

RFID BASED CAR SECURITY SYSTEM WITH GSM



By

Capt Junaid Khan

Capt Omer Fakhar

Capt Rana Baber Waqas

Submitted to the Faculty of Department of Electrical Engineering

Military College of Signals

National University of Sciences and Technology, Islamabad

in partial fulfillment for the requirements of a B.E Degree in

Electrical (Telecom) Engineering

JUNE 2015

ABSTRACT

RFID BASED CAR SECURITY SYSTEM WITH GSM

RFID based car lock system is aimed at providing the best solution for car security system and theft control.

This project will consist of some combination of equipment and components to create a car security system that meets the security features and makes it even more advanced. RFID (Radio Frequency Identification) is the most reliable way to electronically identify, data capture, control and track using RF communication as RFIDs are easy to conceal or incorporate in other items. For example, in 2009 researchers at Bristol University successfully glued RFID micro transponders to live ants in order to study their behavior. This trend towards increasingly miniaturized RFIDs is likely to continue as technology advances.

The project is designed using RFID based smart cards for unlocking the car. Further integration of a GSM module gives GSM based control and alert system through which an instant alert via SMS will be sent to the owner if some unauthorized person tries to unlock the car. Finally the owner can simply lock the car, cut the fuel supply or ignition system by sending an SMS. SIM based location will also be provide in reply to a simple SMS command. Contingency for no GSM area has also been catered for.

Copyright © 2010 by Lt. Col Dr. Adil Masood Siddiqui.

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher at the address below.

Lt. Col Dr. Adil Masood

Head of Computer Software Engineering Department

Military College of Signals

Humayun Road

Rawalpindi.

*Dedicated to Allah Almighty, the Lord of the Worlds, our family and friends
who believed in us and for their unwavering support.*

ACKNOWLEDGEMENTS

Praise be to Allah, the Magnificent and the Merciful, for showering us with His countless blessings and for giving us the strength and patience to bear all hardships. We are grateful to our parents without their prayers, support and hard work this would not have been possible. We are thankful to our teachers and especially our supervisor, Dr. Adil Masood, for being our torch bearer and guiding us when else failed.

We would like to thank our family for bearing with us patiently and our friends who have been there to support us morally and technically.

CHAPTER 1 INTRODUCTION

1.1 MOTIVATION

Smart card based car lock system is a good theft control lock system as Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. Our car security system will require intense research in RFID Readers and Antennas, Passive and Active RFID, integrating and operating of GSM modules.

Car security systems have been in the market for quite long now and their use is increasing exponentially. Now every person owning a car wants a system that can guarantee a 100% security. So looking at this increased demand manufacturers are aiming at producing devices that can provide fool proof security. Today, the RFID industry claims a 90 percent reduction in theft rates for car models equipped with RFID starters, immobilizers and entry systems ^[1]. Both automakers and insurance companies have full faith in the devices, even going so far as to label them unbeatable. And certainly, the technology is an impressive display of security innovation.

The significant problems in the present society are robbery, crime and theft. This raises the security system issue. Several security systems have studied, applied and implemented automatic systems and modern technologies to secure assets against theft. But RFID is one of the most promising technologies, that has been widely applied into the access, control and security systems ^[2]. A typical RFID system consists of a reader and transponder. RFID is a leading automatic identification technology. RFID tags communicate information by radio waves through antennas on small computer chips attached to objects so that such objects may be identified, located, and tracked

1.2 PROJECT OVERVIEW

The objective of this project is to design an intelligent and innovative car security system to secure the car, detect intrusion and finally allow the owner to remotely control and locate his car.

The Wireless Security Car System Using RFID that we have designed operates following the figure shown in Figure 1. When the Passive RFID tag which is with the owner is placed near to the RFID reader that is installed in the car, the RDIF tag will receive the radio frequency via the antenna inside RFID tag. The radio frequency received will be converted into electrical power that is enough for the RFID tag to transmit the data back to the RFID reader. Then, the RFID reader reads the data from RFID tag. Further the RFID reader sends the tag ID of car owner to the PIC microcontroller. The PIC microcontroller process the tag ID i.e. user name, password and so on.

The PIC microcontroller is connected to the car door lock system, car engine and alarm, and the GSM module via relays. If the tag ID is correct then the microcontroller sends instruction to the lock system to unlock the door.

In case some unauthorized person tries to open the car then the tag ID wouldn't match the correct one. In this case the microcontroller will send an alert SMS to the owner via the GSM module. In response the owner can send a predefined command via SMS (GSM Module) to lock the car, seize the engine or any other task that has been predefined. Incase of no GSM service the system will automatically seize the car after a fixed time.

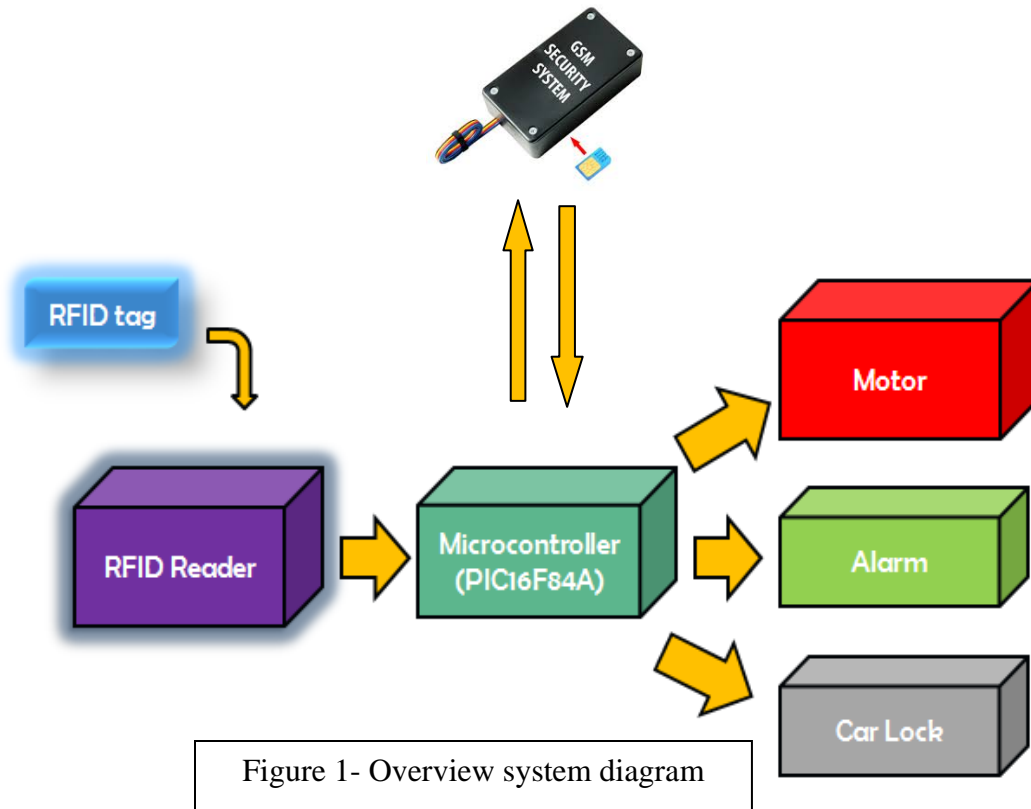


Figure 1- Overview system diagram

1.3 SCOPE AND SPECIFICATIONS OF THE PROJECT:

The project basically involves the design of hardware architecture which uses RFID readers/cards and GSM Module interfaced with a Micro controller to remotely secure and control various car activities. The final design was tested and practically implemented.

PIC16F88 microcontroller has been used as it is ideal for manufacturing equipment for data acquisition, power conditioning, environmental monitoring, telecom and consumer audio/video applications. ^[3]

Microcontroller is used as an interface between RFID reader (RDM 6300) , GSM module (SIM 900D) and car.

A hidden battery backup will be installed to keep the system active incase of car battery failure.

CHAPTER 2 LITERATURE REVIEW

It is well known that there is a requirement for securing cars and avoiding unauthorized entry. A lot of research has been done in the design of various types of automated security systems. Security systems based on alarm , mechanical keys or electronic chips are being constantly breached.

A car alarm going off without apparent reason, is an extremely annoying, not to mention embarrassing, situation for any car owner. Car alarm problems are one of the most common problems that car owners face. Some of the reasons of this problem are :

- Cars with remote entry systems can become faulty if the battery inside the remote starts to die down
- After replacing a remote control battery or a car battery you may find that the alarm system will switch on intermittently and annoy your neighbours at two o'clock in the morning.
- Circuit or wiring Installations can come with certain problems if the installer is not an accomplished mechanic or auto electrician. ^[4]

Mechanical keys are the weakest link in the car security chain. Car thieves can very easily make a duplicate key in a matter of time or can even open these mechanical locks in a matter of time and before one knows his car would be gone.

Instead of the traditional metal key, many cars now have an electronic fob which opens and starts the car. Thieves have discovered how to create copies of these electronic keys. BMW, one of the marques affected, has acknowledged the problem. ^[5]

Shortcomings present in the traditional security systems can be dealt with using our multiple security systems (or multi-layered security systems). Multi layered in the sense of RFID entry, door sensors and GSM based control. However, multi-system implementations will definitely be more demanding in terms of computational cost and organization. This requires careful integration and sharing of resources. Thus, a feasible system should be effective, practical and reasonable in cost. ^[6]

The idea behind this project is to meet the upcoming challenges of the modern practical applications of integrating a security system with wireless communication and to make a practical use of wireless communication and control system. There are many real life situations that require control of different devices remotely and to provide remote security.

Our project mainly deals with understanding and implementing the present technologies. In this we have carried out a thorough understanding of the proposed solution to the problem given in various research papers and come to an ultimate design of our car security system. In addition to this basic understanding, design of a system which uses different technologies and integrating them with each other was dealt with in this portion along with few other academic concepts for better implementation of the system. The approach used to achieve our project is summarized in the following flow chart

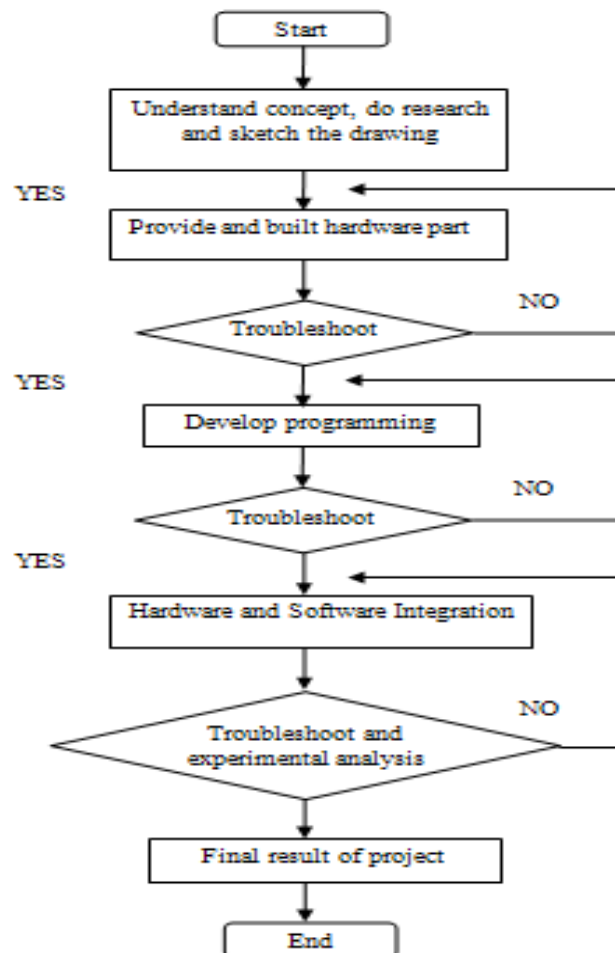


Figure -3 – (Flow Chart in Developing the Wireless Security Car Using RFID) System

CHAPTER 3 DESIGN AND DEVELOPMENT

3.1 Introduction

Car security has been a major issue where crime is increasing and everybody wants to take proper measures to prevent theft and intrusion. In addition there was a need to automate car security so that user can take advantage of the technological advancement in such a way that a person can access his car from anywhere.

In the block diagram shown below all the general parts of the system are shown. This design provides security in a multiple ways. The system allows entry into the car through only a valid RFID card/cards which the owner has. In case of unauthorized entry or intrusion, the control unit will be informed. A message will be sent to the user's cell phone to alert the user about the situation taking place. User will be able to send the necessary instructions about controlling and locating the car.

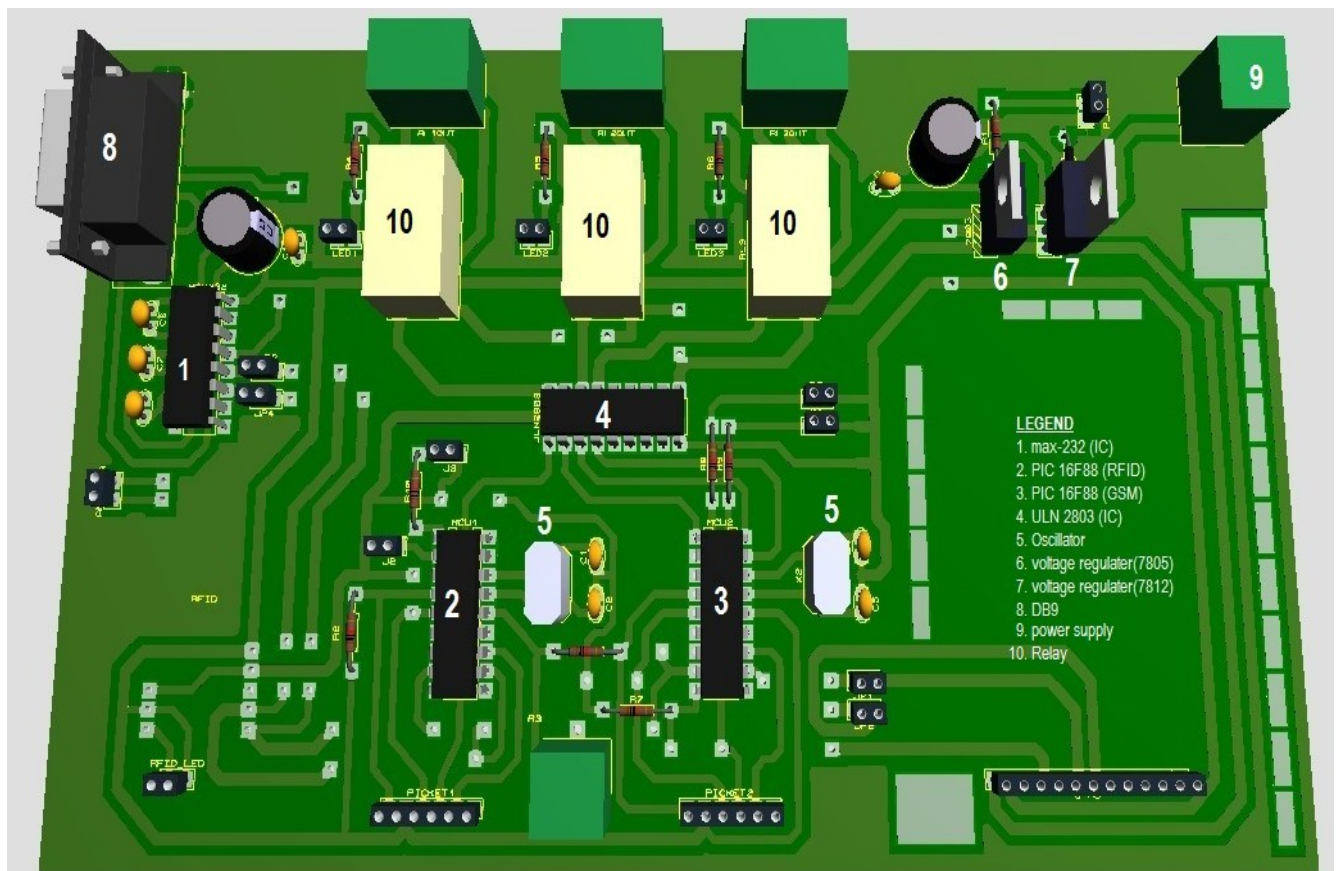


Figure - 4 Board layout

3D visualization of design prepared in ARES is given above. Main components used are shown in this diagram, their detailed description is given below.

3.2 Working of Components ^[7]

The step by step working of each element of the project is described below:

3.2.1 PIC 16F88

This microcontroller acts as an interface between RFID reader , GSM module and car. PIC16F88 microcontroller is ideal for manufacturing equipment for data acquisition, power conditioning, environmental monitoring, telecom and consumer audio/video applications.

The PIC16f88 has 18 pins. Those are two sets of 8 I/O ports and the VDD / VSS pins for the power supply. Except the power pins (#14 and #5), all others have more than one function. There are actually two sets of 8 ports, the RA0 through RA7 and the RB0 through RB7. These are our two main PORT registers. They are called PORTA and PORTB

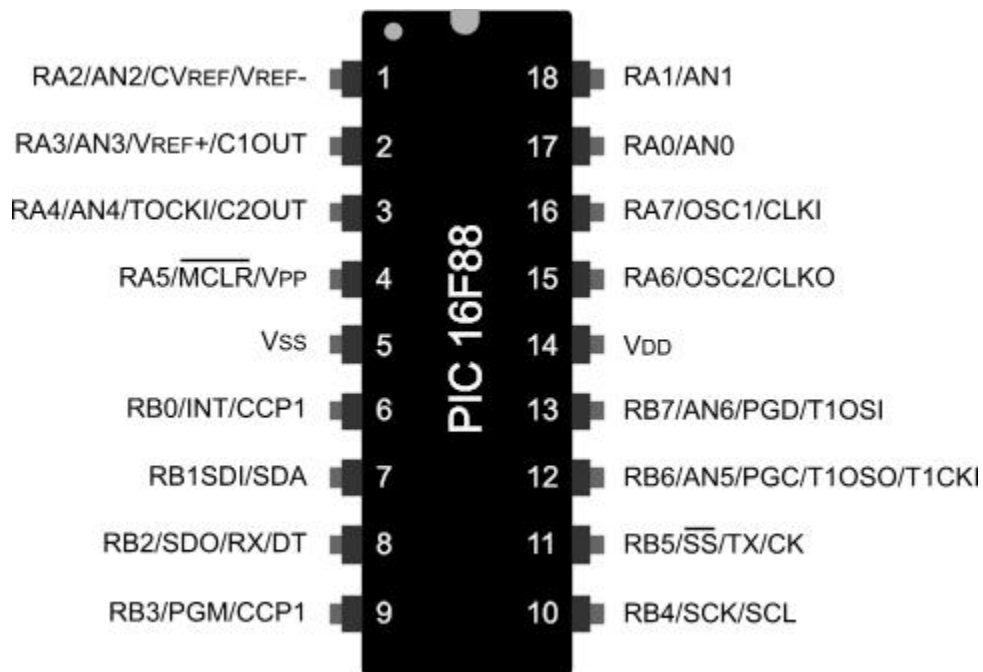


Figure - 5 Pin out of PIC 16F88 (MCU)

We have used two MCUs, one connected to RFID Reader while the other one with GSM module. Pin connections of both the MCUs is discussed below

MCU1 (RFID reader)

Pin #	Description
1 (RA2)	Comparator V_{REF} output connected to an LED to indicate functioning of MCU.
2 (RA3)	GND
4 (RA5)	Master clear (connected to picket) or prog voltage input (connected to V_{cc})
5 (V_{ss})	Connected to gnd of picket.
6 (RB0)	Output pin connected to relay1 via ULN.
8 (RB2)	USART asynchronous connected to the tx of RDM 600
11(RB5)	USART asynchronous tx pin for comm. With serial port via Max 232, connected to RFID Rx pin.
12 (RB6)	I/O pin Serial Programming clock pin connected with picket.
13 (RB7)	Serial programming data pin connected to picket.
14	V_{pp} , connected to V_{cc} coming from 7805.
15(RA6)	Oscillator output
16(RA7)	Connected to oscillator input

MCU2 (GSM module)

Pin #	Description
1 (RA2)	Comparator V_{REF} output connected to pin 2 of ULN to drive relay 2
2 (RA3)	GND , connected to pin 11 of GSM module showing functioning of MCU and GSM module.
3(RA4)	
4 (RA5)	Master clear (connected to picket) or prog voltage input (connected to V_{cc})
5 (V_{ss})	Connected to gnd of picket.
8 (RB2)	USART asynchronous connected to the tx of GSM module also connected to pin 11 of MCU (RFID reader).
9 (RB3)	Connected to door switch indicates opening and closing of doors.
11(RB5)	USART asynchronous tx pin connected to Rx pin of GSM module.
12 (RB6)	I/O pin Serial Programming clock pin connected with picket.
13 (RB7)	Serial programming data pin connected to picket.
14	V_{pp} , connected to V_{cc} coming from 7805.
15(RA6)	Oscillator output
16(RA7)	Connected to oscillator input
18(RA1)	I/O pin, connected to ULN for relay 3.

3.2.2 OSCILLATORS

Two oscillators are used, one with each MCU.

A 20 MHz oscillator is connected with the MCU driving GSM module.

While 10 MHz oscillator is connected with the MCU driving RFID module.

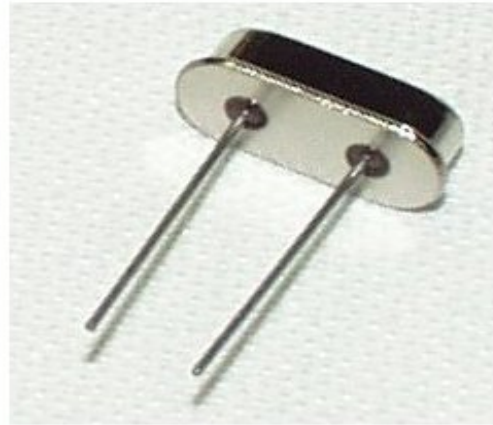


Figure - 6 Oscillator

3.2.3 MAX 232

APPLICATION INFORMATION

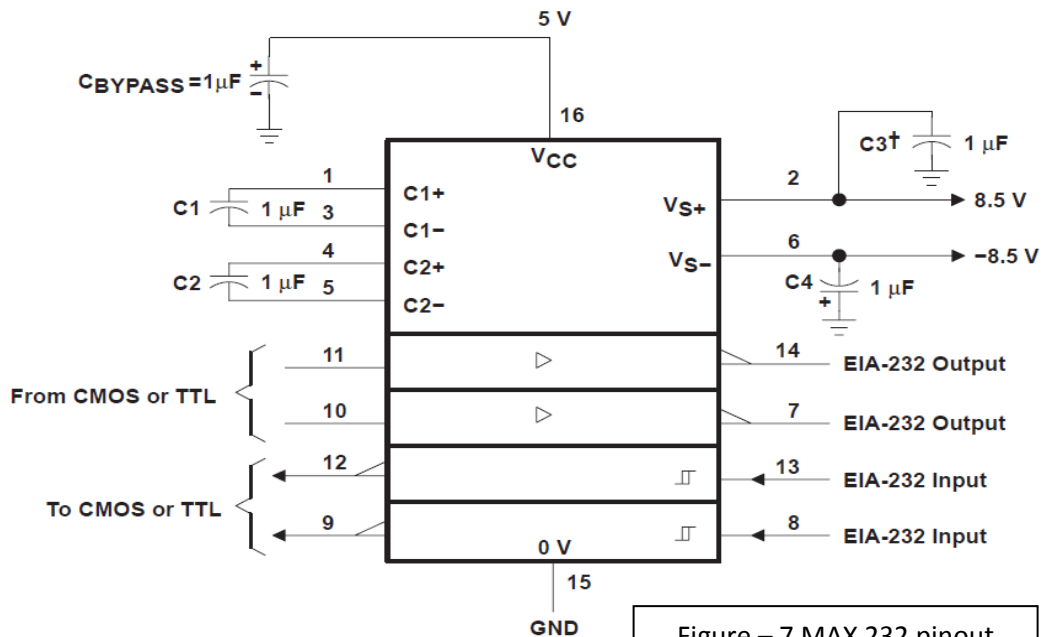


Figure – 7 MAX 232 pinout

Used for connection between computer serial port and RFID reader/MCU. It transforms the input signal from computer to bring it 5V level acceptable by MCU.

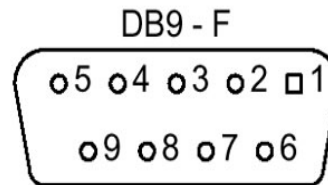
Pin 11 and 12 are connected to RFID reader and MCU. 12 is the output and 11 is the input pin. Pin 13 and 14 are connected to DB9 serial port.

3.2.4 DB9 Connection Detail

Pin 2 – Recieve data. It is connected to pin 14 of MAX-232

Pin 3 – Transmit data. It is connected to pin 13 of MAX-232

Pin 5 – GND



LOOKING INTO THE CONNECTOR

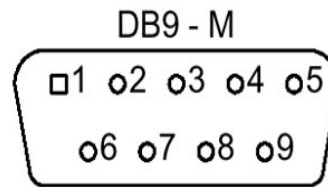


Figure – 8 DB9 connections

3.2.5 ULN 2803A

IC ULN2803 consists of octal high voltage, high current darlington transistor arrays. The eight NPN Darlington connected transistors in this family of arrays are ideally suited for interfacing between low logic level digital circuitry (such as TTL, CMOS or PMOS/NMOS) and the higher current/voltage requirements of lamps, relays, printer hammers or other similar loads for a broad range of computer, industrial, and consumer applications.

Features :

- Eight Darlingtons with Common Emitter.
- Output Current to 500 mA.
- Output Voltage to 50 V.
- Inputs pinned opposite outputs to simplify board layout.

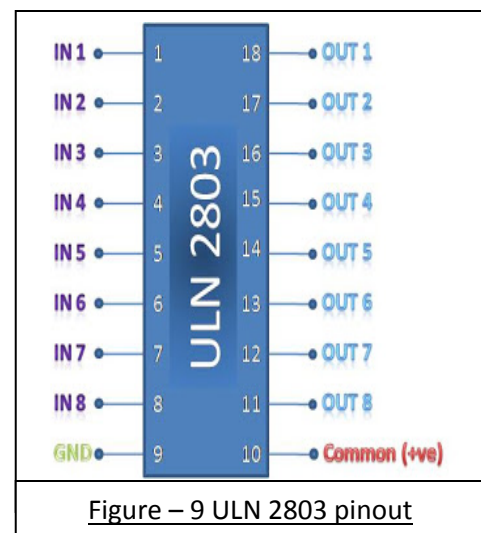


Figure – 9 ULN 2803 pinout

Working :

The ULN 2803 IC consists of eight NPN Darlington connected transistors (often called a Darlington pair). Darlington pair consists of two bipolar transistors such that the current amplified by the first is amplified further by the second to get a high current gain. The figure shown below is one of the eight Darlington pairs of ULN 2803 IC.

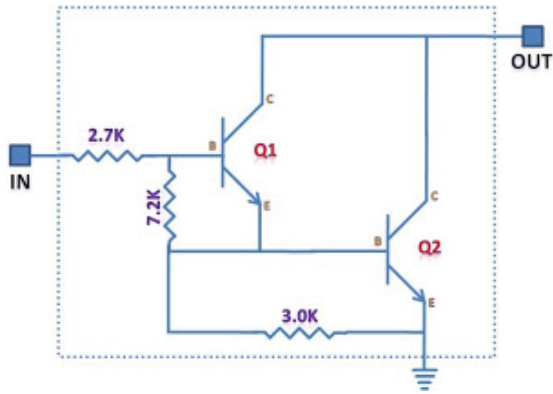


Figure – 10 ULN darlington pair

When a 5V input is applied to any of the input pins (1 to 8), output voltage at corresponding output pin (11 to 18) drops down to zero providing GND for the external circuit. Thus, the external circuit gets grounded at one end while it is provided +V_{cc} at its other end. So, the circuit gets completed and starts operating.

At pin 1,2,3 inputs for the three relays are received from the MCUs. Pin 18 , 16 and 15 are connected to Relay 1,2,3 respectively. 12V input is provided at pin 10. Thus the 5 volt signals obtained from the MCUs are enhanced into 12V and feed to the relays.

3.2.6 RELAYS

Relays are used where it is necessary to control a circuit by a low-power signal. Relays are like remote control switches and are used in many applications because of their relative simplicity, long life, and proven high reliability.

At C1 12V input is given to drive the relay while C2 gets instructions from MCU via ULN. COM1(common), NC1(normal closed) and NO1(normal) are connected to relay output. COM2 is connected to 5V V_{DD} while NO2 is connected to an LED to show relay operation.

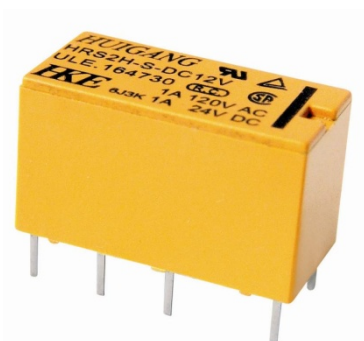


Figure – 11 Relay

3.2.7 Voltage Regulator 7812 & 7805

A voltage regulator is designed to automatically maintain a constant voltage level. 7812 provides an output voltage of 12V which drives ULN, relays and the GSM module. This 12V output is feed into 7805 input which as a result provides an output voltage of 5V which drives the

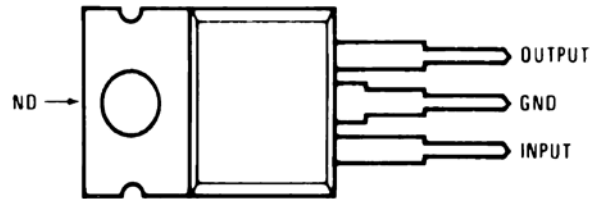


Figure – 12 Voltage Regulator

3.2.8 GSM Module (SIM 900D)

SIM900D delivers GSM/GPRS 850/900/1800/1900MHz performance for voice, SMS, Data, and Fax in a small form factor and with low power consumption. With a tiny configuration of 33mm x 33mm x 3 mm, SIM900D can fit almost all the space requirements in your M2M applications, especially for slim and compact demands of design.



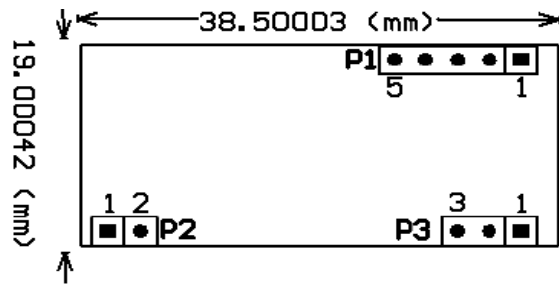
Figure – 13 GSM module with integrated SIM 900D

Connections :

- The Rx pin of the Module is connected pin 11 of MCU
- Tx pin is connected to pin 8 of MCU.
- Pkey pin (public key) connected to Pin 13 of MCU.
- 12 V power supply is given at pin 12 of GSM module.
- Pin 11 is grounded and also connected to pin 2,3 of mcu showing its activity via LEDs.

3.2.9 RDM 6300 (RFID Reader)

RDM6300 125KHz cardreader mini-module is designed for reading code from 125KHz card compatible read-only tags and read/write card . It can be applied in office/home security, personal identification, access control, anti-forgery, interactive toy and production control systems etc.



2. Pin definition (TTL interface RS232 data format):

P1:

PIN1	TX
PIN2	RX
PIN3	
PIN4	GND
PIN5	+5V(DC)

P2:

PIN1	ANT1
PIN2	ANT2

P3:

PIN1	LED
PIN2	+5V(DC)

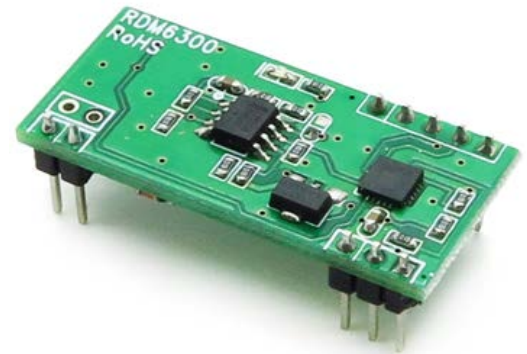


Figure – 14 RDM 6300 and Pinout

3.3 Hardware Implementation

Realization of the idea was made by the hardware implementation. The manufacturing stage of hardware was done in few parts which included installation of RFID and GSM module and then installing of various components for their integration and connectivity. Following steps were undertaken in manufacturing.

1. Designing schematic diagram
2. Transfer of schematic into PCB layout
3. Developing process
4. Soldering process
5. Testing

All these parts are explained according to their built-up sequence.

3.3.1 Design schematic diagram

A schematic is a representation of the elements of a system using abstract, graphic symbols rather than realistic pictures. It is a drawing showing all significant components, parts and their interconnections to a circuit, device or project by means of standard symbol. The very first step in hardware implementation of an electrical project is to make its schematic diagram. Schematic diagrams for major components and overall design were prepared and verified. The schematic diagrams make the implementation process easy because the placement of all the components and the connections of these components with each other became clearly known.

3.3.2 Transfer schematic into PCB layout

The fundamental steps involved in the conversion of schematic into PCB are ^[8]

- Set the Grids & Units to desirable values
- Set the Board outline
- Set the Pads options
- Set the design rules
- Set custom shortcuts

3.3.3 Developing process

In the process of development of the circuit, all the components were placed according to the schematic diagram. Before placement of the components drilling was carried out. All the components were placed according to the schematic diagram.

3.3.4 Soldering process

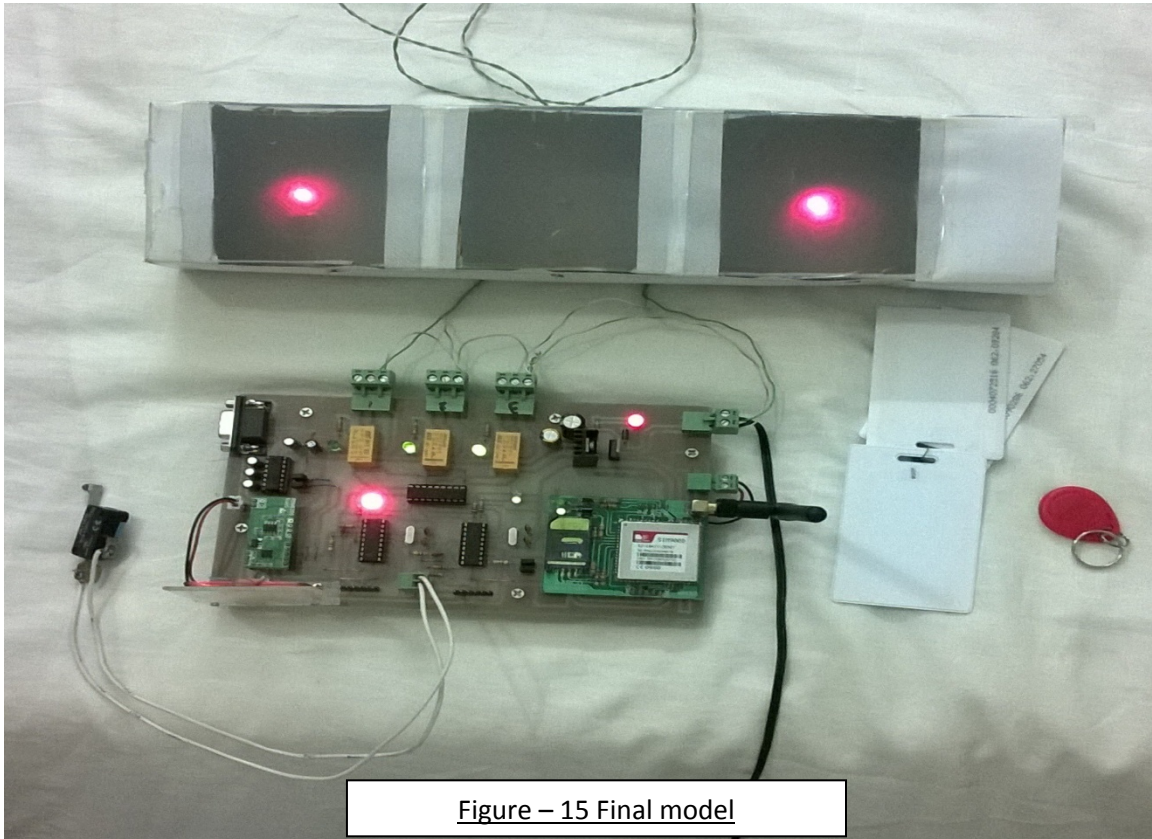
The components were fixed on PCB with the help of soldering. The most common problem suffered during soldering is wrong solder or the loose solder which causes the short circuit or the open circuit respectively. External indication board was connected for displaying relay functionality

3.3.5 Testing

All the circuits were tested with Digital Multi-Meter and oscilloscope. The response of the control actions in was also verified. Interconnectivity and proper responsiveness of RFID, GSM modules and relays was properly tested.

3.3.4 Modeling

The final model is shown below :



Chapter 4: Analysis and Evaluation

4.1 RFID code detection, MCU programming and testing

4.1.1 RFID code detection:

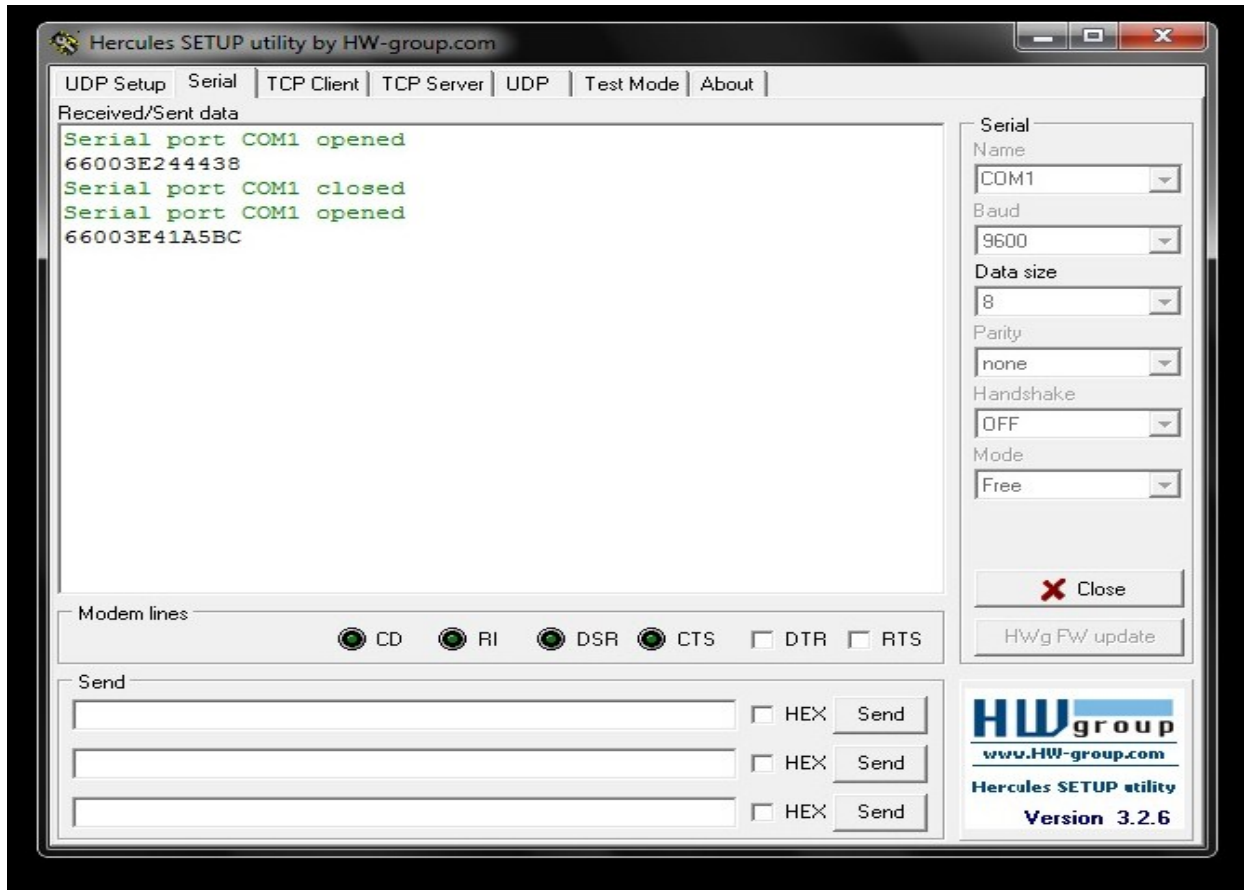


Figure – 16 RFID tag specific code

When RFID tag is brought near the reader antenna, it transmits a 12 character (48 bit) code. This code is shown in the above picture (fig-14). This code can be seen by connecting the RFID reader with the computer's COM port using the Hercules software.

4.1.2 Respective MCU programming: Two such codes from two different RFID tags can be seen in the above picture. In the C code written for the MCU integrated with RFID reader, both these codes were entered (Fig-17). Now when an RFID tag is brought near the RFID antenna, the 12 characters code is checked by the MCU. If the same card was

used then MCU will verify it and send a signal to the door relay to open the car door, if an unauthorized card is brought near then the generated code will not be verified and the car door will not open. Designing of the board has been completed. All the components mentioned in the previous chapter have been installed along with other circuitry components. We have been able to read the code from RFID tag, integrate it in the C code, burn it on the MCU and then operate the car door using the specific RFID tag.

```

18
19 #use rs232(baud=9600,parity=N,xmit=PIN_B5,rcv=PIN_B2,bits=8)
20
21 char ID[26]="66003E41A5BC66003E244438";
22 int8 c=0,counter=0,check=0;
23 char buff[16];
24 int ok_flag=0,rec_flag=0,start_flag=0;
25 #INT_RDA
26 void RDA_isr(void)
27 {

```

Figure – 17 Specific RFID tag code integrated

4.1.3 RFID program testing: Proteus simulation of C code for the MCU integrated with RFID reader is given below. On valid code received from the RFID tx the yellow LED will blink and on invalid code it will not blink. Thus the code was properly tested.

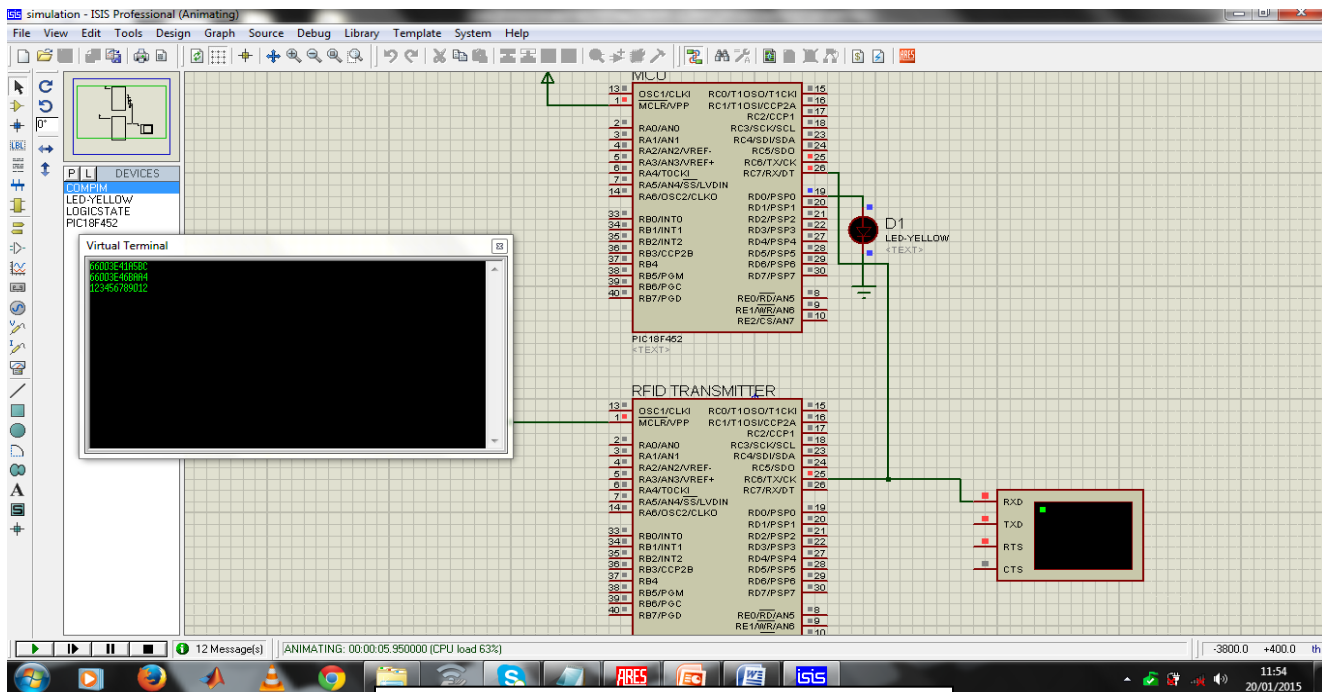


Figure – 18 Proteus simulation for RFID code

4.2 GSM programming and

Activation of GSM module to make it operational for communication between the car and GSM module was next completed. The highlighted numbers in the figure below shows the mobile number on which alert messages would be received from the GSM module. The code shown below (part of c code) was burnt onto the MCU which was then integrated with the GSM module. Fixed text messages have been initialized, which have been integrated into the MCU. These include “ STATUS, FCUT , ICUT , LOCK, location ” with these commands MCU via different relays cuts fuel supply, disables ignition system , locks the car respectively. After securing the car with the same commands the system can be reversed. ‘STATUS’ command shows the battery lvl, door fuel and ignition status. Through the location command approx SIM based location via respective BTS is obtained.

```

191     buff[24]='\0';
192     fputs("AT+CMGF=1",UART1);
193     delay_ms(1000);
194     fputs("AT+CMGS="+923314141687",UART1);
195     delay_ms(1000);
196     bc=buff[8];
197     if(bc=='0'){fputs("DISCHARGING",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c %%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c Volts\n\r",buff[13],buff[14],buff[15]);
198     if(bc=='1'){fputs("CHARGING",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c %%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c Volts\n\r",buff[13],buff[14],buff[15]);
199     if(bc=='2' && buff[12]==' '){fputs("CHARGING ",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c %%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c Volts\n\r",buff[13],buff[14],buff[15]);
200     if(bc=='2' && buff[13]==' '){fputs("CHARGING FULL",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c%c %%\n\r",buff[10],buff[11],buff[12]);fprintf(UART1,"VOLTAGE: %c.%c%c Volts\n\r",buff[13],buff[14],buff[15]);
201     if(door_st==1){fputs("DOOR IS OPEN",UART1);}
202     if(door_st==0){fputs("DOOR IS LOCKED",UART1);}
203     if(FF==1){fputs("FUEL OFF",UART1);}else{fputs("FUEL ON",UART1);}
204     if(IGF==1){fputs("IGNITION OFF",UART1);}else{fputs("IGNITION ON",UART1);}
205     fputs("***RFID & GSM BASED SECURITY SYSTEM IS WORKING ***",UART1);
206     delay_ms(1000);
207     fputc(0x1A,UART1);
208     output_low(LED1);
209

```

Figure – 19 C Code for MCU integrated with

The pictures below show the GSM commands and their response obtained from GSM module and respective status of relays:

4.3 Door security Small switches will be placed at each door. These switches will be connected to the MCU. If someone tries to open any door, the switch will come into play and a signal would be sent to the microcontroller. Now the microcontroller would recognize this as an unauthorized entry and will send an alert SMS to the owner. The MCU is programmed in such a way that if within 100 seconds of the security txt generation a 'LOCK' command is received the MCU will not operate the relays but if the command is not received the car will be locked and ignition/fuel would be cut. This provides security even in no GSM coverage area. The door relay was operated and the response was noted down.

CHAPTER 5: RECOMMENDATIONS FOR FUTURE WORK

The widespread deployment of RFID systems into consumer products may expose potential security threat as the wireless communication between the RFID reader and card may become subject to eavesdrop, replay and manipulation by an adversary to obtain tag identifier, track tag location, impersonate tag and reader, and trigger denial of service. These limitations force RFID protocol designers to build light weight authentication protocols and exclude almost all known authentication protocols based on standard cryptographic algorithms. At our level we can ensure security of our system by integrating latest and temper free RFID cards.

Further integration of a GSM module with build in GPS system would greatly enhance the security of the system. This would allow pin point tracking of the car incase of theft.

CHAPTER 6 CONCLUSION

6.1 Overview

The aim of this project was to design a system which provides a highly reliable security system. The main focus was to make the project easy to use. Keeping this in mind, different easy user interfaces were introduced. Secondly, users are allowed to carry out preventive measures according to the situation.

6.2 Objectives Achieved

A fully ready for operation system has been made. The RFID reader allows only authorized entry into the vehicle. The GSM module sends requested txt messages and on reception of valid commands sends instruction to the MCU which then operates the respective relays. The door sensors immediately notify the owner through an SMS if unauthorized entry is made.

6.3 Applications

The system has the application area ranging from a simple car security system to sensitive rooms and installations security. The system can not only defend against any unwanted interruption but also make a rapid action to stop that theft. Some of the applications of the project are as under.

- It can be used for theft protection which is a major concern nowadays.
- It can be used in banks to protect the entry and exit in locker rooms.
- It can also be used in military to guard against entry into any room which is out of bound for any unauthorized entry.

CHAPTER 5 BIBLIOGRAPHY

- [1] www.rfidjournal.com
- [2] Development and Implementation of RFID Technology by Cristina Turcu
- [3] www.microchip.com/PIC16F88
- [4] <http://www.buzzle.com/articles/car-alarm-problems.html>
- [5] <https://nakedsecurity.sophos.com/2012/09/18/bmw-stolen-hacking-kit>
- [6] Multi-Layered Architecture of Decision Support System, Institute of Mathematics and Informatics, Vilnius University
- [7] <http://www.microchip.com/forums/m107903.aspx>
- PIC Microcontroller and Embedded Systems by M.Ali Mazidi
 - Linear and Switching Voltage Regulator Fundamental Part 1 (www.ti.com/lit/an/snva558/snva558.pdf)
 - Signal Relays - Farnell (www.farnell.com/datasheets/1306687.pdf)
 - DOC_SIM900_AT Command Manual_V1.03
- [8] <http://www.edn.com/design/pc-board/4429670/6-tips-for-transferring-a-PCB-schematic-to-layout>

General references

- Active RFID Based Infant Security System - Springer (link.springer.com/chapter/10)
- www.rfidjournal.com/articles/view?1304
- en.wikipedia.org/wiki/Radio-frequency_identification
- www.autorentalnews.com/article/.../tracking-your-vehicles-with-rfid.aspx
- “Wireless Communication” by Rappaport
- White Paper on GSM Security by Christian Kroger
- Journal of electronics, China.
- The Center for Automotive Embedded Systems Security (CAESS)

APPENDICES

APPENDIX A

RFID BASED CAR SECURITY SYSTEM WITH GSM

<p style="text-align: center;"><u>Smart Card Based Car Lock System With GSM Based Advanced Security Alert And Control System</u></p>
<p><u>Brief Description of The Project / Thesis with Salient Specs:</u></p> <p>In solution to a fancy car alarm that'll go off in the middle of the night when a bird flies by and annoy the whole neighborhood our project consists of RFID based car lock system with GSM based security alert and control system. This project provides best solution for car security system and theft control. By using RFID based lock system user will have configured smart cards by which the car door lock can be operated. Simultaneously there will be a GSM based control and alert system. Whenever an unauthorized person will try to open the car an SMS alert will be given to the owner and the owner can lock the engine by sending an SMS.</p>
<p><u>Scope of Work :</u></p> <p>Smart card based car lock system is a good theft control lock system as Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. Traditional key based lock systems are easily breakable. RFID card based lock cannot be opened unless and until the authorized card is used. This system has additional security alert and control system using SMS service.</p>
<p><u>Academic Objectives :</u></p> <ol style="list-style-type: none">1. RFID Reader / RFID Antennas, Passive RFID, Active RFID2. Microcontroller interfacing3. GSM
<p><u>Application / End Goal Objectives :</u></p> <p>The main application of our project is in Modern car lock systems where it can be utilized instead of the noisy and partially insecure alarm systems. It can also be used in door lock systems for securing sensitive rooms and structures.</p>
<p><u>Previous Work Done on The Subject :</u></p> <p>Smart cards are extensively used in security and recognition systems. Various ideas have been floated in this regards and projects have also been done for inculcating smart</p>

card security systems in cars. An attractive feature that we provide is remote switching on / off and locking of engine.

- <http://www.wikihow.com/Make-a-Smart-Car-Surveillance-System-Using-a-Mobile-Phone>
- <http://www.electronicshub.org/gsm-based-projects/>
- http://www.smartcardbasics.com/pdf/7100030_BKL_Smart-Card-Security-Basics.pdf

Material / Resources Required :

Microcontroller
Smart card / RFID Reader
GSM module

No of Students Required

3

Special Skills Required :

Microcontroller programming and interfacing.
UART communication.
GSM communication

Approval Status:

Supervisor Name: Lt Col. Dr. Adil Masood
MCS NUST

Supervisor Signature: _____








Assigned to: Capt Muhammad Junaid Khan
Capt Omer Fakhar
Capt Rana Babur Waqas

HOD Signature: _____

Coordinator Signature: _____

APPENDIX B

TIMELINE

Ser	Task	2014						2015				
		Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
1	Theoretical study, research and prog guidelines											
2	Requirement Engineering											
3	Design & Architecture											
4	Coding/Implementation											
5	Testing(Unit/Integration)											
6	Testing											
7	Documentation											

APPENDIX C

COST BREAKDOWN

<u>ITEM</u>	<u>COST (Rs)</u>
RFID reader, cards and module	6500
GSM module	4500
MCU burner kit	2500
MCUs	1000
PCB board & designing	2500
Circuit components	2500
Adapters, backup battery	2500
Display design & demo	1000
<u>TOTAL</u>	23000/-

APPENDIX D

Demonstration outline

When the system is switched on, it checks its components connects the GSM module to the network and sends a message “ SECURITY SYSTEM ACTIVATED ” as shown in the diagram below. Now if a “ STATUS ” command is sent to the system, it shows the battery charging and output voltage level, whether door is locked or open, ignition and fuel is on or off in an SMS reply as shown below in fig.

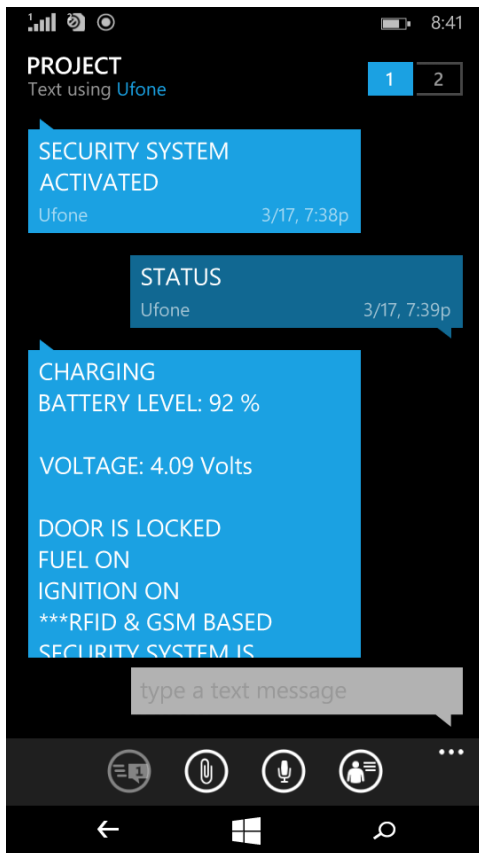


Figure – D.1 Status of the system sent

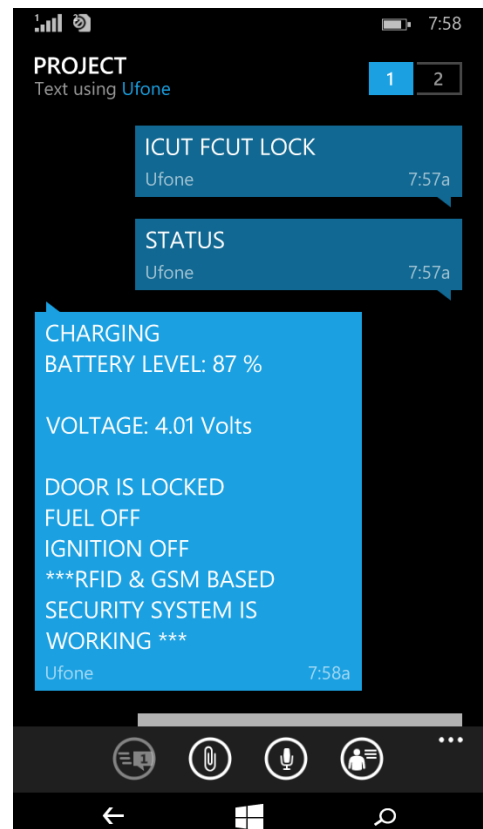


Figure – D.2 Status of the system after

The picture below shows the functioning of the RFID reader, i.e. only when the correct card is brought near the reader then the relay (indicated relay 1 in picture D.3) is operated. If an unauthorized entry into the car happens, an alert is received from the system as shown in figure below. In reply Commands can be sent and after that by

checking the status it becomes clear that the system has taken required action. If GSM service is not available and security is breached the system automatically seizes the car after 100 seconds.

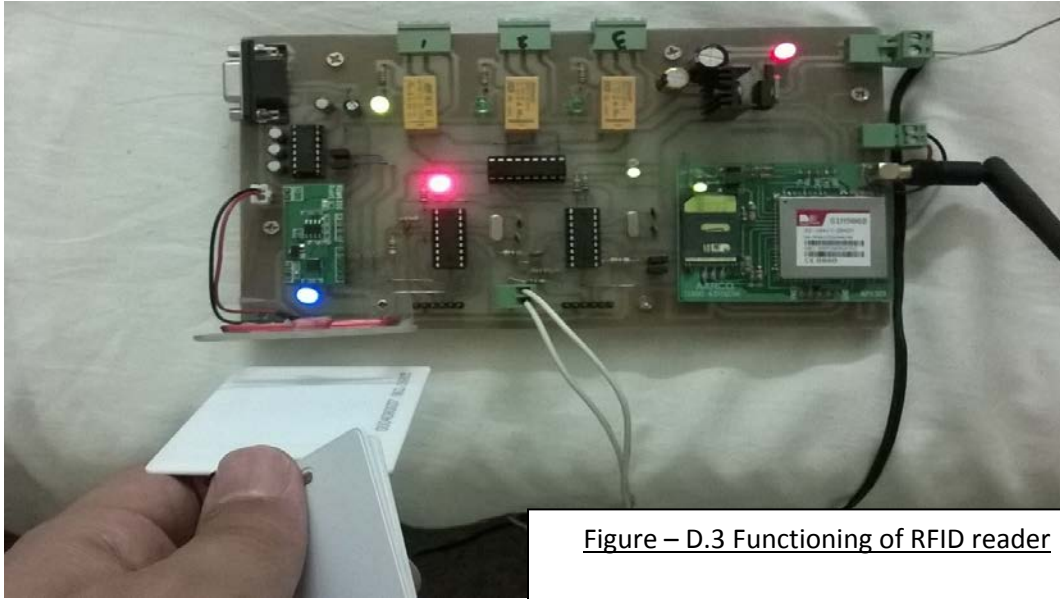


Figure – D.3 Functioning of RFID reader

When location command is sent the GSM module returns particular coordinates(MCC, MNC, loc and cell id) of the BTS with which the module is connected . it can be used to trace the location of car online.

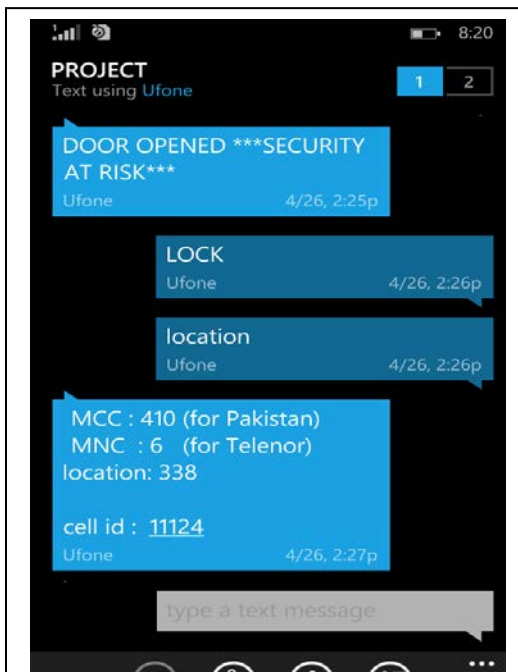


Figure – D.4 Alert and Location command



Figure – D.5 location on google map using opencellid.com

APPENDIX E

PROJECT CODES

RFID CODE

```
#include <16F88.h>

#FUSES NOWDT           //No Watch Dog Timer
#FUSES NOPUT          //No Power Up Timer
#FUSES HS              //High speed Osc (> 4mhz for PCM/PCH) (>10mhz for PCD)
#FUSES MCLR           //Master Clear pin enabled
#FUSES NOBROWNOUT     //No brownout reset
#FUSES NOLVP          //No low voltage prgming, B3(PIC16) or B5(PIC18) used
for I/O
#FUSES NOCPD          //No EE protection
#FUSES NOWRT          //Program memory not write protected
#FUSES NODEBUG        //No Debug mode for ICD
#FUSES NOPROTECT      //Code not protected from reading
#FUSES FCMEN          //Fail-safe clock monitor enabled
#FUSES IESO           //Internal External Switch Over mode enabled

#use delay(clock=10000000)

#use rs232(baud=9600,parity=N,xmit=PIN_B5,rcv=PIN_B2,bits=8)

char ID[26]="66003E41A5BC66003E244438";
int8 c=0,counter=0,check=0;
char buff[16];
int ok_flag=0,rec_flag=0,start_flag=0;
#INT_RDA
void RDA_isr(void)
```

```

{
c=fgetc();
  if(c==0x03)
    {
      rec_flag=1;
      start_flag=0;
      counter=0;
    }

  if(start_flag==1)
  { buff[counter++]=c;

  }
  if(c==0x02){ start_flag=1;counter=0;}

}

void main()
{
  enable_interrupts(INT_RDA);
  enable_interrupts(GLOBAL);

  while(TRUE)
  {
    if(rec_flag==1)
    { setup_uart(0);
      output_high(pin_A2);
      for(int i=0;i<30;i++)
      if(buff[i%12]==ID[i]){ check++;if(check==11){ok_flag=1; rec_flag=0; break;}}
      else check=0;
    }
    if(ok_flag==1)

```

```

    {output_high(PIN_A3);delay_ms(1000);output_low(PIN_A3);
counter=0;ok_flag=0;}
    counter=0;
    rec_flag=0;
    check=0;
    delay_ms(500);
    setup_uart(1);
    output_toggle(pin_A2);
    // enable_interrupts(GLOBAL);
}

}

```

GSM CODE

```

#include <16F88.h>

#FUSES NOWDT           //No Watch Dog Timer
#FUSES NOPUT           //No Power Up Timer
#FUSES HS              //High speed Osc (> 4mhz for PCM/PCH) (>10mhz for PCD)
#FUSES MCLR           //Master Clear pin enabled
#FUSES NOBROWNOUT     //No brownout reset
#FUSES NOLVP          //No low voltage prgming, B3(PIC16) or B5(PIC18) used
for I/O
#FUSES NOCPD          //No EE protection
#FUSES NOWRT          //Program memory not write protected
#FUSES NODEBUG        //No Debug mode for ICD
#FUSES NOPROTECT      //Code not protected from reading
#FUSES FCMEN          //Fail-safe clock monitor enabled
#FUSES IESO           //Internal External Switch Over mode enabled

#use delay(clock=20000000)

```

```
#use rs232(baud=9600,parity=N,xmit=PIN_B5,rcv=PIN_B2,bits=8,stream=UART1)
```

```
#define LED1      PIN_A3
```

```
#define LED2      PIN_A4
```

```
#define P_K       PIN_B7
```

```
#define LOCK_RELAY PIN_A2
```

```
#define IGNITION_RELAY PIN_A1
```

```
#define FUEL_RELAY PIN_A0
```

```
#define DOOR      PIN_B3
```

```
char led_counter=0;
```

```
char rd=0,c=0;
```

```
int1
```

```
ok_flg=0,at_flg=0,lock_flag=0,ign_flag=0,fuel_flag=0,open_flag=0,door_st=0,battery_flg=0,status_flag=0,IGF=0,FF=0;
```

```
unsigned int8 ok=0,lock=0,fuel=0,ign=0,open=0,count=0,status=0;
```

```
char init_sms[26]="SECURITY SYSTEM ACTIVATED";
```

```
char door_open[35]="DOOR OPENED ***SECURITY AT RISK***";
```

```
char buff[25],bc=0;
```

```
int1 gsm_init(void);
```

```
void send_sms(char text[]);
```

```
void statuses(void);
```

```
#INT_RDA
```

```
void RDA_isr(void)
```

```
{
```

```
    rd=fgetc(UART1);
```

```
    if(battery_flag==1){buff[count++]=rd;}
```

```
    if(at_flg==1)
```

```
    {
```

```
        if(rd=='O'||rd=='K') ok++;
```

```

        else ok=0;
    }
    if(ok>=2){
        ok=0;
        ok_flg=1;
    }
    if(rd=='O' || rd=='P' || rd=='E' || rd=='N')open++;
    else open=0;
    if(open==4){open_flag=1;}

    if(rd=='L' || rd=='O' || rd=='C' || rd=='K')lock++;
    else lock=0;
    if(lock==4){lock_flag=1;}

    if(rd=='S' || rd=='T' || rd=='A' || rd=='U')status++;
    else status=0;
    if(status==6){status_flag=1;}

    if(rd=='I' || rd=='C' || rd=='U' || rd=='T')ign++;
    else ign=0;
    if(ign==4){ign_flag=1;}

    if(rd=='F' || rd=='C' || rd=='U' || rd=='T')fuel++;
    else fuel=0;
    if(fuel==4){fuel_flag=1;}
}
void main(void)
{
    int ii;

    for(ii=0;ii<10;ii++){output_high(LED1);delay_ms(50);output_low(LED1);delay_ms(500
);}

```

```

output_low(LOCK_RELAY);output_low(IGNITION_RELAY);output_low(FUEL_REL
AY);
    setup_timer_0(RTCC_INTERNAL|RTCC_DIV_32);
    enable_interrupts(INT_TIMER0);
    enable_interrupts(INT_RDA);
    enable_interrupts(GLOBAL);

while(gsm_init()!=1);
send_sms(init_sms);
delay_ms(2500);
// delay_ms(2500);
// statuses();

while(TRUE)
{
    if(open_flag==1)
        {output_high(LOCK_RELAY);open_flag=0;open=0;door_st=1;}
    if(lock_flag==1)
        {output_low(LOCK_RELAY);lock_flag=0;lock=0;door_st=0;}
    if(ign_flag==1)
        {output_toggle(IGNITION_RELAY);ign_flag=0;ign=0;IGF=~IGF;}
    if(fuel_flag==1)
        {output_toggle(FUEL_RELAY);fuel_flag=0;fuel=0;FF=~FF;}
    if(status_flag==1)
        {statuses();status_flag=0;status=0;}
    if(input(DOOR) &&
door_st==0){delay_ms(10);output_high(LED1);send_sms(door_open);delay_ms(1000);}
        if(input(PIN_B0) &&
door_st==0){output_high(LOCK_RELAY);door_st=1;output_high(LED1);delay_ms(10
00);}

```



```

        if(input(PIN_B0) &&
door_st==1){output_low(LOCK_RELAY);door_st=0;output_high(LED1);delay_ms(100
0);}
        output_low(LED1);
        delay_ms(100);
    }
}

```

```

}

```

```

#INT_TIMER0

```

```

void timer0_isr(){
    led_counter++;
    if(led_counter==0){
        output_toggle(LED2);
    }
}

```

```

int1 gsm_init(void)

```

```

{
    char j,k;
    fputs("ATH",UART1);delay_ms(1000);
    at_flg=1;
    for(j=0;j<4;j++){
        ok=0;ok_flg=0;
        fputs("AT+CNMI=2,2",UART1);
        for(k=0;k<50;k++){
            delay_ms(30);
            if(ok_flg==1){
                k=102;j=20;
                at_flg=0;
            }
        }
    }
}

```

```

        delay_ms(1000);
        fputs("ATE0",UART1);delay_ms(1000);
        setup_timer_0(RTCC_INTERNAL|RTCC_DIV_64);
        return 1;
    }
}
setup_uart(0);setup_uart(1);delay_ms(10);
}

output_low(P_K);delay_ms(1800);output_high(P_K);delay_ms(3000);
setup_timer_0(RTCC_INTERNAL|RTCC_DIV_4);
for(j=0;j<4;j++){
    ok=0;ok_flg=0;at_flg=1;
    fputs("AT\r",UART1);delay_ms(1000);
    if(ok_flg==1){
        k=102;j=20;
        delay_ms(5000);
        ok=0;ok_flg=0;
        fputs("AT+CNMI=2,2,0,0,0\r",UART1);delay_ms(1000);
        at_flg=1;
        if(ok_flg==1){
            fputs("ATE0\r",UART1);delay_ms(1000);
            setup_timer_0(RTCC_INTERNAL|RTCC_DIV_64);
            return 1;
        }
        setup_timer_0(RTCC_INTERNAL|RTCC_DIV_16);
    }
}
setup_uart(0);setup_uart(1);delay_ms(10);
}
at_flg=0;
setup_timer_0(RTCC_INTERNAL|RTCC_DIV_4);

```

```

    return 0;

}

void send_sms(char text[])
{

    fputs("AT+CMGF=1",UART1);
    delay_ms(1000);
    fputs("AT+CMGS=\"+923314141687\"",UART1);
    delay_ms(1000);
    fputs(text,UART1);
    delay_ms(1000);
    fputc(0x1A,UART1);
    delay_ms(1500);
}

void statuses()
{
    output_high(LED1);
    count=0;
    battery_flag=1;
    fputs("AT+CBC",UART1);
    delay_ms(1000);
    battery_flag=0;
    buff[24]='\0';
    fputs("AT+CMGF=1",UART1);
    delay_ms(1000);
    fputs("AT+CMGS=\"+923314141687\"",UART1);
    delay_ms(1000);
    bc=buff[8];
}

```

```

    if(bc=='0'){fputs("DISCHARGING",UART1);fprintf(UART1,"BATTERY LEVEL:
%c%c %%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c
Volts\n\r",buff[13],buff[14],buff[15]);}
    if(bc=='1'){fputs("CHARGING",UART1);fprintf(UART1,"BATTERY LEVEL:
%c%c %%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c
Volts\n\r",buff[13],buff[14],buff[15]);}
    if(bc=='2' && buff[12]==',' ){fputs("CHARGING
",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c
%\n\r",buff[10],buff[11]);fprintf(UART1,"VOLTAGE: %c.%c%c
Volts\n\r",buff[13],buff[14],buff[15]);}
    if(bc=='2' && buff[13]==',' ){fputs("CHARGING
FULL",UART1);fprintf(UART1,"BATTERY LEVEL: %c%c%c
%\n\r",buff[10],buff[11],buff[12]);fprintf(UART1,"VOLTAGE: %c.%c%c
Volts\n\r",buff[14],buff[15],buff[16]);}
    if(door_st==1){fputs("DOOR IS OPEN",UART1);}
    if(door_st==0){fputs("DOOR IS LOCKED",UART1);}
    if(FF==1){fputs("FUEL OFF",UART1);}else{fputs("FUEL ON",UART1);}
    if(IGF==1){fputs("IGNITION OFF",UART1);}else{fputs("IGNITION
ON",UART1);}
    fputs("***RFID & GSM BASED SECURITY SYSTEM IS WORKING
***",UART1);
    delay_ms(1000);
    fputc(0x1A,UART1);
    output_low(LED1);

}

```