AN663

KEELOQ Simple Code Hopping Decoder

Author: *Steven Dawson*
Microchip Technology Inc.

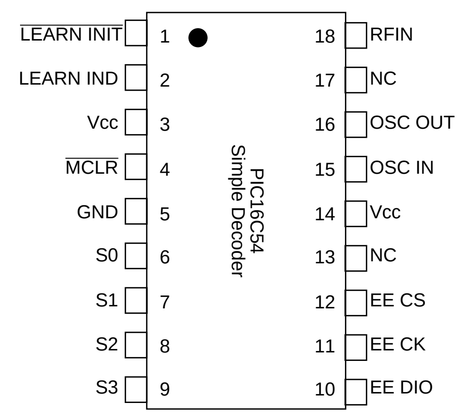
OVERVIEW

This application note fully describes the working of a code hopping decoder implemented on a Microchip PIC16C54 microcontroller. The PIC16C54 is smaller than the PIC16C56 used in the normal decoder (AN642) or the secure learn decoder (AN652). A simplified learning scheme with all encoders sharing a common key and a simplified counter synchronization scheme has been used to reduce the code space requirements. The use of a common key reduces the security of the system. The simple decoder can learn up to 15 encoders. This application note describes the various KEELOQ® code hopping encoders that can be used with the decoder, the decoder hardware, and the various software modules comprising the system. The software can be used to implement a stand alone decoder or integrated with full function security systems. The decoder supports the Microchip HCS200, HCS300, HCS301, HCS360, HCS361 and HCS410 KEELOQ Code Hopping Encoders.

KEY FEATURES

- PIC16C54
- Stand alone decoder
- Compatible with Microchip HCS200, HCS300, HCS301, HCS360, HCS361 and HCS410 encoders
- Automatic bit rate detection
- Automatic encoder type detection
- Four function outputs
- Up to 15 learnable transmitters
- RC Oscillator
- Single press learn

FIGURE 1: PIC16C54 DECODER



Notice:

This is a non-restricted version of Application Note AN659 which is available under the KEELOQ License Agreement. The license agreement can be ordered from the Microchip Literature Center as DS40149.

INTRODUCTION TO KEELOQ ENCODERS

All KEELOQ encoders use the KEELOQ code hopping technology to make each transmission by an encoder unique. The encoder transmissions have two parts. The first part changes each time the encoder is activated and is called the hopping code part and is encrypted. The second part is the unencrypted part of the transmission, principally containing the encoder's serial number identifying it to a decoder. Refer to DS91002, Introduction to KEELOQ.

Hopping Code

The hopping code contains function information, a discrimination value, and a synchronization counter. This information is encrypted by an encryption algorithm before being transmitted. A 64-bit encryption key is used by the encryption algorithm. If one bit in the data that is encrypted changes, the result is that an average of half the bits in the output will change. As a result, the hopping code changes dramatically for each transmission and can not be predicted.

Function Information

The encoder transmits up to four bits of function information. Up to 15 different functions are available.

Discrimination Value

Stored in the encoder EEPROM, this information can be used to check integrity of decryption operation by a decoder. If known information is inserted into the transmitted string before encryption, the same information can be used at the decoder to check whether the information has been decrypted correctly. In the Microchip HCS encoders, up to 12 bits (including overflow bits) are available.

Synchronization Counters

The transmitted word contains a 16-bit synchronization counter. The synchronization information is used at the decoder to determine whether a transmission is valid or is a repetition of a previous transmission. Previous codes are rejected to safeguard against code grabbers. The HCS300 and HCS301 encoders transmit two overflow bits which may be used to extend the range of the synchronization counter from 65,536 to 196,608 button operations. The HCS360 and HCS361 encoders transmit one overflow bit which can be used to extend the range of the synchronization counter from 65,536 to 131,071 button operations.

Unencrypted Code

Serial Number

The encoder's serial number is transmitted every time the button is pressed. The serial number is transmitted unencrypted as part of the transmission and serves to identify the encoder to the decoder.

Other Status and Function Information

The HCS200, HCS300, and HCS301 encoders include provision for four bits of function information and two status bits in the fixed code portion of its transmission. The two status bits indicate whether a repeated transmission is being sent, and whether the battery voltage is low. The HCS200 does not send repeated transmission information, and the bit is permanently set to '0'.

The HCS360/361 and HCS410 encoders transmit two bits that are used as a Cyclic Redundancy check. These bits can be used to check the integrity of the reception. Additionally, the HCS360, HCS361 and HCS410 encoders can extend the length of the serial number from 28 bits to 32 bits, replacing the unencrypted function code. The HCS410 also transmits 2 queuing bits that can be used to detect multiple presses of the same button combination.

Transmission Format Summary

Table 1 contains a summary of the information contained in transmissions from each of the KEELOQ encoders that can be learned by the Microchip decoder.

FIGURE 2: DECODER BLOCK DIAGRAM

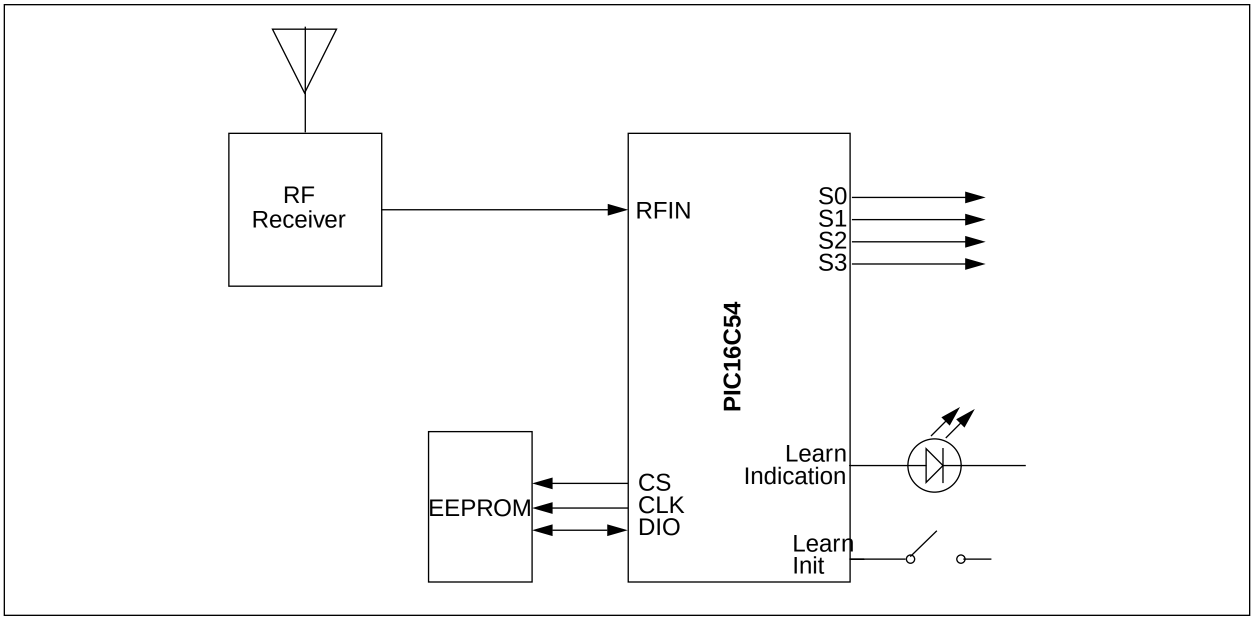


TABLE 1: KEELOQ ENCODER TRANSMISSION SUMMARY

	HCS200/201 # of bits	**HCS300/301** # of bits	**HCS360/361** # of bits	**HCS410** # of bits
Total Transmission Length	66	66	67	69
Code Hopping Portion	32	32	32	32
Sync Counter	16	16	16	16
Discrimination bits	12	10	8	10
User Bits	0	0	2	0
Overflow Bits	0	2	1	2
Independent Mode	0	0	1	0
Function Code	4	4	4	4
Fixed Portion	34	34	35	37
Serial number	28	28	28/32	28/32
Function Code	4	4	4/0	4/0
Low Voltage Indicator	1	1	1	1
Repeat Bit	1	1	0	0
CRC	0	0	2	2
Queue Bits	0	0	0	2

TABLE 2: HCS200/201 AND HCS300/301 CODE HOPPING TRANSMISSION FORMAT

Code Hopping Portion			Fixed Portion		
Sync Counter	Discrimination	Func	Serial Number	Fund	VLOW REPT

TABLE 3: HCS200/201 AND HCS300/301 SEED TRANSMISSION FORMAT

Seed Portion	Fixed Portion		
Seed	Serial Number	Func	VLOW REPT

TABLE 4: HCS360/361 CODE HOPPING TRANSMISSION FORMAT

Code Hopping Portion			Fixed Portion		
Sync Counter	Discrimination OVR, IND	Func	Serial Number (28/32 bits)	Func (4/0 bits)	VLOW REPT

TABLE 5: HCS360/361 SEED TRANSMISSION FORMAT

Seed Portion	Fixed Portion		
Seed (48 bits)	Serial Number (12/16 MS bits)	Func (4/0 bits)	VLOW REPT

TABLE 6: HCS410 CODE HOPPING TRANSMISSION FORMAT

Code Hopping Portion			Fixed Portion		
Sync Counter	Discrimination OVR	Func	Serial Number (28/32 bits)	Func (4/0 bits)	VLOW CRC QUE

TABLE 7: HCS410 SEED TRANSMISSION FORMAT

Seed Portion	Fixed Portion	
Seed (60 bits)	Func (4/0 bits)	VLOW CRC QUE

PWM Format

In general, all KEELOQ encoders share a common transmission format:

A **preamble** to improve biasing of decision thresholds in super-regenerative receivers. The preamble consists of alternate on and off periods, each lasting as long as a single elemental period.

A **calibration** header consisting of a low period of 10 elemental periods. Calibration actions should be performed on the low period of the header to ensure correct operation with header chopping.

A **string** of pulse-width modulated bits, each consisting of three elements. The first element is high, the second contains the data transmitted and is either high or low, the third element is always low.

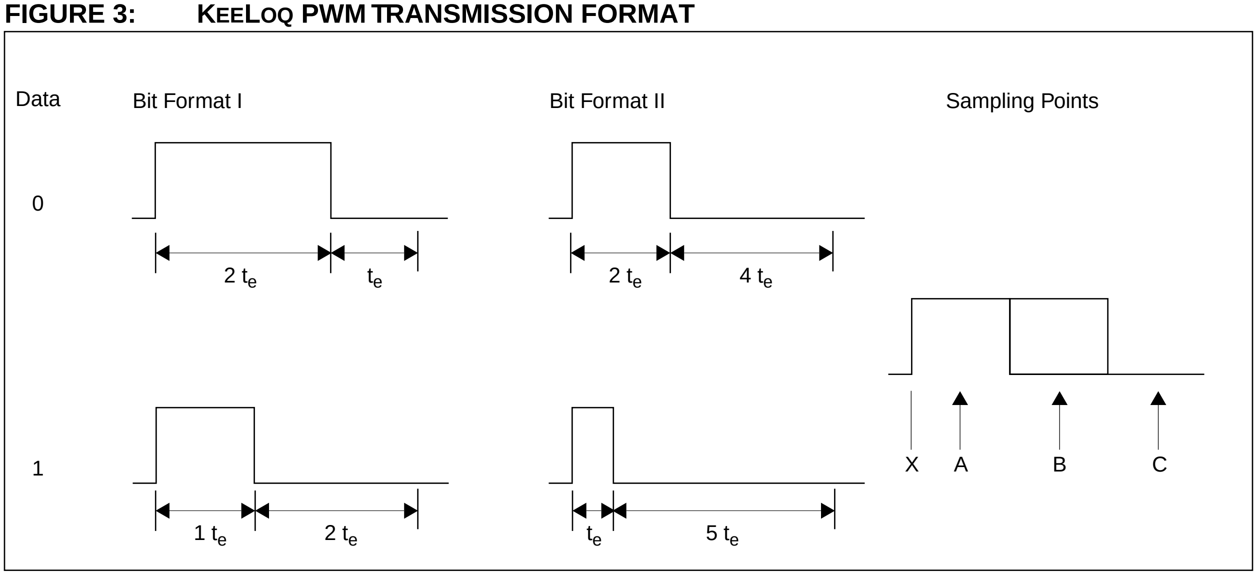
A **guard** period is usually left between the transmissions. During this period nothing is transmitted by the encoder.

Figure 3 shows the sampling points when sampling the data bits. The first and last elements are used exclusively to verify the integrity of the received symbol. The first element (sample point A) is always high, the second (sample point B) is the complement of the data bit being sent, and the final element (sample point C) is always low. Because the period between the low portion of a bit (sample point C) and the rising edge of the following bit (sample point X) can vary, the rising edge of the first element (sample point X) is used to resynchronize the receiving routine to each incoming bit.

If random noise is being received, the probability of a set of three samples producing a valid combination is only $2^{-2} = 1/4$. For a string of 66 bits, the corresponding figure is 2^{-134}.

Integrity checking on incoming signals is important. Code hopping signals require significant processing, as well as EEPROM access, to decrypt. Unnecessary processing can be avoided by not attempting to decrypt incoming codes that have bit errors.

FIGURE 3: KEELOQ PWM TRANSMISSION FORMAT



Microwire is registered trademark of Motorola.

DECODER IMPLEMENTATION

The decoder is implemented on a PIC16C54 RISC microcontroller and a 93LC46B EEPROM as shown in the decoder schematic in Figure 9. However, this solution can be implemented in any PICmicro® microcontroller with at least 500 words of program memory. The operating frequency of the controller is 4 MHz. The microcontroller is used to capture transmissions from the various encoders, decrypt transmissions captured, and check the validity of the transmission based on the information in the decrypted transmission and information stored in the EEPROM. If a transmission from a valid encoder is received, the decoder activates the outputs dictated by the transmission.

Encoder information, such as serial number and synchronization information is stored externally in an EEPROM. The EEPROM used is a Microchip 93LC46B Microwire® Serial EEPROM. The information stored in the EEPROM is encrypted to protect the contents. The EEPROM encryption is less secure than the KEELOQ code hopping algorithm.

As can be seen from the section on encoder transmissions there are differences in the transmission formats of the different encoders that can be used with the decoder. The following section summarizes how the differences in transmitted data are dealt with by the decoder.

As the serial number information follows after the code hopping portion of the transmission, any number of serial number bits can be received and processed. In the Microchip decoder described, the complete serial number (28 bits) is stored.

After matching the received and stored serial number, validation of a received transmission consists of two steps. The first includes checking the integrity of the decryption operation. Here the decoder compares the least significant 8-bits of the discrimination value received with the least significant 8-bits of the serial number. The discrimination value stored with the HCS300/301/360/361 includes overflow bits and user bits.

The second portion of validation involves checking synchronization information for that particular encoder. The synchronization counter transmitted by all encoders is 16 bits long. Two copies of the full synchronization counter are stored for all valid encoders. The storing of two copies of the synchronization information protects the decoder from loosing synchronization with an encoder if one of the counters is corrupted.

TABLE 8: MICROCHIP DECODER FUNCTIONAL INPUTS AND OUTPUTS

Mnemonic	Pin Number	Input / Output	Function
RF IN	18	I	Demodulated PWM signal from RF receiver. The decoder uses this input to receive encoder transmissions.
$\overline{\text{LEARN INIT}}$	1	I	Input to initiate learning, active low.
LEARN IND	2	O	Output to show the status of the learn process (in an integrated system this will be combined with the system status indicator).
S0, S1, S2, S3	6, 7, 8, 9	O	Function outputs—corresponds to encoder input pins.

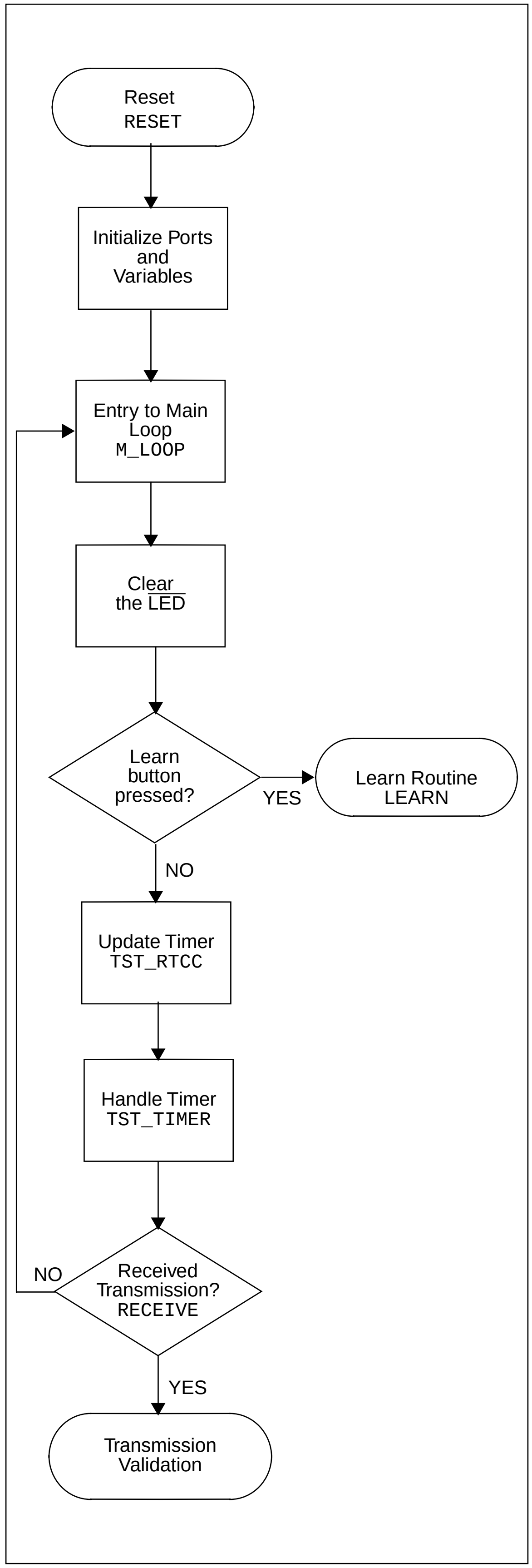
PROGRAM FLOW

The software for the Microchip decoder has been written for the PIC16C54 microcontroller. The compiler used is MPASM version 01.30.01. The operating frequency of the PIC16C54 is 4 MHz. The clock speed should be kept as close as possible to 4 MHz as the reception routine (`RECEIVE`) is dependent on the 4 MHz clock for correct functioning. Other decoder functions that rely on a 4 MHz clock speed are the hold times of the various outputs and time-outs. The main program flow is described here. Detailed descriptions of individual functions can be found further in the application note.

After startup, the encoder enters the main loop where it spends most of its time. The main loop checks to see if the learn button is being activated. If so, the decoder enters the learn mode described in the “Learn” in AN659.

If learn has not been initiated, the microcontroller checks for transmissions from encoders (`RECEIVE`). If a transmission from an encoder has successfully been received, the microcontroller validates the transmission received as described in the “Transmission Validation” section in AN659. If the transmission received is a valid transmission from an encoder learned into the system, the system sets the appropriate outputs (`M_OUTPUT`).

FIGURE 4: MICROCHIP DECODER MAIN PROGRAM FLOW



FUNCTIONAL MODULES

Reception

The reception routine (RECEIVE) is based on a reliable algorithm which has successfully been used in previous implementations of KEELOQ decoders. Automatic bit rate detection is used to compensate for variations in bit rate of different encoders of a specific type, as well as the differences in bit rate between different encoders (HCS200, HCS300, and HCS360). The reception routine is able to receive 64-bit transmissions. This can easily be extended to receive more bits. The decoder only uses the first 60 bits received. The remaining bits are ignored.

The reception algorithm performs a number of functions when an output is detected from the receiver. Figure 5 gives all the major sampling points in the reception algorithm.

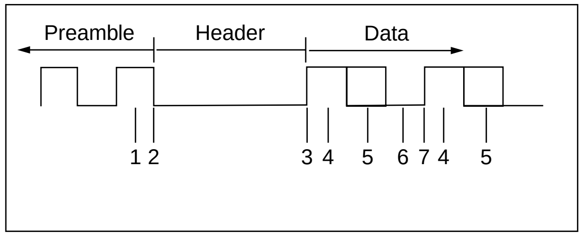
The reception algorithm calibrates on the low period of the header to determine the actual elemental period for the transmission being received. The required elemental period is 10% of the low header period. In Figure 5 the header calibration sample points are marked 1 through 3. The calibration flow chart (Figure 6) shows at what points in the program samples 1, 2, and 3 are taken.

Elemental periods outside the capture range of the algorithm (either too long or too short) are rejected, since they are due either to noise or to reception of an incomplete signal.

Using the determined elemental period, three samples after the first rising edge (sample 3) following the header are taken. The first sample is taken half an elemental period after the rising edge (Sample 4); the second, one elemental period later (Sample 5), and the third, another one elemental period later (Sample 6). The first sample must be high, the second could be either high or low, and the third sample must be low. If either the first or the third sample is not as expected, the attempt at capturing a transmission is abandoned. In Figure 5, the data sample points are points 4 through 6. The flow chart describing data reception (Figure 7) shows where in the code the samples are taken.

If all 64 bits have been captured, each with the correct first and third elements, the transmission can be assumed to be correct, and decryption can commence. The receiving routine should be called often enough to ensure that the high portion in the header is not missed (Sample 1, Figure 5).

FIGURE 5: SAMPLING POINTS USED IN RECEIVE ALGORITHM



In systems where the reception routine is called to check if there is activity on the receiver input, the routine should poll the input for a valid transmission for at least the time taken to complete one transmission if activity is detected on the input line. This makes provision for the reception routine being called while a transmission is in progress. Having missed the first header, the first transmission will be invalid and be discarded. The decoder should continue sampling the input through the guard time in order to catch the next header and transmission (i.e., for a decoder designed to capture HCS300 transmissions the time spent polling for a valid transmission should be at least 100 ms if activity is detected in the input line).

Reception Algorithm Flow Chart

The flow chart in Figure 6 describes the calibration routine which is used to determine the actual transmission rate of the encoder so that the decoder can compensate for deviations from nominal timing. There are four different exit points, each of which should branch to a point in the program where housekeeping and input monitoring can be resumed. There is only one exit point for a valid calibration operation (RCV7). At this point, it is assumed that a valid header has been received and that a string of data bits will follow.

The second flow chart (Figure 7) handles the reception of bits once the calibration routine has been successfully completed. The data bits are all sampled three times each to ensure that a noise free transmission has been received. The reception routine uses the calibrated elemental period, determined in the calibration routine, to ensure that the samples are correctly spaced. The routine resynchronizes itself on the rising flank of each bit. Only 60 bits of the data received are used by the decoder described, the decoder ignores the unencrypted function code and the status bits.

If the control samples in a given bit are sampled correctly (i.e., the first element is high and the last element is low), the routine checks whether 66 bits have been received correctly. If not, the routine returns to the calling procedure.

FIGURE 6: CALIBRATION FLOW CHART

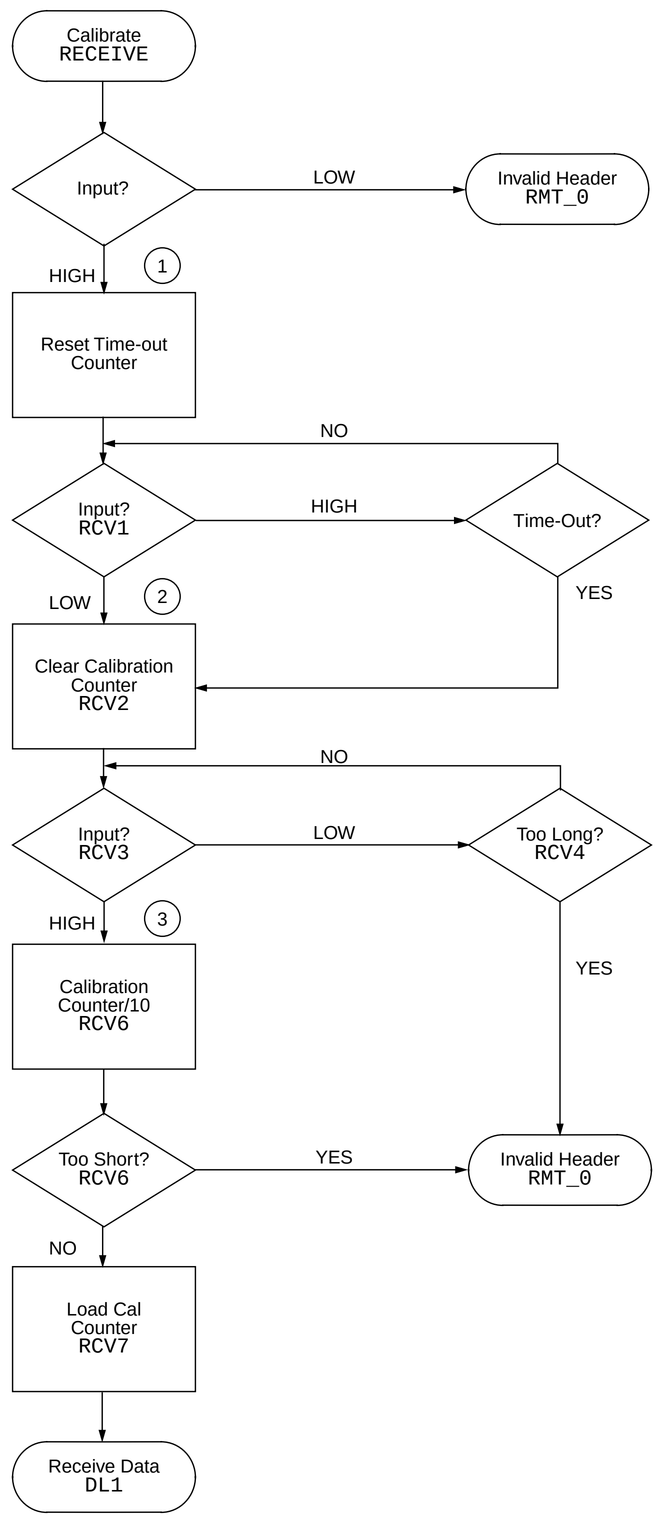
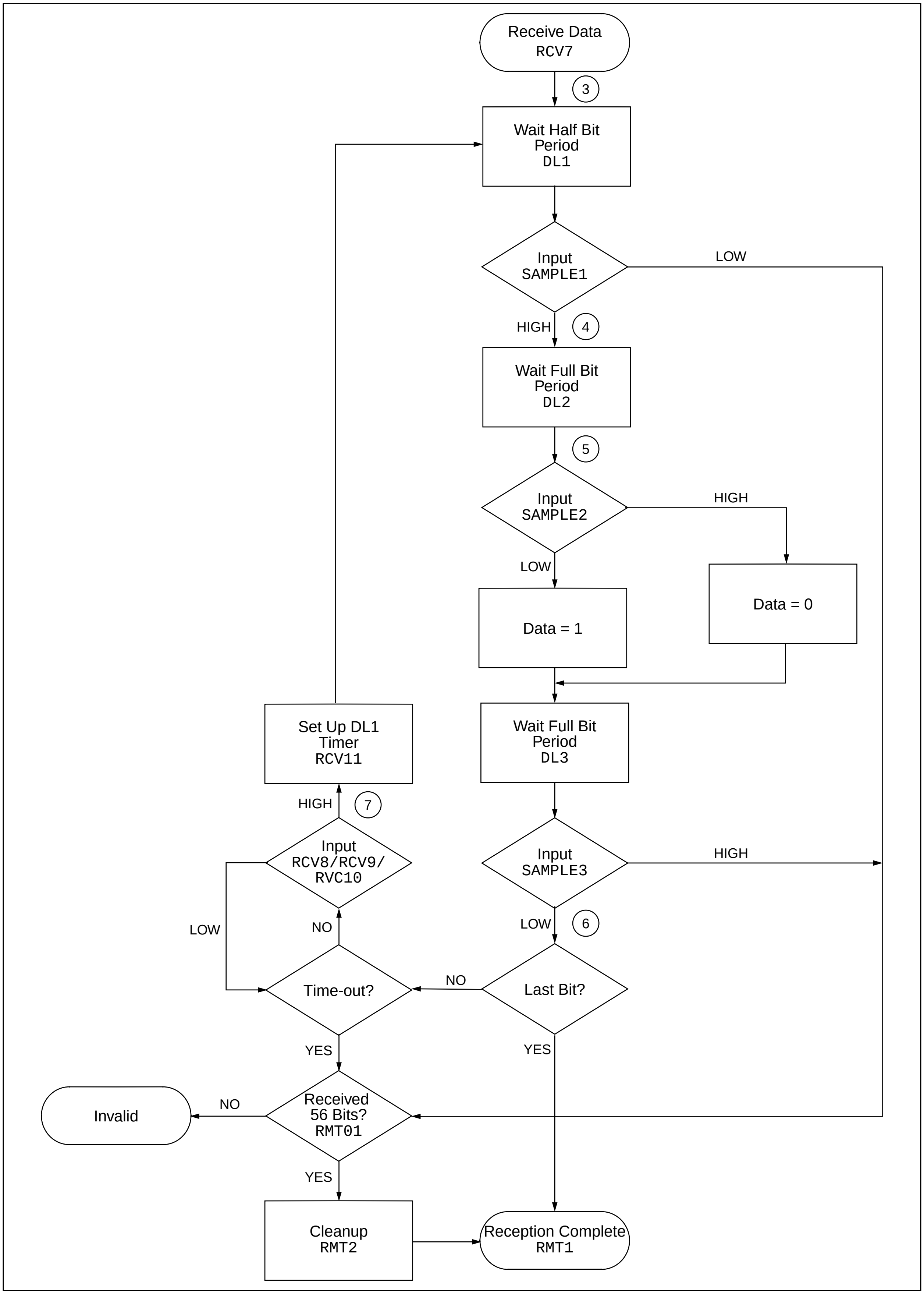


FIGURE 7: DATA RECEPTION FLOW CHART



VALIDATION

SYNCHRONIZATION

FUNCTION INTERPRETATION

OUTPUT ACTIVATION

KEY GENERATION

DECRYPTION

LEARN

ROM MEMORY MAP

EEPROM MEMORY MAP

RAM MEMORY MAP

The confidential and proprietary information contained in this section of AN659 has been removed. The full application note is available under a license agreement and can be ordered as DS40149 from Microchip Technology Inc.

DEVICE PINOUTS

The device used in the application note is a PIC16C54 PDIP or SOIC.

TABLE 9: DEVICE PINOUTS

PIN	PIC16C54 Function	Decoder Function	PIN	PIC16C54 Function	Decoder Function
1	Port A Bit 2	LEARN Input	18	Port A Bit 1	RF Input
2	Port A Bit 3	LEARN Indicator	17	Port A Bit 0	Not used
3	TIMER0	Connect to V_{DD}	16	Osc In	RC osc (4 MHz)
4	$\overline{\text{MCLR}}$	Brown out detect	15	Osc Out	
5	GND	Ground	14	V_{DD}	+5V supply
6	Port B Bit 0	S0	13	Port B Bit 7	Not Used
7	Port B Bit 1	S1	12	Port B Bit 6	CS (93LC46B, pin 1))
8	Port B Bit 2	S2	11	Port B Bit 5	CLK (93LC46B, pin 2)
9	Port B Bit 3	S3	10	Port B Bit 4	DIO (93LC46B, pin 3 & 4)

TIMING PARAMETERS

TABLE 10: TIMING PARAMETERS

Parameter	Typical	Unit
Output activation duration	524	ms
Output pause if new function code received	131	ms
Erase all duration	8.4	s
Learn mode time-out	33.6	s
Learn failure $\overline{\text{LED}}$ on duration	1	s

SOURCE CODE LISTING

A diskette is supplied containing source code for the Microchip decoder in the file `SIMDEC**.ASM`. The code has been compiled using MPASM v01.30.01. Certain functions are dependent on the oscillator speed for correct functioning. Examples of time dependent functions include `RECEIVE` and `TST_TIMER`. The PIC16C54 Microcontroller should run at 4 MHz.

TABLE 11: LIST OF IMPORTANT FUNCTIONS

Function Name	Description
DECRYPT	Decryption routine for Hop Code.
EEREAD	The data in the EEPROM at ADDRESS is read to TMP1 and TMP2 (Note).
EEWRITE	The data in TMP1, and TMP2 is written to the EEPROM at ADDRESS (Note).
M_DIS	Check discrimination value.
M_CNT	Check synchronization (counter) values.
RECEIVE	Start of the RF reception routine.
LEARN	Learn mode.
TST_RTCC	Check Timer0 and update CNT_LW and CNT_HI.
TST_TIMER	Check CNT_LW and CNT_HI and do whatever real-time tasks that are required.

Note: TMP1, TMP2 and ADDRESS are user defined registers.

APPENDIX A: SCHEMATIC DIAGRAMS

FIGURE 8: SCHEMATIC DIAGRAM OF MICROCHIP KEELOQ DECODER

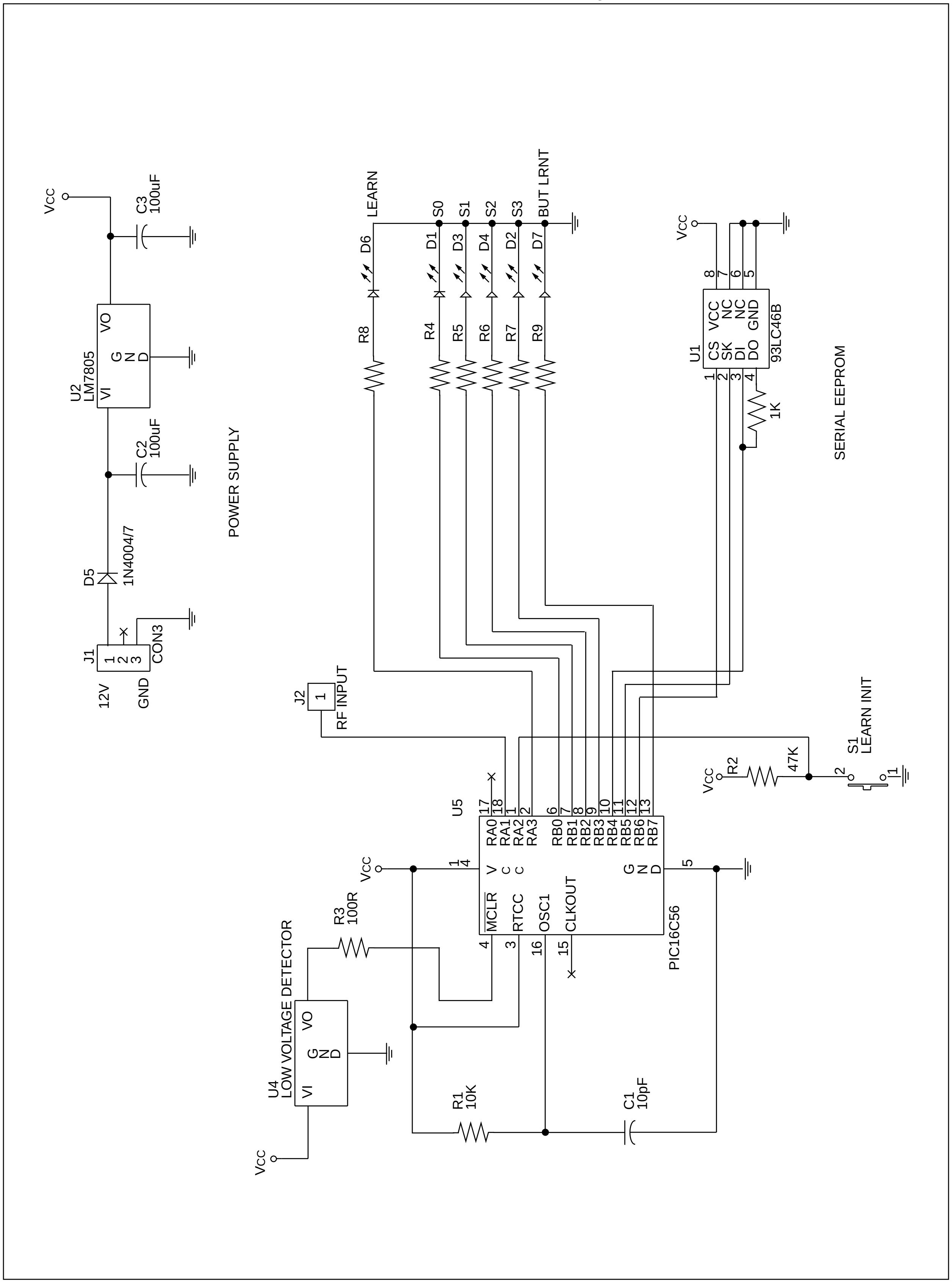


FIGURE 9: TYPICAL GARAGE DOOR OPENER SCHEMATIC

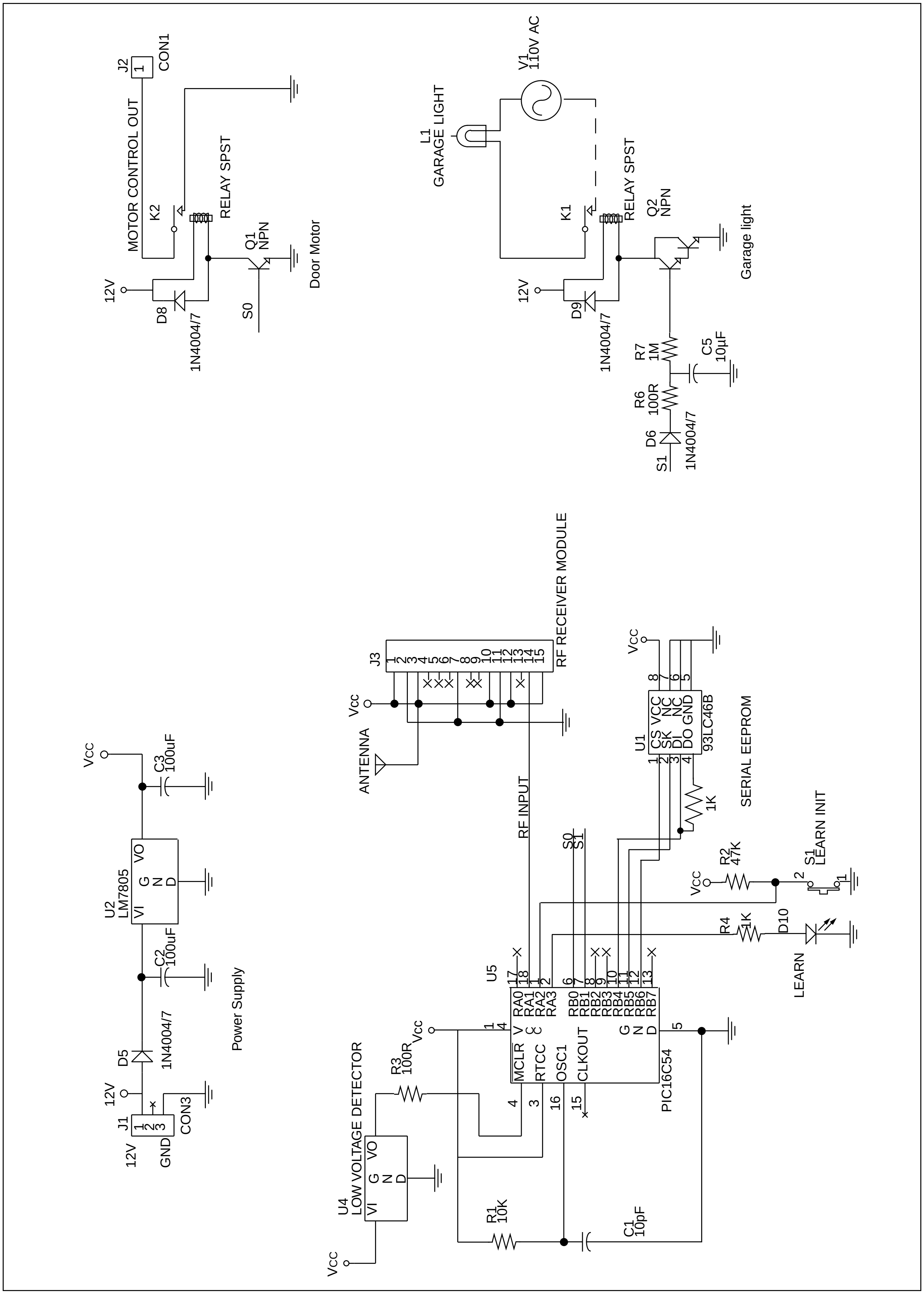
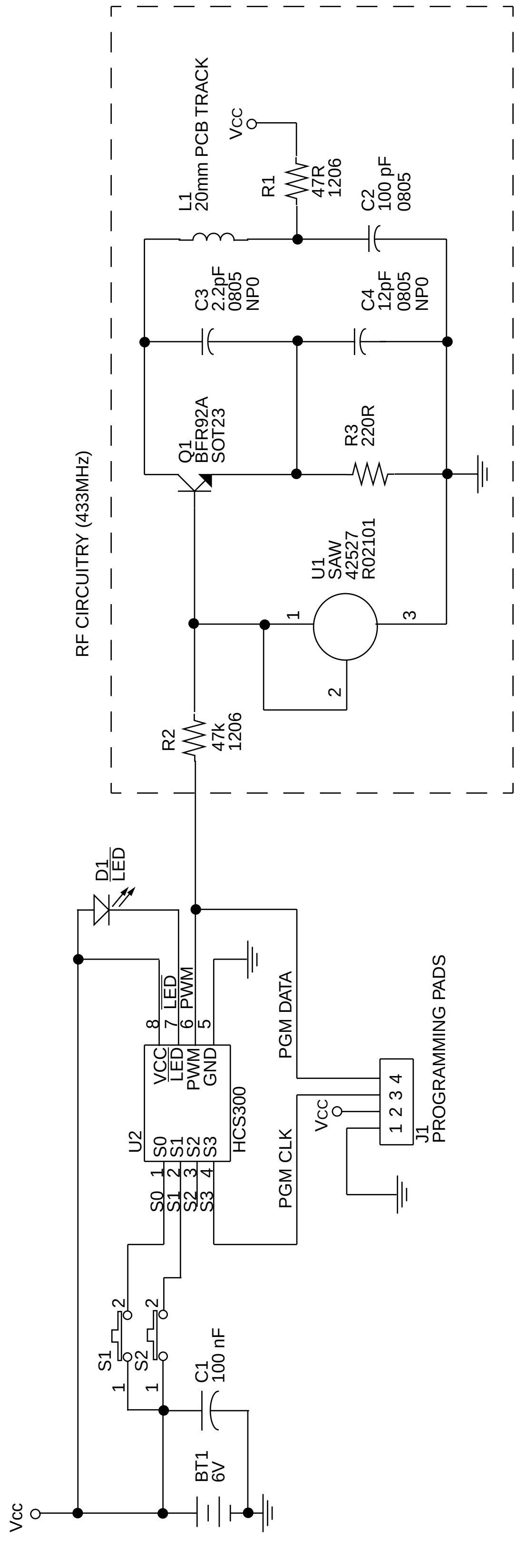


FIGURE 10: HCS200/300/301/360/361 TRANSMITTER DESIGN



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