DESIGN OF A GSM-BASED CAR SECURITY SYSTEM

BY

ATIN PANDEY	021071
HARSH SHARDA	021077
JAIDEEP SINGH CHANDOK	021073

MAY – 2006

Submitted in partial fulfillment of the Degree of Bachelor of Technology

DEPARTMENT OF ELECTRONICS AND COMMUNICATIONS ENGINEERING
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY - WAKNAGHAT

CERTIFICATE

This is to certify that the work entitled, “Design of a GSM based car security system” submitted by Atin Pandey, Jaideep Singh Chandok and Harsh Sharda in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communications Engineering of Jaypee University of Information Technology has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Mr. Vinay Kumar

ACKNOWLEDGEMENT

One of the most wonderful aspects of writing an acknowledgement is the opportunity that the authors get to thank some people and organizations whose names might not appear in the authors or developers lists. First and foremost we would like to express our heartfelt thanks to our project coordinator Mr. Vinay Kumar . His thinking and straightforward attitude have inspired us to complete this project under stiff time limits. We would also like to thank all the faculty members for their sincere devotion to impart us with the best of knowledge and skills available. Also, we would like to express our thanks to our friends who have supported, encouraged, and criticized our efforts which have been instrumental in giving the project its final shape. Along with that we would like to express our thanks to all the authors and publishers for bringing out such great books on the subject. Lastly, we would like to thank our families for their honest support, wisdom and encouragement and for making us capable of graduating as engineers.

ATIN PANDEY
HARSH SHARDA
JAIDEEP SINGH CHANDOK

TABLE OF CONTENTS

PREFACE

Without our even being aware of it, we are surrounded by Embedded systems. In our daily lives, we use a number of Embedded systems- such as those in found in TV's, VCR's, CD Players, digital cameras and mobile phones etc.

Unlike general purpose mainframe computers, desktop computers and Workstations, Embedded systems are designed to carry out well defined, specific tasks. While developing this project our prior goal was to develop an Embedded device which is using a Mobile Phone to fulfill its main purpose of monitoring and controlling.

The art and Science of Embedded systems and system development is changing very rapidly. Instead of the diversity and complexity involved in Embedded system development, it has a very bright future or one can say future is Embedded system.

LIST OF FIGURES

LIST OF ABBREVIATIONS

AUC-	Authentication Centre
BSC-	Base Station Controller
BSS-	Base Station Subsystem
BTS-	Base Transceiver System
CDMA-	Code Division Multiple Access
EIR-	Equipment Identity Register
GSM-	Global System for Mobile Communication
IMEI-	International Mobile equipment Identity
IMSI-	International Mobile Subscriber Identity
MS-	Mobile System
MSC-	Mobile services Switching Centre
PDU-	Packet Description Unit

SIM-	Subscriber Identity Module
SMS-	Short Message Service
SMSC-	Short Message Service Centre
SS7-	Signaling System Number 7
STP-	Serial Transfer Point
HLR-	Home Location Register
VLR-	Visitor Location Register

ABSTRACT

This project which is based on GSM network and monitor intrusion in the car. We will implement this device in a car lock.Device add the feature sending" alarm message" through SMS whenever there is a security threat to the car. Whenever there is a intrusion a signal is generated which stimulates the software present in the microcontroller which in turn communicate with the mobile through AT command sets and send the alarm message to the appropriate mobile. The core device is primarily consisting of a mobile, microcontroller, EPROM and clock logic. This is to be established inside the car and the i/p connections are made with the lock or to sensors. Whenever there is a intrusion in a car ,signals received by the device interact with the software inside the microcontroller to work in accordance with the type of i/p signal received. The software interact with the mobile through AT command send the appropriate message to the mobile .

CHAPTER 1

INTRODUCTION TO GSM AND CDMA

GSM (Global System for Mobile communication)-

This is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

CDMA (Code Division Multiple Access)-

This is a method for transmitting simultaneous signals over a shared portion of the spectrum. The foremost application of CDMA is the digital cellular phone technology from QUALCOMM that operates in the 800MHz band and 1.9GHz PCS band. CDMA phones are noted for their call quality.

CDMA uses unique spreading codes to spread the baseband data before transmission. The signal is transmitted in a channel, which is below noise level. The receiver then uses a correlator to despread the wanted signal, which is passed through a narrow bandpass filter. Unwanted signals will not be despread and will not pass through the filter. Codes take the form of a carefully designed one/zero sequence produced at a much higher rate than that of the baseband data. The rate of a spreading code is referred to as chip rate rather than bit rate.

CHAPTER2

GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION)

A GSM network is composed of several entities, whose functions and interfaces are specified. The GSM network can be divided into four parts.

Mobile Station:

The mobile station (MS) consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. By inserting the SIM card into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI), identifying the subscriber, a secret key for authentication, and other user information. The IMEI and the IMSI are independent, thereby providing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

Base Station Subsystem:

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the specified Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed. The requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

Network Subsystem:

Central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the public fixed network (PSTN or ISDN), and signaling between functional entities uses the ITUT Signaling System Number 7 (SS7), used in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call routing and (possibly international) roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The current location of the mobile is in the form of a Mobile Station Roaming Number (MSRN) which is a regular ISDN number used to route a call to the MSC where the mobile is currently located. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, most manufacturers of switching equipment implement one VLR together with one MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, simplifying the signaling required. Note that the MSC contains no information about particular mobile stations - this information is stored in the location registers

Operational Subsystem:

The other registers are used for authentication and security purposes. The Equipment identity register is a database that contains a list of all valid mobile equipment, where each mobile is identified by IMEI.

The Authentication center is a protected database that stores a copy of the secret key stored in each SIM card, which is used for authentication and encryption over the radio channel.

CHAPTER 3

WHAT IS SMS

Short message service (SMS) is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems.

SMS appeared on the wireless scene in 1991 in Europe. The European standard for digital wireless, now known as the Global System for Mobile Communications (GSM), included short messaging services from the outset.

In North America, SMS was made available initially on digital wireless networks built by early pioneers such as BellSouth Mobility, PrimeCo, and Nextel, among others. These digital wireless networks are based on GSM, code division multiple access (CDMA), and time division multiple access (TDMA) standards.

Network consolidation from mergers and acquisitions has resulted in large wireless networks having nationwide or international coverage and sometimes supporting more than one wireless technology. This new class of service providers demands network-grade products that can easily provide a uniform solution, enable ease of operation and administration, and accommodate existing subscriber capacity, message throughput, future growth, and services reliably. Short messaging service center (SMSC) solutions based on an intelligent network (IN) approach are well suited to satisfy these requirements, while adding all the benefits of IN implementations.

Figure represents the basic network architecture for an IS–41 SMSC deployment handling multiple input sources, including a voice-mail system (VMS), Web-based messaging, e-mail integration, and other external short message entities (ESMEs). Communication with the wireless network elements such as the home location register

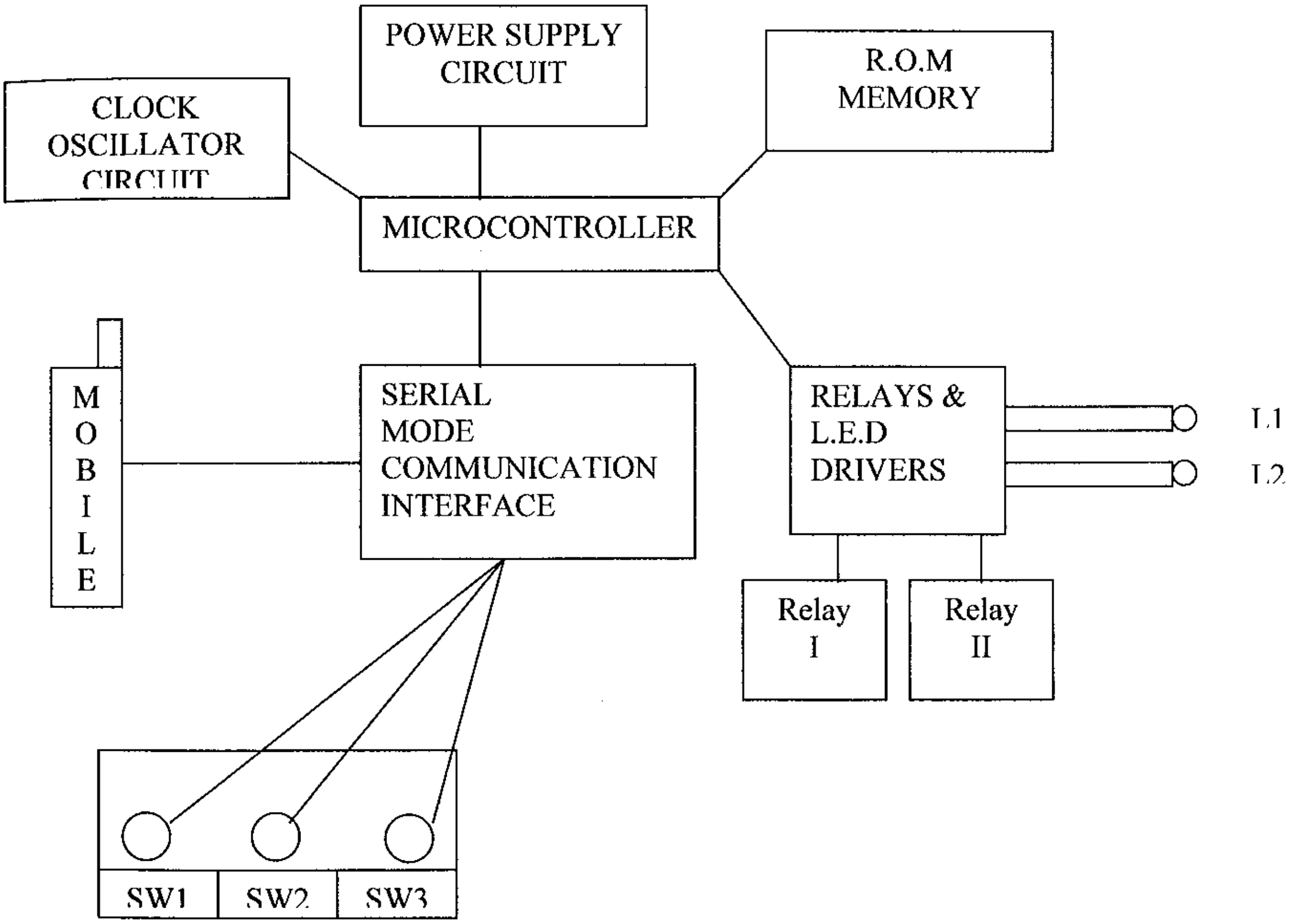
(HLR) and mobile switching center (MSC) is achieved through the signal transfer point (STP).

SMS provides a mechanism for transmitting short messages to and from wireless devices. The service makes use of an SMSC, which acts as a store-and-forward system for short messages. The wireless network provides the mechanisms required to find the destination station(s) and transports short messages between the SMSCs and wireless stations. In contrast to other existing text-message transmission services such as alphanumeric paging, the service elements are designed to provide guaranteed delivery of text messages to the destination. Additionally, SMS supports several input mechanisms that allow interconnection with different message sources and destinations.

A distinguishing characteristic of the service is that an active mobile handset is able to receive or submit a short message at any time, independent of whether a voice or data call is in progress (in some implementations, this may depend on the MSC or SMSC capabilities). SMS also guarantees delivery of the short message by the network. Temporary failures due to unavailable receiving stations are identified, and the short message is stored in the SMSC until the destination device becomes available.

SMS is characterized by out-of-band packet delivery and low-bandwidth message transfer, which results in a highly efficient means for transmitting short bursts of data. Initial applications of SMS focused on eliminating alphanumeric pagers by permitting two-way general-purpose messaging and notification services, primarily for voice mail. As technology and networks evolved, a variety of services have been introduced, including e-mail, fax, and paging integration, interactive banking, information services such as stock quotes, and integration with Internet-based applications. Wireless data applications include downloading of subscriber identity module (SIM) cards for activation, debit, profile-editing purposes, wireless points of sale (POSs), and other field-service applications such as automatic meter reading and remote sensing .

BLOCK DIAGRAM



CHAPTER 4

INTRODUCTION TO RS232

Information being transferred between data processing equipment and peripherals is in the form of digital data which is transmitted in either a serial or parallel mode. Parallel communications are used mainly for connections between test instruments or computers and printers, while serial is often used between computers and other peripherals.

Serial transmission involves the sending of data one bit at a time, over a single communications line. In contrast, parallel communications require at least as many lines as there are bits in a word being transmitted (for an 8-bit word, a minimum of 8 lines are needed). Serial transmission is beneficial for long distance communications, whereas parallel is designed for short distances or when very high transmission rates are required.

Standards:

One of the advantages of a serial system is that it lends itself to transmission over telephone lines. The serial digital data can be converted by modem, placed onto a standard voice-grade telephone line, and converted back to serial digital data at the receiving end of the line by another modem.

Officially, RS-232 is defined as the "Interface between data terminal equipment and data communications equipment using serial binary data exchange." This definition defines data terminal equipment (DTE) as the computer, while data communications equipment (DCE) is the modem. A modem cable has pin-to-pin connections, and is designed to connect a DTE device to a DCE device.

Interfaces:

In addition to communications between computer equipment over telephone lines, RS-232 is now widely used for connections between data acquisition devices and computer systems. As in the definition of RS232, the computer is data transmission equipment (DTE). However, many interface products are not data communications equipment (DCE). Null modem cables are designed for this situation; rather than having the pinto-pin connections of modem cables, null modem cables have different internal wiring to allow DTE devices to communicate with one another.

CHAPTER 5

PIC 16F84A

High Performance RISC CPU Features :

- Only 35 single new instructions to learn .
- All instructions single cycled except the programme instruction which is doubled cycle
- Operating Speed : DC 20 MHz Clock input
  DC 200 ns instuction cycle
- 1024 words of programme memory .
- 68 bytes of data RAM .
- 14 bit wide instruction words .
- 8 bit wide data bytes .
- 15 special function hardware registers .
- Eight level deep hardware stack .
- Direct , Indirest & relative addresing modes .
- Four input sources :
  1 External RBO\INT pins
  2 TMRO timer overflow
  3 Port b : 7 :4 interrupt on change
  4 Data EEPROM(Electrically Erasable Programmable Read Only Memory) write complete

Special Microcontroller features

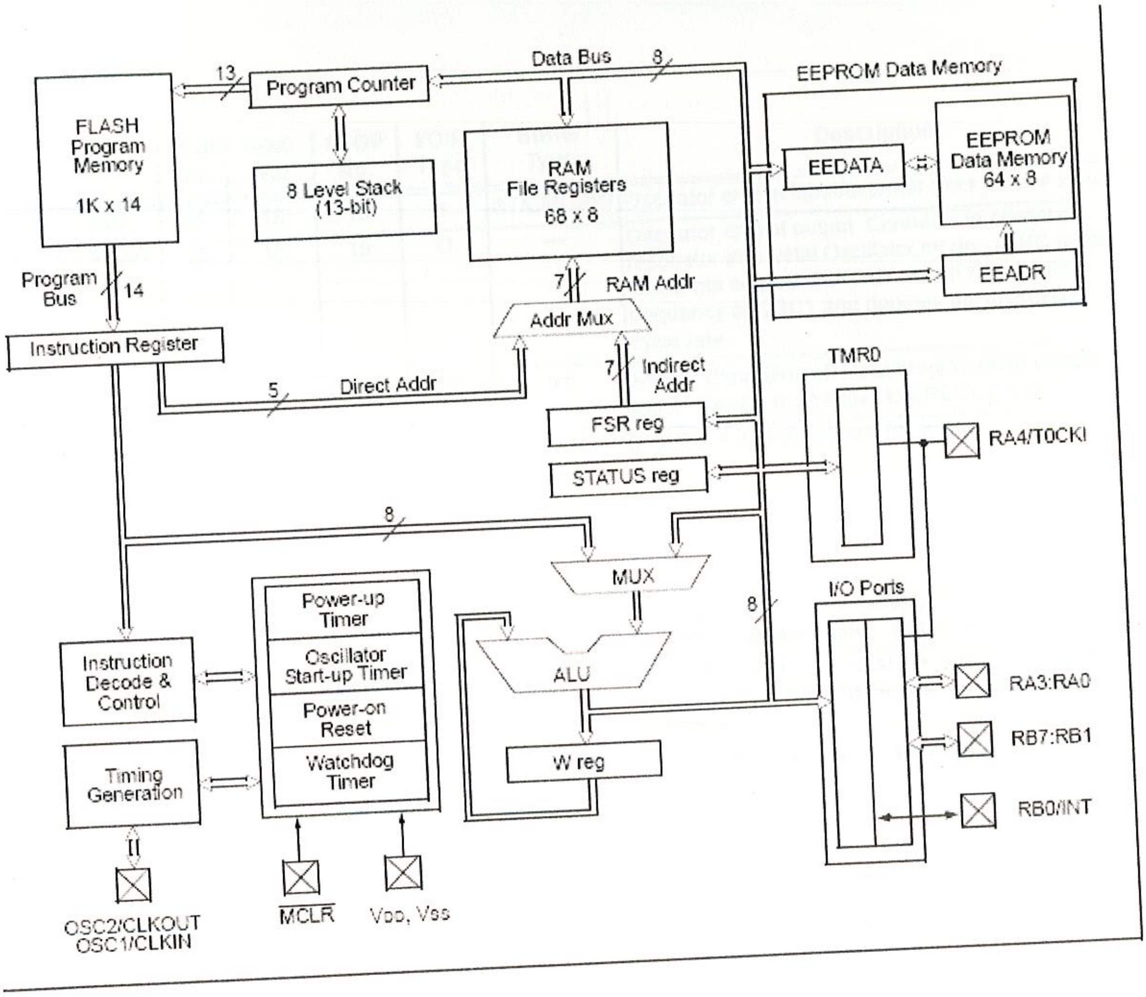
- 10,1000 Erase\Write cycles enhanced flash programme .
- EEPROM data retention > 40 years
- In circuit serial programming via 2 pins

Power on reset ,Power up timer ,Oscilator start up timer

Code Protection

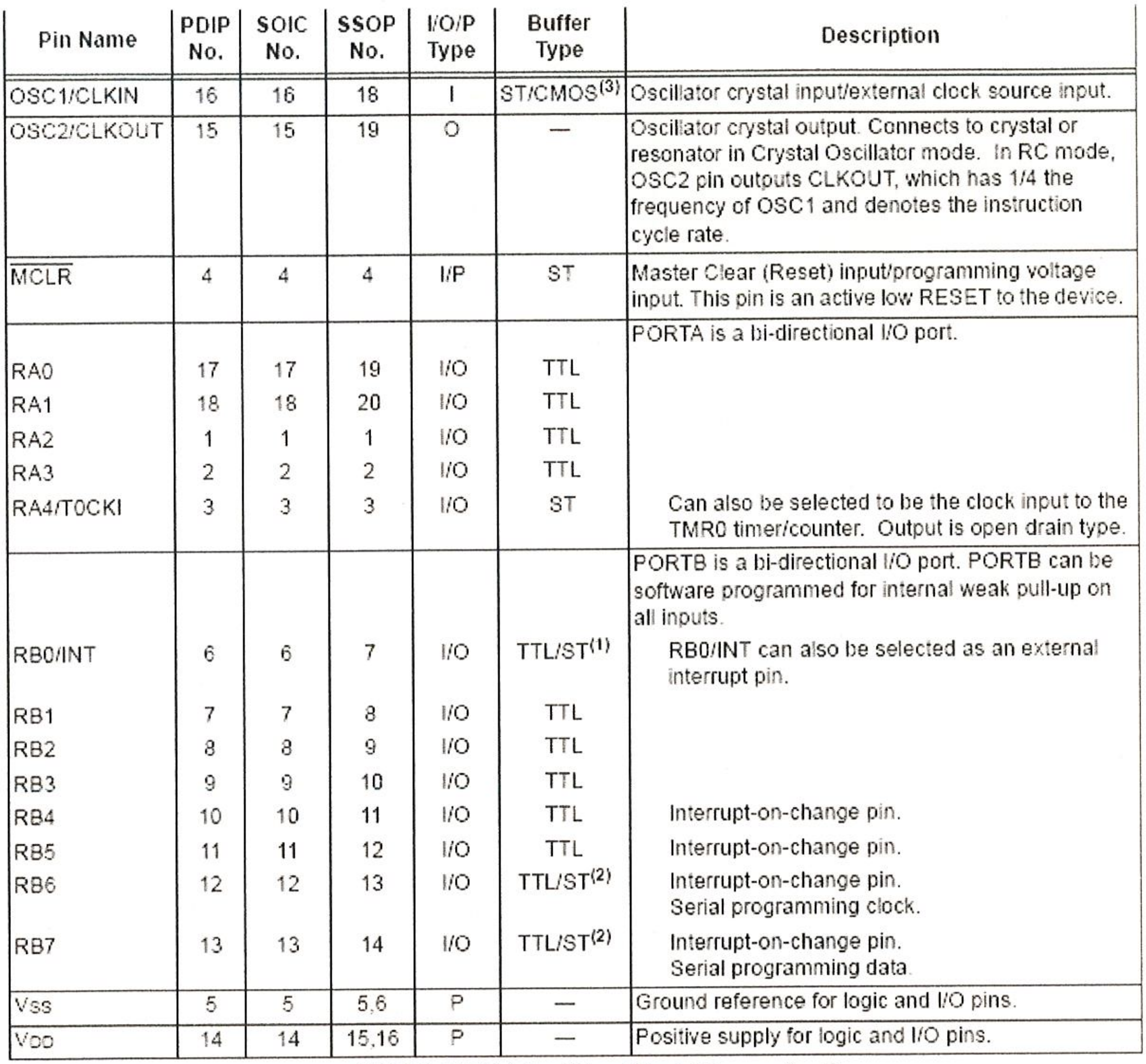
Power Saving SLEEP mode .

Selectable oscillator options .



PIC 16F84A (Block Diagram)

PIC 16F84A belongs to mid range family of PIC Microcontrollers . The programme memory contains 1 K words which translates to 1024 instructions . The data memory(RAM) contains 68 bytes . Data EEPROM is 64 bytes . 13 input pins are user-configured on a pin to pin basis .

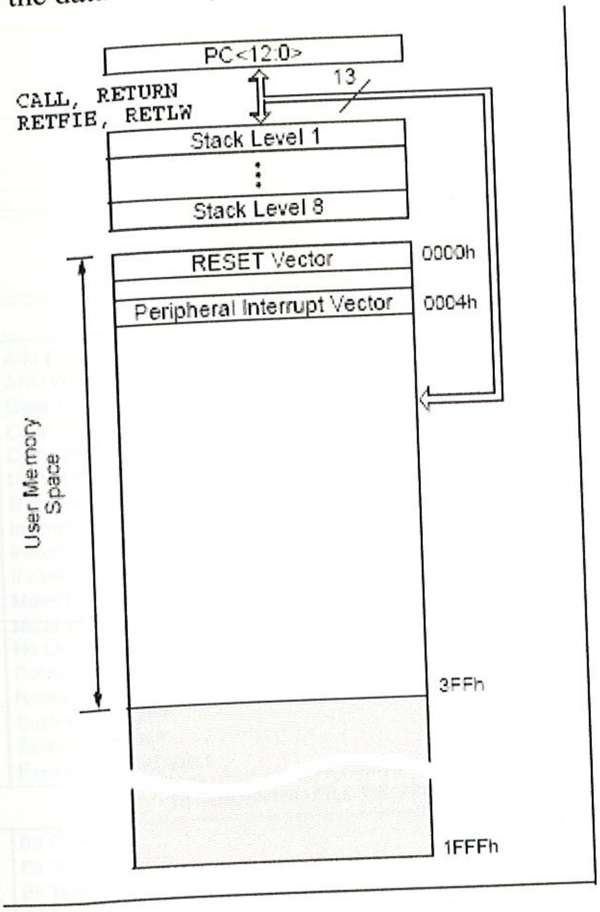


Pin Name	PDIP No.	SOIC No.	SSOP No.	I/O/P Type	Buffer Type	Description
OSC1/CLKIN	16	16	18	I	ST/CMOS(3)	Oscillator crystal input/external clock source input.
OSC2/CLKOUT	15	15	19	O	—	Oscillator crystal output. Connects to crystal or resonator in Crystal Oscillator mode. In RC mode, OSC2 pin outputs CLKOUT, which has 1/4 the frequency of OSC1 and denotes the instruction cycle rate.
$\overline{\text{MCLR}}$	4	4	4	I/P	ST	Master Clear (Reset) input/programming voltage input. This pin is an active low RESET to the device.
						PORTA is a bi-directional I/O port.
RA0	17	17	19	I/O	TTL	
RA1	18	18	20	I/O	TTL	
RA2	1	1	1	I/O	TTL	
RA3	2	2	2	I/O	TTL	
RA4/TOCKI	3	3	3	I/O	ST	Can also be selected to be the clock input to the TMR0 timer/counter. Output is open drain type.
						PORTB is a bi-directional I/O port. PORTB can be software programmed for internal weak pull-up on all inputs.
RB0/INT	6	6	7	I/O	TTL/ST(1)	RB0/INT can also be selected as an external interrupt pin.
RB1	7	7	8	I/O	TTL	
RB2	8	8	9	I/O	TTL	
RB3	9	9	10	I/O	TTL	
RB4	10	10	11	I/O	TTL	Interrupt-on-change pin.
RB5	11	11	12	I/O	TTL	Interrupt-on-change pin.
RB6	12	12	13	I/O	TTL/ST(2)	Interrupt-on-change pin. Serial programming clock.
RB7	13	13	14	I/O	TTL/ST(2)	Interrupt-on-change pin. Serial programming data.
Vss	5	5	5,6	P	—	Ground reference for logic and I/O pins.
Vdd	14	14	15,16	P	—	Positive supply for logic and I/O pins.

PIC16F84A Pin Out Description

lemory Organisation :

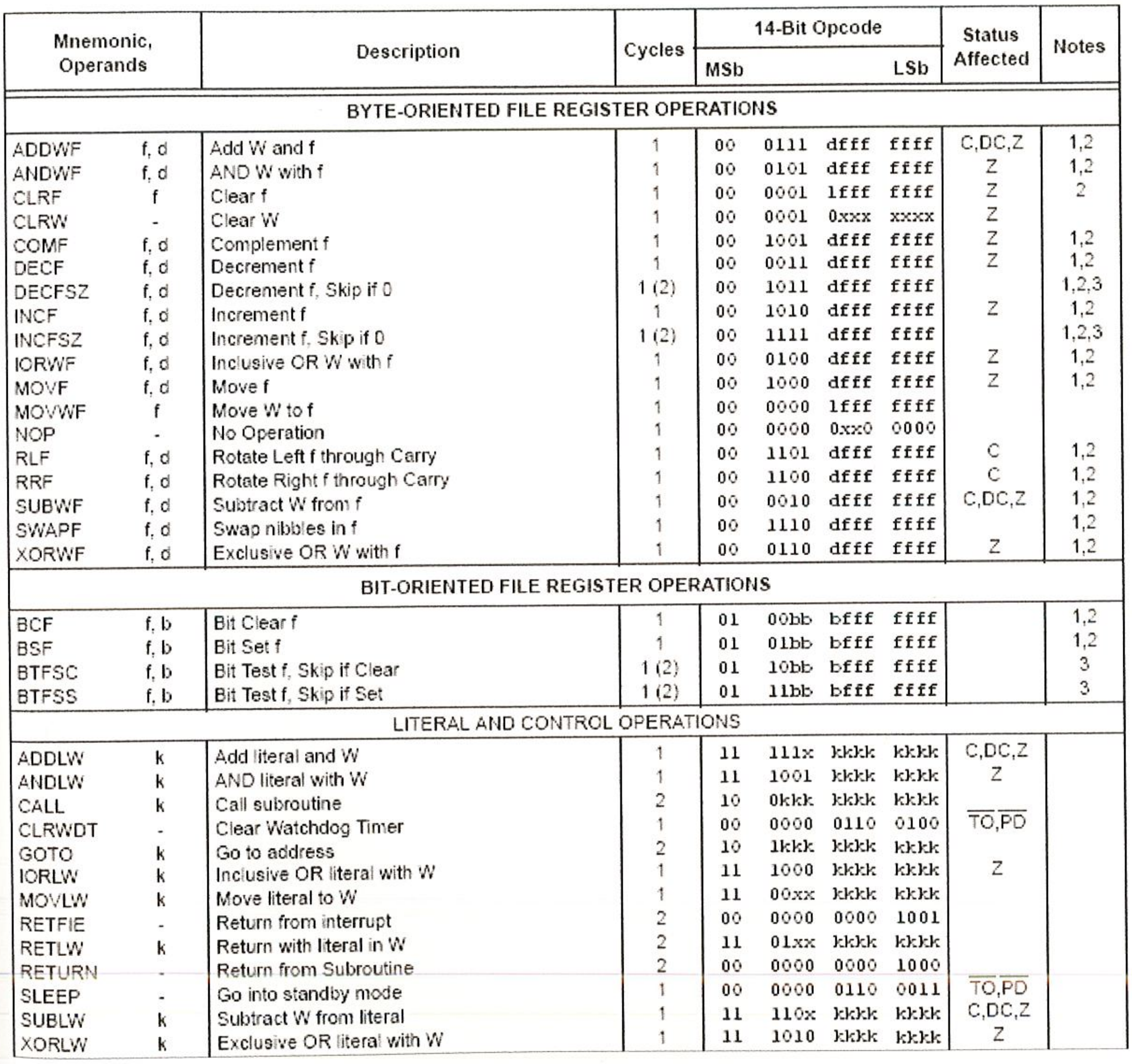
- There are two memory blocks in the PIC16F84A , programme memory and data memory .
- Each block has its own bus so that access to each block can occur during the same oscilator cycle .
- Data memory can further be broken down to general perpose RAM and Special function Registers (SFR's) .
- The data memory area also contains the data EEPROM memory , which is mapped indirectly to the data memory .



Programme memory map and stack

Instruction Set

Each instruction ser of PIC16F84A is a 14 bit word divided into an opcode which specifies the instruction types and one or more operands which further specify the operation of the instruction . The table below lists byte oriented , bit oriented ,control & literal operations . For byte oriented instructions , 'f' represents a file register designator & 'd' represents a destination designator . For bit oriented instructions , b represents a bit field designator which selects the number of the bit affected by the operation ,while 'f' represents the address of the file in which it is located .



Mnemonic, Operands		Description	Cycles	14-Bit Opcode				Status Affected	Notes
				MSb			LSb		
BYTE-ORIENTED FILE REGISTER OPERATIONS									
ADDWF	f, d	Add W and f	1	00	0111	dfff	ffff	C,DC,Z	1,2
ANDWF	f, d	AND W with f	1	00	0101	dfff	ffff	Z	1,2
CLRF	f	Clear f	1	00	0001	1fff	ffff	Z	2
CLRW	-	Clear W	1	00	0001	0xxx	xxxx	Z	
COMF	f, d	Complement f	1	00	1001	dfff	ffff	Z	1,2
DECF	f, d	Decrement f	1	00	0011	dfff	ffff	Z	1,2
DECFSZ	f, d	Decrement f, Skip if 0	1 (2)	00	1011	dfff	ffff		1,2,3
INCF	f, d	Increment f	1	00	1010	dfff	ffff	Z	1,2
INCFSZ	f, d	Increment f, Skip if 0	1 (2)	00	1111	dfff	ffff		1,2,3
IORWF	f, d	Inclusive OR W with f	1	00	0100	dfff	ffff	Z	1,2
MOVF	f, d	Move f	1	00	1000	dfff	ffff	Z	1,2
MOVWF	f	Move W to f	1	00	0000	1fff	ffff		
NOP	-	No Operation	1	00	0000	0xx0	0000		
RLF	f, d	Rotate Left f through Carry	1	00	1101	dfff	ffff	C	1,2
RRF	f, d	Rotate Right f through Carry	1	00	1100	dfff	ffff	C	1,2
SUBWF	f, d	Subtract W from f	1	00	0010	dfff	ffff	C,DC,Z	1,2
SWAPF	f, d	Swap nibbles in f	1	00	1110	dfff	ffff		1,2
XORWF	f, d	Exclusive OR W with f	1	00	0110	dfff	ffff	Z	1,2
BIT-ORIENTED FILE REGISTER OPERATIONS									
BCF	f, b	Bit Clear f	1	01	00bb	bfff	ffff		1,2
BSF	f, b	Bit Set f	1	01	01bb	bfff	ffff		1,2
BTFSC	f, b	Bit Test f, Skip if Clear	1 (2)	01	10bb	bfff	ffff		3
BTFSS	f, b	Bit Test f, Skip if Set	1 (2)	01	11bb	bfff	ffff		3
LITERAL AND CONTROL OPERATIONS									
ADDLW	k	Add literal and W	1	11	111x	kkkk	kkkk	C,DC,Z	
ANDLW	k	AND literal with W	1	11	1001	kkkk	kkkk	Z	
CALL	k	Call subroutine	2	10	0kkk	kkkk	kkkk		
CLRWDT	-	Clear Watchdog Timer	1	00	0000	0110	0100	$\overline{TO}$,$\overline{PD}$	
GOTO	k	Go to address	2	10	1kkk	kkkk	kkkk		
IORLW	k	Inclusive OR literal with W	1	11	1000	kkkk	kkkk	Z	
MOVLW	k	Move literal to W	1	11	00xx	kkkk	kkkk		
RETFIE	-	Return from interrupt	2	00	0000	0000	1001		
RETLW	k	Return with literal in W	2	11	01xx	kkkk	kkkk		
RETURN	-	Return from Subroutine	2	00	0000	0000	1000		
SLEEP	-	Go into standby mode	1	00	0000	0110	0011	$\overline{TO}$,$\overline{PD}$	
SUBLW	k	Subtract W from literal	1	11	110x	kkkk	kkkk	C,DC,Z	
XORLW	k	Exclusive OR literal with W	1	11	1010	kkkk	kkkk	Z	

PIC16f84A is supported with a full range of hardware and software devolpment tools , some of which are mentioned below :

- Integrated Devolpment Environment , MPlab IDB software .
- Asemblers, Compilers and Linkers , MPASM Assembler, MPLAB C17 and MPLAB C18 compilers .
- Simulator , MPLAB SIM software Simulator .
- In circuit debugger , MPLAB ICD .

CHAPTER 6

Executable code in PIC16F84A

```
XTAL =4
 SERIAL _ BAUD =9600
INPUT PORTA
RSOUT_PIN=PORTB.0
RSIN_PIN=PORT B.1
RSOUT_MODE=0
RSIN_MODE=0
SYMBOL LED = PORTB.5
SYMBOL GLED=PORTB.4
SYMBOL SW1=PORTA.1
SYMBOL SW2=PORTA.2
SYMBOL SW3=PORTA.3

Inf :
 LOW GLED
If SW1=1 then GoToDial1
Delayms 409
Toggle LED
If  SW2=1 Then go To Dial2
  Delayms 40
Toggle LED
If SW3 = 1 Then Go To Dial3
Delayms 40
Toggle LED
GoTo inf


Dial1 :
   LOW LED
   High GLED

' Funky reset begins
'Funky reset closes
```

```
'Send Init
            Rsout "AT"
            Rsout 13
            Rsout 10
            Delayms 1500


'BINARY enabled

'Send Ack
  Rsout 6
Delayms 1500

'Ack done

'Start of message 'intrusion detected'@9816188255
   Rsout 6
   Rsout 2
   Rsout 34
   Rsout 65
   Rsout 7
   Rsout  3
   Rsout 2
   Rsout  0
   Rsout  17
   Rsout 0
   Rsout 10
   Rsout 129
   Rsout 57
   Rsout 99
   Rsout 67
   Rsout 18
   Rsout  3
   Rsout 0
   Rsout 0
   Rsout 196
   Rsout 18
   Rsout 204
   Rsout 178
   Rsout 153
   Rsout  14
   Rsout  34
   Rsout  190
   Rsout   223
   Rsout  114
```

```
    Rsout  80
    Rsout 210
    Rsout 61
    Rsout 47
    Rsout 143
    Rsout 235
    Rsout 242
    Rsout 50

'End  of message

 Delayms 4000

'Final Ack
     Rsout 6
     Rsout 0

'End final Ack
    Go To inf


Dial 2
   LOW LED
  High GLED

' Funky reset begins
'Funky reset closes



'Send Init
            Rsout "AT"
            Rsout 13
            Rsout 10
            Delayms 1500


'BINARY enabled

'Send Ack
  Rsout 6
Delayms 1500

'Ack done

'Start of message 'intrusion detected'@9816188255
```

```
Rsout 6
Rsout 2
Rsout 34
Rsout 65
Rsout 7
Rsout  3
Rsout 2
Rsout  0
Rsout  17
Rsout 0
Rsout 10
Rsout 129
Rsout 57
Rsout 99
Rsout 67
Rsout 18
Rsout  3
Rsout 0
Rsout 0
Rsout 196
Rsout 18
Rsout 204
Rsout 178
Rsout 153
Rsout  14
Rsout  34
Rsout  190
Rsout   223
Rsout  114
Rsout   80
Rsout  210
Rsout  61
Rsout  47
Rsout  143
Rsout  235
Rsout  242
Rsout  50

'End  of message

Delayms 4000

'Final Ack
     Rsout 6
     Rsout 0
```

```
'End final Ack
   Go To inf

Dial 3
 LOW LED
  High GLED

' Funky reset begins
'Funky reset closes



'Send Init
         Rsout "AT"
         Rsout 13
         Rsout 10
         Delayms 1500


'BINARY enabled

'Send Ack
 Rsout 6
Delayms 1500

'Ack done

'Start of message 'intrusion detected'@9816188255
  Rsout 6
  Rsout 2
  Rsout 34
  Rsout 65
  Rsout 7
  Rsout  3
  Rsout 2
  Rsout  0
  Rsout  17
  Rsout 0
  Rsout 10
  Rsout 129
  Rsout 57
  Rsout 99
  Rsout 67
  Rsout 18
  Rsout  3
  Rsout 0
```

```
   Rsout 0
   Rsout 196
   Rsout 18
   Rsout 204
   Rsout 178
   Rsout 153
   Rsout  14
   Rsout  34
   Rsout  190
   Rsout   223
   Rsout  114
   Rsout   80
   Rsout  210
   Rsout  61
   Rsout  47
   Rsout  143
   Rsout  235
   Rsout  242
   Rsout  50

'End  of message

 Delayms 4000

'Final Ack
     Rsout 6
     Rsout 0

'End final Ack
    Go To inf
```

CHAPTER 7

AT Command Sct

```
// ==========================================
// AT commands to mobile phones
// ==========================================
//-----------------------------------------------------------------------------------------
// read some information from the mobile phone
//-----------------------------------------------------------------------------------------

//----- get attension

at
ok

//----- get signal quality

at+csq
+CSQ: 31,99

//----- get battery charge

at+cbc
+CBC: 0,90

//----- check if PIN is verified

at+cpin?
+CPIN: READY

//----- check network registration

at+creg?
+CREG: 0,1

//----- request model identification

at+cgmm
Nokia 6210

//----- request model identification
```

```
at+cgmm
SL55

//----- request international mobile subscriber identity

at+cimi
262017130021182

//----- get message format

at+cmgf=?
+CMGF: (0)

//----- get phone activity status

at+cpas
+CPAS: 0

//------------------------------------------------------------------------------------------
// list and delete SMS in mobile phone
//------------------------------------------------------------------------------------------

//----- 1 SMS is stored (index=2) and could be read with "+CMGL"

at+cmgl
+CMGL: 2,1,,43
07919471016700000404850800390040103131316040 20D737DB7C0EBBCF2E69D8B
D6603C865D739
DD22975DE3771B442DCFE9
OK

//----- 2 SMS are stored (index=1, 2)and could be read with "+CMGL"

at+cmgl
+CMGL: 1,0,,51
07919471016700000404850800390040104111713340 29D737DB7C0EBBCF2E69D8B
D6603C865D739
DD22975DE3771B747DB3CDE7B0FB0CA296E774
+CMGL: 2,1,,43
07919471016700000404850800390040103131316040 20D737DB7C0EBBCF2E69D8B
D6603C865D739
DD22975DE3771B442DCFE9
OK

//----- 1 SMS (index=1) will be deleted by "+CMGD=1"
```

```
at+cmgd=1
OK

//----- 1 SMS is stored (index=2) and could be read with "+CMGL"

at+cmgl
+CMGL: 2,1,,43
07919471016700000404850800390040103131316040 20D737DB7C0EBBCF2E69D8B
D6603C865D739
DD22975DE3771B442DCFE9
OK

//----- 1 SMS (index=2) will be deleted by "+CMGD=2"

at+cmgd=2
OK

//----- 0 SMS are stored and could be read with "+CMGL"]

at+cmgl
OK
```

CHAPTER 8

PACKET DISCRIPTION UNIT

The PDU mode offers to send binary information in 7 bit or 8 bit format. That is helpful if you have to send compressed data, binary data or you like to build your own encoding of the characters in the binary bit stream. If you go back on the old encoding of a Fernschreiber, then there are only 5 bit needed to send an alphanumeric text. By 5 bit coding you can contain 224 characters instatt of 160 characters in 7 bit Text mode. An others reason could be the sending of integer data.

If you would like to have the full control of your transmitted data in Text mode you have to understand the PDU mode, because there are a few commands where you can set numeric parameters that change the kind of send and receive of a SMS in text mode also. Please note that there are a few differences of in the kind of implementation of the PDU mode and by the other AT commands. It describes the PDU mode perfect and is very helpful. More details about the PDU mode you can find in the ETSI GSM 03.40 "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP)" and ETSI GSM 03.38 "Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information".

SMS and the PDU format

Introduction:

The SMS message, as specified by the ETSI organization (documents GSM 03.40 and GSM 03.38), can be up to 160 characters long, where each character is 7 bits according to the 7-bit default alphabet. Eight-bit messages (max 140 characters) are usually not viewable by the phones as text messages; instead they are used for data in e.g. smart messaging (images and ringing tones) and OTA provisioning of WAP settings. 16-bit messages (max 70 characters) are used for Unicode (UCS2) text messages, viewable by most phones. A 16-bit text message of class 0 will on some phones appear as a Flash SMS (aka blinking SMS or alert SMS).

The PDU format:

There are two ways of sending and receiving SMS messages: by text mode and by PDU (protocol description unit) mode. The text mode (unavailable on some phones) is just an encoding of the bit stream represented by the PDU mode. Alphabets may differ and there are several encoding alternatives when displaying an SMS message. The most common options are "PCCP437", "PCDN", "8859-1", "IRA" and "GSM". These are all set by the at-command AT+CSCS, when you read the message in a computer application. If you read the message on your phone, the phone will choose a proper encoding. An application capable of reading incoming SMS messages can thus use text mode or PDU mode. If text mode is used, the application is bound to (or limited by) the set of preset encoding options. In some cases, that's just not good enough. If PDU mode is used, any encoding can be implemented.

Receiving a message in the PDU mode:

The PDU string contains not only the message, but also a lot of meta-information about the sender, his SMS service center, the time stamp etc. It is all in the form of hexa-decimal octets or decimal semi-octets. The following string is what we received on a Nokia 6110 when sending the message containing "hellohello" from www.mtn.co.za.

07 917238010010F5 040BC87238880900F10000993092516195800 3C16010

Octet(s)	Description
07	Length of the SMSC information (in this case 7 octets)
91	Type-of-address of the SMSC. (91 means international format of the phone number)
72 38 01 00 10 F5	Service center number(in decimal semi-octets). The length of the phone number is odd (11), so a trailing F has been added to form proper octets. The phone number of this service center is "+27831000015". See below.
04	First octet of this SMS-DELIVER message.
0B	Address-Length. Length of the sender number (0B hex = 11 dec)
C8	Type-of-address of the sender number

72 38 88 09 00 F1	Sender number (decimal semi-octets), with a trailing F
00	TP-PID. Protocol identifier.
00	TP-DCS Data coding scheme
99 30 92 51 61 95 80	TP-SCTS. Time stamp (semi-octets)
0A	TP-UDL. User data length, length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10). If the TP-DCS field were set to indicate 8-bit data or Unicode, the length would be the number of octets (9).
E8329BFD4697D9EC37	TP-UD. Message "hellohello" , 8-bit octets representing 7-bit DATAdata.

All the octets above are hexa-decimal 8-bit octets, except the Service center number, the sender number and the timestamp; they are decimal semi-octets. The message part in the end of the PDU string consists of hexa-decimal 8-bit octets, but these octets represent 7-bit data . The semi-octets are decimal, and e.g. the sender number is obtained by performing internal swapping within the semi-octets from "72 38 88 09 00 F1" to "27 83 88 90 00 1F". The length of the phone number is odd, so a proper octet sequence cannot be formed by this number. This is the reason why the trailing F has been added. The time stamp, when parsed, equals "99 03 29 15 16 59 08", where the 6 first characters represent date, the following 6 represents time, and the last two represents time-zone related to GMT.

Interpreting 8-bit octets as 7-bit messages:

This transformation is described in detail in GSM 03.38, and an example of the "hellohello" transformation is shown here. The transformation is based on the 7 bit default alphabet, but an application built on the PDU mode can use any character encoding.

Sending a message in the PDU mode:

The following example shows how to send the message "hellohello" in the PDU mode from a Nokia 6110.

```
AT+CMGF=0 //Set PDU mode

AT+CSMS=0 //Check if modem supports SMS commands

AT+CMGS=23 //Send message, 23 octets (excluding the two initial zeros)
```

“0011000B916407281553F80000AA0AE8329BFD4697D9EC37”

There are 23 octets in this message (46 'characters'). The first octet ("00") doesn't count, it is only an indicator of the length of the SMSC information supplied (0). The PDU string consists of the following:

Octet(s)	Description
00	Length of SMSC information. Here the length is 0, which means that the SMSC stored in the phone should be used. *Note: This octet is optional. On some phones this octet should be omitted! (Using the SMSC stored in phone is thus implicit)*
11	First octet of the SMS-SUBMIT message.
00	TP-Message-Reference. The "00" value here lets the phone set the message reference number itself.
0B	Address-Length. Length of phone number (11)
91	Type-of-Address. (91 indicates international format of the phone number).
6407281553F8	The phone number in semi octets (46708251358). The length of the phone number is odd (11), therefore a trailing F has been added, as if the phone number were "46708251358F". Using the unknown format (i.e. the Type-of-Address 81 instead of 91) would yield the phone number octet sequence 7080523185 (0708251358). Note that this has the length 10 (A), which is even.
00	TP-PID. Protocol identifier
00	TP-DCS. Data coding scheme.This message is coded according to the 7bit default alphabet. Having "02" instead of "00" here. would indicate that the TP-User-Data field of this message should be interpreted as 8bit rather than 7bit (used in

	e.g. smart messaging, OTA provisioning etc).
AA	TP-Validity-Period. "AA" means 4 days. *Note: This octet is optional, see bits 4 and 3 of the first octet*
0A	TP-User-Data-Length. Length of message. The TP-DCS field indicated 7-bit data, so the length here is the number of septets (10). If the TP-DCS field were set to 8-bit data or Unicode, the length would be the number of octets.
E8329BFD4697D9EC37	TP-User-Data. These octets represent the message "hellohello".

CHAPTER 9

OTHER IMPLEMENTATIONS

Due to high usability and versatility of the device it has various application. Its usability aspects vary from providing security to home and organizations to constantly updating information to the user about real time changes in the stock exchanges.

Providing security to organizations:

The device is effectively implemented in institutions like Banks, Govt. offices. Any intrusion into the organization is detected by the security men.

In Stock Exchange and Financial Institutions:

Any immediate rise or fall in the price of stock is often in the stock exchange. The device is helpful to aware the shareholders about current stock value.

In providing Home Security:

The device can be deployed in home for its security. Any threat to home security can be easily detected by the device in real time so that rescue measures should be taken.

CHAPTER 10

OUR STEPS AND NEXT VERSION:

Currently the device is only able to send SMS. Our aim is to modify the device in such way so that it can both send and receive the SMS.

AUTOMATIC CAR LOCK SYSTEM

The next version of the device will be to lock the car as it receives the desired SMS. The device will be able to work according to the received message.

This is done by using AT-command sets, there are several commands which are especially for receiving the SMS but they are not given officially by Ericssion, so we are not sure of trust and credibility.

We are still working on for finding any alternate way of doing the desired task.

BIBLIOGRAPHY

-Data Sheet for PIC16F84A .
-Jochen Schiller, Mobile Communication.
- Andrew S Tanenbaum , Computer Networks

WEB RESOURCES

www.funsms.net
www. camiresearch.com
www.omega.com
www.gsm-modem.de
www.google.com
www.dreamfabric.com