AN645

PIC16C57 Based Code Hopping Security System

Author: Kobus Marneweck
Secure Data Products

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 PIC16/17 microcontroller for more I/O or code space.

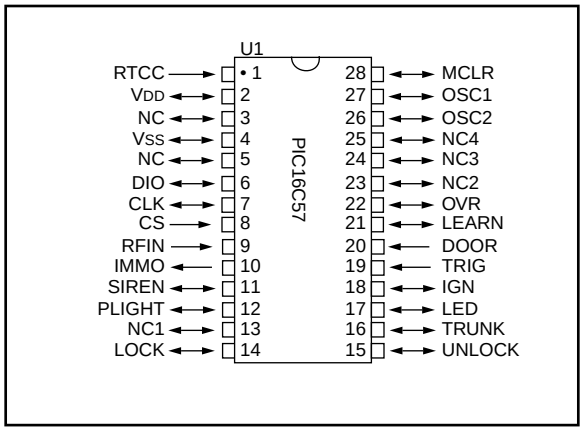
FEATURES

- 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

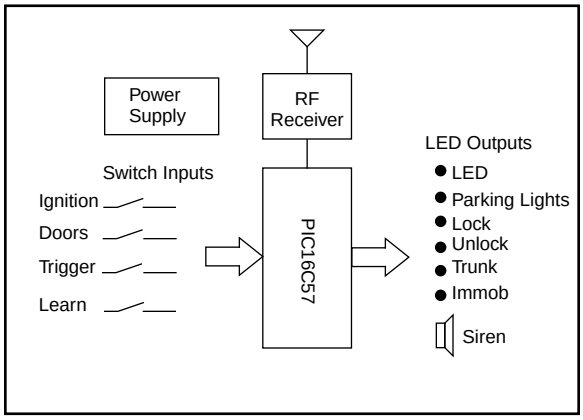
RECOMMENDED READING

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 BBS, 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.

PINOUTS



BLOCK DIAGRAM



MEMORY MAP EEPROM (16 BIT WORDS)

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

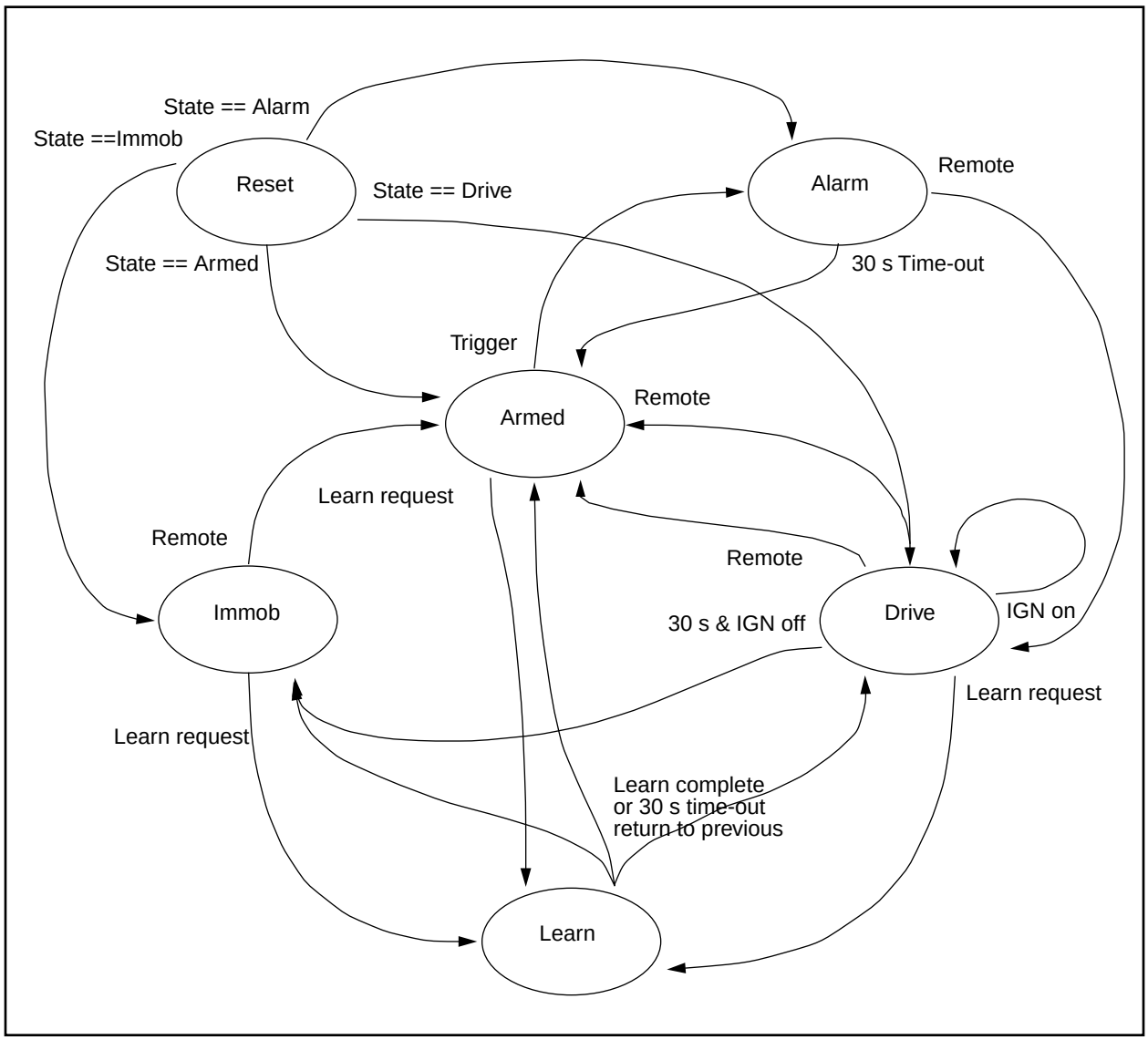
LRN_PTR – Learn pointer points to the next available learn position.

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—et 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 NTQ106). 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 key 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.

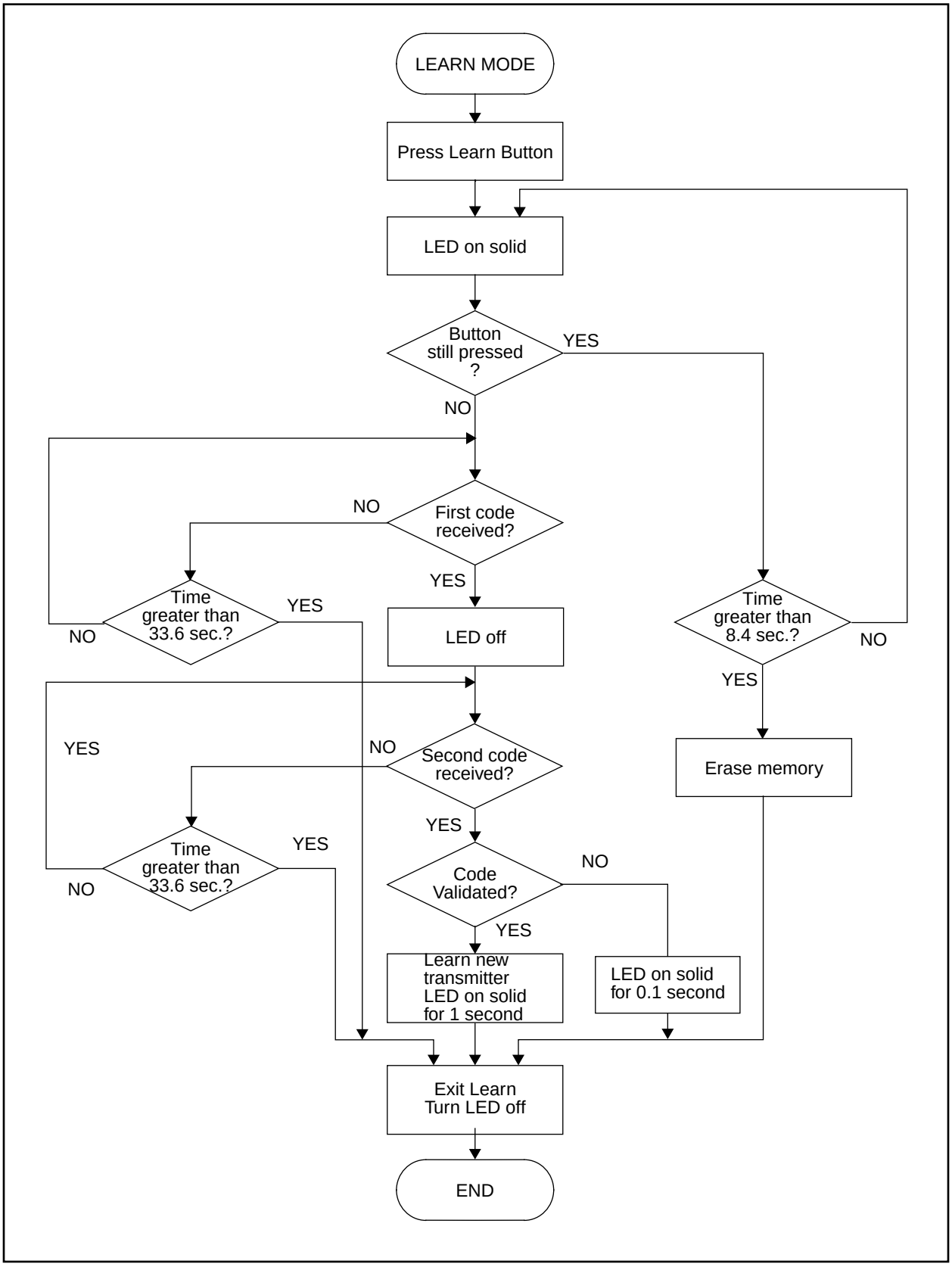
Function Interpretation

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 pointer 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 pointer 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 pointer 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 pointer 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	V_{DD}	+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

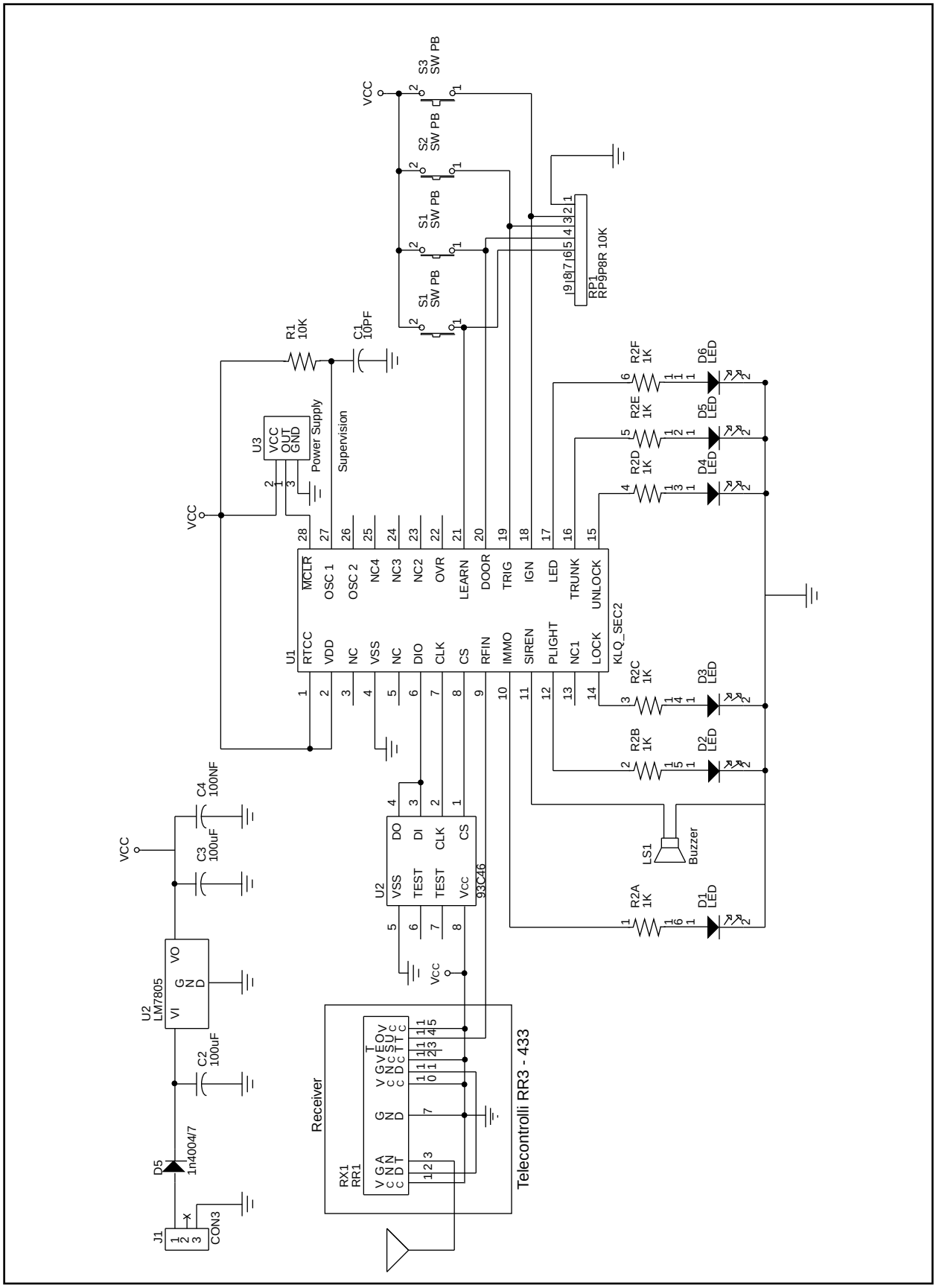
KEELOQ LITERATURE

The following literature is available from Microchip's field application engineers, directly from Microchip, and on both the Microchip BBS and Web site unless otherwise specified.

Document Number	Description	Notes
DS91002	Introduction to KEELOQ	
DS1044	HCS300 Evaluation Kit User's Guide	
DS91000	Secure Learning RKE Systems Using KEELOQ Encoders	
DS00642	Code Hopping Decoder Using a PIC16C56	Note
DS00652	Secure Learn Code Hopping Decoder Using a PIC16C56	Note
DS00645	PIC16C57 Based Code Hopping Security System	Note
DS40138	HCS200 Data Sheet	
DS21137	HCS300 Data Sheet	
DS21143	HCS301 Data Sheet	
DS40152	HCS360 Data Sheet	
DS40146	HCS361 Data Sheet	
DS40147	HCS509 Data Sheet	
DS40151	HCS512 Data Sheet	
DS50136	Programming Station User's Guide	
DS00644	Converting NTQ105/106 Designs to HCS200/300s	

Note: The complete document includes software and is available on diskette. The diskette can be ordered by ordering DS40149.

FIGURE 3: CIRCUIT DIAGRAM



LIST OF CHANGES

Date	Version	Page	Paragraph	Change
08/16/96	1.0			Original

WORLDWIDE SALES & SERVICE

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 602 786-7200 Fax: 602 786-7277
Technical Support: 602 786-7627
Web: http://www.microchip.com

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

Boston
Microchip Technology Inc.
5 Mount Royal Avenue
Marlborough, MA 01752
Tel: 508 480-9990Fax: 508 480-8575

Chicago
Microchip Technology Inc.
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 708 285-0071 Fax: 708 285-0075

Dallas
Microchip Technology Inc.
14651 Dallas Parkway, Suite 816
Dallas, TX 75240-8809
Tel: 214 991-7177 Fax: 214 991-8588

Dayton
Microchip Technology Inc.
Suite 150
Two Prestige Place
Miamisburg, OH 45342
Tel: 513 291-1654 Fax: 513 291-9175

Los Angeles
Microchip Technology Inc.
18201 Von Karman, Suite 1090
Irvine, CA 92612
Tel: 714 263-1888 Fax: 714 263-1338

New York
Microchip Technmgy Inc.
150 Motor Parkway, Suite 416
Hauppauge, NY 11788
Tel: 516 273-5305 Fax: 516 273-5335

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

Toronto
Microchip Technology Inc.
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, Canada
Tel: 905 405-6279 Fax: 905 405-6253

ASIA/PACIFIC

Hong Kong
Microchip Technology
RM 3801B, Tower Two
Metroplaza
223 Hing Fong Road
Kwai Fong, N.T. Hong Kong
Tel: 852 2 401 1200 Fax: 852 2 401 3431

India
Microchip Technology
No. 6, Legacy, Convent Road
Bangalore 560 025 India
Tel: 91 80 526 3148 Fax: 91 80 559 9840

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

Singapore
Microchip Technology
200 Middle Road
#10-03 Prime Centre
Singapore 188980
Tel: 65 334 8870 Fax: 65 334 8850

Shanghai
Microchip Technology
Unit 406 of Shanghai Golden Bridge Bldg.
2077 Yan'an Road West, Hongiao District
Shanghai, Peoples Republic of China
Tel: 86 21 6275 5700
Fax: 011 86 21 6275 5060

Taiwan
Microchip Technology
10F-1C 207
Tung Hua North Road
Taipei, Taiwan, ROC
Tel: 886 2 717 7175 Fax: 886 2 545 0139

EUROPE

United Kingdom
Arizona Microchip Technology Ltd.
Unit 6, The Courtyard
Meadow Bank, Furlong Road
Bourne End, Buckinghamshire SL8 5AJ
Tel: 44 1628 850303 Fax: 44 1628 850178

France
Arizona Microchip Technology SARL
Zone Industrielle de la Bonde
2 Rue du Buisson aux Fraises
91300 Massy - France
Tel: 33 1 69 53 63 20 Fax: 33 1 69 30 90 79

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

Italy
Arizona Microchip Technology SRL
Centro Direzionale Colleone Pas Taurus 1
Viale Colleoni 1
20041 Agrate Brianza
Milan Italy
Tel: 39 39 6899939 Fax: 39 39 689 9883

JAPAN

Microchip Technology Intl. Inc.
Benex S-1 6F
3-18-20, Shin Yokohama
Kohoku-Ku, Yokohama
Kanagawa 222 Japan
Tel: 81 45 471 6166 Fax: 81 45 471 6122

8/13/96

MICROCHIP

Printed on recycled paper.