Sudan University of science and Technology

College of graduate studies

Enhancement of Vehicle's Security System

تحسين نظام حماية المركبات

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of M.Sc. in Mechatronics Engineering

Submitted by: Husam Eldeen Elhadi Osman

Supervisor: Dr. Alaa Eldeen Awouda

February 2018

بسم الله الرحمن الرحيم

ًا إِلَّا وُسْعَهَا ۚ لَهَا مَا كَسَبَتْ وَعَلَيْهَا مَا
تُؤَاخِذْنَا إِن نَّسِينَا أَوْ أَخْطَأْنَا ۚ رَبَّنَا وَلَا تَحْمِلْ
هُ عَلَى الَّذِينَ مِن قَبْلِنَا ۚ رَبَّنَا وَلَا تُحَمِّلْنَا مَا
اعْفُ عَنَّا وَاغْفِرْ لَنَا وَارْحَمْنَا ۚ أَنتَ مَوْلَانَا
فَانصُرْنَا عَلَى الْقَوْمِ الْكَافِرِينَ ﴿286﴾

صدق الله العظيم

سورة البقره الايه (286)

الإهداء

إلى من ركع العطاء أمام قدميها... وأعطتنا من دمها وروحها وعمرها حبا وتصميما ودفعا لغدٍ أجمل.... إلي ملاكي في الحياه إلي معني الحب.. وإلي معني الحنان والتفاني.. إلي بسمة الحياة وسر الوجود...إلي من كان دعائها سر نجاحي وحنانها بلسم جراحي... إلى الغالية التي لا نرى الأمل إلا من عينيها..... **أمي الحبيبة**

إلى كل من ساعدني في انجاز هذا العمل... شكري الجزيل وامتناني

إلى اليد الطاهرة التي أزالت من أمامنا أشواك الطريق ورسمت المستقبل بخطوط من الأمل والثقة... إلي من احمل اسمه بكل افتخار... إلى الذي لا تفيه الكلمات والشكر والعرفان بالجميل..... **أبي الحبيب**

إلى من أخذ بيدي ... ورسم الأمل في كل خطوة مشيتها...... **زوجتي الغاليه**

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إلى رياحين حياتي...... **أخواتي**

إلى من جعلهم الله إخوتي بالله ... إلى الذين تسكن صورهم وأصواتهم أجمل اللحظات والأيام التي عشتها..... **زملائي**

ACKNOWLEDGEMENT

Thanks and appreciation

First of all Thanks to Allah,

We can never thank Allah enough for the countless bounties He blessed us with.

I would like to express my deepest appreciations to All Members of the Faculty of Engineering, Sudan University of Science and Technology, College of Graduate Studies.

I would like to express my sincere thanks and appreciate to

Dr. Alaa Eldeen Awouda

For the time and effort he invested to support the work to be done perfectly and properly.

I take this opportunity to thanks my parents and my wife for their supporting and unceasing encouragement.

And also thanks a lots and appreciation to all who directly or indirectly, have lent their helping hand to contribute with me to complete this work specially Eng. Muaz Awad “ZEC” and Eng. Yusuf Musaad “Zeta Automation Center”.

ABSTRACT

Generally the anti-theft security system becomes very important these days according to the high rate recording of the theft crimes cases around the world. In this project the vehicles security system type will be the focus of the study. The main objective of this vehicle's anti-Theft Security System project is to design a smart security system to provide the highest level of protection to the owners of the vehicles or the authorized persons for unauthorized usage objects. In the result the vehicle's theft crime cases rate will drop off. To provide the security whenever any unauthorized persons use the vehicle or try to drive it by illegally ways or failed to enter the correct password then the system will cutting off the entire power through the main relay and the system will texting message by GSM module. The most important future in this system is the vehicle cannot move for unauthorized persons even the engine was running, because the system will cutting off the power of the fuel and ignitions systems through the second relay in case of touching the fuel pedal. This feature is done by creating two levels of security. Once the second level of the security system is activated that is no move future is enabled, the vehicle cannot come into running position until the user or the authorized persons enter the valid password. After three times wrong entrance of the correct password the system will cutting off the entire power of the vehicle and turn to the first level of the security system.

المستخلص

نظم الحمايه ضد السرقه اصبحت من أهم الأشياء من حولنا وذلك لإرتفاع معدل جريمة السرقه في كل انحاء العالم. في هذا البحث سيكون نظم اجهزة حماية المركبات موضوع او محور الدراسه. من اهم اهداف نظام حماية المركبات تصميم نظام حمايه ذكي لتذويد مالك العربه او من لديه ترخيص او توكيل لأستعمال المركبه بأعلي مستويات الحماية ضد الاستعمال الغير قانوني, مما يؤدي الي تقليل نسبه جرائم سرقة المركبات. ويكون تذويد مالك المركبه او من لديه صلاحيه لإستعمالها بالحماية اللازمه عندما يتم استعمال المركبه بصوره غير قانونيه او فشل في إدخال كلمة المرور عبر قطع طاقة النظام الكليه من خلال المنظم الرئيسي وإرسال رساله نصيه لمالك المركبه او من لديه صلاحية لإستعمالها عبر جهاز GSM ملحق بنظام الحمايه. من اهم مميزات النظام عدم امكانية تحريك المركبه من مكان الي مكان بواسطة اشخاص ليس لديهم صلاحية لذلك حتي ولو كان المحرك يعمل, وذلك لان النظام سيقوم بقطع الطاقة عن كل من نظام مضخة الوقود ونظام الإشتعال الكهربائي للمركبه من خلال المنظم الفرعي او الثاني ويكون ذلك في حالة لمس دواسة الوقود. هذه الخاصيه تمت بواسطة عمل مستويين من الحمايه, وطالما ان نظام الحمايه في المستوي الثاني وتحت التفعيل هذا سيؤدي الى عدم امكانية استعمال المركبه, ولن يتم استعمالها او تحريكها من مكان الي اخر إلا بعد إدخال كلمة المرور الصحيحه بواسطة المالك او من لديه صلاحية لإستعمال المركبه. وفي حالة الفشل في إدخال كلمة المرور الصحيحه ثلاثة مرات سيقوم النظام بقطع الطاقه الكليه للمركبه والتحول الي مستوي الحمايه الاول.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description	Page
LCD	Liquid Crystal Display	1
GSM	Global System for Mobile Communication	4
GPS	Global Positioning System	4
DVD	Digital Video Disc	5
MCU	Microcontroller Unit	5
CPU	Central Process Unit	6
I/O	Input/Output	6
IC	Integrated Circuit	7
DIP	Dual In-Line Package	7
ROM	Read Only Memory	8
RAM	Random Access Memory	8
ALU	Arithmetic Logic Unit	8
SFRs	Special Function Registers	8
GPRs	General Purpose Registers	8
GPRS	General Packet Radio Service	13
EDGE	Enhanced Data Rates for Global (GSM) Evolution	13
3G	3rd Generation	13
IMT	International Mobile Telephone System	13
UMTS	Universal Mobile Telecommunication System	13
DSL	Digital Subscriber Line	14
SMS	Short Message Service	14
HSCSD	High Speed Circuit Switched Data	14
WAP	Wireless Application Protocol	15
PCNs	Personal Communication Networks	15
PCSs	Personal Communication Systems	15

SIM	Subscriber Identity Module	15
RS232	recommended Standard	20
DC	Direct Current	20
COM	Communication Port	23
USB	Universal Serial Bus	25
CR	characters	26
DB	Data Bit	27
TX	Transmit Data	28
RX	Receive Data	28
CTS	Clear to Send Data	28
RTS	Request to Send Data	28
LED	Light Emitting Diode	29
R/S	Register Select	30
PCB	Print Circuit Board	34
ARES	Advanced Routing and Editing Software	34
ISIS	Intelligent Schematic Input System	34

Chapter One

Introduction

1.1. Overview:

These days the vehicles theft cases are higher than any time and higher than any types of crimes. Vehicles theft has become the nation's first property crime. The phenomenon of vehicles theft problem is not only effect on the vehicle’s owner but also had turn to insurance companies, especially if the type of insurance is comprehensive, so many insurance companies are dealing every day with not negligible rate of vehicles theft crimes. The owners of vehicles do their best to protect their vehicles from the theft, but even the sophisticated anti-theft systems are not enough to prevent the vehicles theft crimes. The main functions of the anti-theft system are to detect the vehicle theft and to alert the vehicle owner.

The proposed system in this research can bring down the crime’s rate in case of vehicles theft, it’s uses a combinations of a numeric Keypad, LCD, Relays, Door sensor, Microcontroller and acceleration sensor, that means the vehicles are still safeguarded even the vehicle key gets hold to someone not authorized to drive the vehicle, and still safeguarded even someone not authorized to drive the vehicle gets inside the vehicles and the engine of the vehicle was running. Simply this technology will protect the vehicles from the theft crimes even in case the engine of vehicle is running “started”.

1.2. Problem Statement:

Every day a lots of vehicles theft happened, either by using the owner vehicle’s key or without the key, also the vehicle theft crime can happened either the vehicle engine was running already or not running, but mostly happened during the vehicle’s engine already in running mode and the vehicle without observation.

1.3. Proposed Solution:-

The proposed solution in this research is to design a smart and effective anti-theft system for vehicles using Microcontroller.

1.4. Research Importance:

Importance of this research leads to have:

- Designing a smart anti-theft system for vehicle's security.
- Significantly reduces the likelihood of your vehicle being stolen.
- Useful for insurance companies.

1.5. Research Aim and Objectives

1.5.1. Research Aim

The main aim of the research is to design a smart and effective security system for vehicles.

1.5.2. Research Objectives

- Drop off the vehicle's theft crimes rate.
- Simulate the proposed system.
- Practical implementation for the proposed system.

1.6. Methodology

The technologies which will be used in this research depend on Microcontroller, (numeric Keypad, door sensor and acceleration sensor) input units and (LCD, relays to shut down the power of the vehicle) output units. Designing the proposed control security system and presenting the system flow chart will be the first step after picking and selecting the system components, and then the program will be created to drive the system.

After designing and programming, the simulation will be run for configuration the overall system, after all of that the output of the computer will be setting to match the simulation configuration to implement the proposed system.

Finally the overall system performance testing and evaluation will be repeated until reach the optimum design and the optimum program.

1.7. Thesis Outline

This thesis consists of five chapters:

- **Chapter One** gives an introduction include the problem statement, proposed solution and the objectives.
- **Chapter Two** is about the literature reviews, describe system parts and previous works.
- **Chapter Three** deals with the system design and explain the design of the system.
- **Chapter Four** coverage’s the simulation result and discussion.
- **Chapter Five** conclusion & recommendations.

Chapter Two

Background and Literature Review

2.1. Previous Works

In (2012) Mr. Mohammed abuzalata and Mr. Muntaser Momani designed “Anti-theft Car Protection System Based on Microcontroller”, they used combination keypad, LCD, solenoids directional valve and microcontroller (PIC) to protect the vehicles from not to running the engine [1].

In (2012) Mr. Visa M. Ibrahim and Mr. Asogwa A. Victor designed “Microcontroller Based Anti-theft Security System Using GSM Networks with Text Message as Feedback”, they used GSM, Sensors and microcontroller to stop the engine and protect the vehicle from not to go far away [2].

In (2013) Mr. Arun Sasi and Mr. Lakshami R Nair designed “Vehicle Anti-Theft System Based On An Embedded Platform”, they used fingerprint recognizer, combination keypad, vehicle’s window vibration sensor, GSM module, GPS, microcontroller and wheel pressure sensor to protect the vehicles from not to running the engine and not getting inside the vehicle without a permition, and also to protect the vehicles from theft crime by using lifter trucks to lift the vehicles and escape far away for the vehicle’s owner [3].

In (2013) R.Ramani, S.Valarmathy and Dr.N.Suthanthira Vanitha designed “Vehicle Tracking and Locking System Based on GSM and GPS”; they used a combination keypad, IR sensor, microcontroller, GPS, GSM, LCD, MAX232driver and relay driver to protect the vehicles from theft crimes and to determine the location of the vehicle after the theft crime. The system will lock the doors automatically and gradually decrease the speed until cutoff the power of engine [4].

In (2015) Mr. Pritpal Singh, Mr. Tanjot Sethi and Mr. Bibhuti Bhusan Biswal designed “A Smart Anti-theft System for Vehicle Security”; they used GPS, GSM and microcontroller to determine the location of the vehicle after the theft crime and cutoff the power of engine [5].

In (2015) Mr. Vaishanavi, Mr. K.Priyanga and Mr. S.Sangeetha designed “Vehicle Security System Using GSM Technology”; they used Vibration Sensor, LCD, Buzzer, GSM and microcontroller to protect the vehicle from being stolen [6].

2.2. Microcontroller

The microcontroller is simply a computer on a chip. It is one of the most important developments in electronics since the invention of the microprocessor itself. It is essential for the operation of devices such as mobile phones, DVD players, video cameras, and most self-contained electronic systems. The small LCD screen is a good clue to the presence of an MCU (Microcontroller Unit) – it needs a programmed device to control it. Working sometimes with other chips, but often on its own, the MCU provides the key element in the vast range of small programmed devices which are now commonplace.

Although small microcontrollers are complex, and we have to look carefully at the way the hardware and software (control program) work together to understand the processes at work.

This research will show how to connect the (PIC16F877A) microcontrollers to the outside world, and put them to work. (PIC16F877A) has a good range of features and allows most of the essential techniques to be explained. It has a set of serial ports built in, which are used to transfer data to and from other devices, as well as analogue inputs, which allow measurement of inputs such as temperature.

The microcontroller’s programming language is relatively simple as compared with a microprocessor’s programming language such as the Intel Pentium™, which is used in the PC.

The supporting documentation for the PIC MCU is well designed, and a development system, for writing and testing programs, can be downloaded free from the Microchip website (www.microchip.com). [7]

2.2.1. Processor System

The microcontroller contains the same main elements as any computer system:

- Processor.
- Memory.
- Input/Output.

In a PC, these are provided as separate chips, linked together via bus connections on a printed circuit board, but under the control of the microprocessor (CPU). A bus is a set of lines which carry data in parallel form which are shared by the peripheral devices. The system can be designed to suit a particular application, with the type of CPU, size of memory and selection of input/output (I/O) devices tailored to the system requirements. In the microcontroller, all these elements are on one chip. This means that the MCU for a particular application must be chosen from the available range to suit the requirements. In any given circuit, the microcontroller also tends to have a single dedicated function (in contrast to the PC); this type of system is described as an embedded application (Figure 2.1). [7]

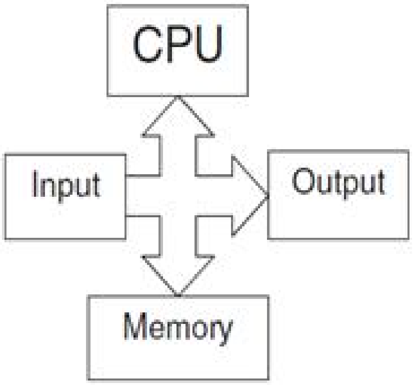


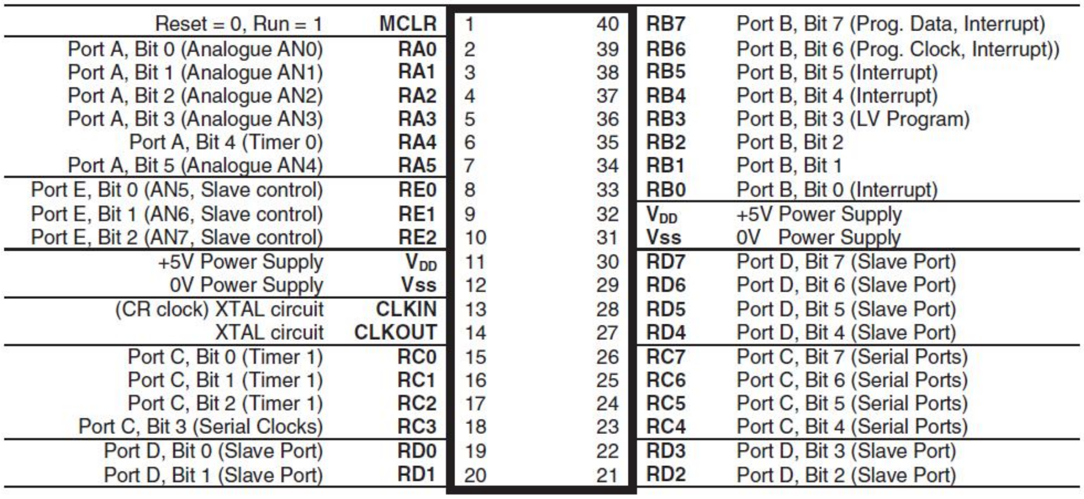
Figure (2.1) Embedded System Components

2.2.2. PIC 16F877A Architecture

Microcontrollers contain all the components required for a processor system in one chip: a CPU, memory and I/O. A complete system can therefore be built using one MCU chip and a few I/O devices such as a keypad, display and other interfacing circuits. We will see in this research how this is done in practice in our typical microcontroller. [7]

2.2.3. PIC 16F877A Pins

Let us first consider the pins that are seen on the IC package, and we can then discover how they relate the internal architecture. The chip can be obtained in different packages, such as conventional 40-pin DIP (Dual In-Line Package), square surface mount or socket format. The DIP version is recommended for prototyping, and is shown in Figure (2.2).



Reset = 0, Run = 1	MCLR	1	40	RB7	Port B, Bit 7 (Prog. Data, Interrupt)
Port A, Bit 0 (Analogue AN0)	RA0	2	39	RB6	Port B, Bit 6 (Prog. Clock, Interrupt))
Port A, Bit 1 (Analogue AN1)	RA1	3	38	RB5	Port B, Bit 5 (Interrupt)
Port A, Bit 2 (Analogue AN2)	RA2	4	37	RB4	Port B, Bit 4 (Interrupt)
Port A, Bit 3 (Analogue AN3)	RA3	5	36	RB3	Port B, Bit 3 (LV Program)
Port A, Bit 4 (Timer 0)	RA4	6	35	RB2	Port B, Bit 2
Port A, Bit 5 (Analogue AN4)	RA5	7	34	RB1	Port B, Bit 1
Port E, Bit 0 (AN5, Slave control)	RE0	8	33	RB0	Port B, Bit 0 (Interrupt)
Port E, Bit 1 (AN6, Slave control)	RE1	9	32	V_{DD}	+5V Power Supply
Port E, Bit 2 (AN7, Slave control)	RE2	10	31	Vss	0V Power Supply
+5V Power Supply	V_{DD}	11	30	RD7	Port D, Bit 7 (Slave Port)
0V Power Supply	Vss	12	29	RD6	Port D, Bit 6 (Slave Port)
(CR clock) XTAL circuit	CLKIN	13	28	RD5	Port D, Bit 5 (Slave Port)
XTAL circuit	CLKOUT	14	27	RD4	Port D, Bit 4 (Slave Port)
Port C, Bit 0 (Timer 1)	RC0	15	26	RC7	Port C, Bit 7 (Serial Ports)
Port C, Bit 1 (Timer 1)	RC1	16	25	RC6	Port C, Bit 6 (Serial Ports)
Port C, Bit 2 (Timer 1)	RC2	17	24	RC5	Port C, Bit 5 (Serial Ports)
Port C, Bit 3 (Serial Clocks)	RC3	18	23	RC4	Port C, Bit 4 (Serial Ports)
Port D, Bit 0 (Slave Port)	RD0	19	22	RD3	Port D, Bit 3 (Slave Port)
Port D, Bit 1 (Slave Port)	RD1	20	21	RD2	Port D, Bit 2 (Slave Port)

Figure (2.2) PIC 16F877A in/out pins

Most of the pins are for input and output, and arranged as 5 ports: A (5), B (8), C (8), D (8) and E (3), giving a total of 32 I/O pins. These can all operate as simple digital I/O pins, but most have more than one function, and the mode of operation of each is selected by initializing various control registers within the chip. Note, in particular, that Ports A & E become ANALOGUE INPUTS by default (on power up or reset), so they have to set up for digital I/O if required.

Port B is used for downloading the program to the chip flash ROM (RB6 and RB7), and RB0 and RB4–RB7 can generate an interrupt. Port C gives access to timers and serial ports, while Port D can be used as a slave port, with Port E providing the control pins for this function. All these options will be explained in detail later.

The chip has two pairs of power pins (VDD_5V nominal and VSS_0 V), and either pair can be used. The chip can actually work down to about 2 V supplies, for battery and power saving operation. A low frequency clock circuit using only a capacitor and resistor to set the frequency can be connected to CLKIN, or a crystal oscillator circuit can be connected across CLKIN and CLKOUT. MCLR is the reset input, when cleared to 0, the MCU stops, and restarts when MCLR _ 1. This input must be tied high allowing the chip to run if an external reset circuit is not connected, but it is usually a good idea to incorporate a manual reset button in all but the most trivial applications. [7]

2.2.4. PIC 16F877A Block Diagram

A block diagram of the 16F877A architecture is given in Figure (2.3), which emphasizes the program execution mechanism.

The main program memory is flash ROM, which stores a list of 14-bits instructions. These are fed to the execution unit, and used to modify the RAM file registers. These include special control registers, the port registers and a set of general purpose registers which can be used to store data temporarily. A separate working register (W) is used with the ALU (Arithmetic Logic Unit) to process data. Various special peripheral modules provide a range of I/O options.

There are 512 RAM File Register addresses (0–1FF h), which are organized in 4 banks (0–3), each bank containing 128 addresses. The default (selected on power up) Bank 0 is numbered from 0 to 7Fh, Bank 1 from 80h to (FF h) and so on. These contain both Special Function Registers (SFRs), which have a dedicated purpose, and the General Purpose Registers (GPRs). The SFRs may be shown in the block diagram as separate from the GPRs, but they are in fact in the same logical block, and addressed in the same way.

Deducting the SFRs from the total number of RAM locations and allowing for some registers which are repeated in more than one bank, leaves 368 bytes of GPR (data) registers.

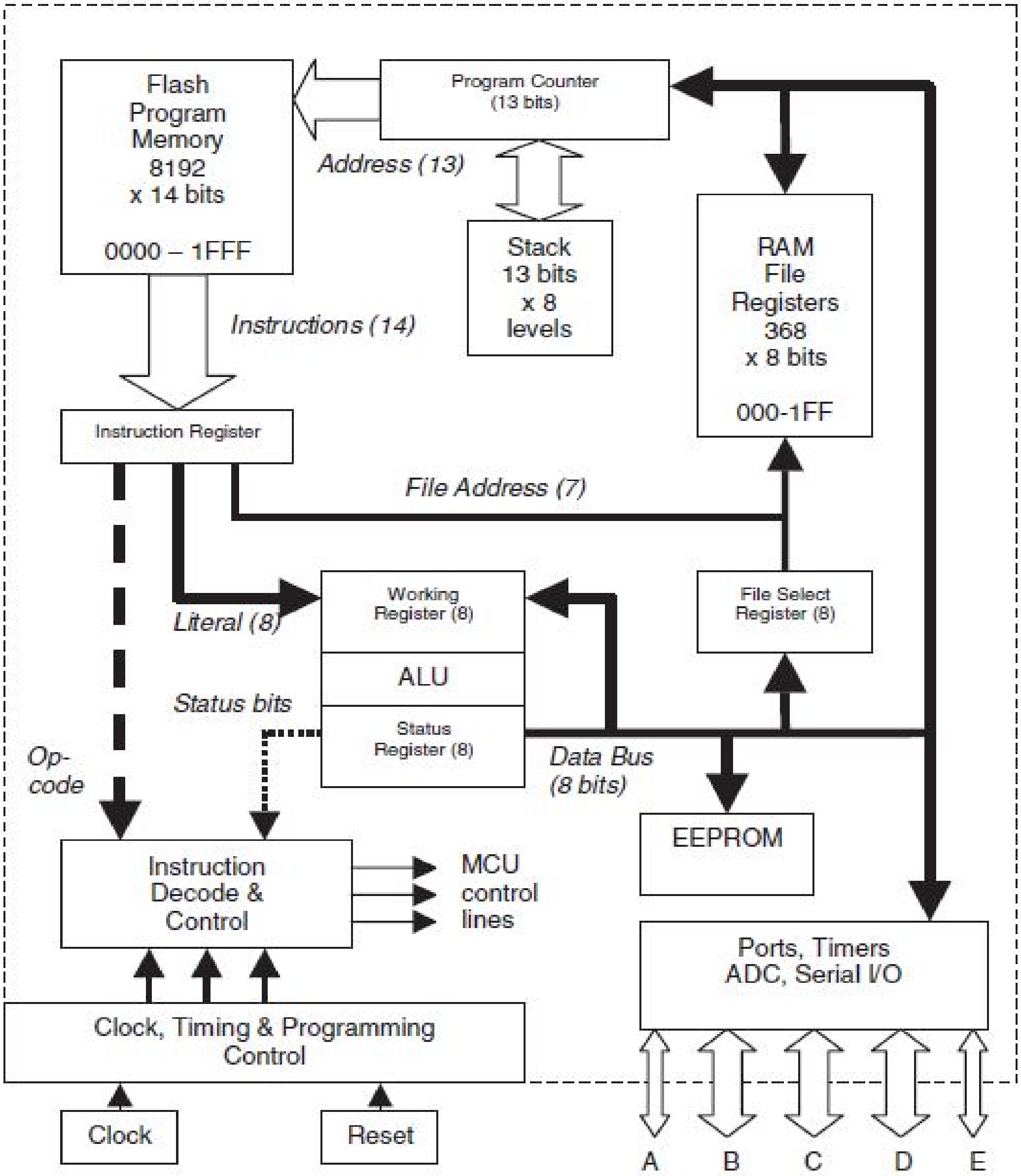


Figure (2.3) PIC 16F877A Block Diagram

2.3. Liquid Crystal Display (LCD)

The LCD is now a very common choice for graphical and alphanumeric displays, these ranges from small, 7-segment monochrome numerical types such as those used in digital MultiMate’s (typically 3 ½ digits, maximum reading 1.999) to large, full color, high-resolution screens which can display full video. Here we shall concentrate on the small monochrome, alphanumeric type which displays alphabetical, numerical and symbolic characters from the standard ASCII character set. This type can also display low-resolution graphics, but we will stick to simple examples. A circuit is shown in Figure (2.4).

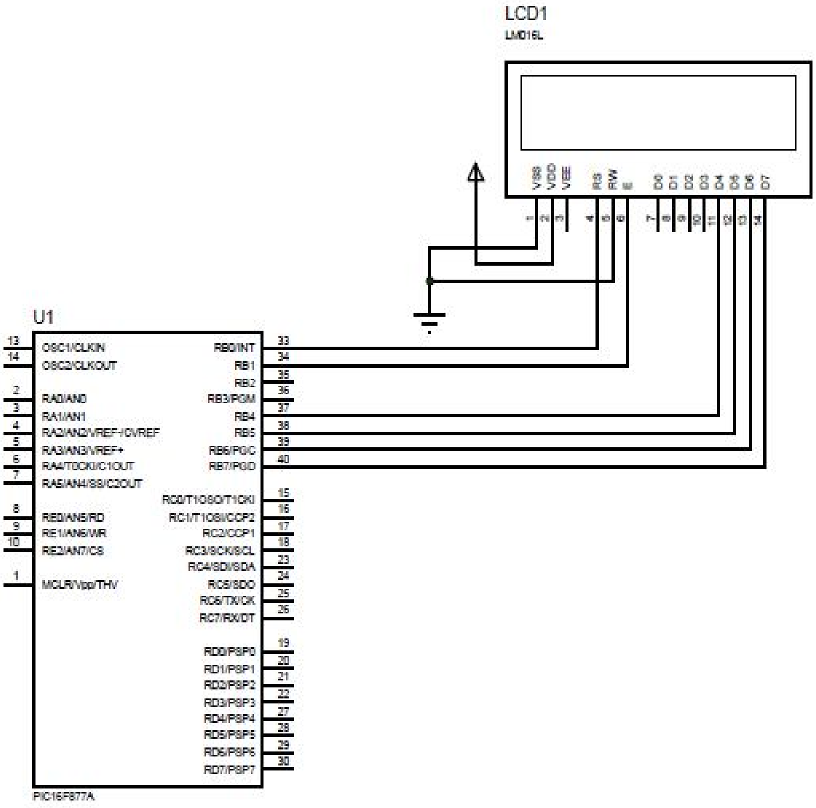


Figure (2.4) PIC 16F877A and LCD connection circuit

The display is a standard LM016L which displays 2 lines of 16 characters (16, 2). Each character is 5_8 pixels, making it 80_16 pixels overall. In the demo program, a fixed message is displayed on line 1, showing all the numerical digits. The second line finishes with a character that counts up from 0 to 9 and repeats, to demonstrate a variable display. The display receives ASCII codes for each character at the data inputs (D0–D7). The data is presented to the display inputs by the MCU, and latched in by pulsing the E (Enable) input.

The RW (Read/Write) line can be tied low (write mode), as the LCD is receiving data only.

The RS (Register Select) input allows commands to be sent to the display.

RS_0 selects command mode, RS_1 data mode. The display itself contains a microcontroller. [7]

2.4. Keypad Input

A keypad is simply an array of push buttons connected in rows and columns, so that each can be tested for closure with the minimum number of connections Figure (2.5). There are 16 keys on a phone type pad (0–9, =, ON/C, +, -, ×, ÷), arranged in a (4, 4) matrix. The columns are labeled 1, 2, 3, 4 and the rows A, B, C, D. If we assume that all the rows and columns are initially high, a keystroke can be detected by setting each row low in turn and checking each column for a zero.

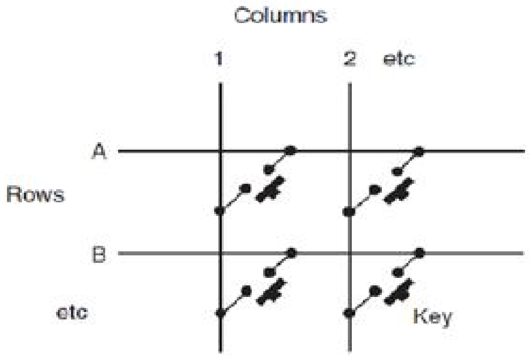


Figure (2.5) Keypad inside connections

In the KEYPAD circuit in Figure (2.6) the 8 keypad pins are connected to Port D. Bits 4–7 are initialized as outputs, and bits 0–3 used as inputs. These input pins are pulled high to logic 1. The output rows are also initially set to 1. If a 0 is now output on row A, there is no effect on the inputs unless a button in row A is pressed. If these are checked in turn for a 0, a button in this row which is pressed can be identified as a specific combination of output and input bits.

A simple way to achieve this result is to increment a count of keys tested when each is checked, so that when a button is detected, the scan of the keyboard is terminated with current key number in the counter. This works because the (non-zero) numbers on the keypad arranged in order:

Row A: 7, 8, 9, ÷

Row B: 4, 5, 6, ×

Row C: 1, 2, 3, -

Row D: ON/C, 0, =, +

Following this system, the (ON/C) symbol is represented by a count of 13 (0Dh), zero by 14(0Eh), (=) by 15 (0Fh) and (+) by 16(00000010h). [7]

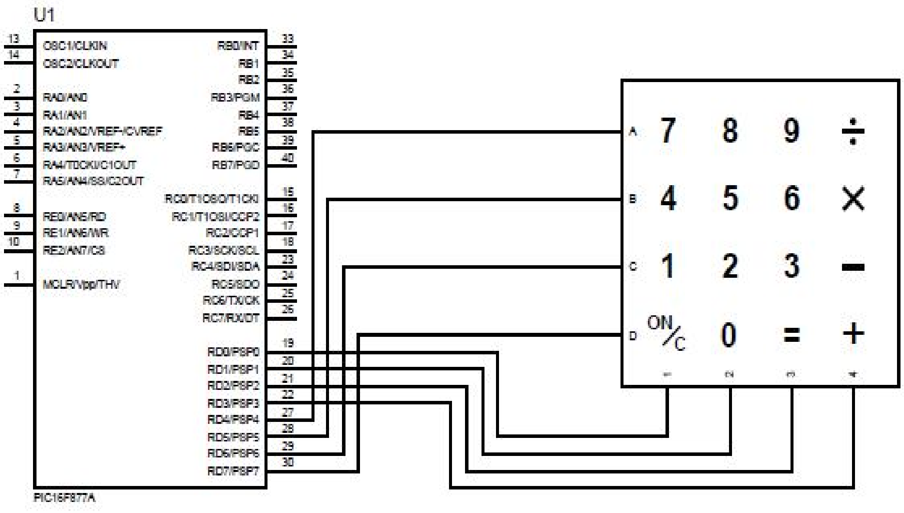


Figure (2.6) PIC 16F877A and Keypad connection circuit

2.5. GSM Modules

The GSM family (GSM, GPRS, and EDGE) has become one of the most successful technical innovations in history. As of June 2008, more than 2.9 billion subscribers were using GSM, corresponding to a market share of more than 81%, and its story continues, even now, despite the introduction and development of next-generation systems such as IMT-2000 or UMTS (3G) and even systems beyond 3G, dubbed IMT-Advanced.

At the same time, wireless local area networks have substantially expanded the wireless market, sometimes drawing market share from GPRS and 3G (e.g. in public Wi-Fi hotspots), sometimes coexisting (e.g. in UMTS home routers used as a replacement for fixed wire connections). However, these are used typically for low mobility applications. Mobile communication with all of its features and stability has become increasingly important: cellular and GSM technology, plus, of course, lately 3G, GSMs sister technology, so-to-say.

Another impressive trend has emerged since our last edition: the permanent evolution in the handheld market, producing fancy mobile phones with cameras, large memory, MP3 players, Email clients and even satellite navigation. These features enable numerous nonvoice or multimedia applications, from which, of course, only a subset is or will be successful on the market. [8]

2.5.1. The Idea of Unbounded Communication

Communication everywhere, with everybody, and at any time – that was the dream and goal of researchers, engineers and users, since the advent of the first wireless communication systems. Today it feels like we have almost reached that goal. Digitalization of communication systems, enormous progress in microelectronics, computers and software technology, the invention of efficient algorithms and procedures for compression, security and processing of all kinds of signals, as well as the development of flexible communication protocols have all been important prerequisites for this progress. Today, technologies are available that enable the realization of high-performance and cost-effective communication systems for many application areas.

Using current wireless communication systems, the most popular of which is GSM (Global System for Mobile Communication), we see that we have the freedom to not only roam within a network, but also between different networks, and that we can in fact communicate (almost) everywhere (unless we are in one of the rare spots still without GSM coverage today), with (almost) everybody (unless our desired communication partner is in one of the rare spots mentioned above or chooses not to be reachable), and at (almost) any time (unless we forgot to pay our last phone bill and the operator decides to lock us out).

If there is one major aspect still missing in order to make our wireless experience flawless, it is the large (albeit diminishing) gap between data rates available through wireless services and those available through wired services, such as Digital Subscriber Line (DSL). This and the limited capability of data representation at the mobile terminal (mostly due to the limited size of mobile phones) is one of the main challenges for future developments in wireless communication.

GSM technology contains the essential intelligent functions for the support of personal mobility, especially with regards to user identification and authentication, and for the localization and administration of mobile users.

Here it is often overlooked that in mobile communication networks by far the largest part of the communication occurs over the fixed network part, which interconnects the radio stations (base stations). Therefore, it is no surprise that in the course of further development and evolution of the telecommunication networks, a lot of thought has been given to the convergence of fixed and mobile networks.

In the beginning, GSM was used almost exclusively for speech communication; however, the Short Message Service (SMS) soon became extremely popular with GSM users: several billion text messages are being exchanged between mobile users each month.

In the mean time, additional data services have been realized most notably the High Speed Circuit Switched Data (HSCSD) and the General Packet Radio Service (GPRS), which enable improved data rate performance by allowing for more than one GSM timeslot to be used by a terminal for a service at a time.

The driving factor for new (and higher bandwidth) data services obviously is wireless access to the Internet. To this end, the Wireless Application Protocol (WAP) is also explained in this book. These additions are already working towards closing the gap between wireless and fixed networks that we discussed above. [8]

2.5.2. The Success of GSM

The relevance of the GSM standard today becomes obvious when we take a brief look at the success story of GSM so far and keeping in mind that many countries are still working towards full wireless coverage, mainly by deploying GSM. GSM was initially designed as a pan-European mobile communication network, but shortly after the successful start of the first commercial networks in Europe, GSM systems were also deployed on other continents (e.g. in Australia, Hong Kong and New Zealand). In the meantime, as of May 2008, 670 networks in 208 countries are in operation according to GSM world.

In addition to GSM networks that operate in the 900 MHz frequency band, other so-called Personal Communication Networks (PCNs) and Personal Communication Systems (PCSs) are in operation. They use frequencies around 1800 MHz, or around 1900 MHz in North America. Apart from the peculiarities that result from the different frequency range, PCNs/PCSs are full GSM networks without any restrictions, in particular with respect to services and signaling protocols. International roaming among these networks is possible based on the standardized interface between mobile equipment and the Subscriber Identity Module (SIM) card, which enables personalization of equipment operating in different frequency ranges (SIM card roaming). Now that UMTS technology has been integrated by most wireless providers into their networks, roaming not only between providers but also between different technologies is already state of the art. To this end, multi-band and multi-standard terminals have been developed and are considered commonplace today. Users of state-of-the-art terminals with a SIM card from one of the major providers in Europe can use their terminals in different frequency ranges as well as in GSM and UMTS networks, without having to configure or select anything. The terminals roam between different networks and technologies automatically. [8]

2.6. Sensors

The devices that inform the control system about what is actually occurring are called sensors (also known as transducers), which are capable of converting a physical quantity to a more readily manipulated electrical quantity. As an example, the human body has an amazing sensor system that continually presents our brain with a reasonably complete picture of the environment, whether we need it all or not. For a control system, the designer must ascertain exactly what parameters need to be monitored. In virtually every engineering application there is the need to measure some physical quantities, such as displacements, speeds, forces, pressures, temperatures, stresses, flows, and so on, and then specify the sensors and data interface circuitry to do the job. Many times a choice is possible. For example, we might measure fluid flow in a pipe with a flow meter, or we could measure the flow indirectly by seeing how long it takes for the fluid to fill a known-sized container. The choice would be dictated by system requirements, cost, and reliability.

The key issues in the selection of sensors are: (a) the field of view and range; (b) accuracy; (c) repeatability and resolution; (d) responsiveness in the target-domain; (e) power consumption; (f) hardware reliability; (g) size; and (h) interpretation reliability.

Most sensors work by converting some physical parameter such as temperature or position into an electrical signal or electrical quantity (e.g. voltage or current). This is why sensors are also called transducers, which are devices that convert energy from one form to another.

Generally sensors classified into distance, movement, proximity, stress/strain/force, and temperature. There are many commercially available sensors but we have picked on the ones that are frequently used in mechatronics applications. [10]

2.6.1. Proximity Sensors

2.6.1.1. Limit Switches

A proximity sensor simply tells the controller whether a moving part is at a certain place. A limit switch is an example of a proximity sensor. A limit switch is a mechanical push-button switch that is mounted in such a way that it is actuated when a mechanical part or lever arm gets to the end of its intended travel. For example, in an automatic garage-door opener, all the controller needs to know is if the door is all the way open or all the way closed. Limit switches can detect these two conditions. Switches are fine for many applications, but they have at least two drawbacks: (1) Being a mechanical device, they eventually wear out, and (2) they require a certain amount of physical force to actuate. Two other types of proximity sensors, which used either in optics or magnetic to determine if an object is near, In this proposed system we will use the mechanical one and its shown in the figure (2.7) below. [10]

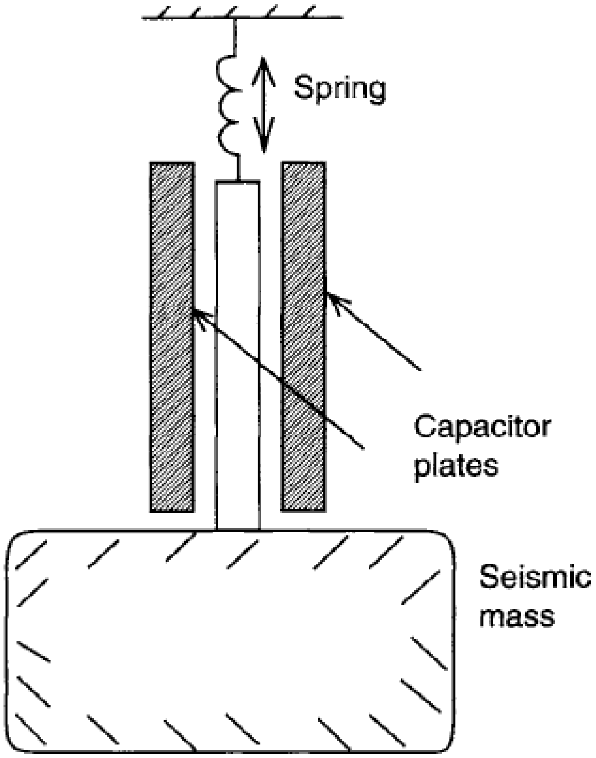


Figure (2.7) Limit switch sensor

2.6.2. Switches

A mechanical switch is a device that can open or close, thereby allowing a current to flow or not. As you have no doubt observed, switches come in many different shapes, sizes, and configurations.

2.6.2.1. Push-Button Switches

Push-button switches [Figure (2.8 (a))] are almost always the momentary type—pressure must be maintained to keep the switch activated. Figure (2.8 (b-d)) shows the symbol for the push-button switch. Notice there are two configurations possible: normally open (NO) and normally closed (NC). For the NO switch [Figure (2.8 (b))], the contacts are open until the button is pushed; and for the NC switch [Figure (2.8 (c))], the contacts are closed when the switch is "at rest" and open when the button is pushed. [9]

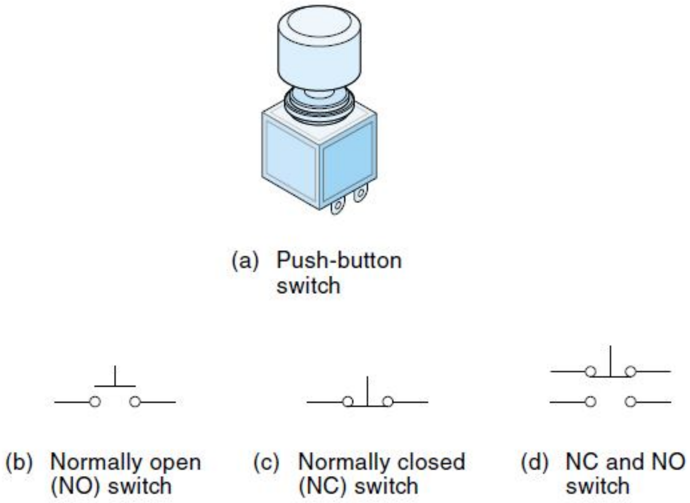

(a) Push-button switch
(b) Normally open (NO) switch
(c) Normally closed (NC) switch
(d) NC and NO switch

Figure (2.8) Push-Button Switches

Chapter Three

Design of a Smart Security System

3.1. Introduction

In this proposed work, a novel method of vehicle security and locking system used to protect the vehicle from theft crimes by using embedded system and GSM technology. This system will turn to sleep mode only by entering the correct password while the vehicle handled by the owner or authorized person otherwise will be in active mode, and the mode of operation changed by in person only. In this system, and after typing the correct password, the system will turn into a sleep mode, and in case if the driver door opened, the system will turn into an active mode again, actually the door's sensor will send a signal to the microcontroller as a reset, and then the user will asked again to type the password. In this system we interfaced PIC16F877A microcontroller with GSM modem to decode the received message and do the required action. The protocol used for this communication between the two is AT command. The commands are standard AT. A Serial communication is used for data communication between GSM modem and PIC16F877A, microcontroller commands (instruction) the GSM modem to send a message alert to the vehicle owner, the GSM modem will issues the message (CAR ATTACKED) to the car owner or authorized person in case if three times failure in typing the correct password by using the keypad, beside that, the microcontroller will issue a cutoff signal to the ignition system and the fuel pump system of the engine to immediately shutdown the power of the engine, which means all the systems will be locked. To restart the system of the vehicle, authorized person needs to enter the unlock code at the first step and the correct passwords at the second step.

3.2. System Block Diagram

The Block diagram of Vehicle's security system based on GSM technology is shown in the figure (3.1). It consists of the power supply section, keypad, Relays, GSM, microcontroller, RS232 connector, LCD and the door sensor.

The GSM board has a valid SIM card with a sufficient recharge amount to make outgoing SMS. The circuits powered by +5v Dc.

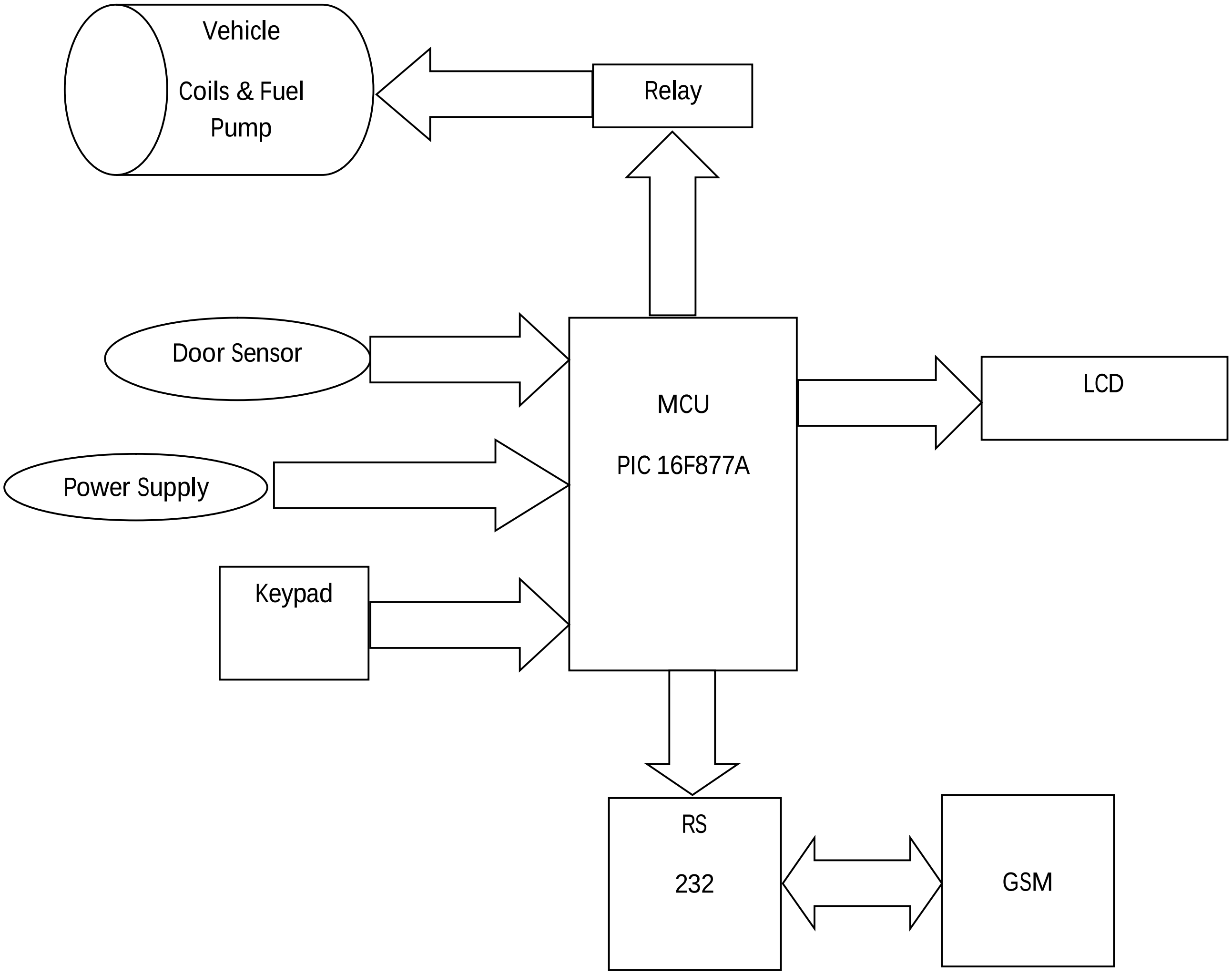


Figure (3.1)

System Block Diagram

3.3. System Flow Chart

Firstly the user will getting inside the car and starts the engine. The user will be asking to type the password code to allow the authorized persons to drive the car, specifically to use the throttle device through the fuel pedal which its allow the vehicle to accelerate and allows the vehicle to move, and then the system will check the entered password through the keypad, notice that the user has only three times efforts to enter a valid password. After verification the user can drive the vehicle smoothly and simply, and the security system will turn to deactivate mode, and the system will be in waiting mode for any interruption signal to turn again to active mode. The interruption signal can be generated by shutting off the engine or by opening the door during the engine in a running mode.

But in case the three times efforts were invalid, then automatically one SMS will send to the registered mobile number and the main power source will shut down and the user will be asking to enter the unlock code first, and if the user entered the correct unlock code then the user will be asking again to enter the password code. Figure (3.2) will illustrate the sequences of the system.

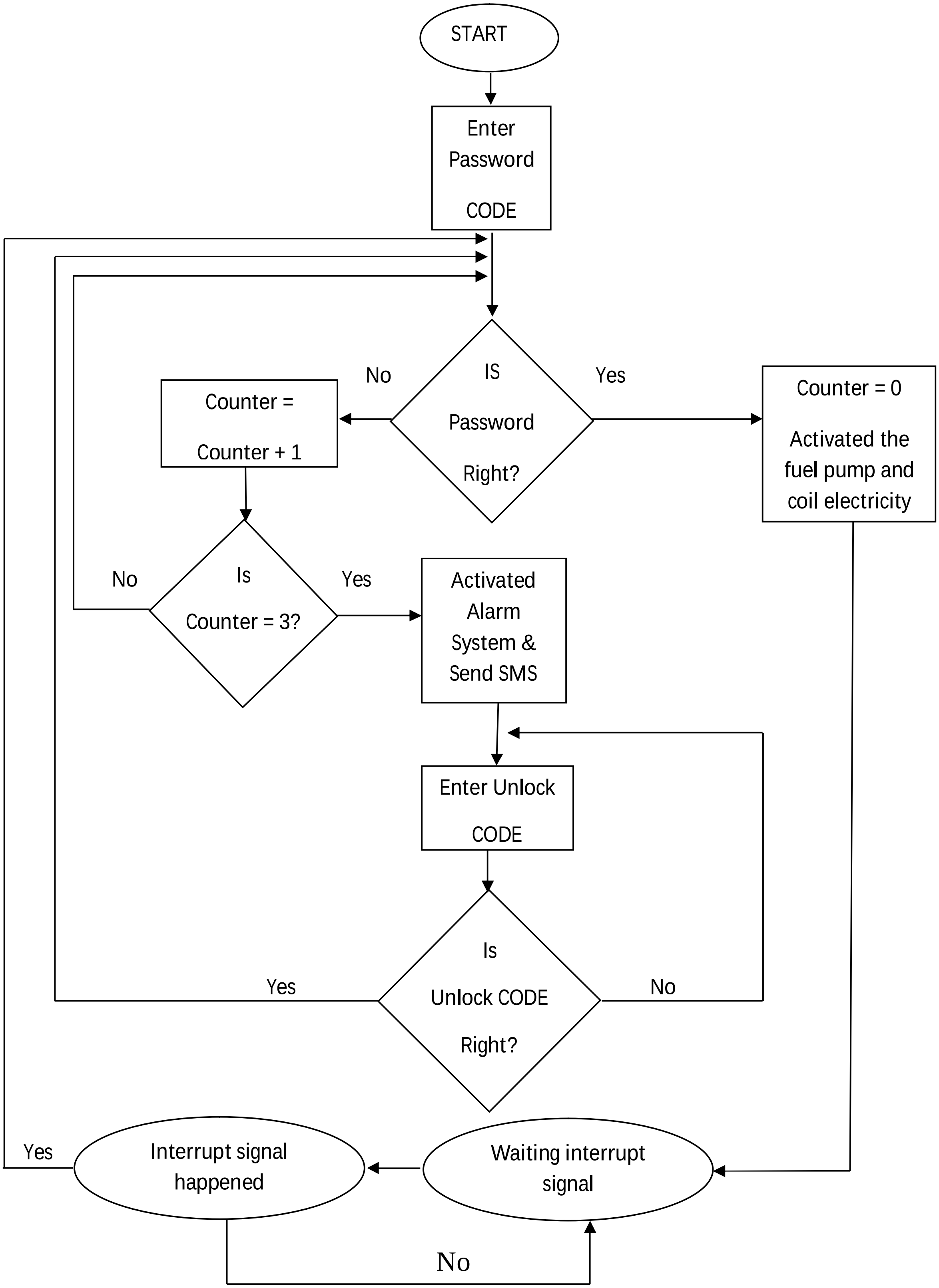
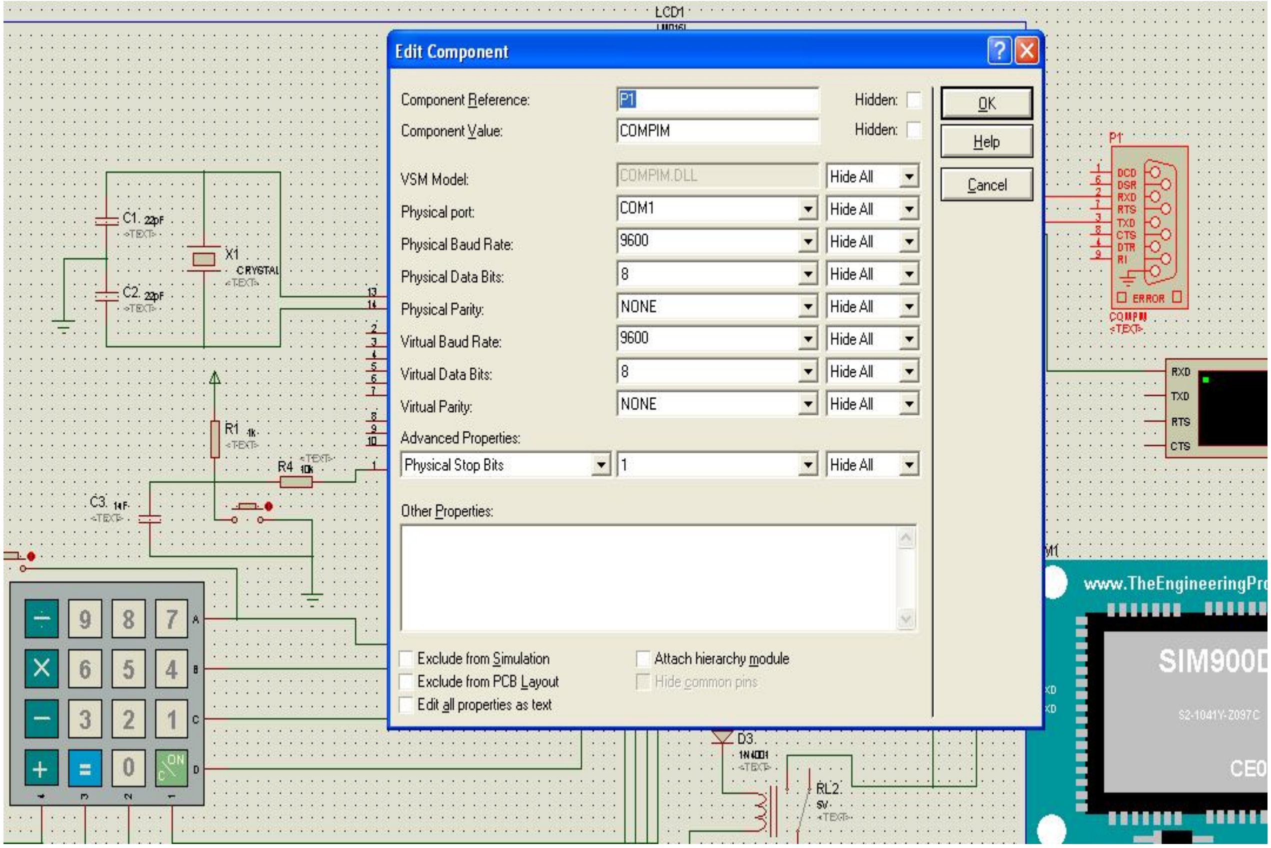


Figure (3.2) System Flow Chart

3.4. GSM Configuration

The configuration of the GSM modem in this proposed work done as the following steps:

- Set the serial connector in the Proteus simulation to the COM1as shown in figure (3.3)



Edit Component

Component Reference:	P1	Hidden: □	
Component Value:	COMPIM	Hidden: □	
VSM Model:	COMPIM.DLL	Hide All	
Physical port:	COM1	Hide All	
Physical Baud Rate:	9600	Hide All	
Physical Data Bits:	8	Hide All	
Physical Parity:	NONE	Hide All	
Virtual Baud Rate:	9600	Hide All	
Virtual Data Bits:	8	Hide All	
Virtual Parity:	NONE	Hide All	
Advanced Properties:			
Physical Stop Bits	1	Hide All	

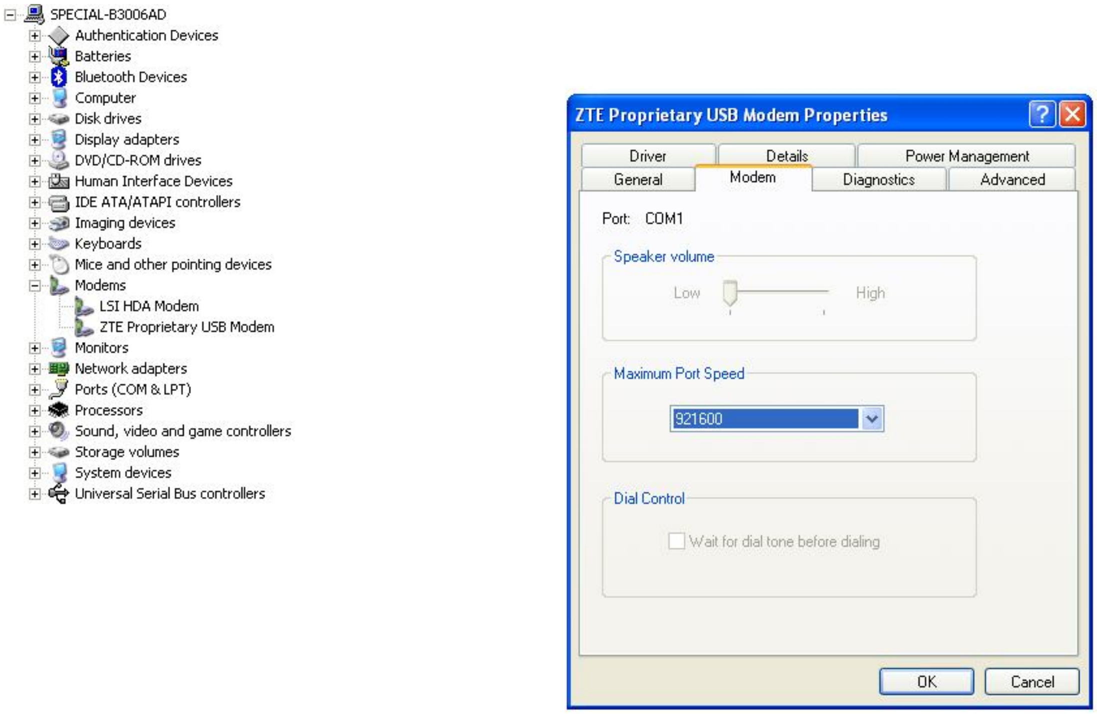
Other Properties:

□ Exclude from Simulation □ Attach hierarchy module
□ Exclude from PCB Layout □ Hide common pins
□ Edit all properties as text

Figure (3.3) GSM Configuration

From simulation the serial connector will be configurated as shown in the above figure by specified the Serial connector properties to compatible the properties of the port of the computer, which will be connected to the GSM. We will set the physical port, physical baud rate, physical data bits, virtual baud rate and virtual data bits as shown in the figure (3.3).

- Set the USB that used to connect to the GSM modem to the COM1 as shown in figure (3.4)



SPECIAL-B3006AD
- Authentication Devices
- Batteries
- Bluetooth Devices
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Imaging devices
- Keyboards
- Mice and other pointing devices
- Modems
  - LSI HDA Modem
  - ZTE Proprietary USB Modem
- Monitors
- Network adapters
- Ports (COM & LPT)
- Processors
- Sound, video and game controllers
- Storage volumes
- System devices
- Universal Serial Bus controllers

ZTE Proprietary USB Modem Properties

Port: COM1

Speaker volume

Maximum Port Speed: 921600

Dial Control

□ Wait for dial tone before dialing

Figure (3.4.a) COM1 Configuration Steps

From computer properties we will select the device manager, and then will open the sub menu of the modems, then we will open the properties of the USB modem to configure the properties of the USB port of the computer to be compatible to the serial connector on the simulation as shown in figures (3.4.a), (3.4.b) and (3.4.c).

All steps of this configuration just to implement the system of the vehicles security as designed on the Proteus simulation and get direct result from the GSM modem.

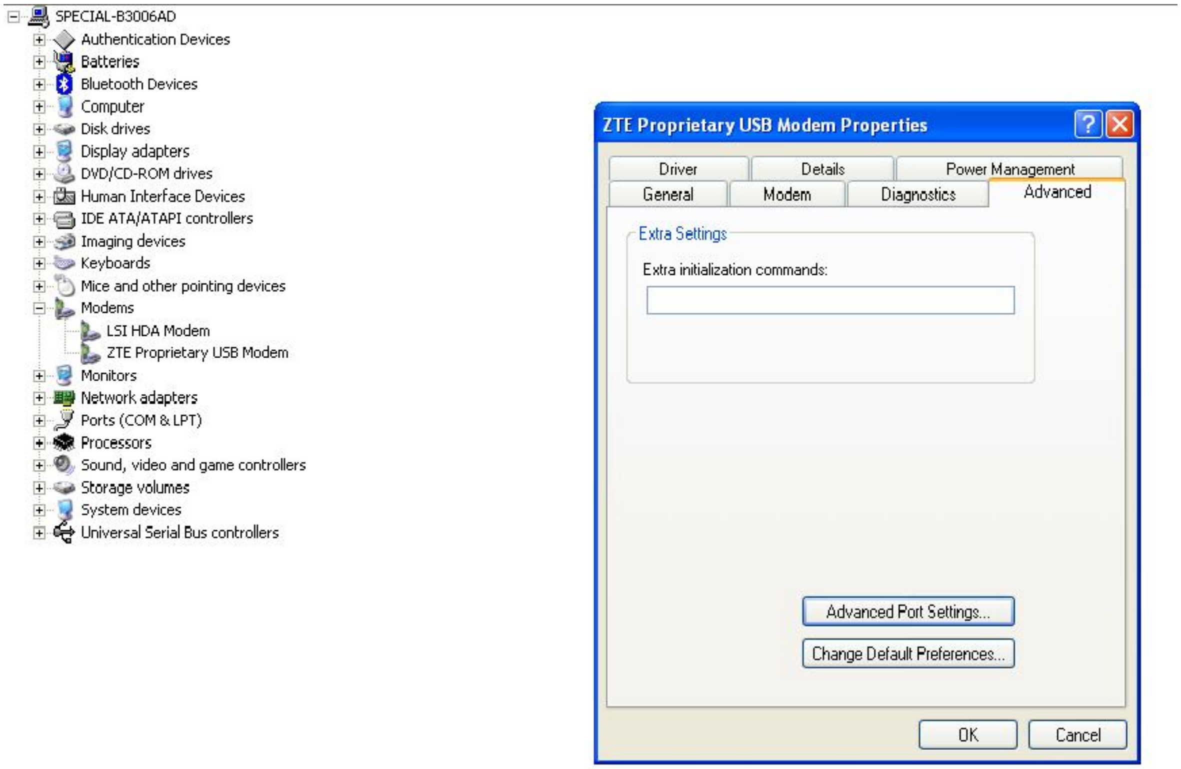
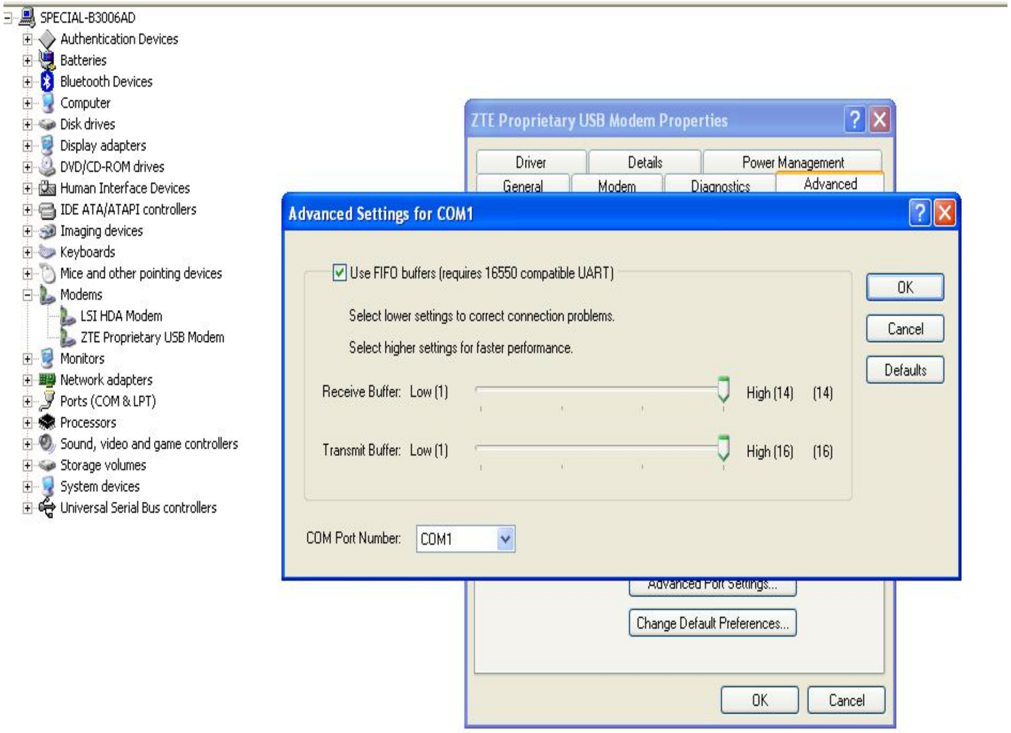


Figure (3.4.b) COM1 Configuration Steps



☑ Use FIFO buffers (requires 16550 compatible UART)

Select lower settings to correct connection problems.

Select higher settings for faster performance.

Receive Buffer: Low (1) High (14) (14)

Transmit Buffer: Low (1) High (16) (16)

COM Port Number: COM1

Figure (3.4.c) COM1 Configuration Steps

3.5. Sending SMS Text

A GSM modem is a specialized type of modem which accepts a subscriber identity module (SIM) card and operates over a subscription to a mobile operator just like a mobile phone. The PIC communicates with the modem and a further piece of equipment using sequential protocol. The GSM modem is controlled by the microcontroller that sends signals to the GSM to receive and transmit messages. The working of GSM modem is based on commands, the commands always start with AT (which means ATtention) and finish with a <CR> character. In this proposed work the step to send a message to the owner will done as following step:

- AT
- AT+CMGF=1

- AT+CSCA=\"01250783330\" (call center)
- AT+CMGS=\"0920106977\" (owner number)
- "Car Attacked" (the message)

3.6. RS 232 Connection

The RS-232 standard was established in 1960 by the Electronic Industry Association (EIA) for interfacing between a computer and a modem.

-1963: RS232A. -1965: RS232B. -1969: RS232C.

RS232 is a serial I/O interfacing standard as shown in figure(3.5), and in this proposed work we will use a 9-wire cable with a male and a female DB-9 pin connector attached to either end, table (3.1) shown the description of the pins.

9-pin connector is more commonly found in PCs but it covers signals for a synchronous serial communication only.

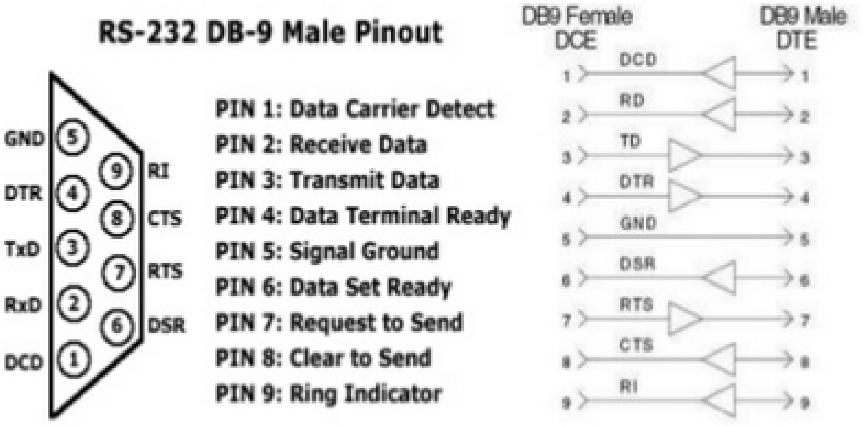
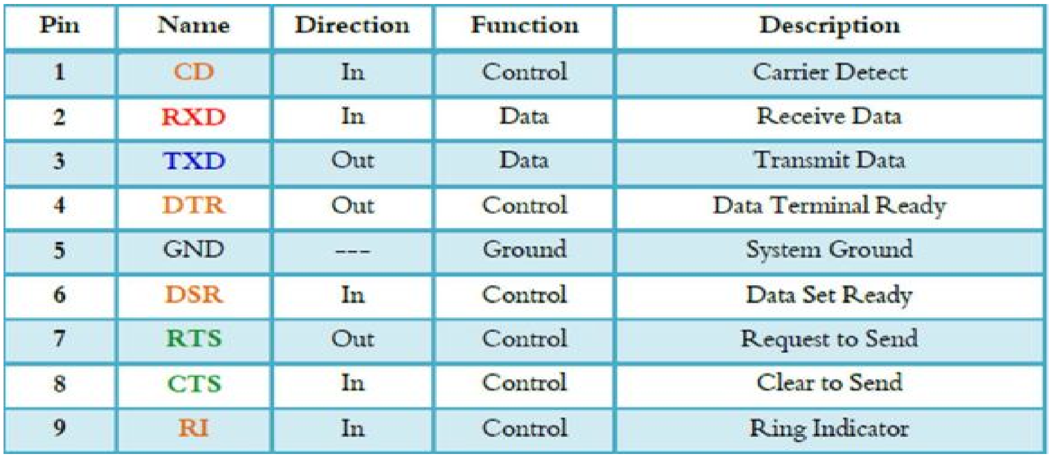


Figure (3.5) RS 232 Connection

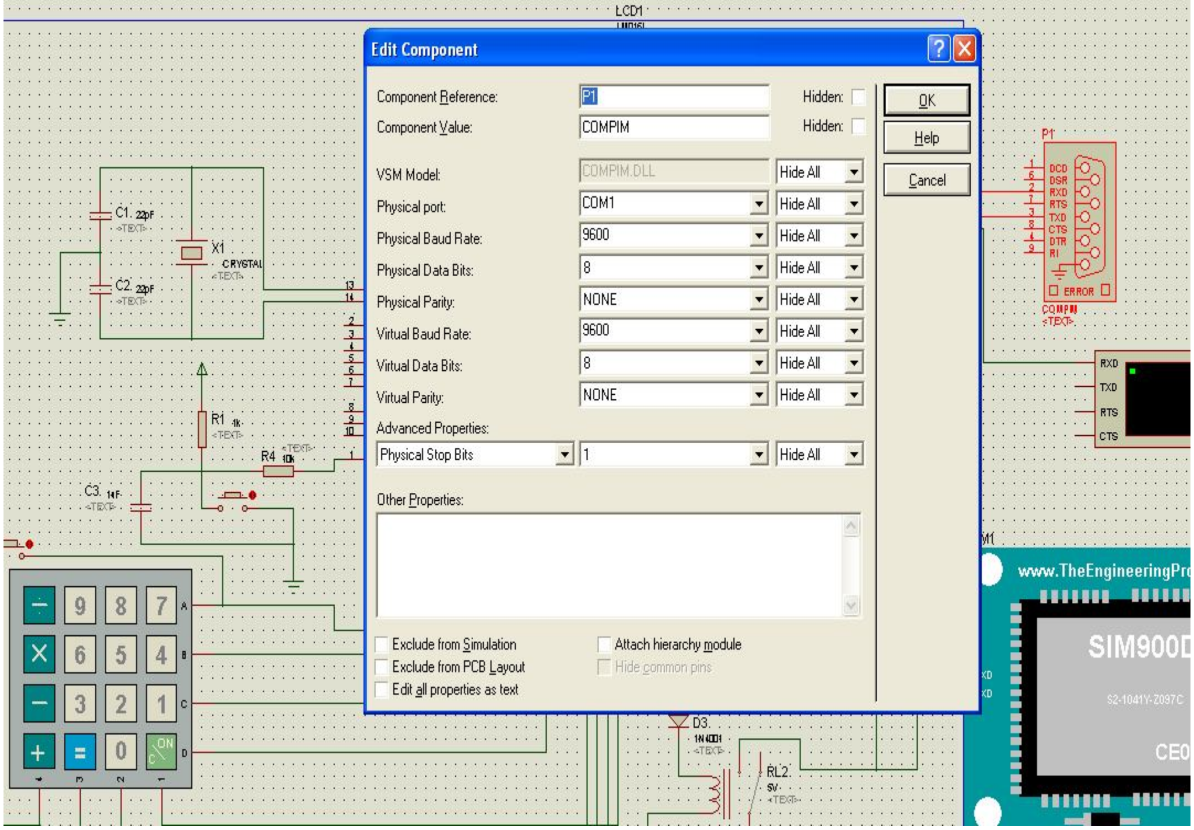
Table (3.1) RS 232 Pin’s Description



Pin	Name	Direction	Function	Description
1	CD	In	Control	Carrier Detect
2	RXD	In	Data	Receive Data
3	TXD	Out	Data	Transmit Data
4	DTR	Out	Control	Data Terminal Ready
5	GND	---	Ground	System Ground
6	DSR	In	Control	Data Set Ready
7	RTS	Out	Control	Request to Send
8	CTS	In	Control	Clear to Send
9	RI	In	Control	Ring Indicator

3.6.1. RS 232 Connection Configuration

The default settings for RS-232 communication are set to 9600 baud, 8 bits, no parity, and no software handshaking. Only the Transmit (TX), Receive (RX), and Ground signals are used. The Request to Send (RTS) and Clear to Send (CTS) signals are tied together at the board level so that devices requiring the CTS signal will always be enabled to send data. This works because the device will set its own RTS signal high, so connecting these two signals will ensure that CTS will be held high as long as the device is connected. If an attached device requires settings different from the board default, this can be changed in the software with the exception that this board does not accommodate devices that require handshaking beyond the CTS signal.



Edit Component

Component Reference: P1 Hidden: □

Component Value: COMPIM Hidden: □

VSM Model: COMPIM.DLL Hide All

Physical port: COM1 Hide All

Physical Baud Rate: 9600 Hide All

Physical Data Bits: 8 Hide All

Physical Parity: NONE Hide All

Virtual Baud Rate: 9600 Hide All

Virtual Data Bits: 8 Hide All

Virtual Parity: NONE Hide All

Advanced Properties:

Physical Stop Bits 1 Hide All

Other Properties:

□ Exclude from Simulation □ Attach hierarchy module

□ Exclude from PCB Layout □ Hide common pins

□ Edit all properties as text

Figure (3.3) GSM Configuration

3.7. Ports Configurations

- Port A: Not used.
- Port B: Connected to the LCD.
- Port C: the configuration as following as shown in table (3.2):

Table (3.2) Port C Configuration

Port pin	Connected to
C0	Main relay (power source)
C1	Relays (ignition/fuel pump)
C2	LED (System active/not active)
C3	Not used
C4	Not used
C5	Not used
C6	(TX) GSM Modem
C7	(RX) GSM Modem

- Port D: Connected to the keypad.
- Port E: not used.

3.8. LCD Configuration

Liquid Crystal Display (LCD) used in this proposed work as showing in figure (2.4) as discussed in chapter (2) connected to port B as shown in table (3.3) as following:

Table (3.3) LCD Configuration & Connection

Pin no.	**Description**	**Pin no.**	**Description**
Pin1	Ground	Pin9	D2 Not used
Pin2	VCC (+5)	Pin10	D3 Not used
Pin3	contrast	Pin11	D4
Pin4	Data/command (R/S)	Pin12	D5
Pin5	Read/Write	Pin13	D6
Pin6	Enable	Pin14	D7
Pin7	D0 Not used	Pin15	-
Pin8	D1 Not used	Pin16	-

Figure (3.6) Liquid Crystal Display (LCD)

3.9. Keypad Configuration

In this proposed work the keypad used as showing in figure (2.6) as discussed in chapter (2) connected to port D as shown in table (3.4) as following:

Table (3.4) Keypad Configuration & Connection

Pin No.	Description
Pin1	Colum 1
Pin2	Colum 2
Pin3	Colum 3
Pin4	Colum 4
Pin5	Row A
Pin6	Row B
Pin7	Row C
Pin8	Row D

3.10. Circuit Diagram

In this proposed work the circuit diagram of the entire system as shown in figure (3.8), which shown the all components starting from the power supplying unit (Battery DC), relay 2 to connect and disconnect the power to the entire system, relay 1 to connect and disconnect the power to the fuel and ignitions systems, keypad to insert the required passwords (CODE, UNLOCK), LCD to inform the authorized person about the system status and what the user exactly should insert to the system, RS232 to connect the GSM module to the microcontroller, GSM module to sent SMS to the authorized persons and to inform the users the vehicles had been used illegally, door switch to reset the system and turn the system to the active mode in case it was in sleep mode or deactivated mode, and finally the microcontroller (PIC 16F877A) to run all the system operations. In this proposed work and as shown in the figure (3.7); the relay 2 considerer to be the main relay of the system and responsible of cutting off and supplying the power to the entire system.

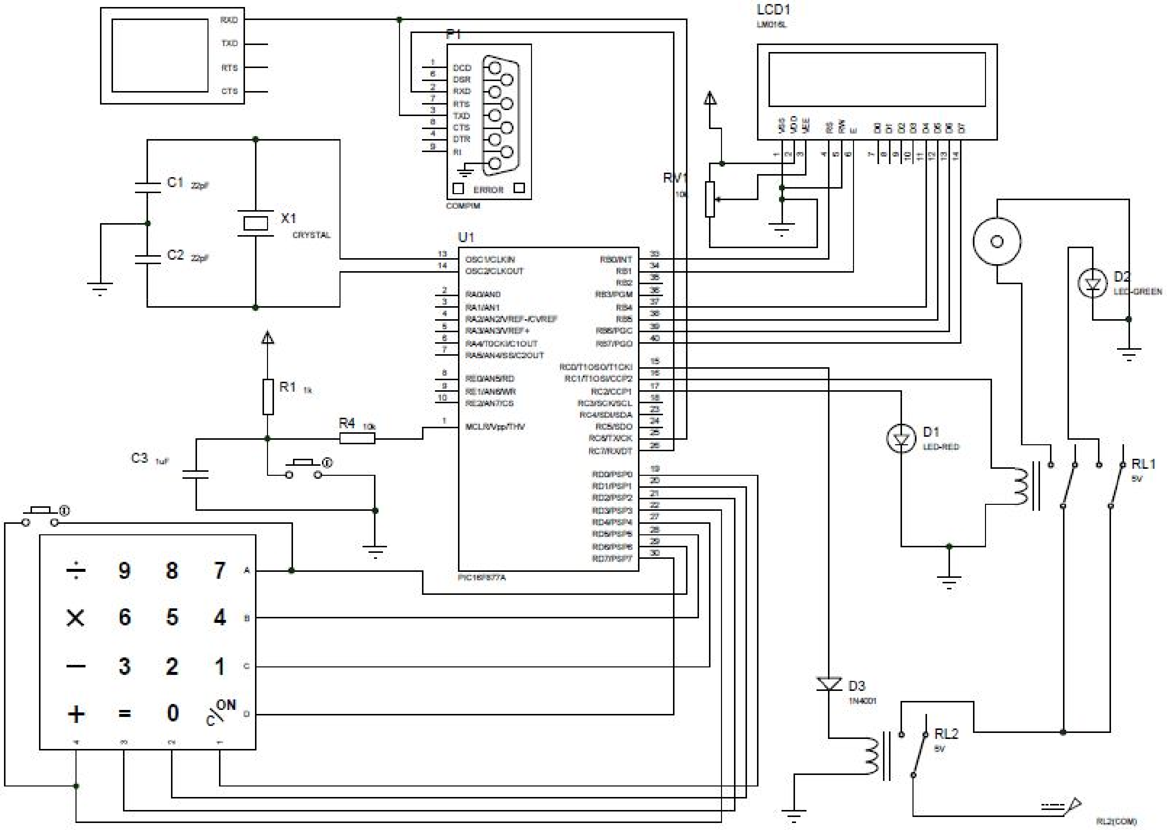


Figure (3.7) System Circuit Diagram

Notice that the relay 2 working in the first level of this system. So when the system asks for the UNLOCK CODE and the user couldn’t to enter the correct password then the relay 2 will cut off the power. Relay 1 responsible of cutting and supplying the power to fuel and ignitions systems, notice that the relay 1 working only in the second level of the system. So when system asks for the password CODE and the user couldn’t to enter the correct one then relay 1 automatically will shutdown the engine by cutting off the power to the fuel and ignitions systems.

The switch connected to the keypad presented the throttle sensor. So when the users try to drive the vehicle by pushing the fuel’s pedal the switch will work and pass signal to the microcontroller, and the system will check the registers if they already got the password. So if the registers got the correct password then the system will work perfectly and if not the system will shutdown the engine and will wait for the correct password.

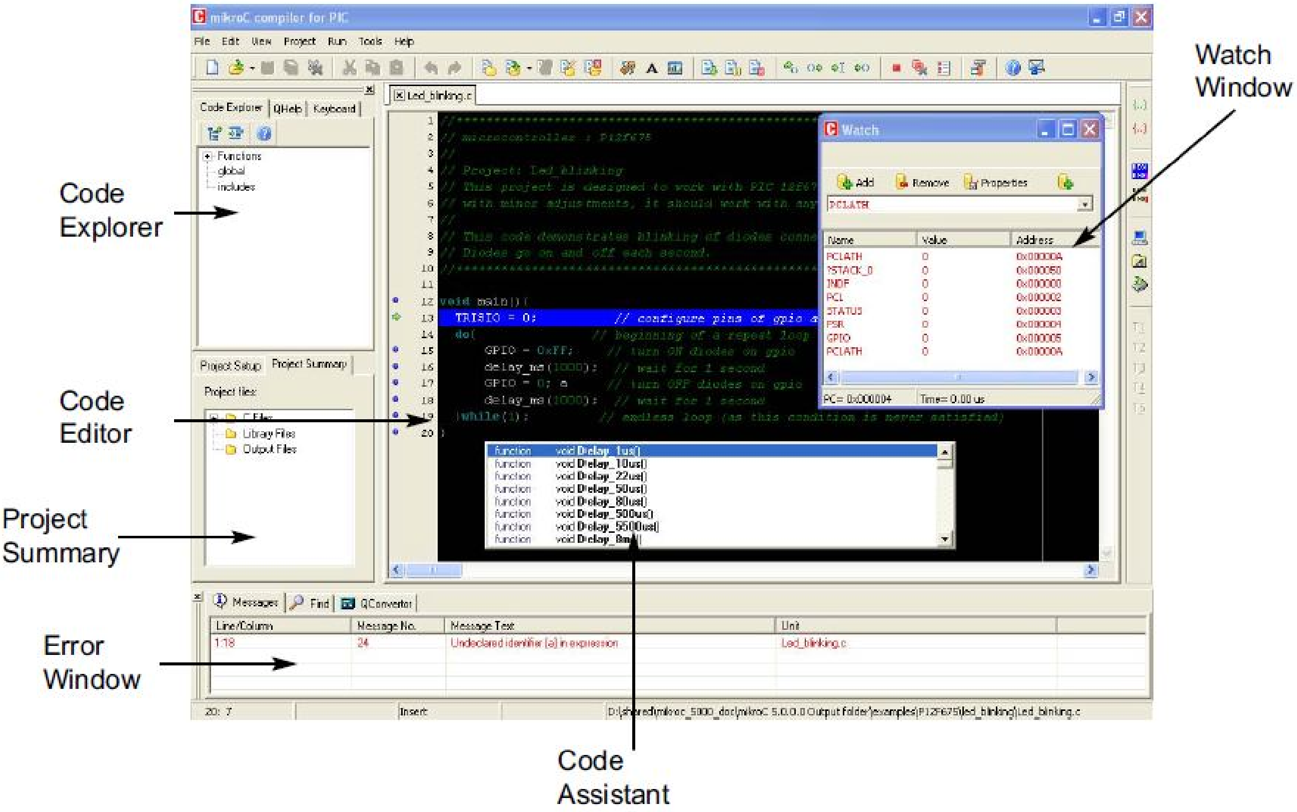
3.11. Required Software’s

3.11.1. Mikro C

MikroC is a powerful, feature rich development tool for PICmicros, it’s designed to provide the costumer with the easiest possible solution for the developing application for the embedded systems, without compromising performance or control.

Mikroc allowed you to quickly develop and deploy complex application:

- Write your C source code using the highly advanced code editor.
- Use the included MikroC liberties to dramatically speed up the development: data acquisition, memory, displays, conversations, communications……
- Monitor your program structure, variables and functions in the code explorer. Generate commented, human-readable assemble, and standard HEX compatible with all programs.
- Inspect program flow and debug executable logic with the integrated debugger. Get detailed reports and graphs on code statistics, assembly listing, calling tree….
- So many examples to expand, develop, and use as building bricks in your project.



```
//*************************************************
// microcontroller : P12f675
//
// Project: Led_blinking
// This project is designed to work with PIC 12F67
// with minor adjustments, it should work with any
//
// This code demonstrates blinking of diodes conne
// Diodes go on and off each second.
//*************************************************

void main() {
  TRISIO = 0;              // configure pins of gpio a
  do{                   // beginning of a repeat loop
      GPIO = 0xFF;     // turn ON diodes on gpio
      delay_ms(1000);  // wait for 1 second
      GPIO = 0; a      // turn OFF diodes on gpio
      delay_ms(1000);  // wait for 1 second
  }while(1);           // endless loop (as this condition is never satisfied)
}
```

```
function    void Delay_1us()
function    void Delay_10us()
function    void Delay_22us()
function    void Delay_50us()
function    void Delay_80us()
function    void Delay_500us()
function    void Delay_5500us()
function    void Delay_8ms()
```

PCLATH

Name	Value	Address
PCLATH	0	0x00000A
?STACK_0	0	0x000050
INDF	0	0x000000
PCL	0	0x000002
STATUS	0	0x000003
FSR	0	0x000004
GPIO	0	0x000005
PCLATH	0	0x00000A

PC= 0x000004 Time= 0.00 us

Line/Column	Message No.	Message Text	Unit
1:18	24	Undeclared identifier [a] in expression	Led_blinking.c

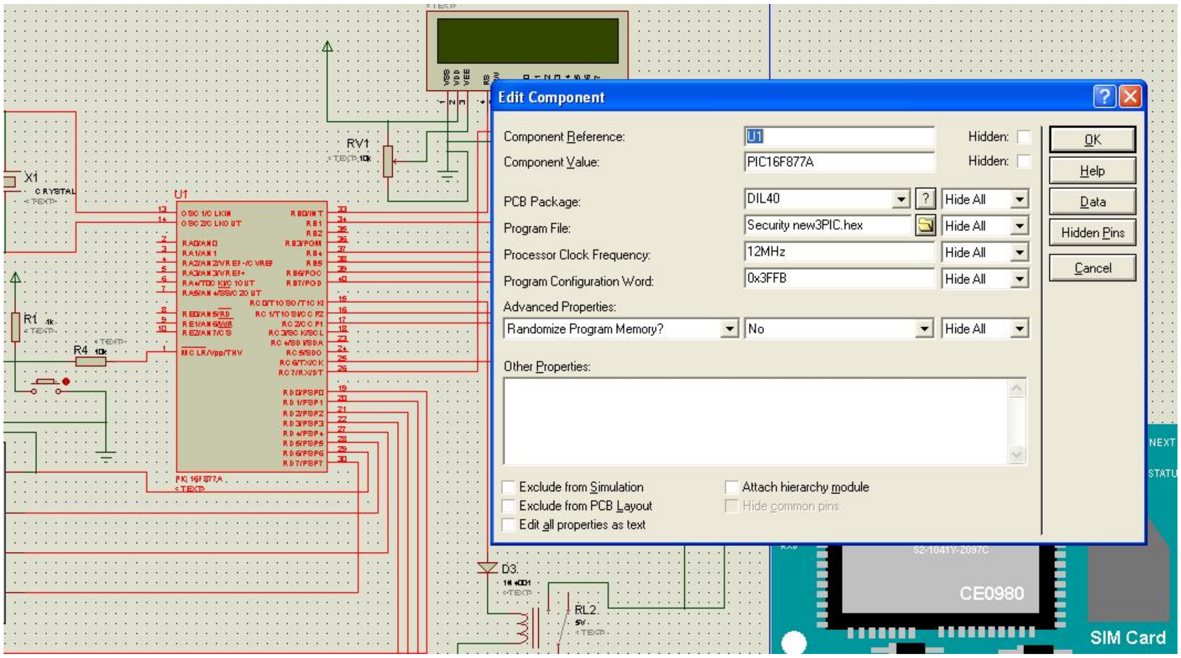
20: 7 Insert D:\shared\mikroc_5000_doc\mikroC 5.0.0.0 Output folder\examples\P12F675\led_blinking\Led_blinking.c

Figure (3.8) MiKro C Software Interface

3.11.2. Proteus v7.7

Proteus PCB design combines the ISIS schematic capture and ARES PCB layout programs to provide a powerful, integrated and easy to use suite of tools for professional PCB. All Proteus PCB design products include an integrated shape based auto router and a basic SPICE simulation capability. More advanced router modes are included in Proteus PCB design level 2 and higher whilst simulation capabilities can be enhanced by purchasing the advanced simulation option and/or micro-controller simulation capabilities.

ISIS lies at the heart of the Proteus system, and is far more than just another schematics package. It combines a powerful design environment with the ability to define most aspects of the drawing appearance. Whether your requirement is the rapid entry of complex design for simulation and PCB layout, or the creation of attractive schematics for publication, ISIS is the tool for the job.



Edit Component

Component Reference: U1 Hidden: □

Component Value: PIC16F877A Hidden: □

PCB Package: DIL40 Hide All

Program File: Security new3PIC.hex Hide All

Processor Clock Frequency: 12MHz Hide All

Program Configuration Word: 0x3FFB Hide All

Advanced Properties:

Randomize Program Memory? No Hide All

Other Properties:

□ Exclude from Simulation

□ Exclude from PCB Layout

□ Edit all properties as text

□ Attach hierarchy module

□ Hide common pins

Figure (3.9) Proteus Software Interface

Chapter Four

Simulation Result and Discussion

4.1. Results and Discussion

Various test was carried out before, during and after the construction has been completed. Each unit selected was tested and confirmed efficient. After the construction of the entire system, the program has been written and tested into the microcontroller simulation program by using PROTEUS SOFTWARE. After all of that the GSM modem interfaced to the PROTEUS SOFTWARE through the computer's I/O units, and then all of the system tested and the result was OK as it performed the objective of the design. In case of entering a wrong password, the system automatically disconnected the ignition and fuel pump system, and after three times of entering a wrong password, the system automatically disconnected the main power supply and sent a text message to the owner or authorized person.

After three times failures to enter a valid password, vehicle's main power will be shut down. To start the engine again and drive the vehicle normally, the user most enter a valid unlock code to reconnect the main power to the vehicle's engine again, and after that the user most enter a valid password code to deactivate the security system.

The mission of the design was accomplished. The entire system has tow output, which are: - the output from the controller to shutdown the ignitions and fuel system and shutdown the entire system after three times failures of typing a valid password, and the output from the GSM modem to sent text message to the owner of the vehicle. The system powered and was tapped from car battery and for this reason it made it easier for dc use. With these a system that sends text message as alarming to the vehicle's owner is designed and implemented.

This proposed anti-theft Security System for vehicles is simulated using PROTEUS SOFTWARE and their results are obtained and had been presented here. The following points will illustrate how the system is working and what exactly should the users to do to keep their vehicles in safe conditions.

- The following figure (4.1) shows the complete construction of system circuit.

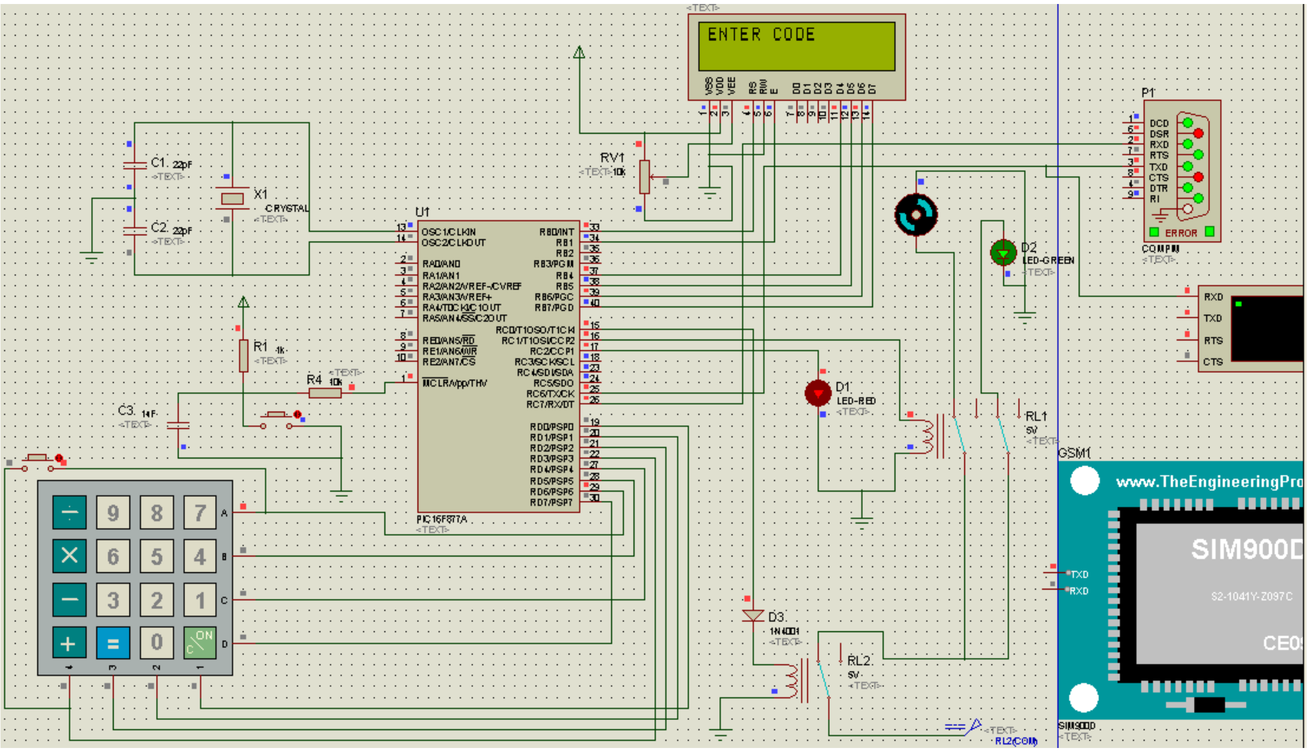


Figure (4.1) Entire System's Circuit

- The figure (4.2) below shows the simulation result when a valid password entered to the system. The system will issue the following response:
- The LCD will issue "CAR OK" message displayed on the screen.
- The red LED will turn off to indicate the system turned to sleep mode, while ignitions and fuel systems will work normally and perfectly.

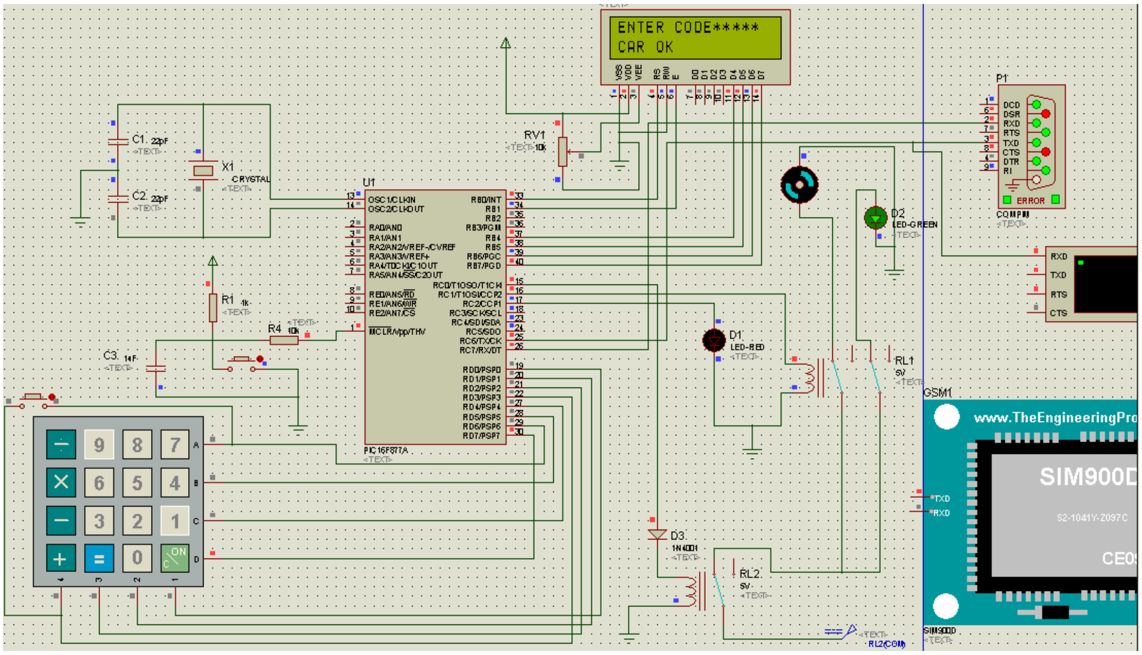


Figure (4.2) System Turned to Sleep Mode

- The figure (4.3) below shows the simulation result when not a valid password entered to the system. The system will issue the following response:
  1. The LCD will issue “WRONG CODE” message displayed on the screen.
  2. The red LED will be ON to indicate the system still activated.
  3. The ignitions and fuel systems will be disconnected from the power supply through relay1.

The proposed system in the second level of the security will check the password combination one by one, and that means if the user entered the first digit and was wrong, the system will response immediately and will cut off the engine’s power and the system will start counting the failure of trying. Notice that the second level of the security system’s password combination contained a five digits “(1, 5) matrix” and the number of errors entrance allowed in this level of security limited to three times only.

In this proposed system the correct password is “1, 9, 8, 1, C”. When the user start insert the password by typing the first digit “1” and followed by the second digit “8” the system will not accept it. As you realized digit “8” actually included the combination of the password but not in the exactly position of the combination sequences when the user inserted it. After disconnected the engine’s power, the user can normally restart the engine again but still the user most insert a valid password to drive the vehicle.

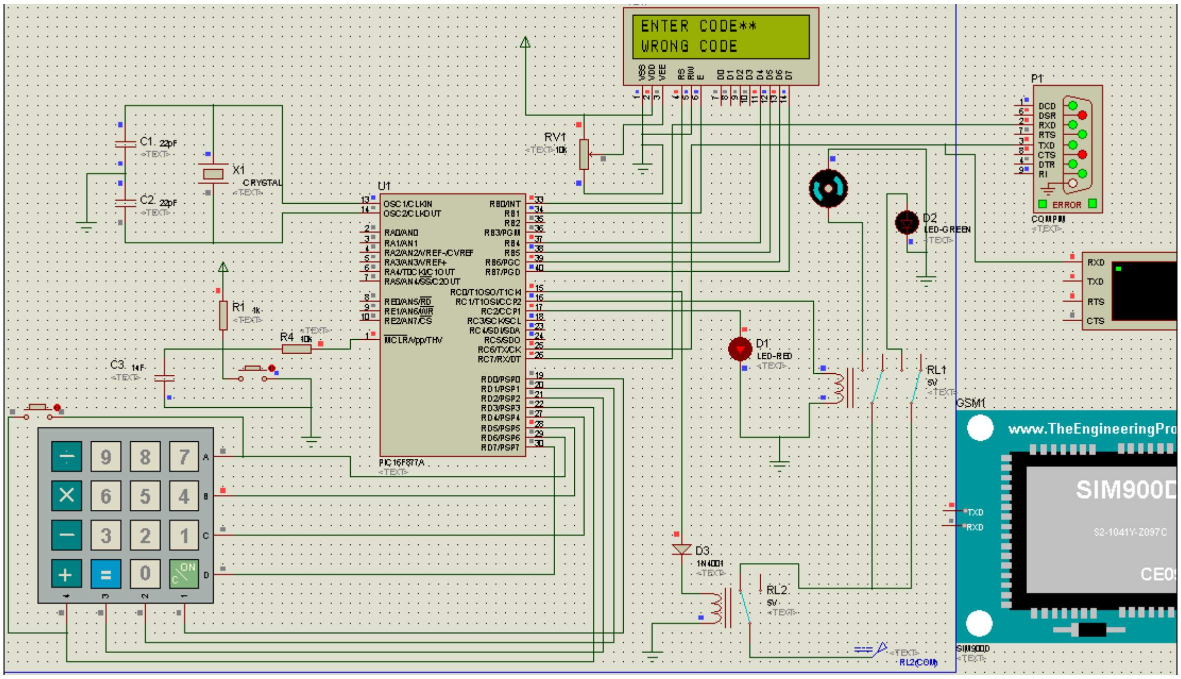
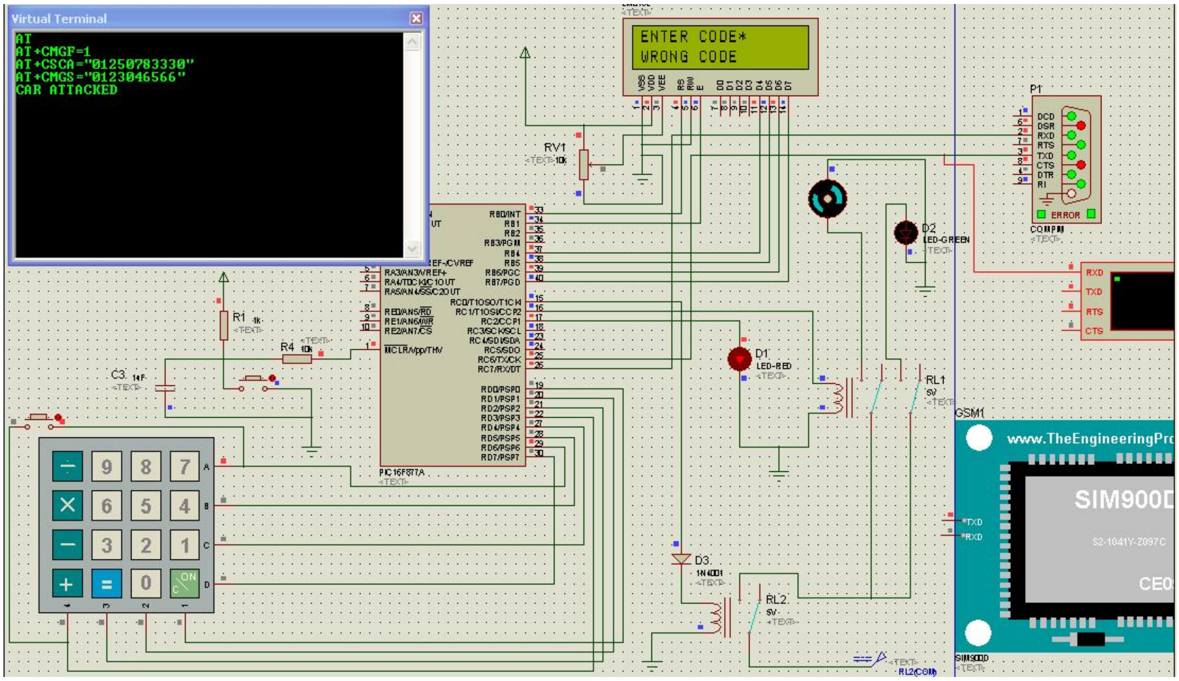


Figure (4.3) System on Activated Mode

- The figure (4.4) below shows the simulation result when a three time’s not a valid password entered to the system. The system will issue the following response:
  1. The LCD will issue “ENTER UNLOCK” message displayed on the screen.
  2. The red LED will be alarming on to indicate the system still activated.

3. The ignitions and fuel systems will be disconnected from power supply through relay1.
4. The main relay2 will turn to OFF mode and that will cut off the all system’s power.
5. The very important issue of the system in this case, the system will send “CAR ATTACKED” SMS to the owner or the authorized person to inform him the car had been illegally used.



Virtual Terminal

```
AT
AT+CMGF=1
AT+CSCA="01250783330"
AT+CMGS="0123046566"
CAR ATTACKED
```

```
ENTER CODE*
WRONG CODE
```

Figure (4.4.a) System Sending SMS to the Owner

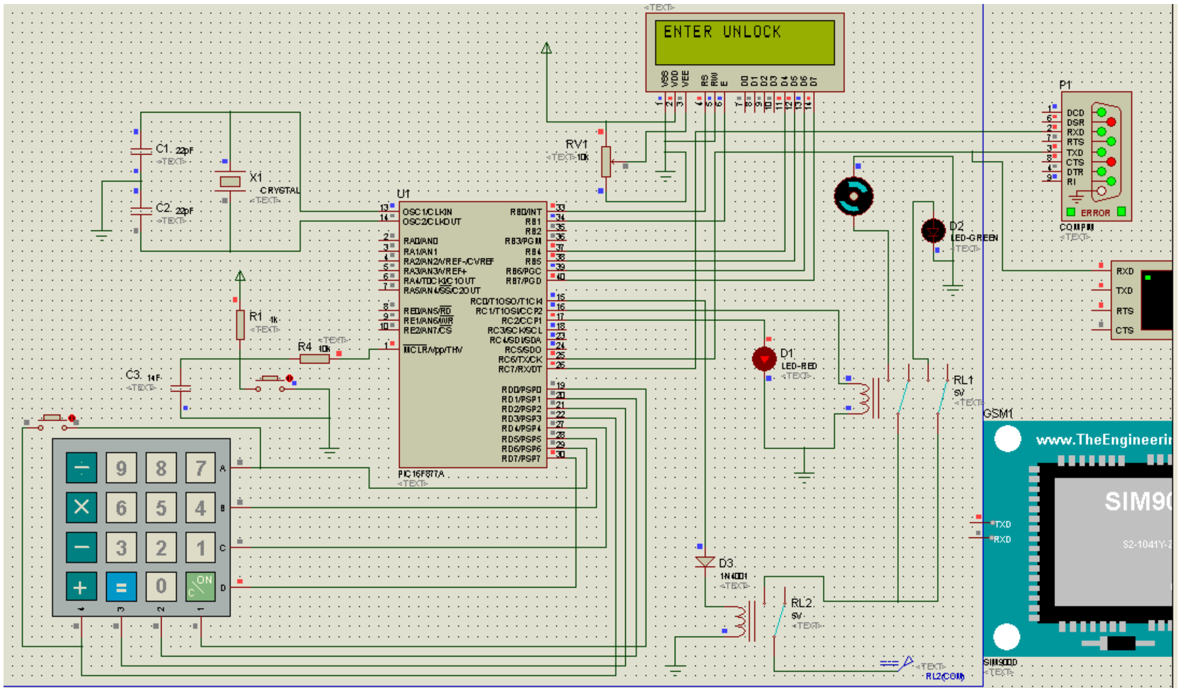


Figure (4.4.b) System Shutting Down the Entire Power

In this case, the system had turned to the first level of the security after three times of failures in entering the correct password. As shown in figure (4.4), the system asking for entering the unlock code, which is a combination of a three digits. But in the first level of the security, the system will check the password's combination after typing the all digits of the password, that means the user required to enter a three digits and then the system will check it if it's valid or not.

If the unlock code was wrong the system will ask the user again to enter the code and the main power supply will remind in the shut down mode. But if it's correct, the system immediately will response and will reconnect the main power supply through the main relay2, and the user will be able to start the engine but cannot drive the vehicle. Notice that the first level of the security system's password contained a three digits "(1, 3) matrix".

Chapter Five

Conclusions and Recommendations

5.1. Conclusion

In this research, we have proposed a novel method of vehicle security and locking systems used to protect the vehicles by using microcontroller and GSM technology. Vehicles security system is becoming a very important these days cause the theft crimes of vehicles become very higher than any crime cases else. This system turns to the sleeping mode by the owner or authorized persons only; otherwise the system will be in active mode. This proposed anti-theft protection system has two stages of security levels. When the theft succeed illegally to enter inside the vehicle and succeed to turn on the engine, the theft most enter the second level of the security system’s password by using the keypad to drive the vehicle, and if he failed to enter a valid password the system will turn off the engine and after three times failures for entering the correct password the system will turn to the first level of the security system’s password and the entire power of the vehicle will cutoff through the main relay and the system will send SMS to the owner or the authorized persons.

To restart the engine again, authorized person needs to enter the first level security password as the first stage and then the second level security password as the second stage.

5.2. Recommendations

The proposed system based vehicles Security System is perceived to be an upcoming technology which will make use of microcontroller in the most optimum manner. This proposed anti-theft security system when put into proper functioning will keep the vehicle in a secure mode and significantly the owner will reduce thinking about the likelihood of vehicle being stolen. This proposed system will provide a cheap, reliable and efficient solution for vehicles theft crimes which can be implemented by anyone on any car.

For future work:

- More security methods will add since the microcontroller can perform more tasks.
- Connect the system by internet to simplify the control of the vehicle.
- Upgrade the system according to the vehicles since the vehicles become more complicated.

References

1. Mohammed Abuzalata, Muntaser Momani, Sayel Fayyad and Suleiman Abu-Ein (2012). “A Practical Design of Anti-Theft Car Protection System Based on Microcontroller”
   American Journal of Applied Sciences 9 (5): 709-716, 2012.
   ISSN 1546-9239 © 2012 Science Publications.

2. Visa M. Ibrahim, Asogwa A. Victor.(2012). “Microcontroller Based Anti-theft Security System Using GSM Networks with Text Message as Feedback”.
   International Journal of Engineering Research and Development.
   e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume2, Issue 10 (August 2012), PP.18-22.

3. Arun Sasi,Lakshmi R Nair (2013). “Vehicle Anti-Theft System Based on an Embedded Platform”
   IJRET: International Journal of Research in Engineering and Technology. e-ISSN: 2319-1163 | p-ISSN: 2321-7308.

4. R.Ramani, S.Valarmathy, (2013). “Vehicle Tracking and Locking System Based on GSM and GPS”
   I.J. Intelligent Systems and Applications, 2013, 09, 86-93
   Published Online August 2013 in MECS (http://www.mecs-press.org/)
   DOI: 10.5815/ijisa.2013.09.10.

5. Pritpal Singh, Tanjot Sethi, Bibhuti Bhusan Biswal, and Sujit Kumar Pattanayak (2015). “A Smart Anti-Theft System for Vehicle Security”
   International Journal of Materials, Mechanics and Manufacturing, Vol. 3, No. 4, November 2015
   DOI: 10.7763/IJMMM.2015.V3.205.

6. Vaishanavi.K, K.Priyanga, S.Sangeetha, C.Thilagavathi and R.Vinodhini (2015). "VEHICLE SECURITY SYSTEM USING GSM TECHNOLOGY"
National Conference on Research Advances In Communication, Computation, Electrical Science And Structures (NCRACCESS-2015)
ISSN: 2348- 8549 (www.internationaljournalssrg.org)

7. Interfacing PIC Microcontrollers
Embedded Design by Interactive Simulation
Martin Bates, Hastings, UK (2006).

8. GSM – Architecture, Protocols and Services
3rd Edition.
Jörg Eberspächer, Hans-Jörg Vögel, Christian Bettstetter and Christian Hartmann. (2009).

9. Modern Control technology: components and Systems.
Christopher T.Kilian. (2001).

10. Mechatronics Principles and Applications.
Godfrey C. Onwublu. (2005).

Appendix

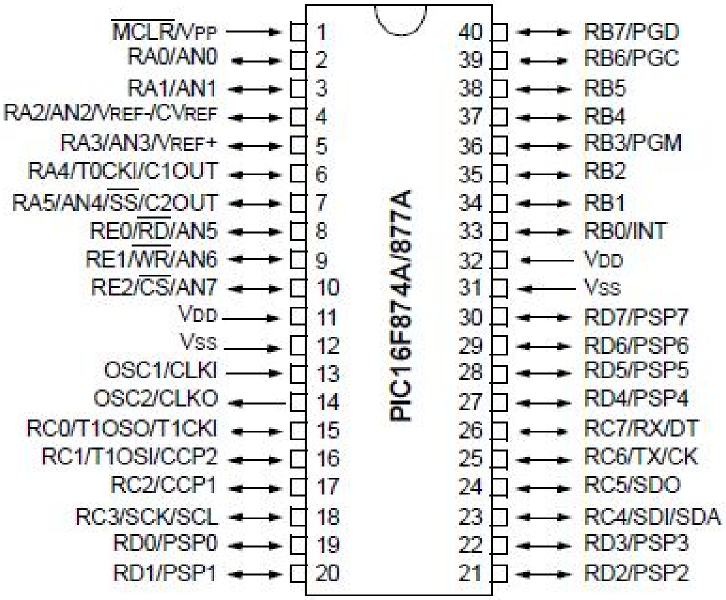
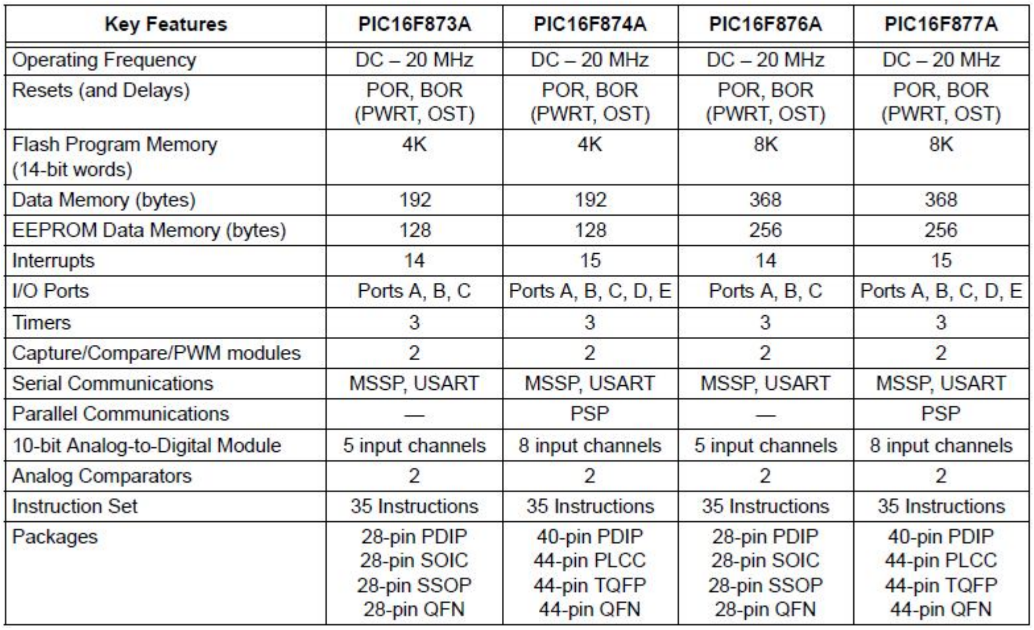


Figure (1) Pin Diagrams

Table(1) Pic16f87xa Device Features



Key Features	PIC16F873A	PIC16F874A	PIC16F876A	PIC16F877A
Operating Frequency	DC – 20 MHz	DC – 20 MHz	DC – 20 MHz	DC – 20 MHz
Resets (and Delays)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)
Flash Program Memory (14-bit words)	4K	4K	8K	8K
Data Memory (bytes)	192	192	368	368
EEPROM Data Memory (bytes)	128	128	256	256
Interrupts	14	15	14	15
I/O Ports	Ports A, B, C	Ports A, B, C, D, E	Ports A, B, C	Ports A, B, C, D, E
Timers	3	3	3	3
Capture/Compare/PWM modules	2	2	2	2
Serial Communications	MSSP, USART	MSSP, USART	MSSP, USART	MSSP, USART
Parallel Communications	—	PSP	—	PSP
10-bit Analog-to-Digital Module	5 input channels	8 input channels	5 input channels	8 input channels
Analog Comparators	2	2	2	2
Instruction Set	35 Instructions	35 Instructions	35 Instructions	35 Instructions
Packages	28-pin PDIP 28-pin SOIC 28-pin SSOP 28-pin QFN	40-pin PDIP 44-pin PLCC 44-pin TQFP 44-pin QFN	28-pin PDIP 28-pin SOIC 28-pin SSOP 28-pin QFN	40-pin PDIP 44-pin PLCC 44-pin TQFP 44-pin QFN

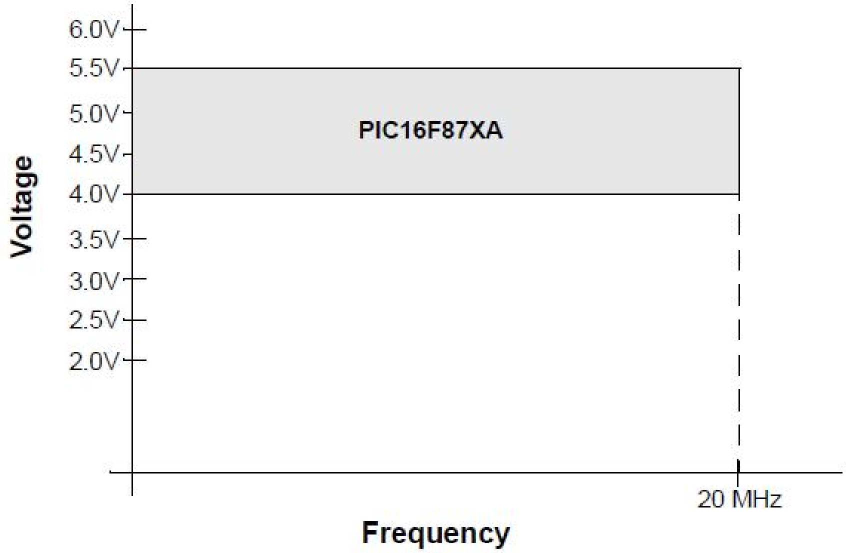


Figure (2) Pic16f87xa Voltage-Frequency Graph (Industrial, Extended)

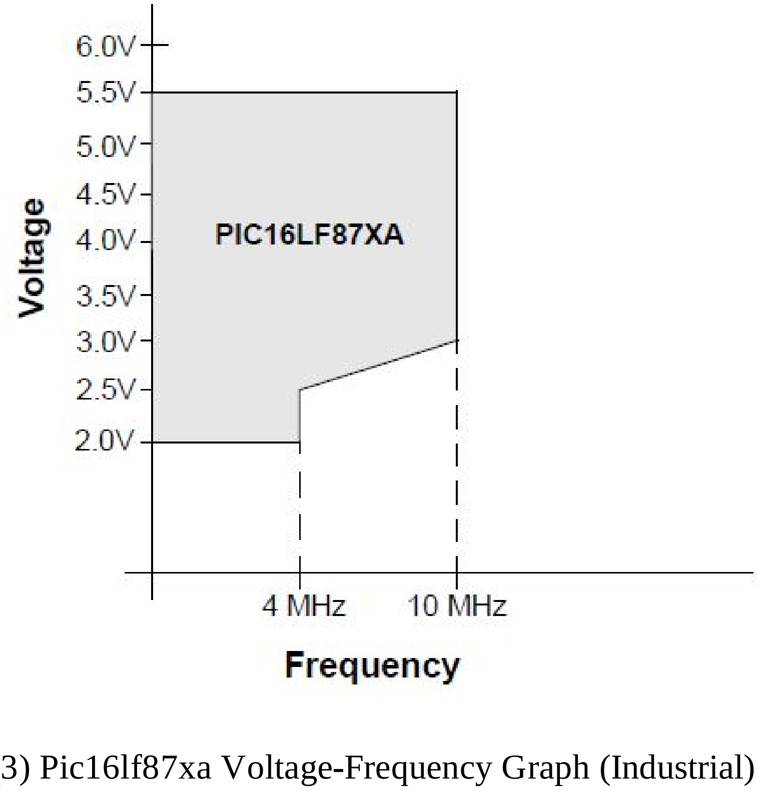


Figure (3) Pic16lf87xa Voltage-Frequency Graph (Industrial)