AN652

KEELOQ™ Code Hopping Decoder Using Secure Learn

Author: Steven Dawson
Standard Microcontroller and
ASSP Division

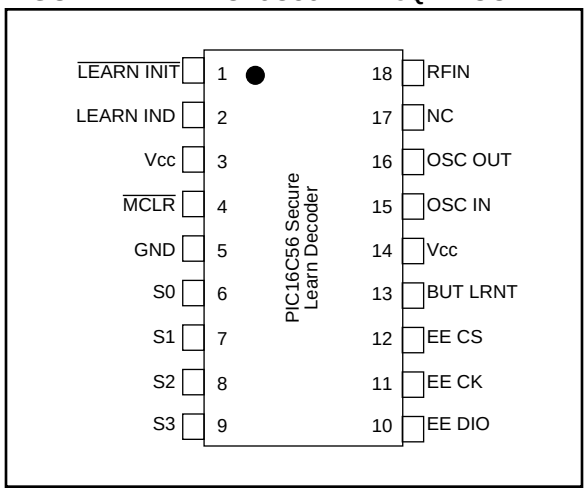
OVERVIEW

This application note fully describes the working of a code hopping decoder implemented on a Microchip PIC16C56 microcontroller. This decoder uses the secure learn (seed-based) method of learning new transmitters. 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 integrate with full function security systems. The decoder supports the Microchip HCS200, HCS300, HCS301, HCS360, and HCS361 KEELOQ code hopping encoders.

KEY FEATURES

- Stand alone decoder
- Compatible with Microchip HCS200, HCS300, HCS301, HCS360, and HCS361 encoders
- Automatic bit rate detection
- Automatic encoder type detection
- Four function outputs
- Six learnable transmitters
- RC Oscillator

FIGURE 1: PIC16C56 KEELOQ DECODER



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. 12 bits (including overflow bits) are available in the Microchip HCSXXX encoders.

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 HSC300 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 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 and HCS361 encoders can extend the length of the serial number from 28 bits to 32 bits, replacing the unencrypted function code.

Seed Transmissions

The Microchip HCSXXX encoders all have the ability to transmit a fixed seed. The seed value is programmed into the encoder when the encoder is first initialized along with the counters, key, serial number, and other information. The seed length differs from encoder to encoder with the HCS200, HCS300, and HCS301 having a 32-bit seed. The HCS360 and HCS361 encoders have a 48-bit seed. The HCS200, HCS300, and HCS301 encoders transmit the seed if all the inputs are activated simultaneously (S0, S1, S2, and S3). The HCS360 and HCS361 encoders transmit the seed immediately if S0 and S3 are activated or delayed if S0 and S1 are activated for more than 3 seconds.

Table 1 summarizes seed transmissions in the Microchip HCSXXX encoders

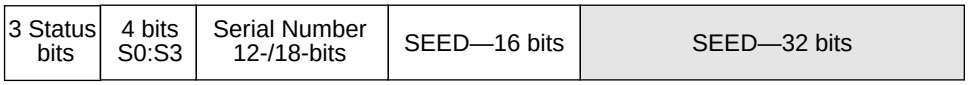
TABLE 1: HCSXXX ENCODER SEED TRANSMISSION SUMMARY

Encoder	Seed Length	Seed Transmission Activation
HCS200	32 bits	Seed transmitted immediately if S0, S1, and S2 are activated.
HCS300	32 bits	Seed transmitted immediately if S0, S1, S2, and S3 are activated.
HCS301	32 bits	Seed transmitted immediately if S0, S1, S2, and S3 are activated.
HCS360	48 bits	Seed transmitted immediately if S0 and S3 are activated. Seed transmitted after 3 seconds if S0 and S1 are activated.
HCS361	48 bits	Seed transmitted immediately if S0 and S3 are activated. Seed transmitted after 3 seconds if S0 and S1 are activated.

The seed transmission is transmitted in place of the HOP transmission and is not encrypted. When the seed is transmitted, the transmitted word changes as shown in Figure 2 below.

FIGURE 2: SEED TRANSMISSION FORMAT

HCS200/300/301 Seed Transmission Format



HCS360/361 Seed Transmission Format

Transmission Format Summary

Table 2 contains a summary of the information contained in transmissions from each of the KEELOQ encoders that can be learned by the Microchip decoder.

FIGURE 3: DECODER BLOCK DIAGRAM

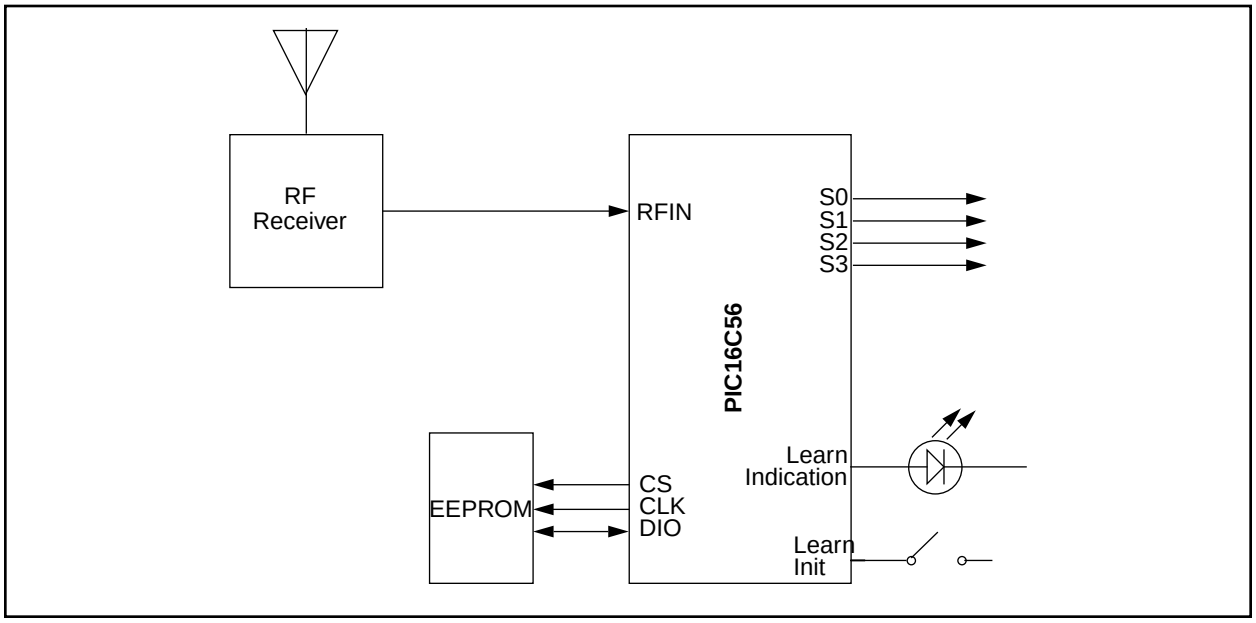


TABLE 2: KEELOQ ENCODER TRANSMISSION SUMMARY

	HCS200[1]	HCS300/301	HCS360/361
Total transmission length	66 bits	66 bits	67 bits
Hopping code portion (total length)	32 bits	32 bits	32 bits
Function bits	3 bits (+1[1])	4 bits	4 bits
Discrimination bits	12 bits	12 bits	12 bits
Synchronization	16 bits	16 bits	16 bits
Fixed portion (total length)	34 bits	34 bits	35 bits
Serial number	28 bits	28 bits	28/32 bits[2]
Function bits	3 bits (+1[1])	4 bits	4/0 bits[2]
Status bits			
VLOW	1 bit	1 bit	1 bit
RPT	0	1 bit	0
CRC	0	0	2 bits

[1]The HCS200 transmissions are padded to retain compatibility with the HCS300/301 encoders.
[2]User selectable with a 32-bit serial number or a 28-bit serial number, and 4 unencrypted function bits.

The code hopping portion is always transmitted first (LSB to MSB), followed by the fixed portion (LSB to MSB).

TABLE 3: HCS200† AND HCS300/301 TRANSMISSION FORMAT

Hop Code			Serial Number			Function	Status
LSB	32 bits	MSB	LSB	28 bits	MSB	4 bits	2 bits

†The HCS200 transmissions are padded to retain compatibility with the HCS300/301 encoders.

TABLE 4: HCS360/361 TRANSMISSION FORMAT

Hop Code			Serial Number			Function	Status
LSB	32 bits	MSB	LSB	28/32 bits	MSB	4/0 bits	3 bits

Bits are transmitted from left to right (i.e., the code hopping part first).

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 66 or 67 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 4 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 $2^{-132} < 2 \times 10^{-40}$.

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 4: KEELOQ PWM TRANSMISSION FORMAT

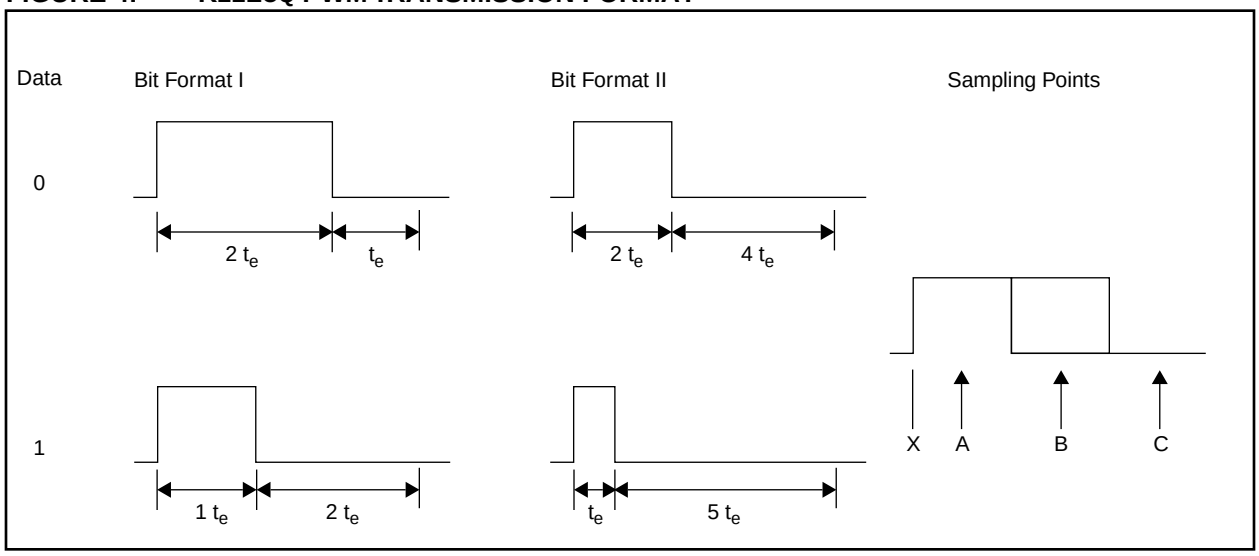


TABLE 5: TRANSMISSION FORMATS

Encoder	Preamble	Header Chopping	PWM Bit Format		Hopping Code Length	Unencrypted Code Length
			I	II		
HCS200	•	•	•	—	32 bits	34 bits
HCS300/301	•	•	•	—	32 bits	34 bits
HCS360	•	•	•	—	32 bits	35 bits
HCS361	•	•	•	•	32 bits	35 bits

Microwire is registered trademark of Motorola.

DECODER IMPLEMENTATION

The Microchip decoder's primary hardware components are a PIC16C56 RISC microcontroller and a 93C46 EEPROM as shown in the decoder schematic in Figure 22. However, this solution can be implemented in any PIC16/17 microcontroller with at least 1K 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, synchronization information, and decryption key is stored externally in an EEPROM. The EEPROM used is a Microchip 93C46 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.

The serial number is used to identify the memory block used to store the 64-bit decryption key for a particular encoder because of the relationship between serial number, seed, and the decryption key. In other words, the serial number is stored with the key. When a transmission is received, the decoder finds the correct memory block by checking all blocks until a matching serial number is found. The key is then retrieved from that particular memory block. A serial number of 0000000_{16} is considered invalid and is ignored by the decoder.

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 12-bit discrimination value received with the stored discrimination value. 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.

PINOUTS OF MICROCHIP KEELOQ DECODER

FIGURE 5: FUNCTIONAL INPUTS AND OUTPUTS

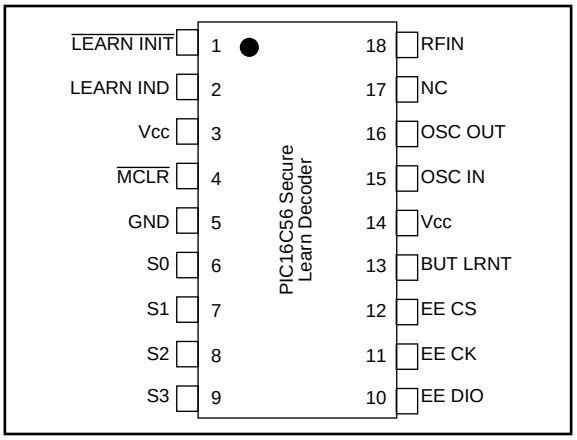


TABLE 6: MICROCHIP DECODER FUNCTIONAL INPUTS AND OUTPUTS

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).
BUT LRNT	13	O	Indication that the received function code matches the learned function code.
S0, S1, S2, S3	6, 7, 8, 9	O	Function outputs—corresponds to encoder input pins.

Microwire is registered trademark of Motorola.

PROGRAM FLOW

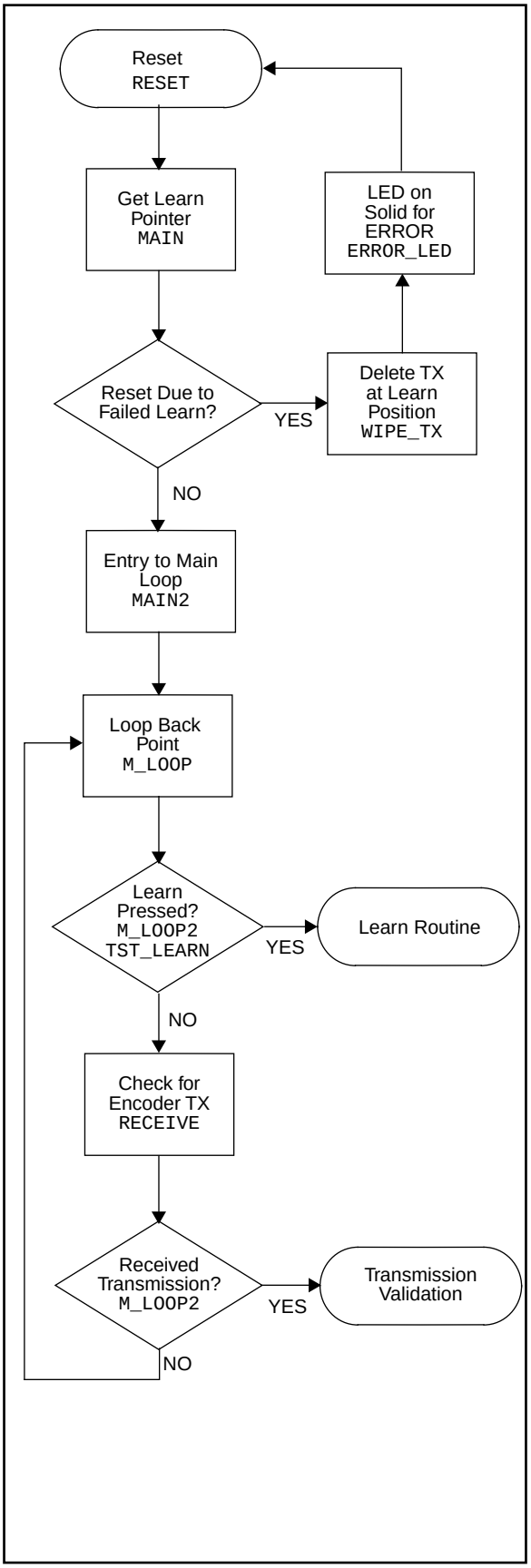
The software for the Microchip decoder has been written for the PIC16C56 microcontroller. The compiler used is MPASM version 01.30.01. The operating frequency of the PIC16C56 is 4 MHz. The clock speed should be kept as close as possible to 4 MHz as the reception routine (RECEIVE) is dependent on the 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.

As can be seen from Figure 6, the decoder reads the learn pointer, which stores the next position to be overwritten when the decoder enters a learn sequence and decoder status flags, from the external EEPROM on power-up. The status flags are checked to see if a learn routine was interrupted when the microcontroller was reset. If so, it is assumed the learn cycle was not successfully completed, and the encoder at the learn pointer is subsequently deleted (WIPE_TX).

The encoder then enters the main loop where it spends most of its time. The main loop checks to see if the learn button is being activated (TST_LEARN). If so, the decoder enters the learn mode described in the “Learn” section (page 20).

If learn has not been initiated, the microcontroller then checks for transmissions from encoders (RECEIVE) as described on page 8. If a transmission from an encoder has successfully been received, the microcontroller validates the transmission received as described in the “Transmission Validation” section (page 11). If the transmission received is a valid transmission from an encoder learned into the system, the system sets the appropriate outputs (M_BUT).

FIGURE 6: MICROCHIP DECODER MAIN PROGRAM FLOW



FUNCTIONAL MODULES

Reception

The reception routine (called 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 66-bit transmissions. The reception routine is able to determine the number of bits in the transmission.

The reception algorithm performs a number of functions when an output is detected from the receiver. Figure 7 gives all the major sampling points in the reception algorithm.

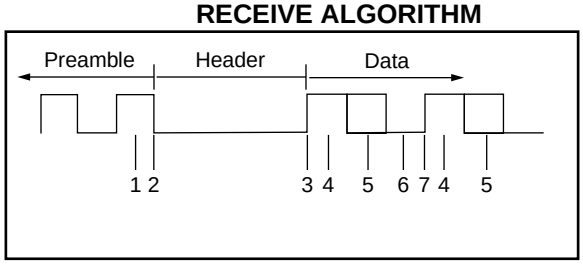
The reception algorithm calibrates on the low period of the header to determine the actual elemental period for the transmission being received. The required elemental period is 10% of the low header period. In Figure 7 the header calibration sample points are marked 1 through 3. The calibration flow chart (Figure 8) 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 7, the data sample points are points 4 through 6. The flow chart describing data reception (Figure 9) shows where in the code the samples are taken.

If all 66 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 7).

FIGURE 7: 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 first flow chart (Figure 8) 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 9) 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 Microchip 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 more than 56 bits have been received correctly. If not, the routine returns to the calling procedure.

FIGURE 8: CALIBRATION FLOW CHART

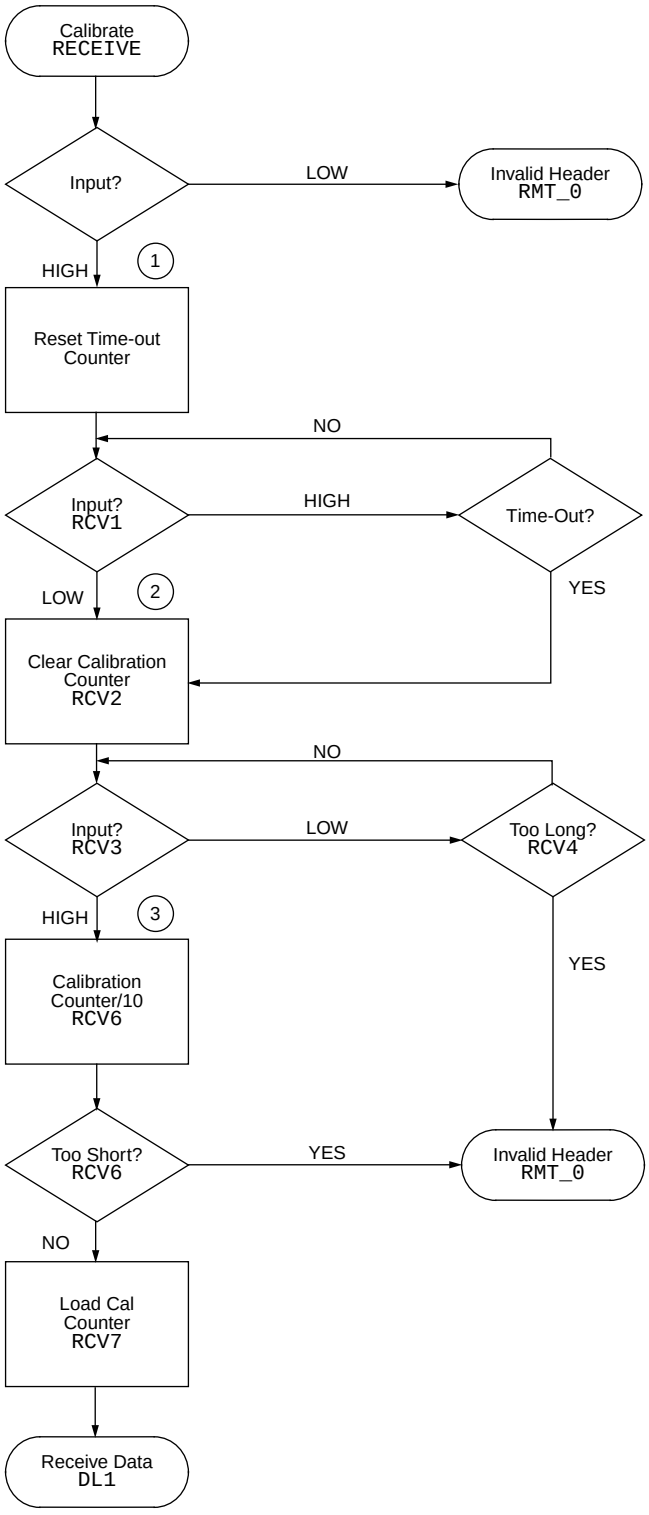
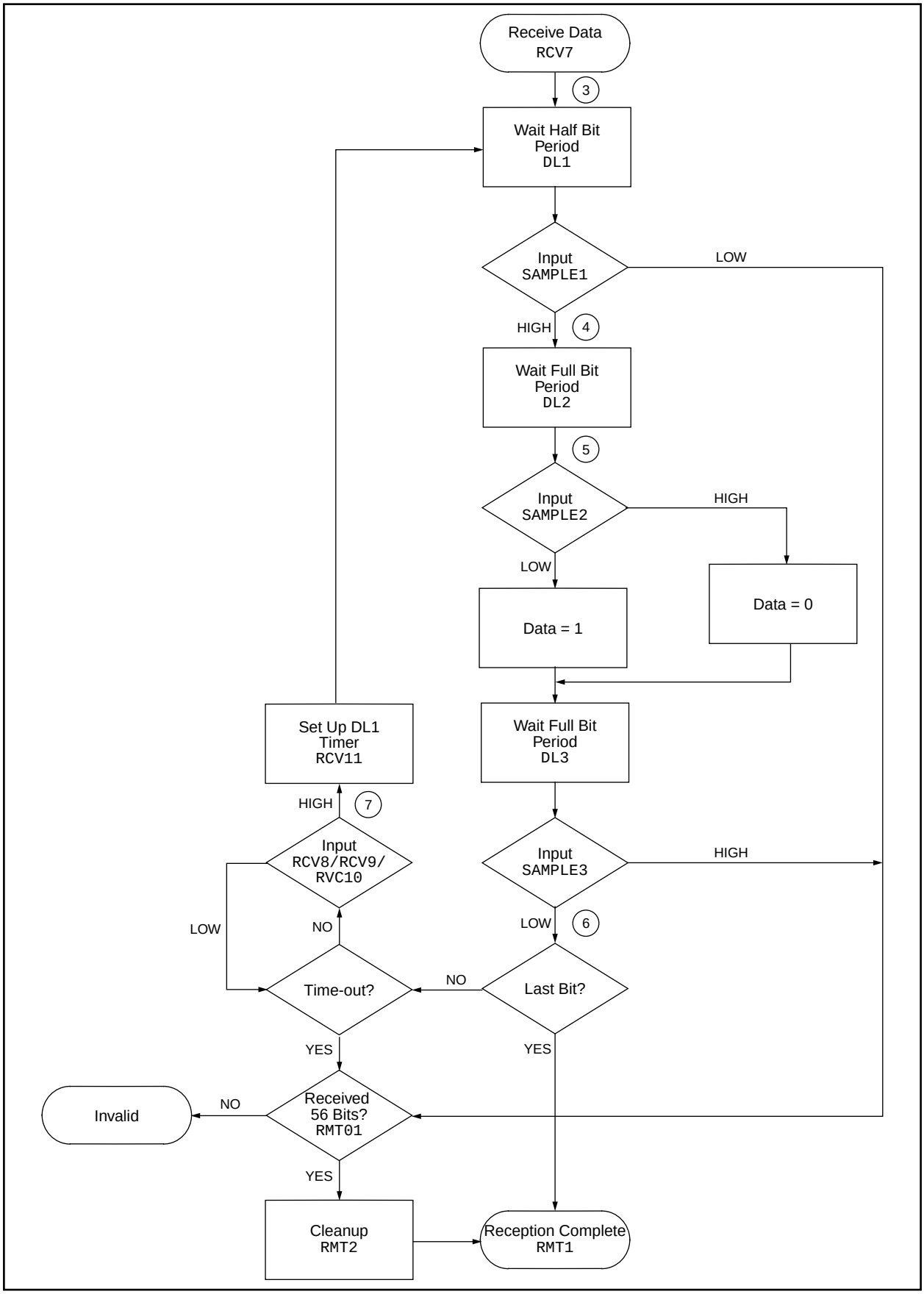


FIGURE 9: DATA RECEPTION FLOW CHART



Transmission Validation

Once a complete transmission has been received from an encoder, the transmission needs to be validated before any further action is taken. Validation consists of the following steps and is shown in Figure 10:

1. Check the serial number (28 bits) received against the stored encoder serial numbers (M_SERIAL).
2. Decrypt the transmission received (M_HOP).
3. Compare the 12 bit discrimination value in the decrypted hopping portion of the transmission against the stored discrimination value (M_DIS).
4. Check if the synchronization counter falls within the resynchronization window (M_CHECK1).
5. Check if the synchronization counter falls within the open window. If not, then decoder resynchronization is necessary (M_CHECK2).
6. If resynchronization is necessary wait for a second transmission from the encoder with a consecutive synchronization counter (M_RESYNC).
7. Update the synchronization counters in EEPROM (M_UPDATE).
8. Set the appropriate outputs (M_BUT).
9. Return to MAIN routine and continue normal housekeeping chores.

Discrimination Values

After decryption, the Code Shift Register (CSR) used by the KEELOQ decryption algorithm contains the same 32 bits of information originally encrypted in the encoder before transmission. Twelve of these bits are discrimination bits.

The decryption operation can be checked by comparing parts of the decrypted 32-bit word (the discrimination values) with known values.

When using an HCS200 encoder all 12 bits are user selectable discrimination bits. The HCS300/301 encoders have 10 bits of user programmable bits and 2 user programmable overflow bits. The HCS360/361 encoders set the least significant 8 bits of the discriminator to the least significant 8 bits of the serial number. The remaining 4 bits are made up of a user-programmable overflow bit, 2 user bits, and a bit showing whether independent mode is enabled.

If the discrimination bits are programmed to a known value, the integrity of the decryption can be easily verified. The encoder uses this to check whether the two transmissions received are a HOP/ SEED transmission pair. The decoder checks that the least significant 8 bits of the discrimination value are identical to the least significant 8 bits of the serial number before signaling a successful learn (M_SL_UPDATE).

All 12 discrimination bits are stored in the external EEPROM during learn. These are checked whenever a transmission is received to check for a valid transmission. If one of the overflow bits are cleared during a counter overflow, the decoder will cease to recognize the encoder. The overflow bits in the transmitter should be set to zero if the user wants to prevent this from happening.

TABLE 7: HCS200 AND HCS300/301 DECRYPTED HOPPING CODE TRANSMISSION FORMAT

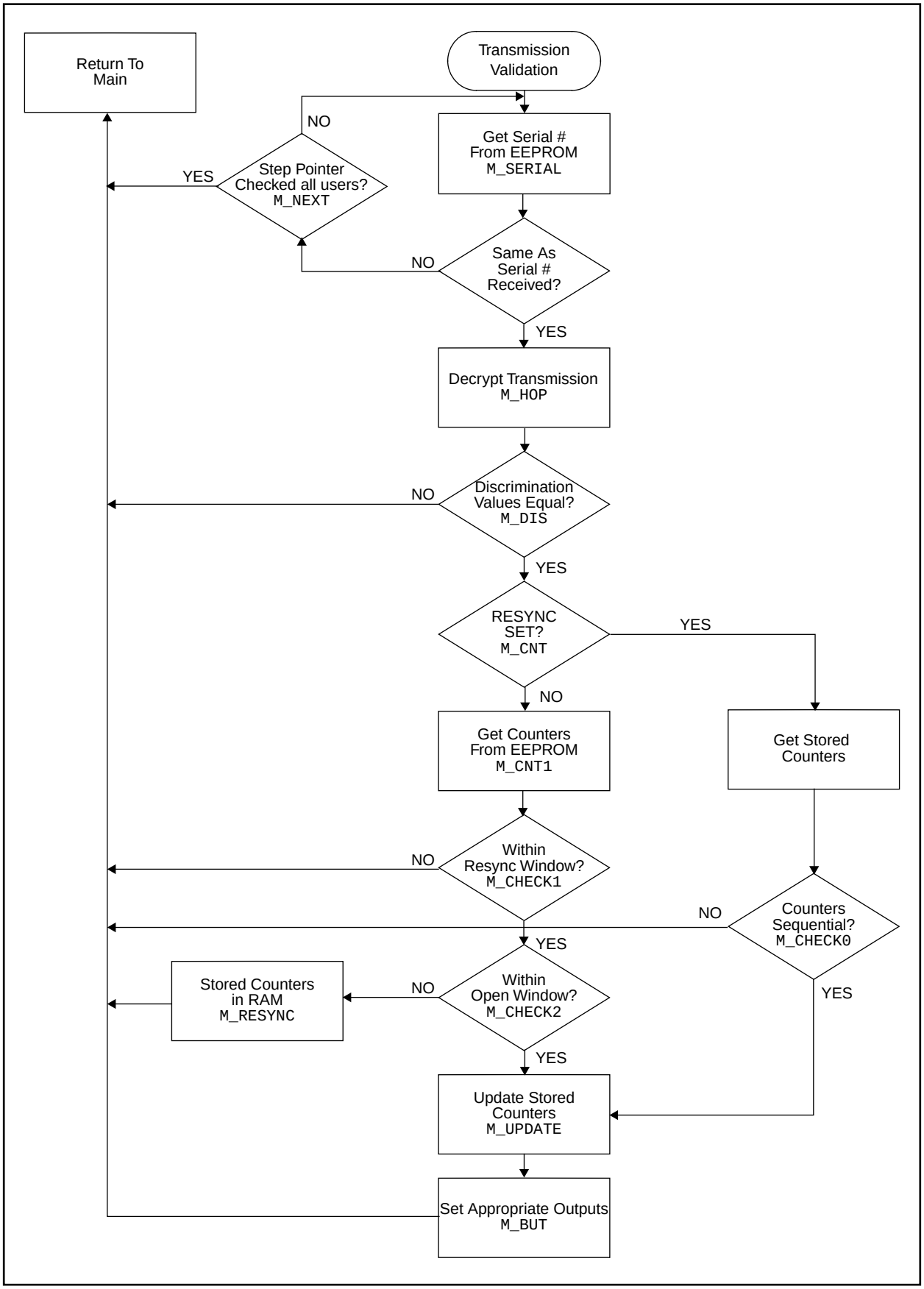
Function[1]	MSB	Encoder disc. bits	LSB	MSB	Synchronization counter	LSB
(4 bits)		(12 bits)			(16 bits)	

[1]The HCS200 has padding in S3 button position since no S3 button is present.

TABLE 8: HCS360/361 DECRYPTED HOPPING CODE TRANSMISSION FORMAT

Function	MSB	Encoder disc. bits	LSB	MSB	Synchronization counter	LSB
(4 bits)		(12 bits)			(16 bits)	

FIGURE 10: TRANSMISSION VALIDATION FLOWCHART



Synchronization Checking

The synchronization information is used at the decoder to determine whether the transmission is valid or whether it is a repetition of a previous transmission. Repetitious codes are rejected to safeguard the system against code grabbers.

The transmitting encoder has a 16-bit synchronization counter, stored in EEPROM, which is incremented every time the encoder is activated. The synchronization counter value received is stored in the decoder's EEPROM every time a valid transmission is received from a particular encoder. When a following transmission is received from the same transmitter it is possible to quickly verify whether the transmission is valid. For example, a grabbed code from the legitimate user's previous transmission will result in a synchronization counter value that has already been received.

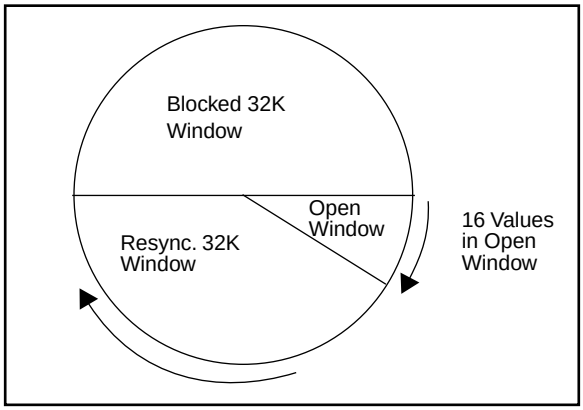
Provision must be made for the transmitter being pressed while out of range of the decoder. The Microchip decoder does this by allowing two 'synchronization windows'. The Open Window is a reception of a transmission where the synchronization counter is 1 to 16 higher than the previous counter value received and is checked in M_CHECK2. The reception of such a signal will result in an immediate counter update by the decoder and the appropriate outputs being activated.

If the transmitter is pressed more than 16 times out of range of the receiver, resynchronization needs to take place (M_CHECK1). The Resynchronization Window is a half of the total counter range, 32K. When the decoder receives a transmission with a synchronization counter value more than 16 above the stored counter value and less than 32,768 counts above the stored value, the decoder temporarily stores the value of the synchronization counter received (M_RESYNC). If the next transmission received has a sequential synchronization counter value, the decoder resynchronizes on the last transmission received, storing the latest counter in EEPROM and activates the appropriate outputs.

If any of the above tests fail, the transmission received is discarded. It is easy to change the size of the various windows in the source code. Modifications to the synchronization windows can be made in the M_CHECK routine.

The decoder stores two copies of the synchronization counter. If the power supply is interrupted during a counter update the synchronization counter can be corrupted. When the counters are read from EEPROM the decoder checks whether the counters are identical (M_CNT1). If not, the decoder forces a resynchronization, waiting for two consecutive transmissions from the transmitter to resynchronize itself on.

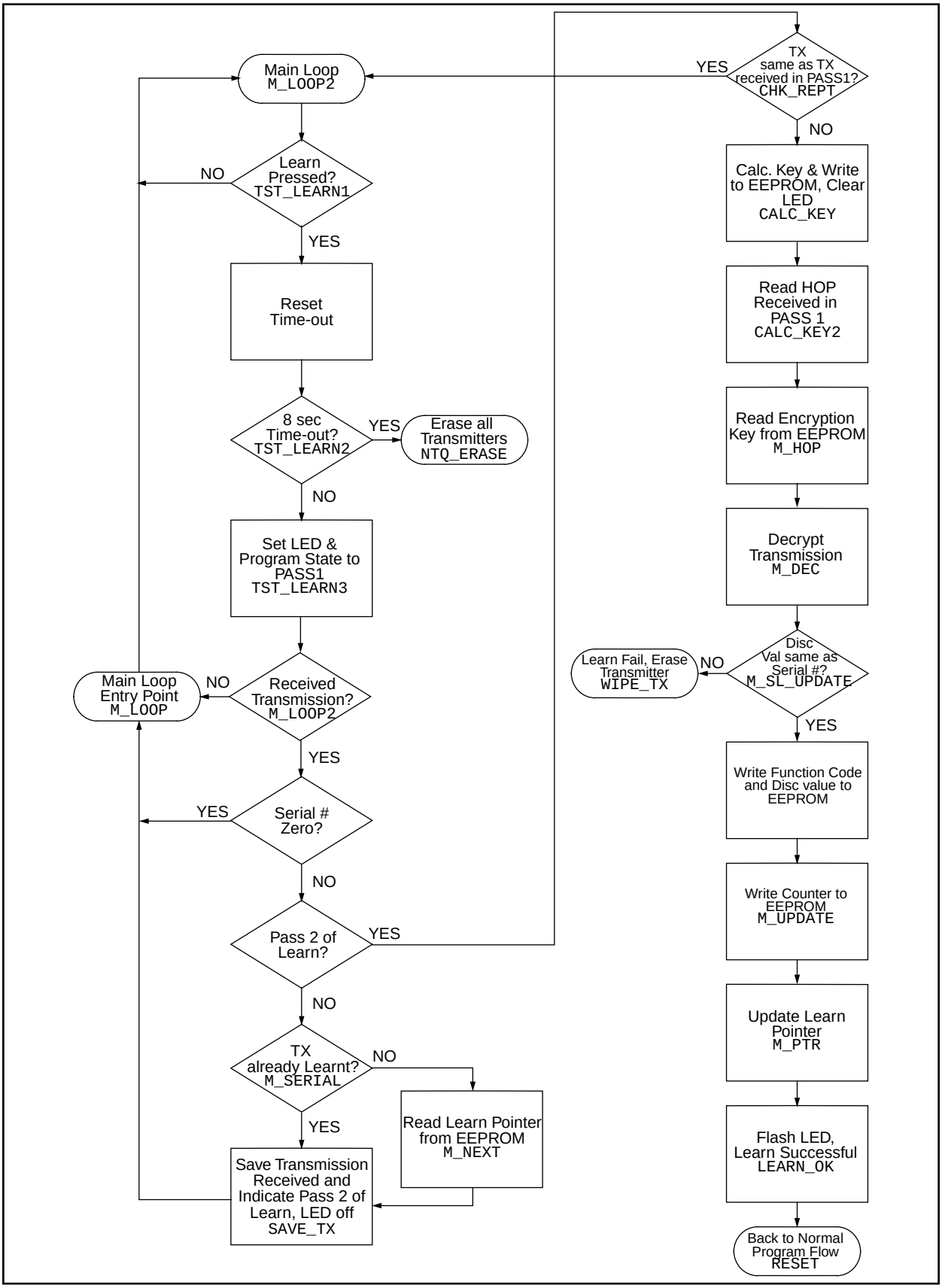
FIGURE 11: DECODER WINDOW OPERATION



Function Interpretation

In a single-chip system, where the code hopping decoder and the control program are combined into one device, the function code is interpreted to deter-

FIGURE 19: PROGRAM FLOW DURING LEARN



Operation of Learn

The following steps need to be followed by a user to learn an encoder onto the decoder. The steps are shown in Figure 20.

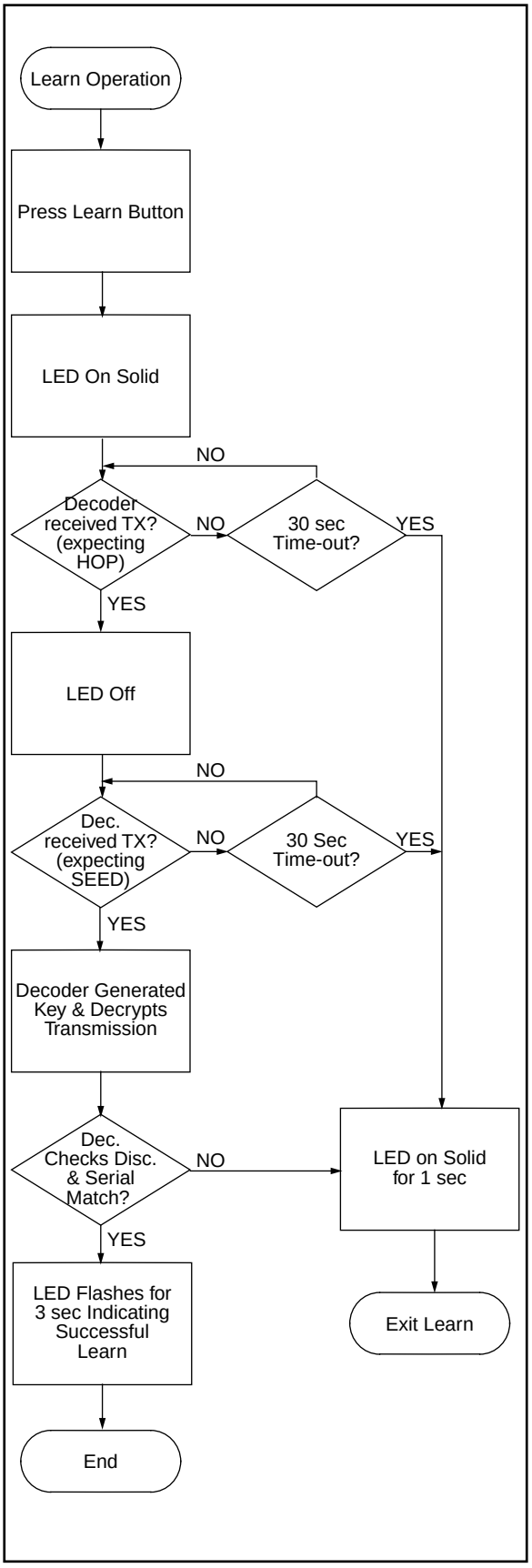
1. Press and release the LEARN button. Indicator LED will turn on to indicate learn mode is now active.
2. Press transmitter to transmit a normal transmission The LED will turn off.
3. Press transmitter a second time, this time transmitting a seed transmission. The LED will blink to indicate that the transmitter was learned successfully.
4. To learn up to six transmitters, repeat steps 1-3. The seventh transmitter will overwrite the first transmitter that was learned.
5. Learn will be terminated if the eight least significant bits of the discrimination value do not match those of the serial number or if two acceptable codes were not decrypted within 33 seconds. An invalid learn will be indicated by the LED turning on solid for one 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 all the transmitters were erased. The learn pointer is reset to the first position.

HCS360 and HCS361 in Secure Learn

The HCS360 and HCS361 encoders are ideally suited for use with the secure learn decoder. Both of these transmitters feature a 'transmit seed on delayed mode'. If either of these decoders are activated with S0 and S1 continuously for more than 3 seconds, the transmitter will transmit a seed instead of the normal hop transmission.

Using this feature the entire learn procedure can be accomplished with one extended press of a button, assuming S0 and S1 are connected to a single button.

FIGURE 20: LEARN OPERATION



TIMER0 (RTCC) Multiplexing

A time keeping scheme is needed to ensure that the system timing is not abandoned while receiving an incoming signal, during learn cycles, key generation, and decryption. The system timing is used to allow periodic monitoring of sensors and pulsing outputs with a specific period.

TIMER0 is used to keep track of system time. TIMER0 is an 8-bit timer on the PIC16C56. On the Microchip decoder described, TIMER0 is prescaled to increment every 256 instruction cycles. This makes TIMER0 very useful for keeping track of real time. While various routines are being run, including reception routines and decryption, TIMER0 is periodically checked for a time-out value calculated at the beginning of a certain period (i.e., switch off time of a LED).

The routine checking TIMER0 is called TST_RTCC. The most significant bit (MSB) of TIMER0 changes every 32 ms. In order to extend the range of TIMER0, two additional 8-bit counters are used, CNT_LW and CNT_HI, which extend the range of TIMER0 to 134 seconds. The MSB of TIMER0 is mirrored in the MSB of the STATUS register during startup. During TST_RTCC the two bits are compared. If the bits differ, the MSB of TIMER0 has changed, indicating that 32 ms has passed. The MSB of STATUS is changed to match the MSB of TIMER0 and the extended counter (CNT_LW and CNT_HI) incremented.

The second portion of the TST_RTCC routine checks appropriate time-out values based on the system status bits in SREG (i.e., to check for the 30-second time-out in the learn routine TST_RTCC checks to see if bit three of CNT_HI is set).

ROM MEMORY MAP (8-BIT BYTES)

TABLE 10: ROM MEMORY MAP (8-BIT BYTES)

Word Address	Mnemonic	Description
43	EKEY_0	64-Bit EEPROM Key (Used to encrypt EEPROM data)
44	EKEY_1	
45	EKEY_2	
46	EKEY_3	
47	EKEY_4	
48	EKEY_5	
49	EKEY_6	
4A	EKEY_7	

EEPROM MEMORY MAP (16-BIT BYTES)

TABLE 11: EEPROM MEMORY MAP (16-BIT WORDS)

Address	Mnemonic	Address	Mnemonic
00	USER0	20	CNT20
01	Learn pointer	21	CNT21
02	DIS0	22	SER20
03	DIS1	23	SER21
04	TMP_HOP0	24	KEY20
05	TMP_HOP1	25	KEY21
06	TMP_SEED0	26	KEY22
07	TMP_SEED1	27	KEY23
08	DIS2	28	CNT30
09	DIS3	29	CNT31
0A	DIS4	2A	SER30
0B	DIS5	2B	SER31
0C	USER1	2C	KEY30
0D	USER2	2D	KEY31
0E	USER3	2E	KEY32
0F	USER4	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

RAM MEMORY MAP

TABLE 12: RAM MEMORY MAP

Address	Mnemonic	Description
07	FLAGS	Decoder flags.
08	ADDRESS	Address register—points to address in EEPROM.
09	TXNUM	Current transmitter.
0A	OUTBYT	General data register.
0B	CNT0	Loop counters.
0C	CNT1	
OD	CNT2	
OE	CNT_HI	16-bit clock counter.
OF	CNT_LO	
10	TMP1	Temporary registers.
11	TMP2	
12	TMP3	
13	TMP4	
14	CSR4	64-bit shift register. Used in reception, decryption, and key generation.
15	CSR5	
16	CSR6	
17	CSR7	
18	CSR0	
19	CSR1	
1A	CSR2	
1B	CSR3	
1C	OLD_BUT	Store previous button code.
1D	RAM_HI	16-bit RAM counter (used in resynchronization).
1E	RAM_LW	
1F	SREG	Program state register.

ALTERNATE NAMES AND FUNCTIONS

Many of the memory locations in RAM are used by multiple routines. A list of alternate names and functions are given in Table 13 below.

TABLE 13: ALTERNATE NAMES AND FUNCTIONS

Address	Mnemonic	Also known as	Description
0A	MASK	OUTBYT	Mask used in decryption.
10	TMP_CNT	TMP1	Counter used in the reception routine.
10	KEY0	TMP1	64-bit shift register holds decryption key
11	KEY1	TMP2	
12	KEY2	TMP3	
13	KEY3	TMP4	
14	KEY4	CSR4	
15	KEY5	CSR5	
16	KEY6	CSR6	
17	KEY7	CSR7	
18	HOP1	CSR0	32-bit hop code register.
19	HOP2	CSR1	
1A	HOP3	CSR2	
1B	HOP4	CSR3	
17	SER_0	CSR7	28-bit serial number is stored here by the reception routine.
16	SER_1	CSR6	
15	SER_2	CSR5	
14	SER_3	CSR4	
1B	FUNC	CSR3	Function code and user nibble of discrimination value.
1A	CODE	CSR2	Discrimination value.
19	CNTR_HI	CSR1	16-bit received counter.
18	CNTR_LW	CSR0	
11	CSR8	TMP2	Most significant byte of the code shift register.

DEVICE PINOUTS

The device used in the application note is a PIC16C56 PDIP.

TABLE 14: DEVICE PINOUTS

PIN	PIC16C56 Function	Decoder Function	PIN	PIC16C56 Function	Decoder Function
1	Port A Bit 2	LEARN Input	18	Port A Bit 1	RF Input
2	Port A Bit 3	LRN INDICATOR	17	Port A Bit 0	Not used
3	TIMER0	Connect to VDD	16	Osc In	RC osc (4 MHz)
4	$\overline{MCLR}$	Brown out detect	15	Osc Out	
5	GND	Ground	14	VDD	+5V supply
6	Port B Bit 0	S0	13	Port B Bit 7	BUT LRNT
7	Port B Bit 1	S1	12	Port B Bit 6	CS (93C46, pin 1))
8	Port B Bit 2	S2	11	Port B Bit 5	CLK (93C46, pin 2)
9	Port B Bit 3	S3	10	Port B Bit 4	DIO (93C46, pin 3 & 4)

TIMING PARAMETERS

TABLE 15: 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 successful LED flash duration	4.2	s
Learn successful LED flash rate	3.8	Hz
Learn failure LED on duration	1	s

SOURCE CODE LISTING

A diskette is supplied containing source code for the Microchip decoder in the file mslrn**.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_RTCC. The PIC16C56 Microcontroller should run at 4 MHz.

TABLE 16: LIST OF IMPORTANT FUNCTIONS

Function Name	Description
CALC_KEY	Key generation routine.
DECRYPT	Decryption routine for Hop Code.
EEREAD	The data in the EEPROM at ADDRESS is read and decrypted to TMP1 and TMP2 (Note).
EEWRITE	The data in TMP1, and TMP2 is encrypted and 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.
TST_LEARN1	Check for learn mode and entry to learn.
TST_RTCC	Check TIMER0 and do whatever real time tasks are required.

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

APPENDIX A: SCHEMATIC DIAGRAMS

FIGURE 21: SCHEMATIC DIAGRAM OF MICROCHIP KEELOQ DECODER

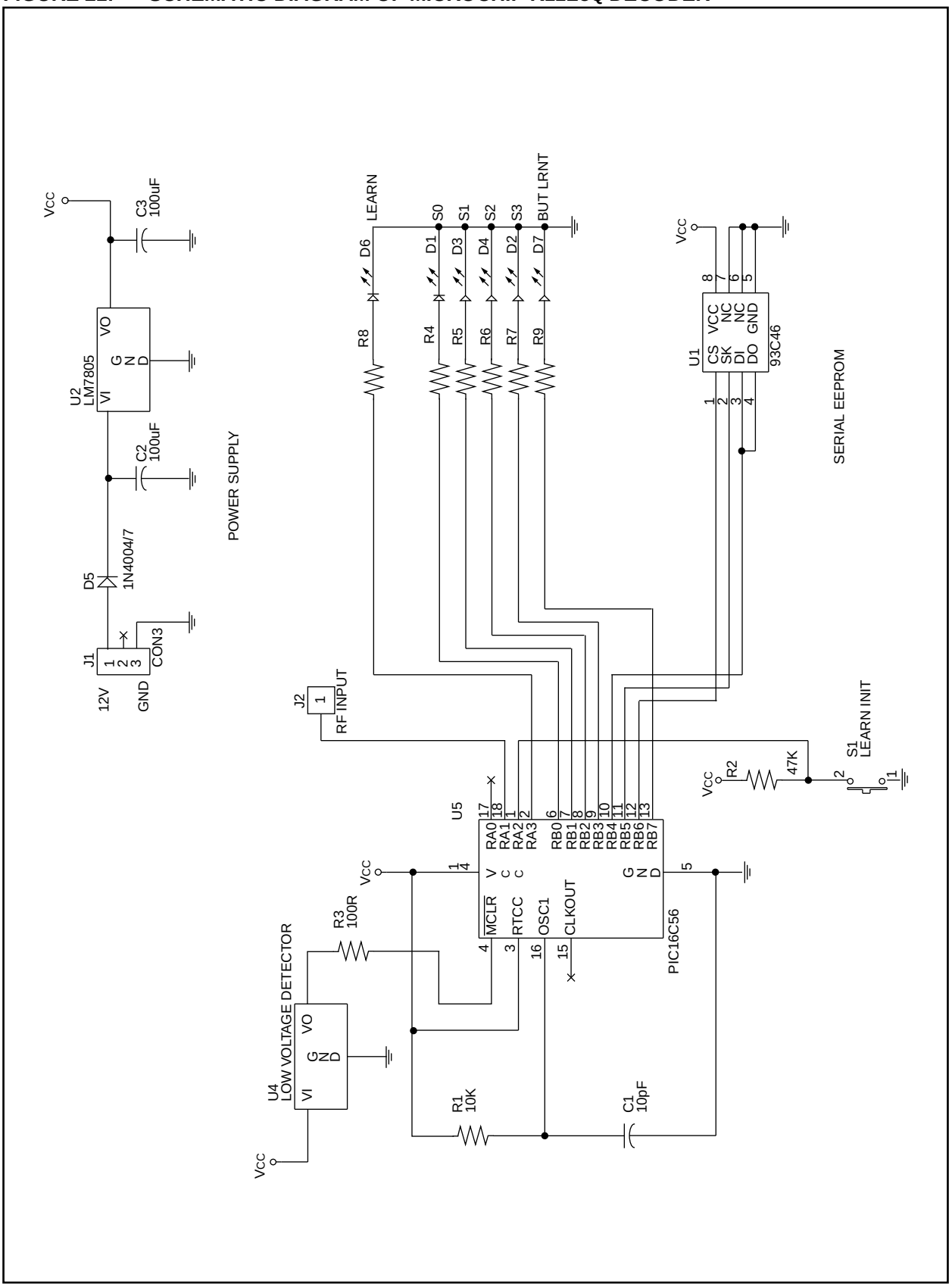


FIGURE 22: TYPICAL GARAGE DOOR OPENER SCHEMATIC

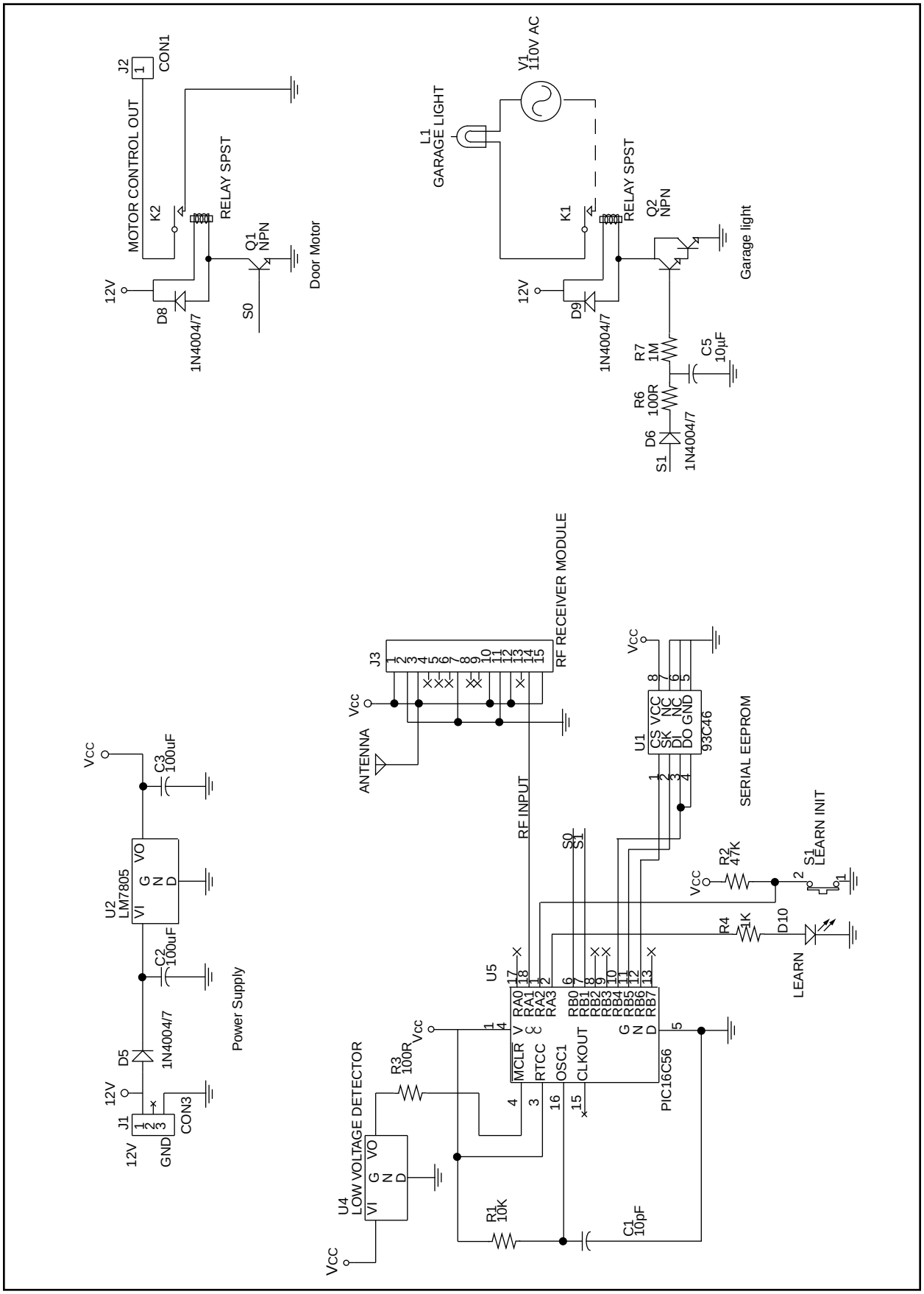


FIGURE 23: HCS200/300/301 TRANSMITTER DESIGN

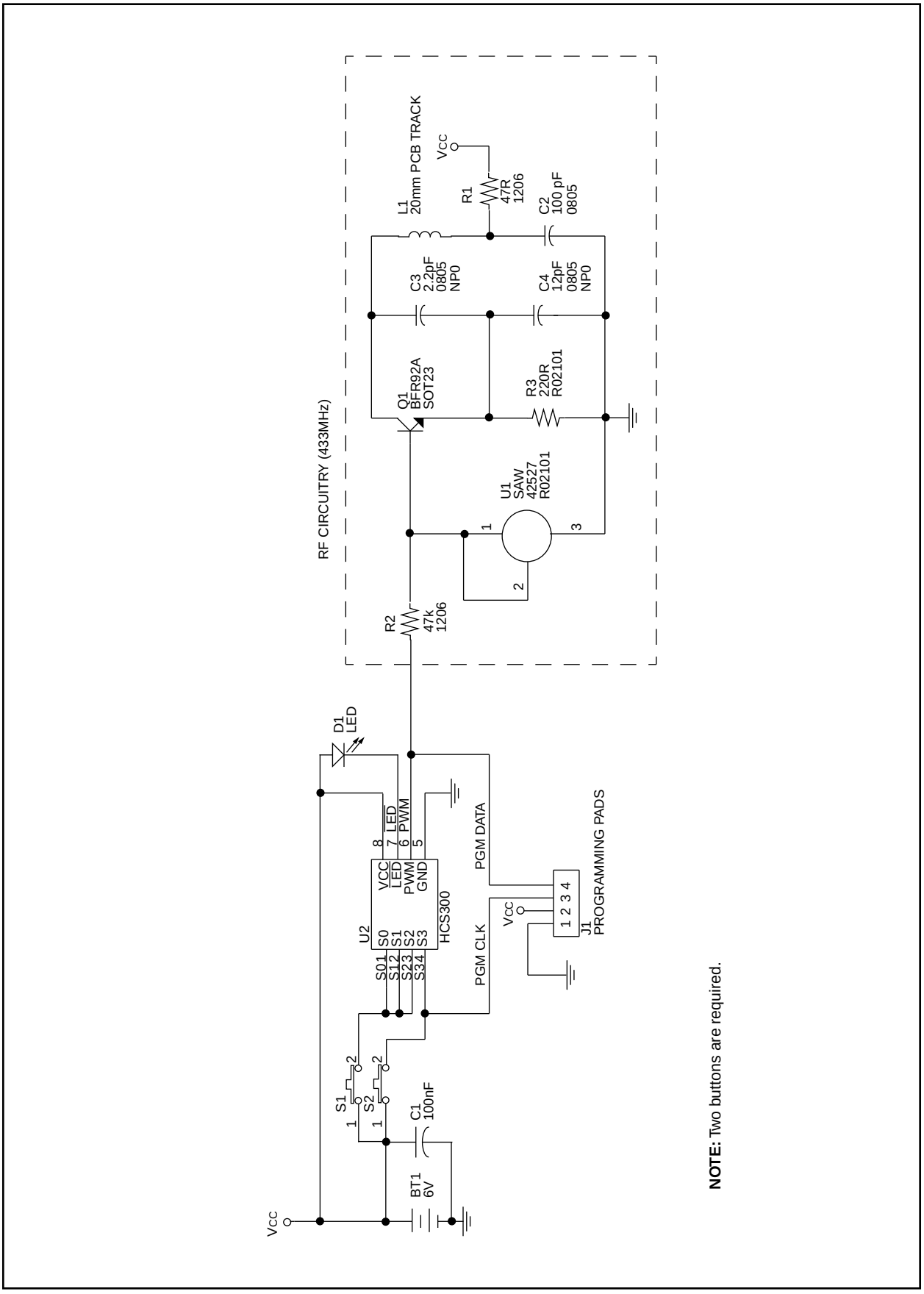
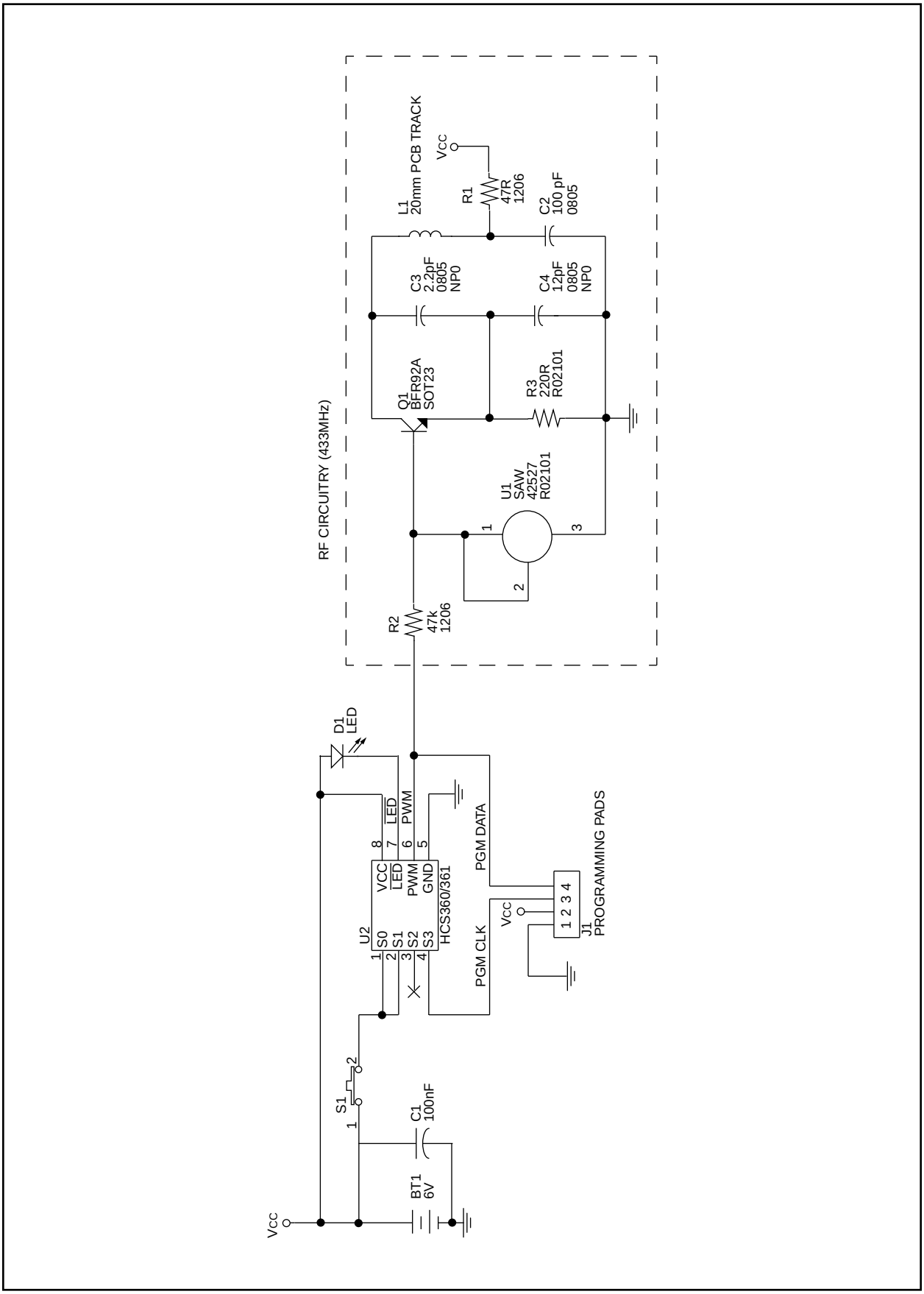


FIGURE 24: HCS360/361 SINGLE BUTTON TRANSMITTER DESIGN



NOTES:

NOTES:

NOTES:

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: 508 480-9990 Fax: 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: 972 991-7177 Fax: 972 991-8588

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 Technology 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

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

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

Taiwan, R.O.C
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

11/7/96

MICROCHIP

Printed on recycled paper.