AN645

PIC16C57 Based Code Hopping Security System

Author: *Kobus Marneweck*
Microchip Technology Inc.

OVERVIEW

This document describes a PIC16C57 based code hopping automotive security system. The security system implements all the basic features found on security systems and can be changed to modify or add features as required. The code can also be moved to a higher functionality PICmicro® microcontroller for more I/O or code space.

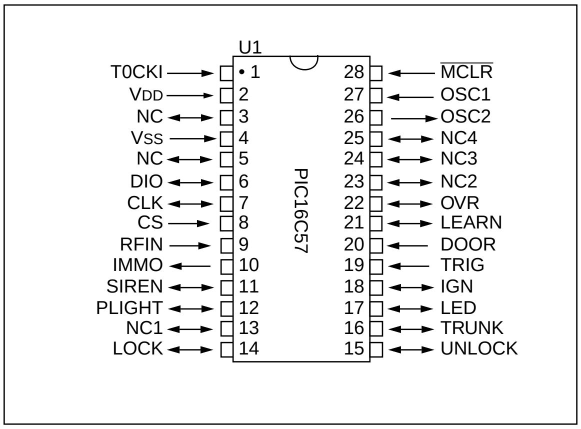
FEATURES

- Code hopping alarm system
- System can handle up to six transmitters
- Learning of new transmitters
- Arm/Disarm
- Trunk release
- Car finder
- Panic
- Locking/unlocking of doors
- Door and shock sensor trigger inputs

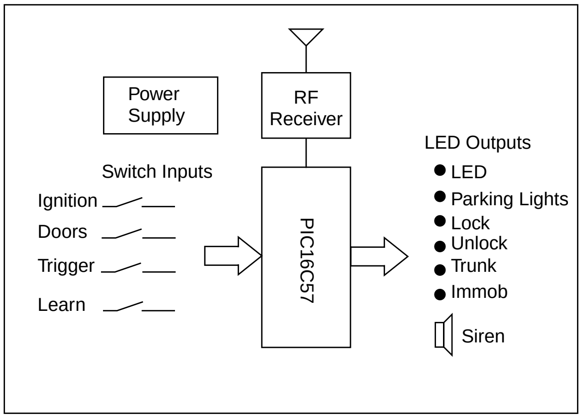
RECOMMENDED READING

If the reader is unfamiliar with KEELOQ Code Hopping it would be helpful to read *Introduction to KEELOQ®* (DS91002). This and other KEELOQ literature can be found on Microchip's Web site or from a Microchip field application engineer. The software described in this application note is available on a diskette from Microchip by ordering DS40149. A complete list of KEELOQ literature can be found at the end of the application note.

PINOUT



BLOCK DIAGRAM



KEELOQ is a registered trademark of Microchip Technology, Inc.
PICMicro is a trademark of Microchip Technology, Inc.
Microchip's Secure Data Products are covered by some or all of the following patents:
Code hopping encoder patents issued in Europe, U.S.A., and R.S.A. — U.S.A.: 5,517,187; Europe: 0459781; R.S.A.: ZA93/4726
Secure learning patents issued in the U.S.A. and R.S.A. — U.S.A.: 5,686,904; R.S.A.: 95/5429

MEMORY MAP EEPROM (16 BIT WORDS)

Address		Address	
00h	USER0	20h	CNT20
01h	LRN_PTR	21h	CNT21
02h	BSTATUS	22h	SER20
03h	SSTATUS	23h	SER21
04h	TMPCNT	24h	KEY20
05h	USER1	25h	KEY21
06h	USER2	26h	KEY22
07h	USER3	27h	KEY23
08h	USER4	28h	CNT30
09h	USER5	29h	CNT31
0Ah	DIS0	2Ah	SER30
0Bh	DIS1	2Bh	SER31
0Ch	DIS2	2Ch	KEY30
0Dh	DIS3	2Dh	KEY31
0Eh	DIS4	2Eh	KEY32
0Fh	DIS5	2Fh	KEY33
10h	CNT00	30h	CNT40
11h	CNT01	33h	CNT41
12h	SER00	32h	SER40
13h	SER01	33h	SER41
14h	KEY00	34h	KEY40
15h	KEY01	35h	KEY41
16h	KEY02	36h	KEY42
17h	KEY03	37h	KEY43
18h	CNT10	38h	CNT50
19h	CNT11	39h	CNT51
1Ah	SER10	3Ah	SER50
1Bh	SER11	3Bh	SER51
1Ch	KEY10	3Ch	KEY50
1Dh	KEY11	3Dh	KEY51
1Eh	KEY12	3Eh	KEY52
1Fh	KEY13	3Fh	KEY53

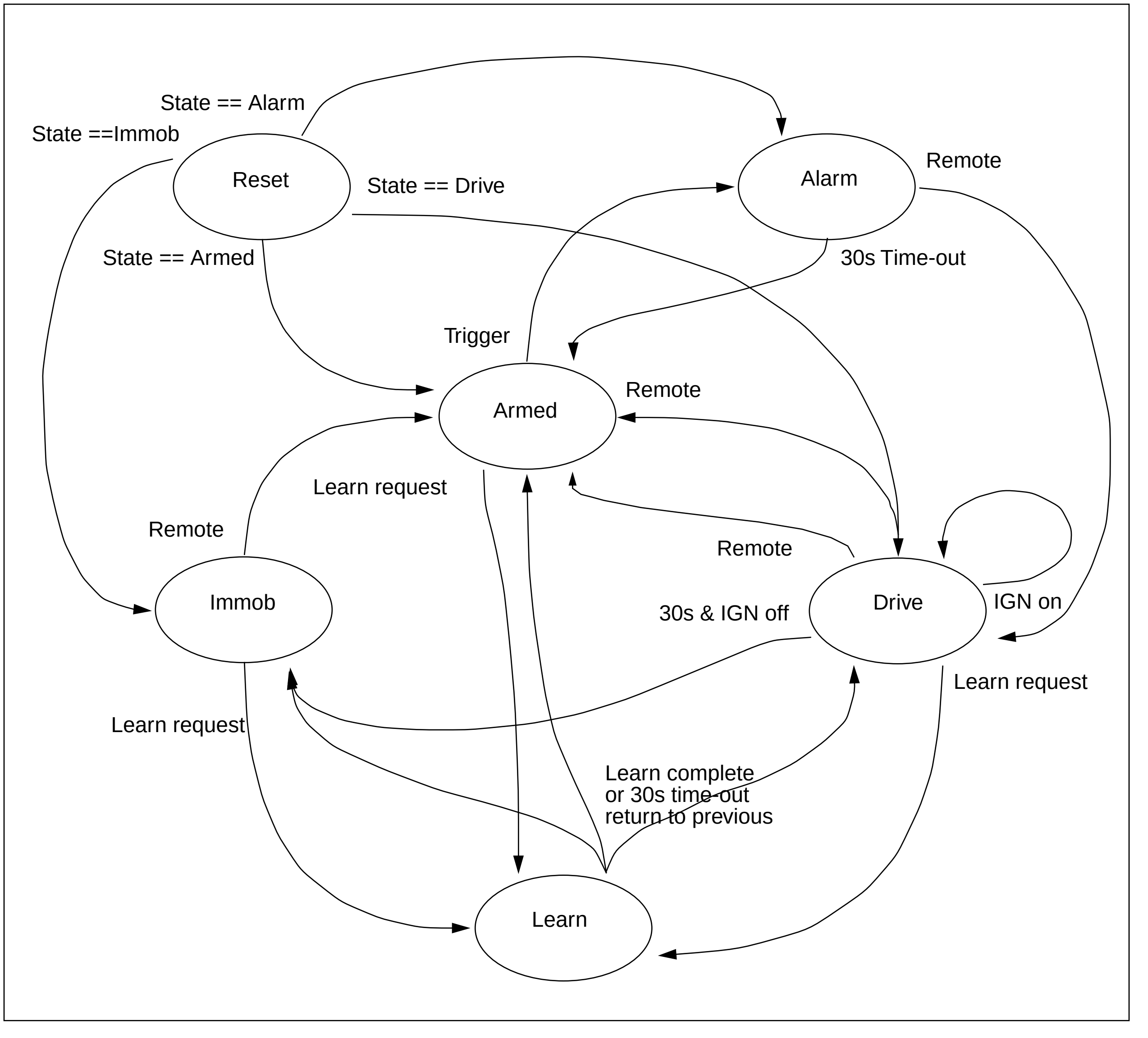
LRN_PTR – Learn indicator points to the next available learn position.

SSTATUS – Stores the system status.

BSTATUS – Backup copy of system status.

TMPCNT – Stores the temporary counter for resynchronization.

FIGURE 1: ALARM STATE DIAGRAM



OPERATION

Reset

Reset initializes the I/O ports, variables, and flags. The system status is read from EEPROM and the status is restored.

Armed

When the system enters armed state, the doors are locked (activate LOCK) and the SIREN and PLIGHT are activated for 50 ms. The LED changes to a slow flash rate. If a trigger is detected (IGN, DOOR or TRIGGER) the system changes to the alarm state.

Actions upon entry:

1. Flash parking lights for 50 ms.
2. Chirp siren for 50 ms.
3. Lock doors for 500 ms.
4. Update system status.
5. LED flash.
6. Disable start.

TABLE 1: STATE CHANGE TABLE

Condition	Next State
IGN high	Alarm
TRIG high	Alarm
DOOR high	Alarm
Panic (any button activated for 2 seconds)	Alarm
Remote function 1	Drive
Remote function 2 (trunk release)	Armed
Remote function 3 (car finder)	Armed
LEARN high	Learn

Alarm

Alarm state is entered whenever a trigger is detected in armed state. SIREN is activated and PLIGHT is turned on and off at a 1 Hz rate. If a remote is detected in this state, the system changes to drive state. After a 30-second delay, SIREN and PLIGHT will be deactivated and the system returned to armed state.

Actions upon entry:

1. Flash parking lights.
2. Siren on.
3. LED flash.
4. Update system status.
5. Disable start.

TABLE 2: STATE CHANGE TABLE

Condition	Next state
Panic (any button activated for 2 seconds)	Alarm
Remote function 1	Drive
Remote function 2 (trunk release)	Armed
30-second timeout	Drive

Drive

When the system enters drive state, the doors are unlocked (activate UNLOCK), and the SIREN and PLIGHT are activated twice for 50 ms.The IMMOB output is activated to enable the starting of the vehicle and LED is turned off. A remote signal will return the system to armed state.

Actions upon entry:

1. Flash parking lights for 50 ms.
2. Chirp siren for 50 ms.
3. Unlock doors for 500 ms.
4. Flash parking lights for 50 ms.
5. Chirp siren for 50 ms.
6. Update system status.
7. LED off.
8. Enable start.

TABLE 3: STATE CHANGE TABLE

Condition	Next State
Panic (any button activated for 2 seconds)	Alarm
Remote function 1 & IGN low	Armed
Remote function 1 & IGN high	Drive
Remote function 2 (trunk release)	Drive
Remote function 3 (car finder)	Drive
30-second timeout & IGN off	Immob
LEARN high	Learn

Immob

If the IGN is turned off for more than 30 seconds, the system will immobilize. The IMMOB output is turned off, and the LED is turned on. A remote signal only will change the state to armed, and a remote signal with the IGN on will return to drive state.

Actions upon entry:

1. Update system status.
2. LED off.
3. Disable start.

TABLE 4: STATE CHANGE TABLE

Condition	Next State
Panic (any button activated for 2 seconds)	Alarm
Remote function 1 & IGN low	Armed
Remote function 1 & IGN high	Drive
Remote function 2 (trunk release)	Immob
Remote function 3 (car finder)	Immob
LEARN high	Learn

Learn

A LEARN input in any state will put the system in learn mode. After learn is completed or timed out the system returns to the previous state.

Actions upon entry:

1. Update system status—set PASS1.
2. LED on.

After first transmission:

1. Update system status—set PASS2.
2. LED off.

After second transmission:

1. Update system status—set NORMAL.
2. LED on for 1 second.
3. Return to previous state.

TABLE 5: STATE CHANGE TABLE

Condition	Next State
Remote first operation	Pass2
Remote second operation	Return to previous state
LEARN high for 8 seconds	Erase all transmitters

FUNCTIONAL MODULES

Reception

The reception routine is based on reliable algorithms used in previous implementations of KEELOQ decoders. Automatic baud rate detection is used to compensate for variations in baud rate from different encoders of a specific type as well as the difference in baud rate between different encoders (HCS200, HCS300, HCS301, HCS360, HCS361, and HCS410). The reception routine will be able to handle 56- and 66-bit transmissions. The reception routine will determine the type of transmission by the number of bits in the transmission. This routine will be the same for all implementations.

Key Generation and Decryption

Decryption is done in software in the implementation. The decryption and key generation algorithms is implemented in software. The manufacturer’s code is stored in program memory and code protected to securely store the key.

Validation

Validation consists of the following steps:

1. Checking the serial number (24 or 28 bits) against the stored transmitters.
2. Comparing the discrimination value (12 bits) against the stored discrimination value.
3. Checking that the synchronization counter falls within the first synchronization window.
4. Checking if the synchronization counter falls within the second synchronization window.
5. If found to be correct, updating the synchronization counter.

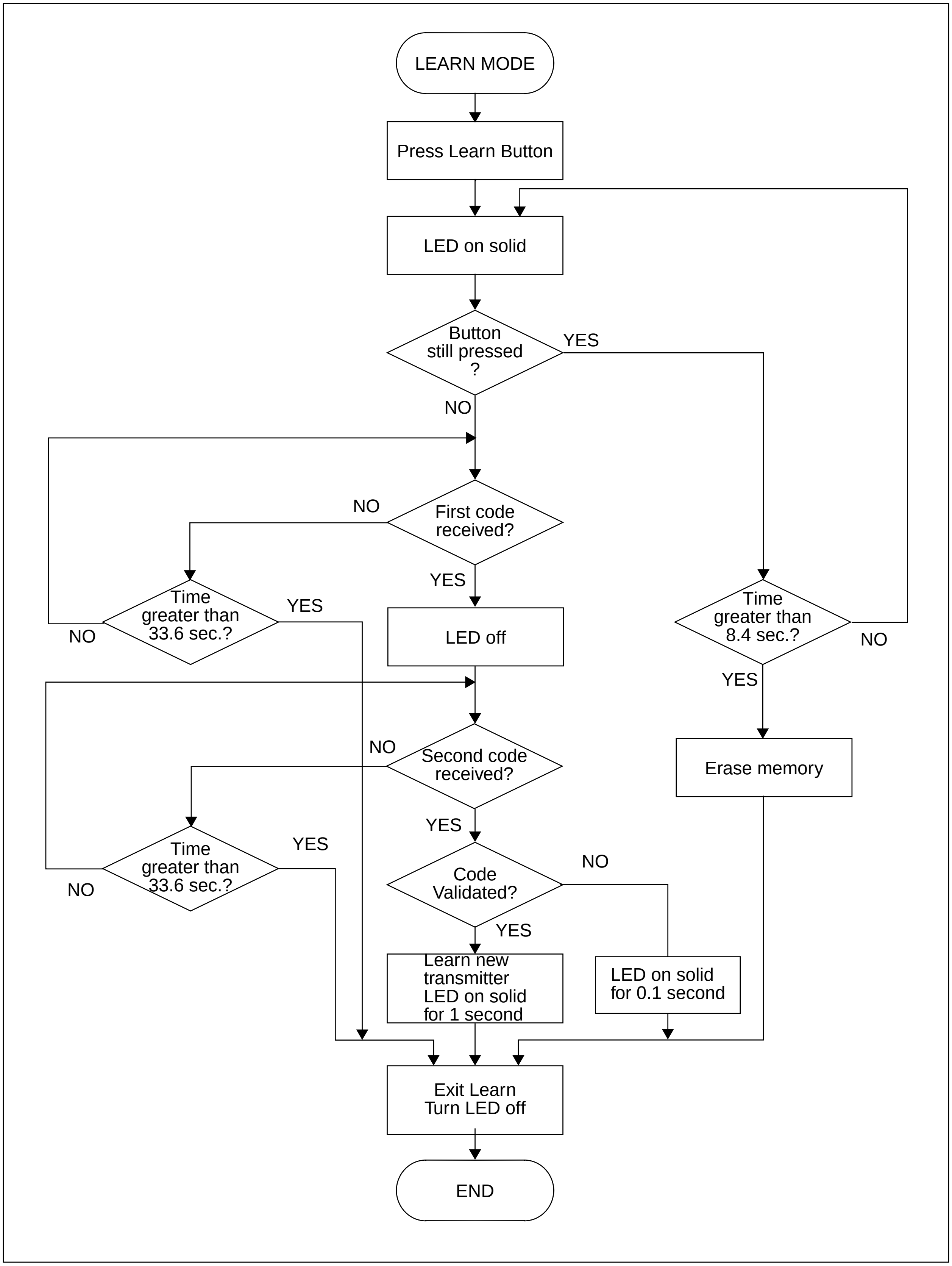
Function Interpretation

Transmitter Button	Function Code	System Function
1	0001	Arm/Disarm
2	0010	Trunk release
3	0011	Car finder
1, 2 or 3 for 2 seconds	00XX	Panic

Learn

The LEARN input is active high. Learning is initiated by momentarily pressing the LEARN button. The decoder uses the current learning position as a scratch pad area. This means that an unsuccessful learn will delete the information stored at that learn position. The learn indicator will not be incremented if the learn was unsuccessful. The flow chart (Figure 1) shows the learning operation.

FIGURE 2: LEARN OPERATION



The following checks will be performed on the received codes to determine if the transmitter is valid:

1. The first code that is received is checked for bit integrity.
2. The stored serial numbers are searched to check if a transmitter is relearned. If a relearn is taking place, that position is used. Otherwise, the position pointed to by the learn indicator will be used.
3. The serial number is stored in the current learn position and used to generate a key.
4. The hop code is decrypted and the result stored temporarily.
5. The serial number of the second code that is received will be compared to the first received serial number.
6. The second hop code is decrypted and the discrimination values compared.
7. The synchronization counters of the decrypted codes will be compared to check that they are sequential codes.
8. If all the checks pass the learn were successful, the learn indicator is incremented. Otherwise, the position is erased.

Operation

1. Press and release the LEARN button. Indicator LED will turn on to indicate learn mode.
2. Press transmitter button. The LED will turn off.
3. Press transmitter a second time. The LED will turn on for 1 second to indicate that the transmitter was learned successfully.
4. Repeat steps 1-3 to learn up to six transmitters. The seventh transmitter will overwrite the first transmitter that was learned.
5. Learn will be terminated if two nonsequential codes were received or if two acceptable codes were not decoded within 33.6 seconds. A valid learn will be indicated by the LED turning on solid for 1 second.
6. Erasing all the transmitters is accomplished by pressing and holding the LEARN button for 8.4 seconds. The LED will turn off at the end of the 8.4 seconds to indicate that the transmitters were erased. The learn indicator will be reset to the first position.

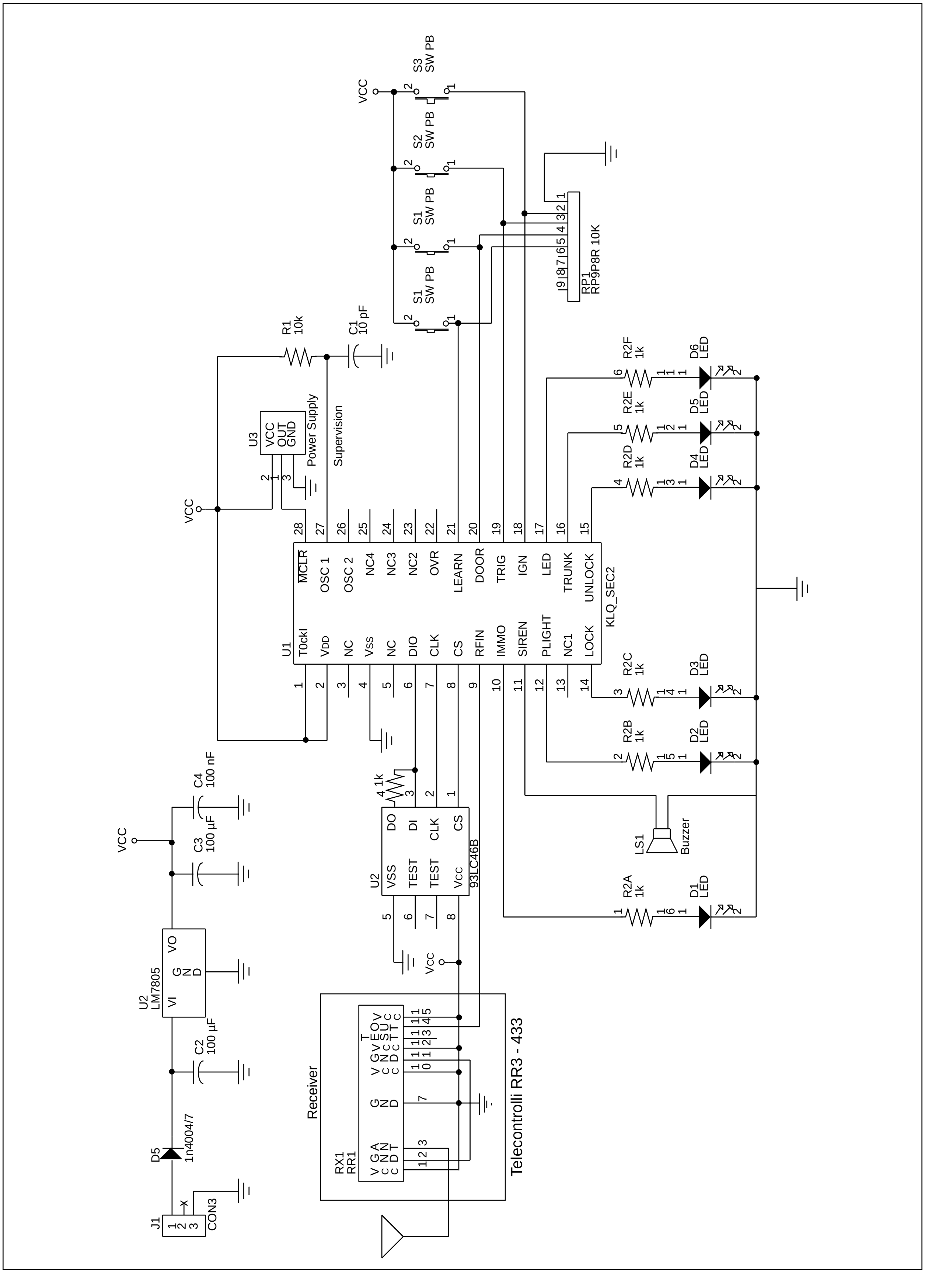
TABLE 6: DEVICE PINOUT

PIN	PIC16C57 Function	Alarm Function	PIN	PIC16C57 Function	Alarm Function
1	RTCC	APP select	28	$\overline{\text{MCLR}}$	RESET
2	VDD	+5V supply	27	Osc In	RC osc (4 MHz)
3	NC		26	Osc Out	
4	GND	Ground	25	Port C Bit 7	NC
5	NC		24	Port C Bit 6	NC
6	Port A Bit 0	EEPROM DIO(3+4)	23	Port C Bit 5	NC
7	Port A Bit 1	EEPROM CLK (2)	22	Port C Bit 4	OVR
8	Port A Bit 2	EEPROM CS (1)	21	Port C Bit 3	LEARN
9	Port A Bit 3	RFIN	20	Port C Bit 2	DOOR
10	Port B Bit 0	IMMOB	19	Port C Bit 1	TRIG
11	Port B Bit 1	SIREN	18	Port C Bit 0	IGN
12	Port B Bit 2	PLIGHT	17	Port B Bit 7	LED
13	Port B Bit 3	NC	16	Port B Bit 6	TRUNK
14	Port B Bit 4	LOCK	15	Port B Bit 5	UNLOCK

TABLE 7: TIMING PARAMETERS

Parameter	Typical	Unit
Armed LED flash rate	1	per second
Siren time-out	33	second
Drive time-out	33	second
Learn time-out	33	second
All erase	8	second
LOCK, UNLOCK, TRUNK activation	500	ms
Siren chirp (arm & disarm)	50	ms
Parking light (arm & disarm)	50	ms
Parking light flash rate (siren)	1	per second
Panic	2	seconds

FIGURE 3: CIRCUIT DIAGRAM



LIST OF CHANGES

Date	Version	Page	Paragraph	Change
08/16/96	1.0			Original
10/20/98	2.0			EEPROM Changed from 93C46 to 93LC46B, adding a series resistor on DIO

NOTES:

Note the following details of the code protection feature on PICmicro® MCUs.

- The PICmicro family meets the specifications contained in the Microchip Data Sheet.
- Microchip believes that its family of PICmicro microcontrollers is one of the most secure products of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the PICmicro microcontroller in a manner outside the operating specifications contained in the data sheet. The person doing so may be engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable”.
- Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our product.

If you have any further questions about this matter, please contact the local sales office nearest to you.

Information contained in this publication regarding device applications and the like is intended through suggestion only and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. No representation or warranty is given and no liability is assumed by Microchip Technology Incorporated with respect to the accuracy or use of such information, or infringement of patents or other intellectual property rights arising from such use or otherwise. Use of Microchip’s products as critical components in life support systems is not authorized except with express written approval by Microchip. No licenses are conveyed, implicitly or otherwise, under any intellectual property rights.

Trademarks

The Microchip name and logo, the Microchip logo, FilterLab, KEELOQ, microID, MPLAB, PIC, PICmicro, PICMASTER, PICSTART, PRO MATE, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

dsPIC, ECONOMONITOR, FanSense, FlexROM, fuzzyLAB, In-Circuit Serial Programming, ICSP, ICEPIC, microPort, Migratable Memory, MPASM, MPLIB, MPLINK, MPSIM, MXDEV, PICC, PICDEM, PICDEM.net, rfPIC, Select Mode and Total Endurance are trademarks of Microchip Technology Incorporated in the U.S.A.

Serialized Quick Turn Programming (SQTP) is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

Printed on recycled paper.

DNV Certification, Inc.
USA

ANSI★RAB
QMS
ACCREDITED

DNV

DNV MSC
The Netherlands
Accredited by the RvA

ISO 9001 / QS-9000
REGISTERED FIRM

Microchip received QS-9000 quality system certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona in July 1999. The Company’s quality system processes and procedures are QS-9000 compliant for its PICmicro® 8-bit MCUs, KEELOQ® code hopping devices, Serial EEPROMs and microperipheral products. In addition, Microchip’s quality system for the design and manufacture of development systems is ISO 9001 certified.

MICROCHIP

WORLDWIDE SALES AND SERVICE

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200 Fax: 480-792-7277
Technical Support: 480-792-7627
Web Address: http://www.microchip.com

Rocky Mountain
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7966 Fax: 480-792-7456

Atlanta
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770-640-0034 Fax: 770-640-0307

Boston
2 Lan Drive, Suite 120
Westford, MA 01886
Tel: 978-692-3848 Fax: 978-692-3821

Chicago
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

Dallas
4570 Westgrove Drive, Suite 160
Addison, TX 75001
Tel: 972-818-7423 Fax: 972-818-2924

Detroit
Tri-Atria Office Building
32255 Northwestern Highway, Suite 190
Farmington Hills, MI 48334
Tel: 248-538-2250 Fax: 248-538-2260

Kokomo
2767 S. Albright Road
Kokomo, Indiana 46902
Tel: 765-864-8360 Fax: 765-864-8387

Los Angeles
18201 Von Karman, Suite 1090
Irvine, CA 92612
Tel: 949-263-1888 Fax: 949-263-1338

New York
150 Motor Parkway, Suite 202
Hauppauge, NY 11788
Tel: 631-273-5305 Fax: 631-273-5335

San Jose
Microchip Technology Inc.
2107 North First Street, Suite 590
San Jose, CA 95131
Tel: 408-436-7950 Fax: 408-436-7955

Toronto
6285 Northam Drive, Suite 108
Mississauga, Ontario L4V 1X5, Canada
Tel: 905-673-0699 Fax: 905-673-6509

ASIA/PACIFIC

Australia
Microchip Technology Australia Pty Ltd
Suite 22, 41 Rawson Street
Epping 2121, NSW
Australia
Tel: 61-2-9868-6733 Fax: 61-2-9868-6755

China - Beijing
Microchip Technology Consulting (Shanghai)
Co., Ltd., Beijing Liaison Office
Unit 915
Bei Hai Wan Tai Bldg.
No. 6 Chaoyangmen Beidajie
Beijing, 100027, No. China
Tel: 86-10-85282100 Fax: 86-10-85282104

China - Chengdu
Microchip Technology Consulting (Shanghai)
Co., Ltd., Chengdu Liaison Office
Rm. 2401, 24th Floor,
Ming Xing Financial Tower
No. 88 TIDU Street
Chengdu 610016, China
Tel: 86-28-6766200 Fax: 86-28-6766599

China - Fuzhou
Microchip Technology Consulting (Shanghai)
Co., Ltd., Fuzhou Liaison Office
Unit 28F, World Trade Plaza
No. 71 Wusi Road
Fuzhou 350001, China
Tel: 86-591-7503506 Fax: 86-591-7503521

China - Shanghai
Microchip Technology Consulting (Shanghai)
Co., Ltd.
Room 701, Bldg. B
Far East International Plaza
No. 317 Xian Xia Road
Shanghai, 200051
Tel: 86-21-6275-5700 Fax: 86-21-6275-5060

China - Shenzhen
Microchip Technology Consulting (Shanghai)
Co., Ltd., Shenzhen Liaison Office
Rm. 1315, 13/F, Shenzhen Kerry Centre,
Renminnan Lu
Shenzhen 518001, China
Tel: 86-755-2350361 Fax: 86-755-2366086

Hong Kong
Microchip Technology Hongkong Ltd.
Unit 901-6, Tower 2, Metroplaza
223 Hing Fong Road
Kwai Fong, N.T., Hong Kong
Tel: 852-2401-1200 Fax: 852-2401-3431

India
Microchip Technology Inc.
India Liaison Office
Divyasree Chambers
1 Floor, Wing A (A3/A4)
No. 11, O'Shaugnessey Road
Bangalore, 560 025, India
Tel: 91-80-2290061 Fax: 91-80-2290062

Japan
Microchip Technology Japan K.K.
Benex S-1 6F
3-18-20, Shinyokohama
Kohoku-Ku, Yokohama-shi
Kanagawa, 222-0033, Japan
Tel: 81-45-471- 6166 Fax: 81-45-471-6122

Korea
Microchip Technology Korea
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku
Seoul, Korea 135-882
Tel: 82-2-554-7200 Fax: 82-2-558-5934

Singapore
Microchip Technology Singapore Pte Ltd.
200 Middle Road
#07-02 Prime Centre
Singapore, 188980
Tel: 65-334-8870 Fax: 65-334-8850

Taiwan
Microchip Technology Taiwan
11F-3, No. 207
Tung Hua North Road
Taipei, 105, Taiwan
Tel: 886-2-2717-7175 Fax: 886-2-2545-0139

EUROPE

Denmark
Microchip Technology Nordic ApS
Regus Business Centre
Lautrup hoj 1-3
Ballerup DK-2750 Denmark
Tel: 45 4420 9895 Fax: 45 4420 9910

France
Microchip Technology SARL
Parc d'Activite du Moulin de Massy
43 Rue du Saule Trapu
Batiment A - ler Etage
91300 Massy, France
Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany
Microchip Technology GmbH
Gustav-Heinemann Ring 125
D-81739 Munich, Germany
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

Italy
Microchip Technology SRL
Centro Direzionale Colleoni
Palazzo Taurus 1 V. Le Colleoni 1
20041 Agrate Brianza
Milan, Italy
Tel: 39-039-65791-1 Fax: 39-039-6899883

United Kingdom
Arizona Microchip Technology Ltd.
505 Eskdale Road
Winnersh Triangle
Wokingham
Berkshire, England RG41 5TU
Tel: 44 118 921 5869 Fax: 44-118 921-5820

01/18/02