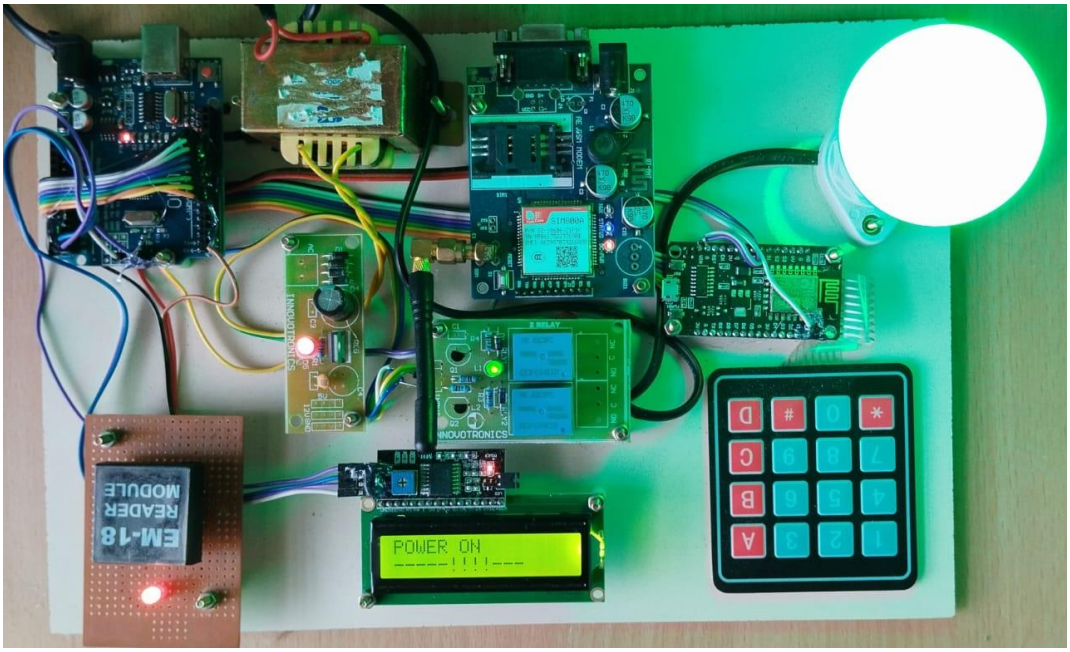


Figure 6.3 Turn ON Transformer after entering correct password

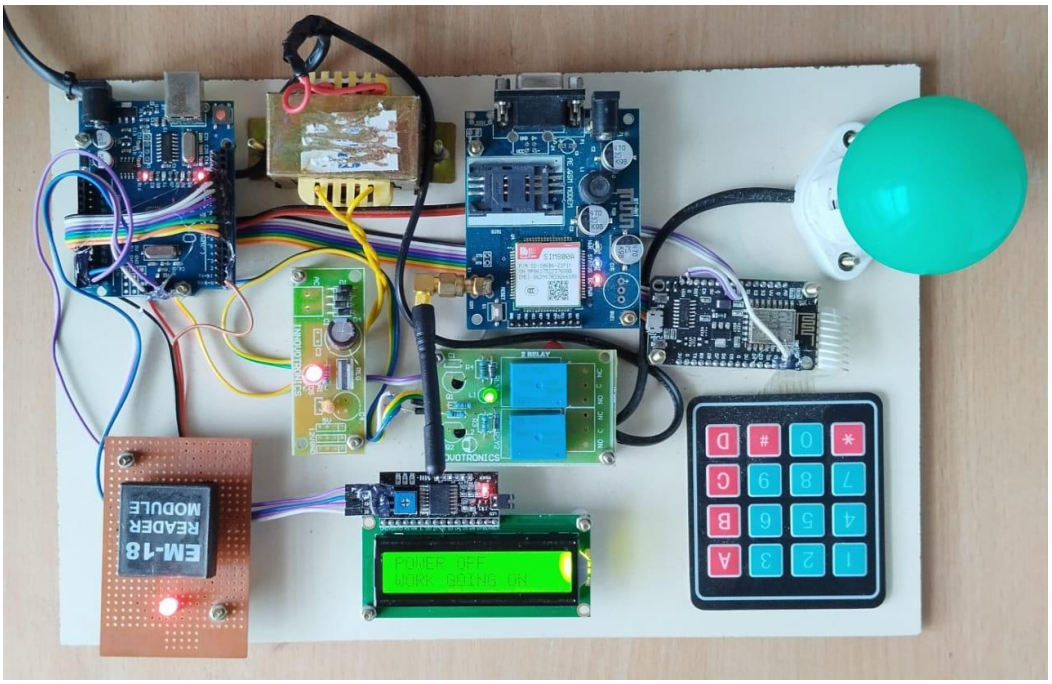


Figure 6.4 Turn OFF Transformer after entering correct password .

CHAPTER 7
CONCLUSION AND FUTURE SCOPE

7.1 FUTURE ENHANCEMENTS

Using wireless communication this system can be operated from other areas besides the substation such as on the transformer. The SCADA is a system used in the communication channels to help easy troubleshoot to locate the fault location directly and the line man can easily rectify it.

7.2 CONCLUSION

- This project can be used to ensure the safety of the maintenance staff, e.g., linemen. The line can only be turned off or on by the lineman.
- This system provides an arrangement such that an RFID tag and a password are required to operate the circuit breaker (on or off).
- Linemen can turn off the supply and comfortably repair it, and then turn on the line by entering the correct password.
- Since it has the provision of entering the password through registered keypad device, only an authorized person can enter the password and circuit breaker**.**

REFERENCES

[1]"RFID-Enabled Secure Transformer Control System: Design and Implementation" Sharma (2022)

[2]"Smart Transformer Monitoring System Based on IoT and RFID Technology" Han(2021)

[3]"Design of RFID-Based Transformer Inspection and Management System" Zhang(2020)

[4]IoT-Enabled Condition Monitoring and Security Control of Power TransformersAmir H. Rasekh(2020)

[5]"IoT and RFID-based Transformer Health Monitoring System “Gaur (2019)

[6]An Intelligent Transformer Monitoring and Security System Based on LoRa and RFID Jinjiang Xie(2019)

[7]"Design and Implementation of Transformer Monitoring System Based on IoT and RFID Technology "Wang(2018)

[8]Smart Grid Cyber Security by Using RFID Technology Akshay Kumar Bhatia(2018)

APPENDIX

OTP SOURCE CODE

```
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#define relay 4
#define red 16
#define green 15
#include <Servo.h>
Servo myservo;  // create servo object to control a servo
// twelve servo objects can be created on most boards
int pos = 0, rp = 0, D;
const byte ROWS = 4;
const byte COLS = 4;
char hexaKeys[ROWS][COLS] =
{
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};
byte rowPins[ROWS] = {13, 12, 11, 10};
byte colPins[COLS] = {9, 8, 7, 6};
Keypad customKeypad = Keypad( makeKeymap(hexaKeys), rowPins, colPins, ROWS, COLS);
LiquidCrystal_I2C lcd(0x27, 16, 2);
SoftwareSerial sim800l(3, 2);
int irsensor = A0;
```

```
int otp;
char input[12];
String otpstring = "";
int i = 0; int count = 0;
void setup()
{
  sim800l.begin(9600);
  Serial.begin(9600);
  lcd.init();
  lcd.backlight();
  Serial.print("Welcome to SIM800L Project");
  sim800l.println("AT");
  updateSerial();
  pinMode(relay, OUTPUT);
  digitalWrite(relay, LOW);
  delay(500);
  sim800l.println("AT+CSQ");
  updateSerial();
  delay(1000);
  if (D == 0) {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("POWER OFF");
    lcd.setCursor(0, 1);
    lcd.print("WORK GOING ON");
  }
  if (D == 1) {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("POWER ON");
    lcd.setCursor(0, 1);
```

```
    lcd.print("-----!!!!---");;
  }
}
void updateSerial()
{
  delay(500);
  while (Serial.available())
  {
    sim800l.write(Serial.read());
  }
  while (sim800l.available())
  {
    Serial.write(sim800l.read());
  }
}
void loop()
{
main:
  if (Serial.available()) // check serial data ( RFID reader)
  {
    count = 0; // Reset the counter to zero
    while (Serial.available() && count < 12)
    {
      input[count] = Serial.read(); // Read 1 Byte of data and store it in the input[] variable
      count++; // increment counter
      delay(5);
    }
    // Serial.println("I received: ");
    lcd.clear();
    for (int i = 0; i < 12; i++)
```

```
  lcd.print(input[i]);
delay(3000);
if (input[11] == '6')
{
  lcd.clear();
  lcd.print("SORRY ");
  lcd.setCursor(0, 1);
  lcd.print("INVAILD ID");
  delay(1000);
}
if  ((input[11] == 'F') ||   (input[11] == '9') )
{
  lcd.clear();
  lcd.print("REJESTRED");
  lcd.setCursor(0, 1);
  lcd.print("PLS VERIFY ");
  delay(3000);
  lcd.clear();
  lcd.print("     OTP");
  lcd.setCursor(0, 1);
  lcd.print("     SENT ");
  delay(3000);
  while (1)
  {
    otp = random(2000, 9999);
    otpstring = String(otp);
    Serial.println(otpstring);
    while (digitalRead(irsensor) == LOW)
    {}
    lcd.clear();
    lcd.setCursor(0, 0);
```

```
      lcd.print(" OTP Sent to");
      lcd.setCursor(0, 1);
      lcd.print(" Your Mobile");
      Serial.print("OTP is ");
      delay(100);
      Serial.println(otpstring);
      delay(100);
      SendSMS();
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Enter OTP :");
      getotp();
      if (D == 0) {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("POWER OFF");
        lcd.setCursor(0, 1);
        lcd.print("WORK GOING ON");
      }
      if (D == 1) {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("POWER ON");
        lcd.setCursor(0, 1);
        lcd.print("-----!!!!---");;
      }
      goto main;
    }
  }
 }
}
```

```
void getotp() {
opt:
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enter OTP :");
  String y = "";
  int a = y.length();
  while (a < 4)
  {
    char customKey = customKeypad.getKey();
    if (customKey) {
      lcd.setCursor(0, 1);
      y = y + customKey;
      lcd.print(y);
      a = y.length();
    }
  }
  Serial.print("Entered OTP is ");
  Serial.println(y);
  if (otpstring == y)
  {
    lcd.setCursor(0, 0);
    lcd.print("Access Granted");
    lcd.setCursor(0, 1);
    if (rp == 0)
    {
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("POWER ON");
      digitalWrite(relay, 1);
      rp = 1;
```

```
  delay(1000);
  sim800l.print("AT+CMGS=\"+919361031783\"\r");
  delay(500);
  sim800l.print(" Transformer POWER ON");
  delay(500);
  sim800l.print((char)26);
  delay(1000);
  sim800l.println();
  delay(5000);
  sim800l.print("AT+CMGS=\"+919361831983\"\r");
  delay(500);
  sim800l.print(" Transformer POWER ON");
  delay(500);
  sim800l.print((char)26);
  delay(1000);
  sim800l.println();
  D = 1;
 }
 else
 {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("POWER OFF");
  digitalWrite(relay, 0);
  D = 0;
  rp = 0;
  delay(1000);
  sim800l.print("AT+CMGS=\"+919361031783\"\r");
  delay(500);
  sim800l.print(" Transformer POWER OFF");
  delay(500);
```

```
    sim800l.print((char)26);
    delay(500);
    sim800l.println();
    //  Serial.println("Text Sent.");
    delay(5000);
    delay(1000);
    sim800l.print("AT+CMGS=\"+919361831983\"\r");
    delay(500);
    sim800l.print(" Transformer POWER OFF");
    delay(500);
    sim800l.print((char)26);
    delay(500);
    sim800l.println();
    //  Serial.println("Text Sent.");
    delay(1000);
   }
  }
  else
  {
   lcd.setCursor(0, 0);
   lcd.print("Invaild OTP");
   lcd.setCursor(0, 1);
   lcd.print("Try Again !!!");
   delay(3000);
   goto opt;
  }
}
void SendSMS()
{
  Serial.println("Sending SMS...");
  sim800l.print("AT+CMGF=1\r");
```

```
  delay(1000);
  sim800l.print("AT+CMGS=\"+919361031783\"\r");
  delay(500);
  sim800l.print("Your OTP is " + otpstring + " Just Type OTP And control the Transformer");
  delay(500);
  sim800l.print((char)26);
  delay(500);
  sim800l.println();
  //  Serial.println("Text Sent.");
  delay(5000);
  Serial.println("Sending SMS...");
  sim800l.print("AT+CMGF=1\r");
  delay(1000);
  sim800l.print("AT+CMGS=\"+919361831983\"\r");
  delay(500);
  sim800l.print("Your OTP is " + otpstring + " Just Type OTP And control the Transformer");
  delay(500);
  sim800l.print((char)26);
  delay(500);
  sim800l.println();
}
```

SURYA

SURYA GROUP OF INSTITUTIONS

SCHOOL OF ENGINEERING AND TECHNOLOGY

(INTEGRATED CAMPUS) G.S.T Road, Vikiravandi - 605 652. Villupuram Dt.
www.suryagroup.edu.in

2nd INTERNATIONAL CONFERENCE

On

"Emerging Trends in Artificial Intelligence and Block Chain Technology"

INCETAIBCT'24

This is to certify that ~~Dr./Mr./Ms.~~ DINESHKUMAR . P
of University College of ~~Engineering~~ - Villupuram *has presented a paper titled* RFID Based Secure Transformer Control System

in the 2nd International Conference on "Emerging Trends in Artificial Intelligence and Block Chain Technology" INCETAIBCT '24 organized by the Department of Computer Science and Engineering & Artificial Intelligence and Data Science on 30th April 2024.

CO-ORDINATOR CONVENER VICE-PRINCIPAL PRINCIPAL CHAIRMAN

SURYA

SURYA GROUP OF INSTITUTIONS

SCHOOL OF ENGINEERING AND TECHNOLOGY

(INTEGRATED CAMPUS) G.S.T Road, Vikiravandi - 605 652. Villupuram Dt.
www.suryagroup.edu.in

2nd INTERNATIONAL CONFERENCE

On

"Emerging Trends in Artificial Intelligence and Block Chain Technology"

INCETAIBCT'24

This is to certify that ~~Dr./Mr./Ms.~~ JAYASURIYA .S
of University College of Engineering - Villupuram *has presented a paper titled* RFID Based Secure Transformer Control System
in the 2nd International Conference on "Emerging Trends in Artificial Intelligence and Block Chain Technology" INCETAIBCT '24 organized by the Department of Computer Science and Engineering & Artificial Intelligence and Data Science on 30th April 2024.

CO-ORDINATOR | CONVENER/VICE-PRINCIPAL | PRINCIPAL | CHAIRMAN

SURYA

SURYA GROUP OF INSTITUTIONS

SCHOOL OF ENGINEERING AND TECHNOLOGY

(INTEGRATED CAMPUS) G.S.T Road, Vikiravandi - 605 652. Villupuram Dt.
www.suryagroup.edu.in

2nd INTERNATIONAL CONFERENCE

On

"Emerging Trends in Artificial Intelligence and Block Chain Technology"

INCETAIBCT'24

This is to certify that ~~Dr./~~Mr./~~Ms.~~ KESAVAN. V
of University College of Engineering - Villupuram *has presented a paper titled* RFID Based Secure Transformer Control System
in the 2nd International Conference on "Emerging Trends in Artificial Intelligence and Block Chain Technology" INCETAIBCT '24 organized by the Department of Computer Science and Engineering & Artificial Intelligence and Data Science on 30th April 2024.

CO-ORDINATOR | CONVENER/VICE-PRINCIPAL | PRINCIPAL | CHAIRMAN

SURYA GROUP OF INSTITUTIONS

SURYA

SCHOOL OF ENGINEERING AND TECHNOLOGY

(INTEGRATED CAMPUS) G.S.T Road, Vikiravandi - 605 652. Villupuram Dt.
www.suryagroup.edu.in

2nd INTERNATIONAL CONFERENCE

On

"Emerging Trends in Artificial Intelligence and Block Chain Technology"

INCETAIBCT'24

This is to certify that ~~Dr./Mr./Ms.~~ SARATHI . D
of University College of Engineering - Villupuram *has presented a paper titled* RFID Based Secure Transformer Control System
in the 2nd International Conference on "Emerging Trends in Artificial Intelligence and Block Chain Technology" INCETAIBCT '24 organized by the Department of Computer Science and Engineering & Artificial Intelligence and Data Science on 30th April 2024.

CO-ORDINATOR | CONVENER/VICE-PRINCIPAL | PRINCIPAL | CHAIRMAN