HCS362

KEELOQ® Code Hopping Encoder

FEATURES

Security

- Programmable 28/32-bit serial number
- Two programmable 64-bit encryption keys
- Programmable 60-bit seed
- Each transmission is unique
- 69-bit transmission code length
- 32-bit hopping code
- 37-bit fixed code (28/32-bit serial number, 4/0-bit function code, 1-bit status, 2-bit CRC/time, 2-bit queue)
- Encryption keys are read protected

Operation

- 2.0V – 6.3V operation
- Four button inputs
- 15 functions available
- Selectable baud rates and code word blanking
- Programmable minimum code word completion
- Battery low signal transmitted to receiver with programmable threshold
- Non-volatile synchronization data
- PWM and Manchester modulation

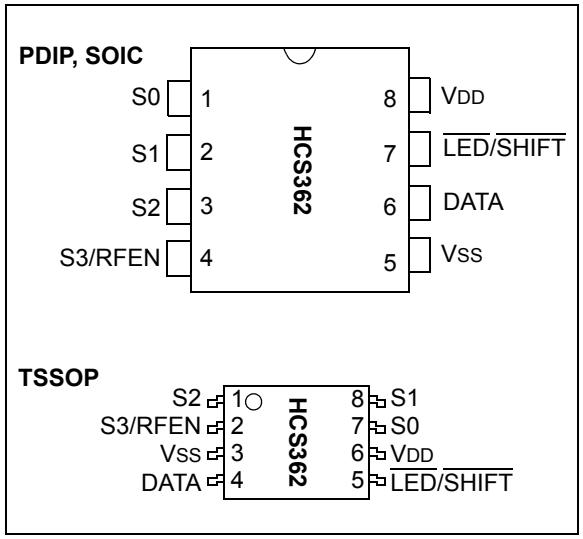
Other

- RF Enable output – PLL interface
- Easy to use programming interface
- On-chip EEPROM
- On-chip tunable oscillator and timing components
- Button inputs have internal pull-down resistors
- Current limiting on $\overline{\text{LED}}$ output
- Minimum component count

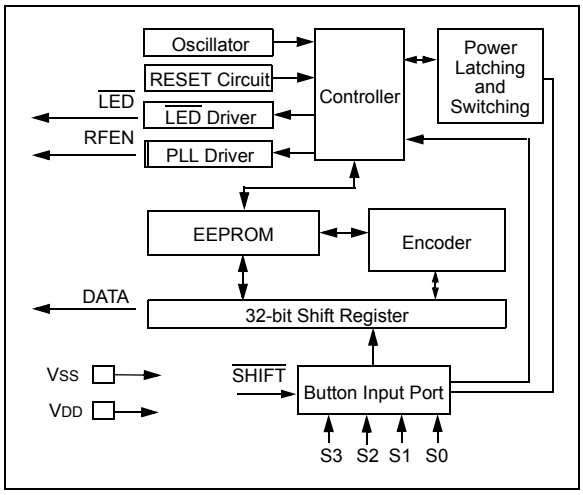
Enhanced Features Over HCS300

- 60-bit seed vs. 32-bit seed
- 2-bit CRC for error detection
- 28/32-bit serial number select
- Tunable oscillator (+/-10% over specified voltage ranges)
- Time bits option
- Queue bits
- TSSOP package
- Programmable Time-out and Guard Time

PACKAGE TYPES



HCS362 BLOCK DIAGRAM



Typical Applications

The HCS362 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

- Automotive RKE systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Identity tokens
- Burglar alarm systems

© 2011 Microchip Technology Inc.

GENERAL DESCRIPTION

The HCS362 is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS362 utilizes the KEELOQ® code hopping technology, which incorporates high security, a small package outline and low cost, to make this device a perfect solution for unidirectional remote keyless entry systems and access control systems.

The HCS362 combines a 32-bit hopping code generated by a nonlinear encryption algorithm, with a 28/32-bit serial number and 9/5 status bits to create a 69-bit transmission stream. The length of the transmission eliminates the threat of code scanning. The code hopping mechanism makes each transmission unique, thus rendering code capture and resend (code grabbing) schemes useless.

The crypt key, serial number and configuration data are stored in an EEPROM array which is not accessible via any external connection. The EEPROM data is programmable but read protected. The data can be verified only after an automatic erase and programming operation. This protects against attempts to gain access to keys or manipulate synchronization values. The HCS362 provides an easy to use serial interface for programming the necessary keys, system parameters and configuration data.

1.0 SYSTEM OVERVIEW

Key Terms

The following is a list of key terms used throughout this data sheet. For additional information on KEELOQ and Code Hopping, refer to Technical Brief 3 (TB003).

- **RKE** - Remote Keyless Entry
- **Button Status** - Indicates what button input(s) activated the transmission. Encompasses the 4 button status bits S3, S2, S1 and S0 (Figure 3-2).
- **Code Hopping** - A method by which a code, viewed externally to the system, appears to change unpredictably each time it is transmitted.
- **Code word** - A block of data that is repeatedly transmitted upon button activation (Figure 3-2).
- **Transmission** - A data stream consisting of repeating code words (Figure 8-1).
- **Crypt key** - A unique and secret 64-bit number used to encrypt and decrypt data. In a symmetrical block cipher such as the KEELOQ algorithm, the encryption and decryption keys are equal and will therefore be referred to generally as the crypt key.
- **Encoder** - A device that generates and encodes data.
- **Encryption Algorithm** - A recipe whereby data is scrambled using a crypt key. The data can only be interpreted by the respective decryption algorithm using the same crypt key.
- **Decoder** - A device that decodes data received from an encoder.
- **Decryption algorithm** - A recipe whereby data scrambled by an encryption algorithm can be unscrambled using the same crypt key.
- **Learn** – Learning involves the receiver calculating the transmitter's appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter value and crypt key in EEPROM. The KEELOQ product family facilitates several learning strategies to be implemented on the decoder. The following are examples of what can be done.
  - **Simple Learning**
    The receiver uses a fixed crypt key, common to all components of all systems by the same manufacturer, to decrypt the received code word's encrypted portion.
  - **Normal Learning**
    The receiver uses information transmitted during normal operation to derive the crypt key and decrypt the received code word's encrypted portion.
  - **Secure Learn**
    The transmitter is activated through a special button combination to transmit a stored 60-bit seed value used to generate the transmitter's crypt key. The receiver uses this seed value to derive the same crypt key and decrypt the received code word's encrypted portion.
- **Manufacturer's code** – A unique and secret 64-bit number used to generate unique encoder crypt keys. Each encoder is programmed with a crypt key that is a function of the manufacturer's code. Each decoder is programmed with the manufacturer code itself.

The HCS362 code hopping encoder is designed specifically for keyless entry systems; primarily vehicles and home garage door openers. The encoder portion of a keyless entry system is integrated into a transmitter, carried by the user and operated to gain access to a vehicle or restricted area. The HCS362 is meant to be a cost-effective yet secure solution to such systems, requiring very few external components (Figure 2-1).

Most low-end keyless entry transmitters are given a fixed identification code that is transmitted every time a button is pushed. The number of unique identification codes in a low-end system is usually a relatively small number. These shortcomings provide an opportunity for a sophisticated thief to create a device that 'grabs' a transmission and retransmits it later, or a device that quickly 'scans' all possible identification codes until the correct one is found.

The HCS362, on the other hand, employs the KEELOQ code hopping technology coupled with a transmission length of 66 bits to virtually eliminate the use of code 'grabbing' or code 'scanning'. The high security level of

© 2011 Microchip Technology Inc.

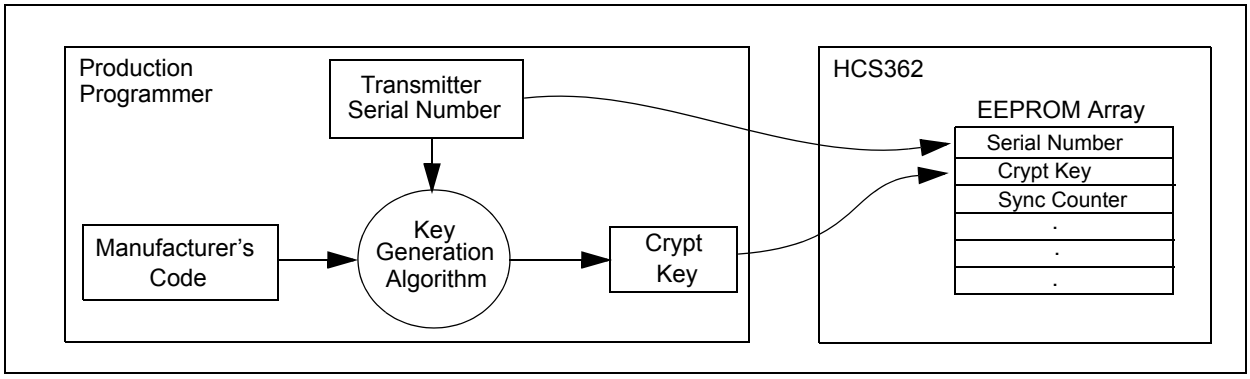
the HCS362 is based on the patented KEELOQ technology. A block cipher based on a block length of 32 bits and a key length of 64 bits is used. The algorithm obscures the information in such a way that even if the transmission information (before coding) differs by only one bit from that of the previous transmission, the next coded transmission will be completely different. Statistically, if only one bit in the 32-bit string of information changes, greater than 50 percent of the coded transmission bits will change.

As indicated in the block diagram on page one, the HCS362 has a small EEPROM array which must be loaded with several parameters before use; most often programmed by the manufacturer at the time of production. The most important of these are:

- A 28-bit serial number, typically unique for every encoder
- A crypt key
- An initial 16-bit synchronization value
- A 16-bit configuration value

The crypt key generation typically inputs the transmitter serial number and 64-bit manufacturer's code into the key generation algorithm (Figure 1-1). The manufacturer's code is chosen by the system manufacturer and must be carefully controlled as it is a pivotal part of the overall system security.

FIGURE 1-1: CREATION AND STORAGE OF CRYPT KEY DURING PRODUCTION



The 16-bit synchronization counter is the basis behind the transmitted code word changing for each transmission; it increments each time a button is pressed. Due to the code hopping algorithm's complexity, each increment of the synchronization value results in greater than 50% of the bits changing in the transmitted code word.

Figure 1-2 shows how the key values in EEPROM are used in the encoder. Once the encoder detects a button press, it reads the button inputs and updates the synchronization counter. The synchronization counter and crypt key are input to the encryption algorithm and the output is 32 bits of encrypted information. This data will change with every button press, its value appearing externally to 'randomly hop around', hence it is referred to as the hopping portion of the code word. The 32-bit hopping code is combined with the button information and serial number to form the code word transmitted to the receiver. The code word format is explained in greater detail in Section 3.1.

A receiver may use any type of controller as a decoder, but it is typically a microcontroller with compatible firmware that allows the decoder to operate in conjunction with an HCS362 based transmitter. Section 6.0 provides detail on integrating the HCS362 into a system.

A transmitter must first be 'learned' by the receiver before its use is allowed in the system. Learning includes calculating the transmitter's appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter value and crypt key in EEPROM.

In normal operation, each received message of valid format is evaluated. The serial number is used to determine if it is from a learned transmitter. If from a learned transmitter, the message is decrypted and the synchronization counter is verified. Finally, the button status is checked to see what operation is requested. Figure 1-3 shows the relationship between some of the values stored by the receiver and the values received from the transmitter.

© 2011 Microchip Technology Inc.

FIGURE 1-2: BUILDING THE TRANSMITTED CODE WORD (ENCODER)

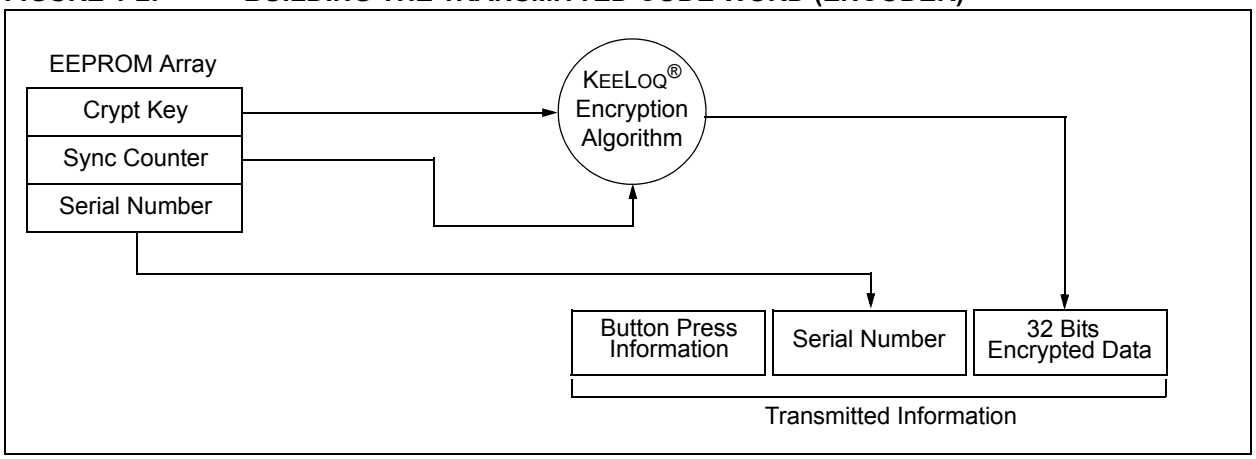
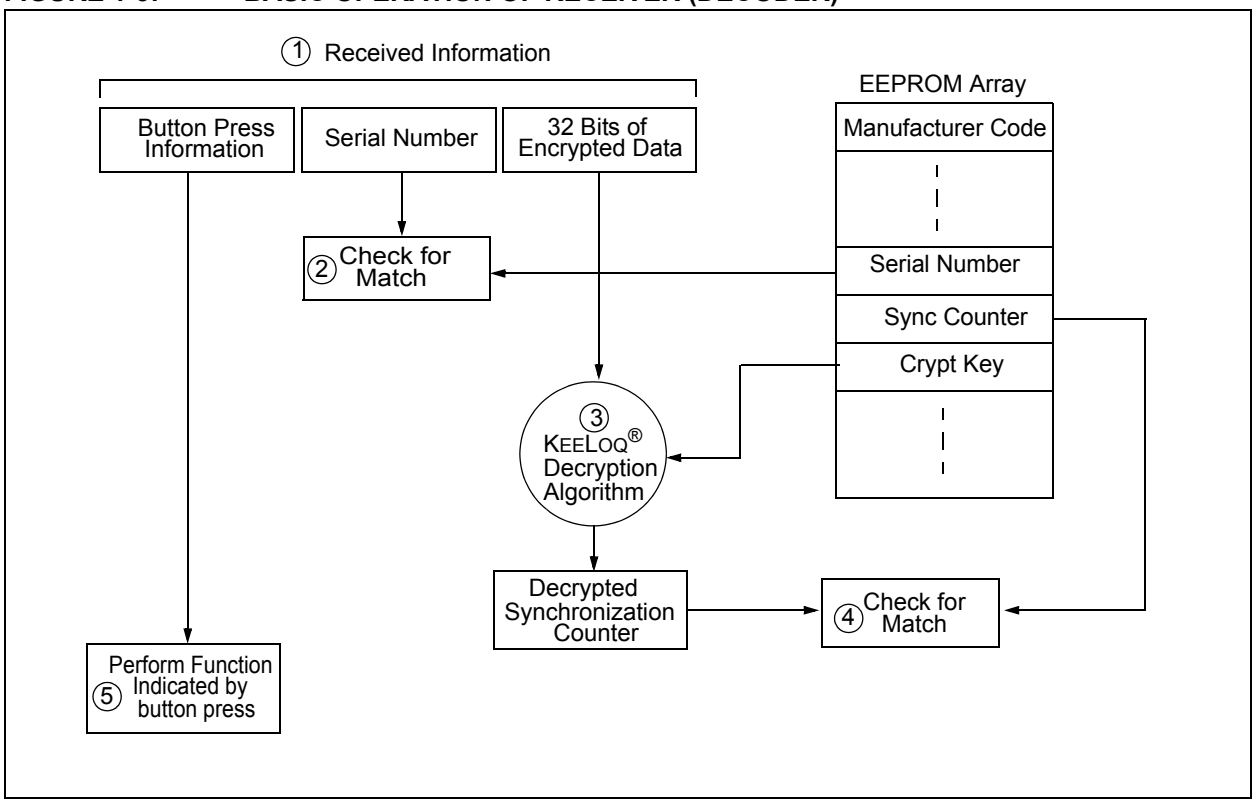


FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



NOTE: Circled numbers indicate the order of execution.

© 2011 Microchip Technology Inc.

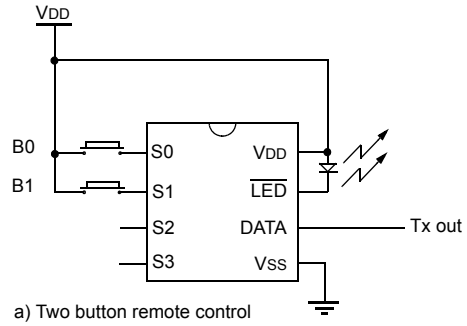
2.0 DEVICE DESCRIPTION

As shown in the typical application circuits (Figure 2-1), the HCS362 is a simple device to use. It requires only the addition of buttons and RF circuitry for use as the transmitter in your security application. See Table 2-1 for a description of each pin and Figure 2-1 for typical circuits. Figure 2-2 shows the device I/O circuits.

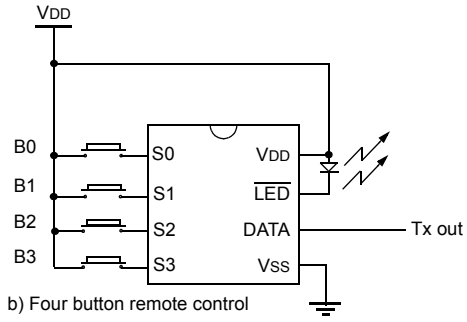
TABLE 2-1: PIN DESCRIPTIONS

Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2 / Clock pin when in Programming mode
S3/ RFEN	4	Switch input 3 / RF enable output
VSS	5	Ground reference connection
DATA	6	Data output pin / DATA I/O pin for Programming mode
$\overline{\text{LED}}$/ $\overline{\text{SHIFT}}$	7	Cathode connection for $\overline{\text{LED}}$ and DUAL mode $\overline{\text{SHIFT}}$ input
VDD	8	Positive supply voltage

FIGURE 2-1: TYPICAL CIRCUITS

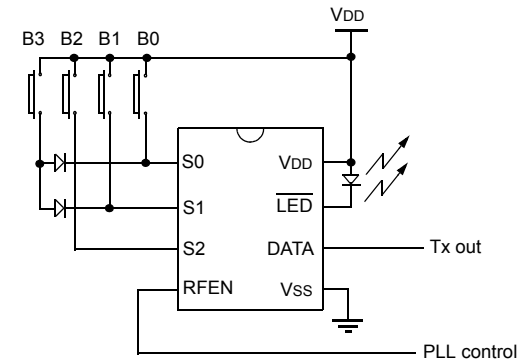


a) Two button remote control

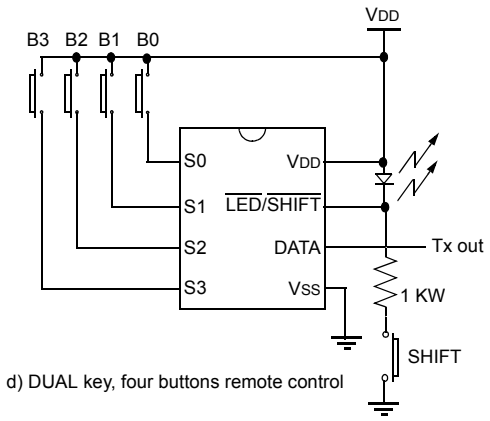


b) Four button remote control with PLL output **(Note)**

Note: Up to 15 functions can be implemented by pressing more than one button simultaneously or by using a suitable diode array.

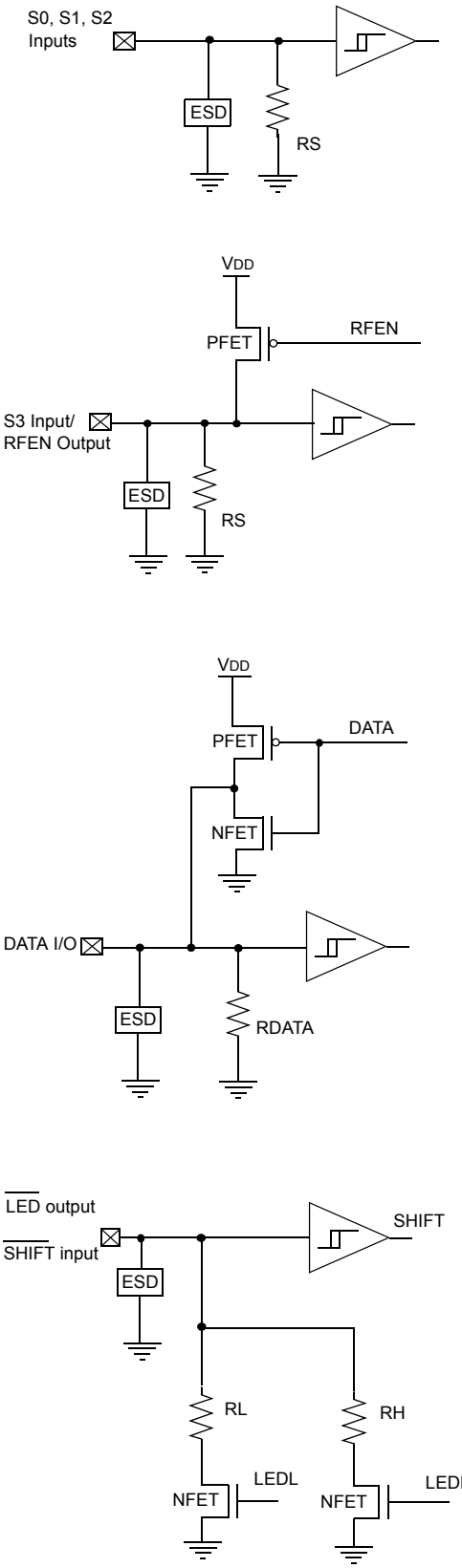


c) Four button remote control with RF Enable



d) DUAL key, four buttons remote control

FIGURE 2-2: I/O CIRCUITS



2.1 Architectural Overview

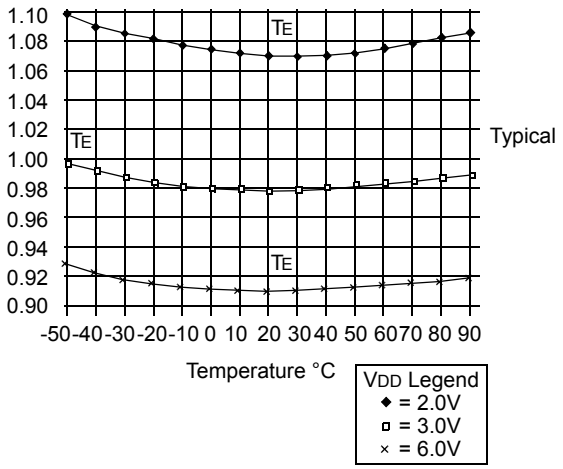
2.1.1 ONBOARD EEPROM

The HCS362 has an onboard non-volatile EEPROM, which is used to store user programmable data. The data can be programmed at the time of production and include the security-related information such as encoder keys, serial numbers, discrimination and seed values. All the security related options are read protected. The HCS362 has built in protection against counter corruption. Before every EEPROM write, the internal circuitry also ensures that the high voltage required to write to the EEPROM is at an acceptable level.

2.1.2 INTERNAL RC OSCILLATOR

The HCS362 has an onboard RC oscillator that controls all the logic output timing characteristics. The oscillator frequency varies within ±10% of the nominal value (once calibrated over a voltage range of 2V – 3.5V or 3.5V – 6.3V). All the timing values specified in this document are subject to the oscillator variation.

FIGURE 2-3: HCS362 NORMALIZED TE VS. TEMPERATURE



Note: Values are for calibrated oscillator

2.1.3 LOW VOLTAGE DETECTOR

A low battery voltage detector onboard the HCS362 can indicate when the operating voltage drops below a predetermined value. There are eight options available depending on the VLOW[0..2] configuration options. The options provided are:

000 - 2.0V	100 - 4.0V
001 - 2.1V	101 - 4.2V
010 - 2.2V	110 - 4.4V
011 - 2.3V	111 - 4.6V

© 2011 Microchip Technology Inc.

FIGURE 2-4: HCS362 VLOW DETECTOR (TYPICAL)

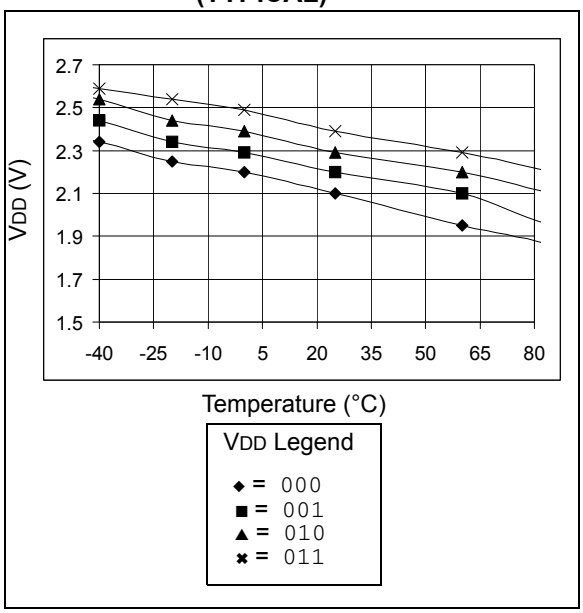
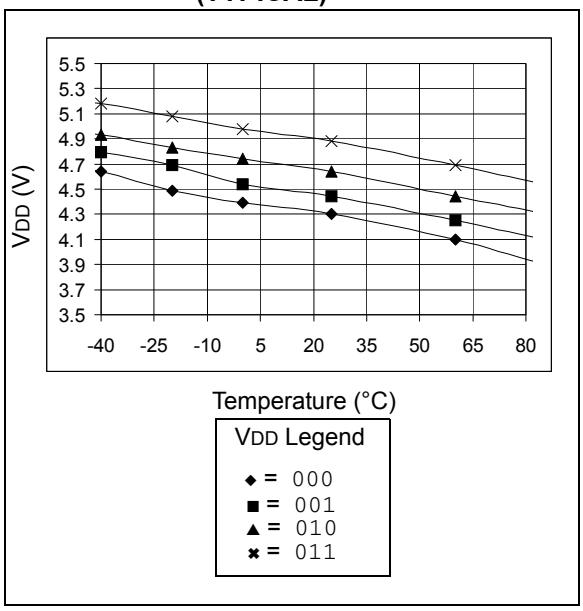


FIGURE 2-5: HCS362 VLOW DETECTOR (TYPICAL)



The output of the low voltage detector is transmitted in each code word, so the decoder can give an indication to the user that the transmitter battery is low. Operation of the $\overline{\text{LED}}$ changes as well to further indicate that the battery is low and needs replacing.

2.2 Dual Encoder Operation

The HCS362 contains two crypt keys (possibly derived from two different Manufacturer's Codes), but only one Serial Number, one set of Discrimination bits, one 16-bit Synchronization Counter and a single 60-bit Seed value. For this reason the HCS362 can be used as an encoder in multiple (two) applications as far as they share the same configuration: transmission format, baud rate, header and guard settings. The SHIFT input pin (multiplexed with the LED output) is used to select between the two crypt keys.

A logic 1 on the $\overline{\text{SHIFT}}$ input pin selects the first crypt key.

A logic 0 on the $\overline{\text{SHIFT}}$ input pin will select the second crypt key.

3.0 DEVICE OPERATION

The HCS362 will wake-up upon detecting a switch closure and then delay for switch debounce (Figure 3-1). The synchronization information, fixed information and switch information will be encrypted to form the hopping code. The encrypted or hopping code portion of the transmission will change every time a button is pressed, even if the same button is pushed again. Keeping a button pressed for a long time will result in the same code word being transmitted until the button is released or time-out occurs.

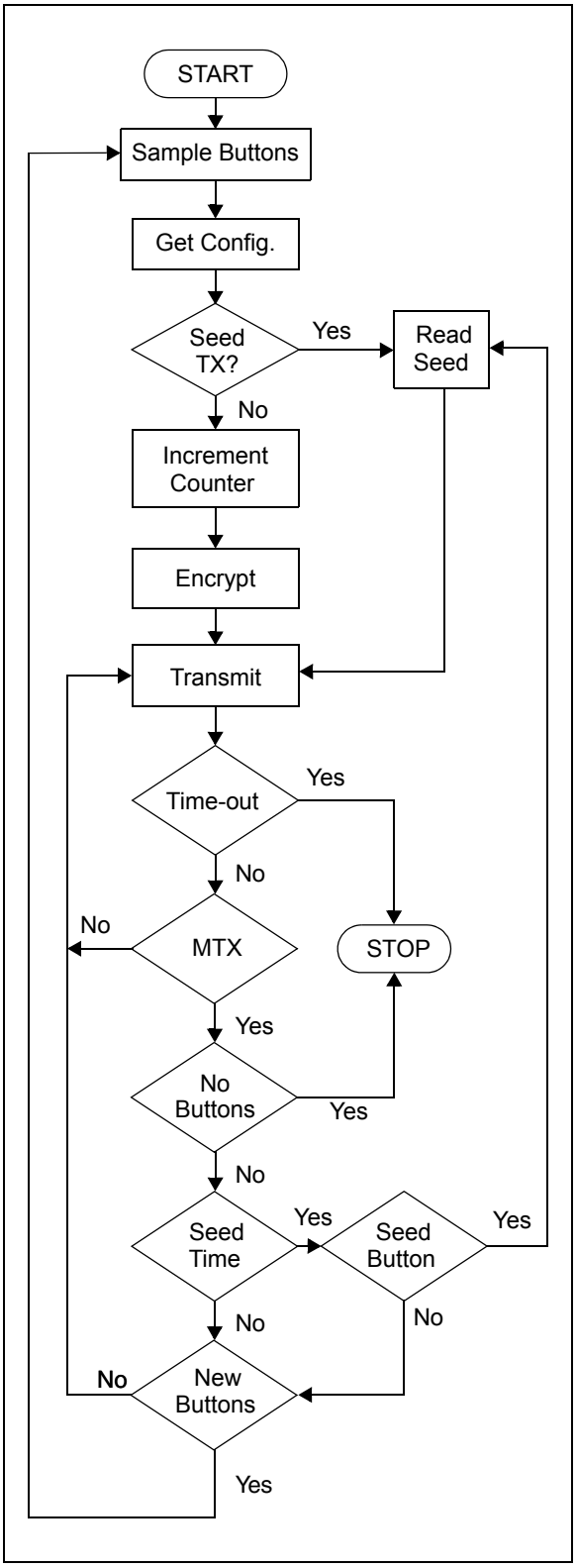
The time-out time can be selected with the Time-out (TIMOUT[0..1]) configuration option. This option allows the time-out to be disabled or set to 0.8 s, 3.2 s or 25.6 s. When a time-out occurs, the device will go into SLEEP mode to protect the battery from draining when a button gets stuck.

If in the transmit process, it is detected that a new button is pressed, the current code word will be aborted. A new code word will be transmitted and the time-out counter will RESET. If all the buttons are released, the minimum code words will be completed. The minimum code words can be set to 1,2,4 or 8 using the Minimum Code Words (MTX[0..1]) configuration option. If the time for transmitting the minimum code words is longer than the time-out time, the device will not complete the minimum code words.

Note:	Buttons removed will not have any effect on the code word unless no buttons remain pressed in which case the current code word will be completed and the power-down will occur.

A code that has been transmitted will not occur again for more than 64K transmissions. This will provide more than 18 years of typical use before a code is repeated based on 10 operations per day. Overflow information programmed into the encoder can be used by the decoder to extend the number of unique transmissions to more than 192K.

FIGURE 3-1: BASIC FLOW DIAGRAM OF THE DEVICE OPERATION



© 2011 Microchip Technology Inc.

3.1 Transmission Modulation Format

The HCS362 transmission is made up of several code words. Each code word starts with a preamble and a header, followed by the data (see Figure 3-1 and Figure 3-2).

The code words are separated by a **Guard Time** that can be set to 0 ms, 6.4 ms, 25.6 ms or 76.8 ms with the Guard Time Select (GUARD[0..1]) configuration option. All other timing specifications for the modulation formats are based on a basic timing element (TE). This **Timing Element** can be set to 100 µs, 200 µs, 400 µs or 800 µs with the Baud Rate Select (BSEL[0..1]) configuration option. The **Header Time** can be set to 3 TE or 10 TE with the Header Select (HEADER) Configuration option.

There are two different modulation formats available on the HCS362 that can be set according to the Modulation Select (MOD) configuration option:

- Pulse Width Modulation (PWM)
- Manchester Encoding

The various formats are shown in Figure 3-3 and Figure 3-4.

FIGURE 3-2: CODE WORD TRANSMISSION SEQUENCE

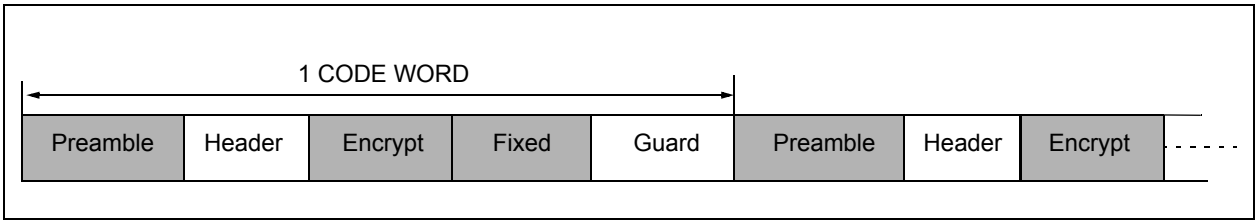


FIGURE 3-3: TRANSMISSION FORMAT (PWM)

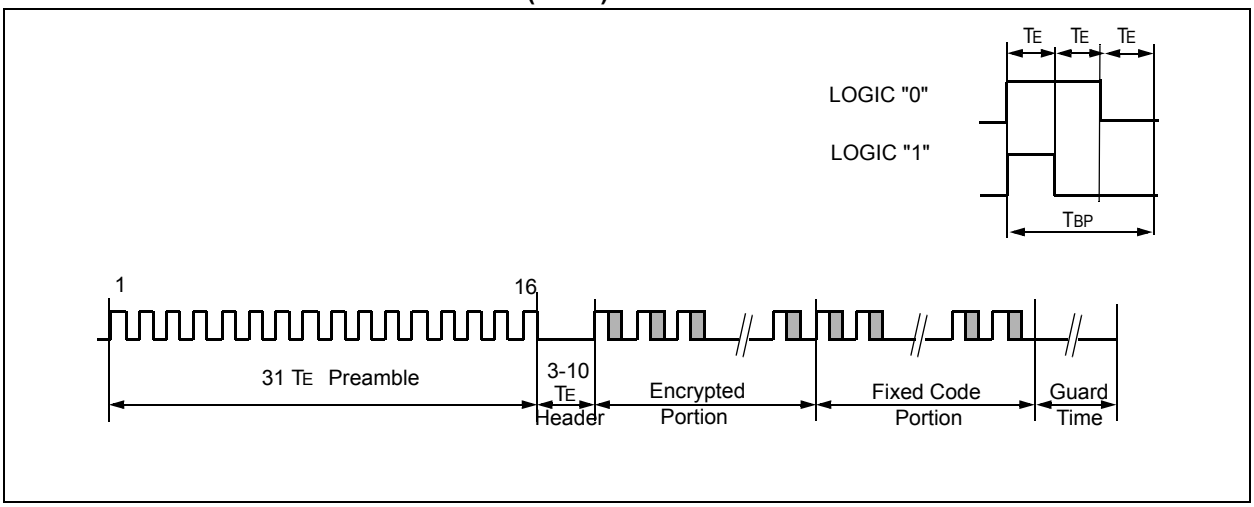
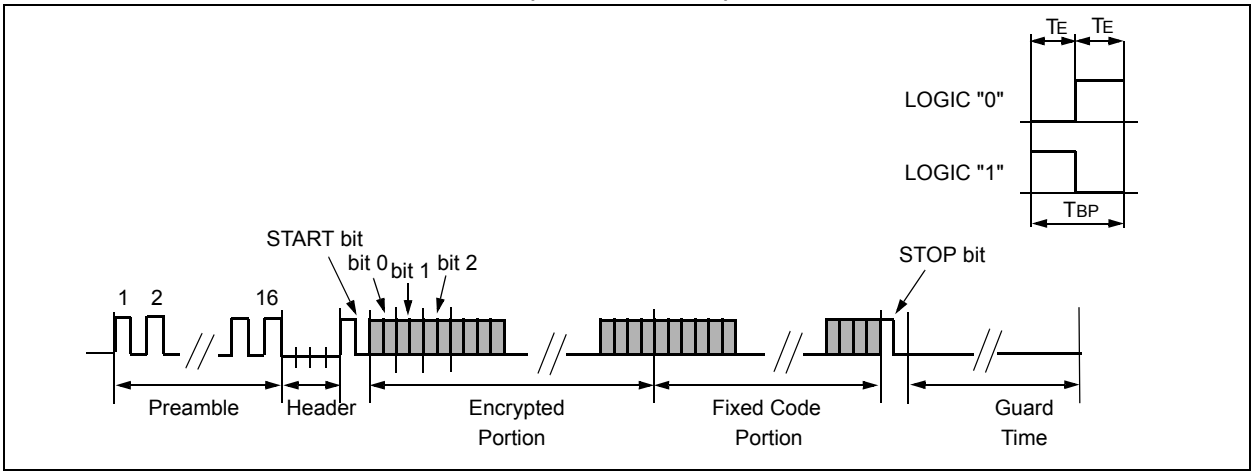


FIGURE 3-4: TRANSMISSION FORMAT (MANCHESTER)



3.1.1 CODE HOPPING DATA

The hopping portion is calculated by encrypting the counter, discrimination value and function code with the Encoder Key (KEY). The counter is a 16-bit counter. The discrimination value is 10 bits long and there are 2 counter overflow bits (OVR) that are cleared when the counter wraps to 0. The rest of the 32 bits are made up of the function code also known as the button inputs.

3.1.2 FIXED CODE DATA

The 32 bits of fixed code consist of 28 bits of the serial number (SER) and another copy of the function code. This can be changed to contain the whole 32-bit serial number with the Extended Serial Number (XSER) configuration option.

3.1.3 STATUS INFORMATION

The status bits will always contain the output of the Low Voltage detector (VLOW), the Cyclic Redundancy Check (CRC) bits (or TIME bits depending on CTSEL) and the Button Queue information.

3.1.3.1 Low Voltage Detector Status (VLOW)

The output of the low voltage detector is transmitted with each code word. If VDD drops below the selected voltage, a logic '1' will be transmitted. The output of the detector is sampled before each code word is transmitted.

3.1.3.2 Button Queue Information (QUEUE)

The queue bits indicate a button combination was pressed again within 2 s after releasing the previous activation. Queuing or repeated pressing of the same buttons (or button combination) is detected by the HCS362 button debouncing circuitry.

The Queue bits are added as the last two bits of the standard code word. The queue bits are a 2-bit counter that does not wrap. The counter value starts at '00b' and is incremented, if a button is pushed within 2 s of the previous button press. The current code word is terminated when the buttons are queued. This allows additional functionality for repeated button presses.

The button inputs are sampled every 6.4 ms during this 2 s period.

00 - first activation

01 - second activation

10 - third activation

11 - from fourth activation on

3.1.3.3 Cyclic Redundancy Check (CRC)

The CRC bits are calculated on the 65 previously transmitted bits. The decoder can use the CRC bits to check the data integrity before processing starts. The CRC can detect all single bit errors and 66% of double bit errors. The CRC is computed as follows:

EQUATION 3-1: CRC Calculation

$$CRC[1]_{n+1} = CRC[0]_n \oplus Di_n$$

and

$$CRC[0]_{n+1} = (CRC[0]_n \oplus Di_n) \oplus CRC[1]_n$$

with

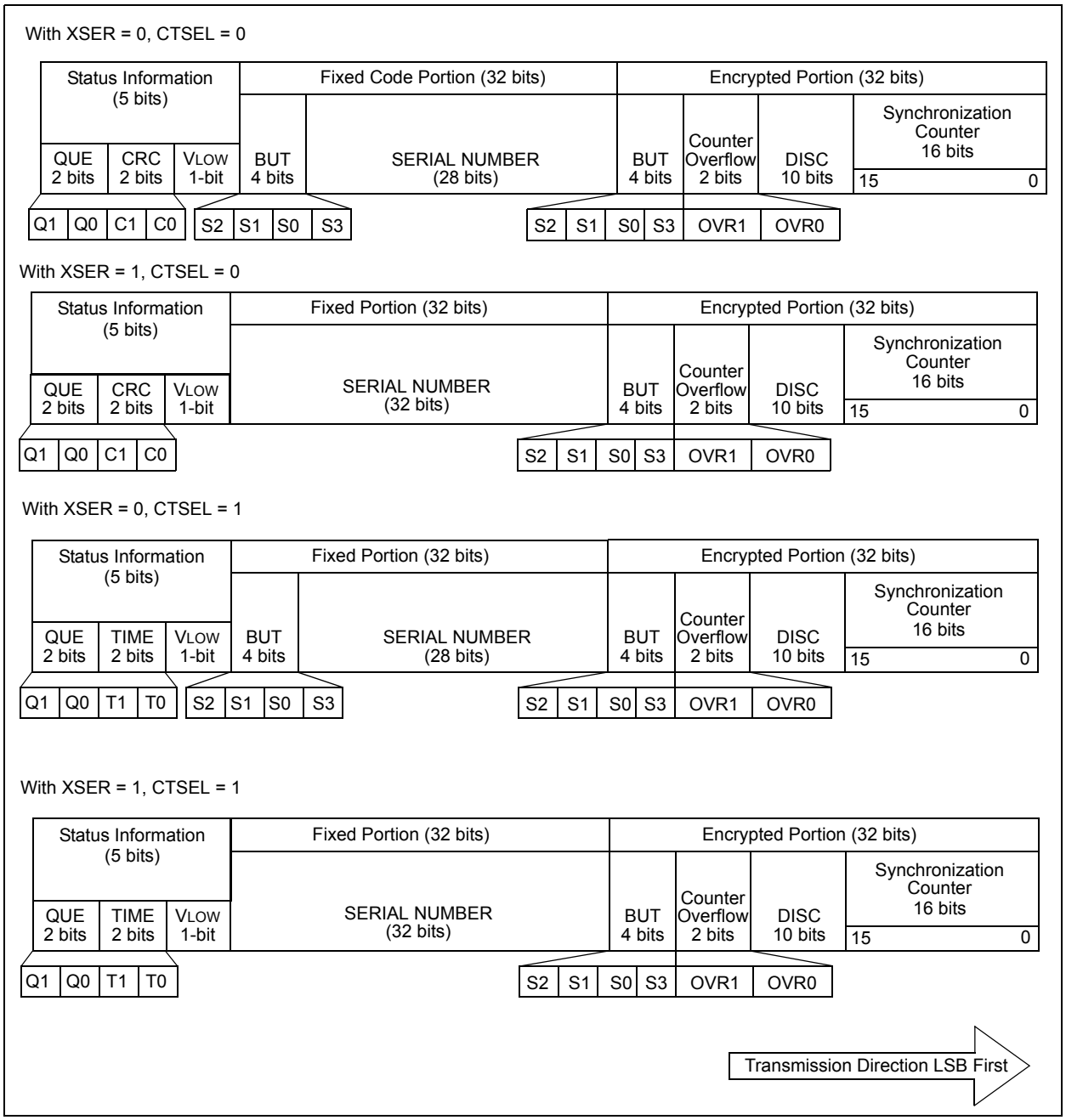
$$CRC[1, 0]_0 = 0$$

and Di_n the nth transmission bit $0 \leq n \leq 64$

Note:	The CRC may be wrong when the battery voltage is around either of the VLOW trip points. This may happen because VLOW is sampled twice each transmission, once for the CRC calculation (PWM is LOW) and once when VLOW is transmitted (PWM is HIGH). VDD tends to move slightly during a transmission which could lead to a different value for VLOW being used for the CRC calculation and the transmission. **Work around:** If the CRC is incorrect, recalculate for the opposite value of VLOW.

© 2011 Microchip Technology Inc.

FIGURE 3-5: CODE WORD DATA FORMAT



3.1.4 MINIMUM CODE WORDS

MTX[0..1] configuration bits selects the minimum number of code words that will be transmitted. If the button is released after 1.6 s (or greater) and MTX code words have been transmitted, the code word being transmitted will be terminated. The possible values are:

00 - 1

01 - 2

10 - 4

11 - 8

3.1.5 TIME BITS

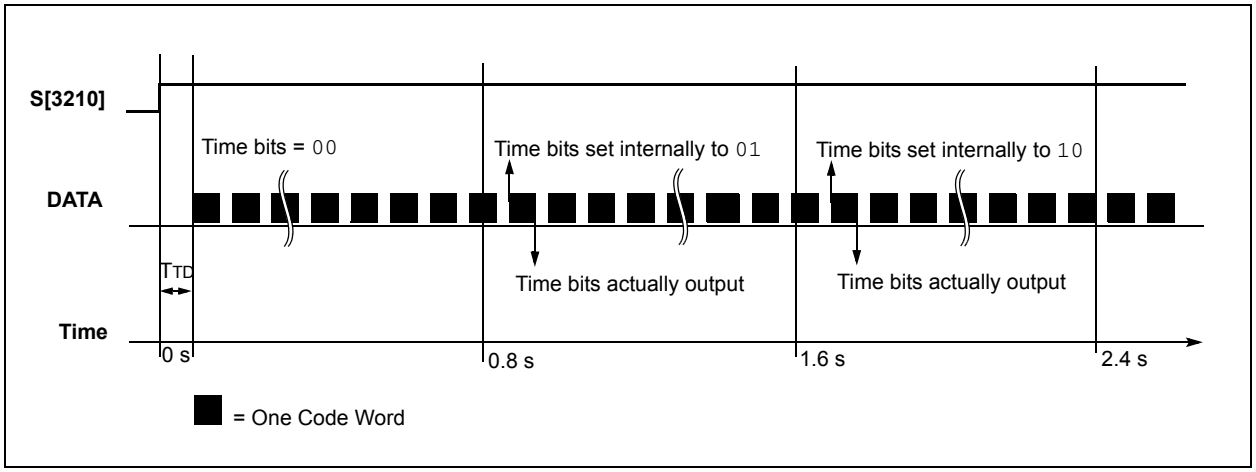
The time bits indicate the duration that the inputs were activated:

00 - immediate
01 - after 0.8 s
10 - after 1.6 s
11 - after 2.4 s

The TIME bits are incremented every 0.8 s and does not wrap once it reaches '11'.

Time information is alternative to the CRC bits availability and is selected by the CTSEL configuration bit.

FIGURE 3-6: TIME BITS OPERATION

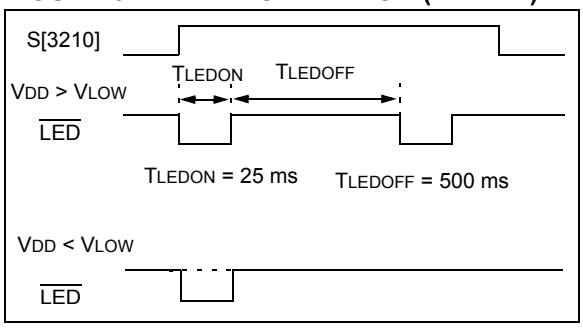


3.2 $\overline{\text{LED}}$ Output

The $\overline{\text{LED}}$ pin will be driven LOW periodically while the HCS362 is transmitting data, in order to switch on an external LED.

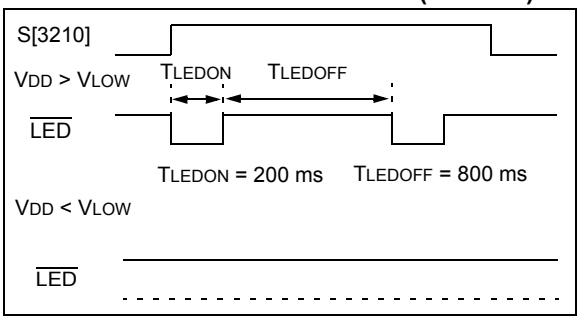
The duty cycle (TLEDON/TLEDOFF) can be selected between two possible values by the configuration option (LED).

FIGURE 3-7: LED OPERATION (LED = 1)



The same configuration option determines whether when the VDD Voltage drops below the selected VLOW trip point, the LED will blink only once or stop blinking.

FIGURE 3-8: LED OPERATION (LED = 0)



Note: When the HCS362 encoder is used as a Dual Encoder the $\overline{\text{LED}}$ pin is used as a $\overline{\text{SHIFT}}$ input (Figure 2-2). In such a configuration the LED is always ON during transmission. To keep power consumption low, it is recommended to use a series resistor of relatively high value. VLOW information is not available when using the second Encryption Key.

© 2011 Microchip Technology Inc.

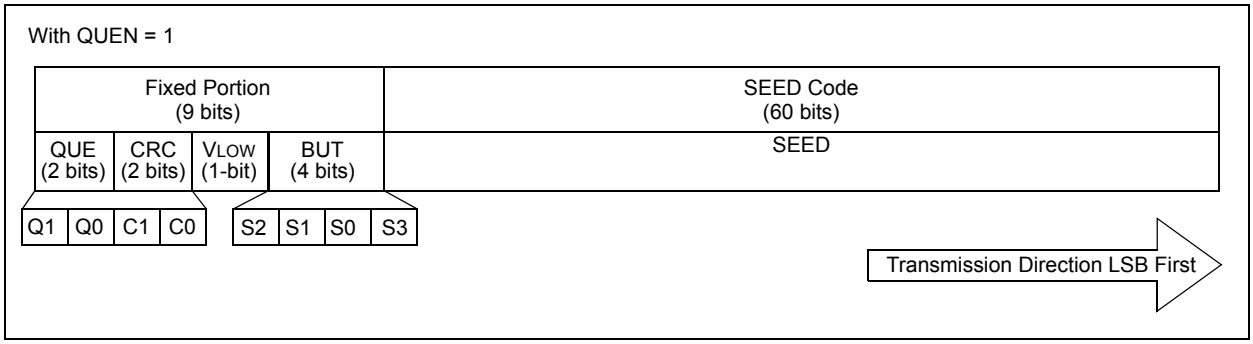
3.3 Seed Code Word Data Format

A seed transmission transmits a code word that consists of 60 bits of fixed data that is stored in the EEPROM. This can be used for secure learning of encoders or whenever a fixed code transmission is required. The seed code word further contains the function code and the status information (VLOW, CRC and QUEUE) as configured for normal code hopping code words. The seed code word format is shown in Figure 3-9. The function code for seed code words is always '1111b'.

Seed code words can be configured as follows:

- Enabled permanently.
- Disabled permanently.
- Enabled until the synchronization counter is greater than 7Fh, this configuration is often referred to as **Limited Seed**.
- The time before the seed code word is transmitted can be set to 1.6 s or 3.2 s, this configuration is often referred to as **Delayed Seed**. When this option is selected, the HCS362 will transmit a code hopping code word for 1.6 s or 3.2 s, before the seed code word is transmitted.

FIGURE 3-9: SEED CODE WORD FORMAT



3.3.1 SEED OPTIONS

The button combination (S[3210]) for transmitting a Seed code word can be selected with the Seed and SeedC (SEED[0..1] and SEEDC) configuration options as shown in Table 3-1 and Table 3-2:

TABLE 3-1: SEED OPTIONS (SEEDC = 0)

SEED	Seed S[3210]	1.6 s Delayed Seed S[3210]
00	–	–
01	0101*	0001*
10	0101	0001
11	0101	–
Note:	*Limited Seed	

TABLE 3-2: SEED OPTIONS (SEEDC = 1)

SEED	Seed S[3210]	3.2 s Delayed Seed S[3210]
00	–	–
01	1001*	0011*
10	1001	0011
11	1001	–
Note:	*Limited Seed	

Example A): Selecting SEEDC = 1 and SEED = 11: makes SEED transmission available every time the combination of buttons S3 and S0 is pressed simultaneously, but Delayed Seed mode is not available.

Example B): Selecting SEEDC = 0 and SEED = 01: makes SEED transmission available only for a limited time (only up to 128 times). The combination of buttons S2 and S0 produces an immediate transmission of the SEED code. Pressing and holding for more than 1.6 seconds the S0 button alone, produces the SEED code word transmission (Delayed Seed).

3.4 RF Enable and PLL Interface

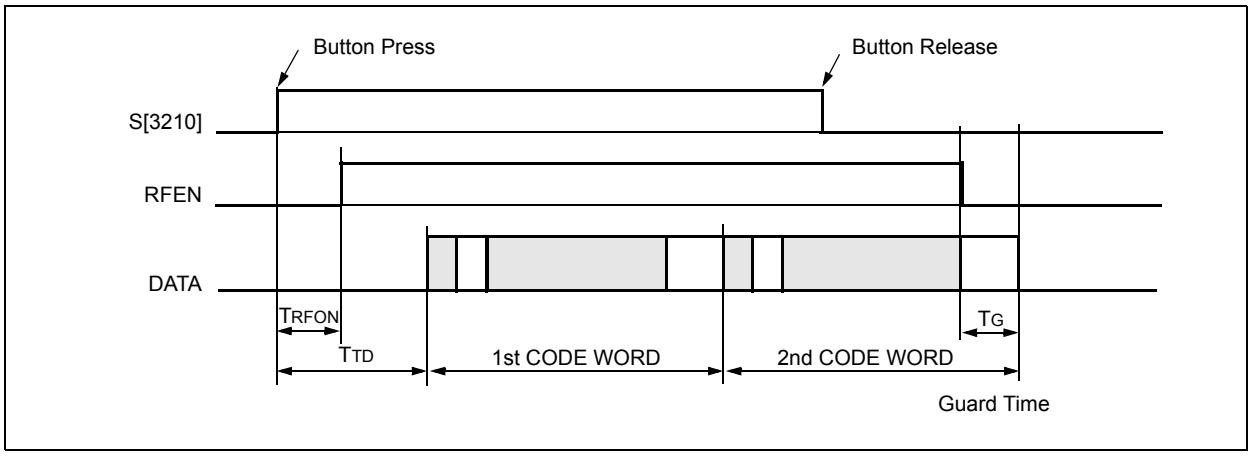
The S3/RFEN pin of the HCS362 can be configured to function as an RF Enable output signal. This is selected by the RF Enable Output (RFEN) configuration option. When enabled, this pin will be driven HIGH before data is transmitted through the DATA pin.

The RF Enable and DATA output are synchronized so to interface with RF PLL circuits operating in ASK mode. Figure 3-10 shows the startup sequence. The RFEN signal will go LOW at the end of the last code word, including the Guard time.

When the RF Enable output is selected, the S3 pin can still be used as a button input. The debouncing logic will be affected though, considerably reducing the responsiveness of the button input.

Note: When the RF Enable output feature is used and a four (or more) buttons input configuration is required, the use of a scheme similar to Figure 2-1 (scheme C) is recommended.

FIGURE 3-10: PLL INTERFACE



© 2011 Microchip Technology Inc.

4.0 EEPROM MEMORY ORGANIZATION

The HCS362 contains 288 bits (18 x 16-bit words) of EEPROM memory (Table 4-1). This EEPROM array is used to store the encryption key information and synchronization value. Further descriptions of the memory array is given in the following sections.

TABLE 4-1: EEPROM MEMORY MAP

Word Address	Field	Description
0	KEY1_0	64-bit Encryption Key1 (Word 0) LSB
1	KEY1_1	64-bit Encryption Key1 (Word 1)
2	KEY1_2	64-bit Encryption Key1 (Word 2)
3	KEY1_3	64-bit Encryption Key1 (Word 3) MSB
4	KEY2_0	64-bit Encryption Key2 (Word 0) LSB
5	KEY2_1	64-bit Encryption Key2 (Word 1)
6	KEY2_2	64-bit Encryption Key2 (Word 2)
7	KEY2_3	64-bit Encryption Key2 (Word 3) MSB
8	SEED_0	Seed value (Word 0) LSB
9	SEED_1	Seed value (Word 1)
10	SEED_2	Seed value (Word 2)
11	SEED_3	Seed value (Word 3) MSB
12	CONFIG_0	Configuration Word (Word 0)
13	CONFIG_1	Configuration Word (Word 1)
14	SERIAL_0	Serial Number (Word 0) LSB
15	SERIAL_1	Serial Number (Word 1) MSB
16	SYNC	Synchronization counter
17	RES	Reserved – Set to zero

4.1 KEY_0 - KEY_3 (64-bit Crypt Key)

The 64-bit crypt key is used to create the encrypted message transmitted to the receiver. This key is calculated and programmed during production using a key generation algorithm. The key generation algorithm may be different from the KEELOQ algorithm. Inputs to the key generation algorithm are typically the transmitter's serial number and the 64-bit manufacturer's code. While the key generation algorithm supplied from Microchip is the typical method used, a user may elect to create their own method of key generation. This may be done providing that the decoder is programmed with the same means of creating the key for decryption purposes.

4.2 SYNC (Synchronization Counter)

This is the 16-bit synchronization value that is used to create the hopping code for transmission. This value will be incremented after every transmission.

4.3 SEED_0, SEED_1, SEED_2, and SEED 3 (Seed Word)

This is the four word (60 bits) seed code that will be transmitted when seed transmission is selected. This allows the system designer to implement the secure learn feature or use this fixed code word as part of a different key generation/tracking process or purely as a fixed code transmission.

Note:	Upper four Significant bits of SEED_3 contains extra configuration information (see Table 4-4).

4.4 SERIAL_0, SERIAL_1 (Encoder Serial Number)

SER_0 and SER_1 are the lower and upper words of the device serial number, respectively. There are 32 bits allocated for the serial number and a selectable configuration bit determines whether 32 or 28 bits will be transmitted. The serial number is meant to be unique for every transmitter.

4.5 Configuration Words

There are 36 configuration bits stored in the EEPROM array. They are used by the device to determine transmission speed, format, delays and Guard times. They are grouped in three Configuration Words: CONFIG_0, CONFIG_1 and the upper nibble of the SEED_3 word. A description of each of the bits follows this section.

TABLE 4-2: CONFIG_0

Bit Address	Field	Description	Values
0	OSC_0	Oscillator adjust	0000 - nominal 1000 - fastest 0111 - slowest
1	OSC_1		
2	OSC_2		
3	OSC_3		
4	VLOW_0	VLOW select	nominal values 000 - 2.0V 100 - 4.0V 001 - 2.1V 101 - 4.2V 010 - 2.2V 110 - 4.4V 011 - 2.3V 111 - 4.6V
5	VLOW_1		
6	VLOW_2		
7	BSEL_0	Bitrate select	00 - TE = 100 µs 01 - TE = 200 µs 10 - TE = 400 µs 11 - TE = 800 µs
8	BSEL_1		
9	MTX_0	Minimum number of code words	00 - 1 01 - 2 10 - 4 11 - 8
10	MTX_1		
11	GUARD_0	Guard time select	00 - 0 ms (1 TE) 01 - 6.4 ms + 2 TE 10 - 25.6 ms + 2 TE 11 - 76.8 ms + 2 TE
12	GUARD_1		
13	TIMOUT_0	Time-out select	00 - No Time-out 01 - 0.8 s to 0.8 s + 1 code word 10 - 3.2 s to 3.2 s + 1 code word 11 - 25.6 s to 25.6 s + 1 code word
14	TIMOUT_1		
15	CTSEL	CTSEL	0 = TIME bits 1 = CRC bits

4.5.1 OSC

The internal oscillator can be tuned to ±10%. (0000 selects the nominal value, 1000 the fastest value and 0111 the slowest). When programming the device, it is the programmer's responsibility to determine the optimal calibration value.

4.5.2 VLOW[0..2]

The low voltage threshold can be programmed to be any of the values shown in the following table:

4.5.3 BSEL[0..1]

The basic timing element TE, determines the actual transmission Baud Rate. This translates to different code word lengths depending on the encoding format selected (Manchester or PWM), the Header length selection and the Guard time selection, from approximately 40 ms up to 220 ms. Refer to Table 8-4 and Table 8-5 for a more complete description.

4.5.4 MTX[0..1]

MTX selects the minimum number of code words that will be transmitted. A minimum of 1, 2, 4 or 8 code words will be transmitted.

Note:	If MTX and BSEL settings in combination require a transmission sequence to exceed the TIMOUT setting, TIMOUT will take priority.

© 2011 Microchip Technology Inc.

4.5.5 GUARD

The Guard time between code words can be set to 0 ms, 6.4 ms, 25.6 ms and 76.8 ms. If during a series of code words, the output changes from Hopping Code to Seed the Guard time will increase by 3 x TE.

4.5.6 TIMOUT[0..1]

The transmission time-out can be set to 0.8 s, 3.2 s, 25.6 s or no time-out. After the time-out period, the encoder will stop transmission and enter a low power Shutdown mode.

TABLE 4-3: CONFIG_1

Bit Address	Field	Description	Values
0	DISC_0	Discrimination bits	DISC[9:0]
1	DISC_1		
2	DISC_2		
...	...		
8	DISC_8		
9	DISC_9		
10	OVR_0	Overflow	OVR[1:0]
11	OVR_1		
12	XSER	Extended Serial Number	0 - Disable 1 - Enable
13	SEEDC	Seed Control	0 = Seed transmission on: S[3210] = 0001 (delay 1.6 s) S[3210] = 0101 (immediate) 1 = Seed transmission on: S[3210] = 0011 (delay 3.2 s) S[3210] = 1001 (immediate)
14	SEED_0	Seed options	00 - No Seed 01 - Limited Seed (Permanent and Delayed) 10 - Permanent and Delayed Seed 11 - Permanent Seed only
15	SEED_1		

4.5.7 DISC[0..9]

The discrimination bits are used to validate the decrypted code word. The discrimination value is typically programmed with the 10 Least Significant bits of the serial number or a fixed value.

4.5.8 OVR[0..1]

The overflow bits are used to extend the possible code combinations to 192K. If the overflow bits are not going to be used they can be programmed to zero.

4.5.9 XSER

If XSER is enabled a 32-bit serial number is transmitted. If XSER is disabled a 28-bit serial number and a 4-bit function code are transmitted.

4.5.10 SEED[0..1]

The seed value which is transmitted on key combinations (0011) and (1001) can be disabled, enabled or enabled for a limited number of transmissions determined by the initial counter value.

In limited Seed mode, the device will output the seed if the sync counter (Section 4.2) is from 00hex to 7Fhex. For a counter higher than 7F, a normal hopping code will be output.

Note:	Whenever a SEED code word is output, the 4 function bits (Figure 8-4) will be set to all ones [1,1,1,1].

4.5.11 SEEDC

SEEDC selects between seed transmission on 0001 and 0101 (SEEDC = 0) and 0011 and 1001 (SEEDC = 1). The delay before seed transmission is 1.6 s for (SEEDC = 0) and 3.2 s for (SEEDC = 1).

TABLE 4-4: SEED_3

Bit Address	Field	Description	Values
0	SEED_48	Seed Most Significant word	—
1	SEED_49		
2	SEED_50		
...	...		
9	SEED_57		
10	SEED_58		
11	SEED_59		
12	LED	LED output timing	0 = VBOT>VLOW LED blink 200/800 ms VBOT<VLOW LED not blinking 1 = VBOT>VLOW LED blink 25/500 ms VBOT<VLOW LED blink once
13	MOD	Modulation Format	0 = PWM 1 = MANCHESTER
14	RFEN	RF Enable/S3 multiplexing	0 - Enabled (S3 only sensed 2 seconds after the last button is released) 1 - Disabled (S3 same as other S inputs)
15	HEADER	Header Length	0 = short Header, TH = 3 x TE 1 = standard Header, TH = 10 x TE

4.5.12 HEADER

When PWM mode is selected the header length (low time between preamble and data bits start) can be set to 10 x TE or 3 x TE. The 10 x TE mode is recommended for compatibility with previous KEELOQ encoder models. In Manchester mode, the header length is fixed and set to 4 x TE.

4.5.13 RFEN

RFEN selects whether the RFEN output is enabled or disabled. If enabled, S3 is only sampled 2 s after the last button is released and at the start of the first transmission. If disabled S3 functions the same as the other S inputs.

© 2011 Microchip Technology Inc.

4.6 SYNCHRONOUS MODE

In Synchronous mode, the code word can be clocked out on DATA using S2 as a clock. To enter Synchronous mode, DATA and S0 must be taken HIGH and then S2 is taken HIGH. After Synchronous mode is entered, S0 must be taken LOW. The data is clocked out on DATA on every rising edge of S2. Auto-shutoff timer is not disabled in Synchronous mode. This can be used to implement RF testing.

FIGURE 4-1: SYNCHRONOUS TRANSMISSION MODE

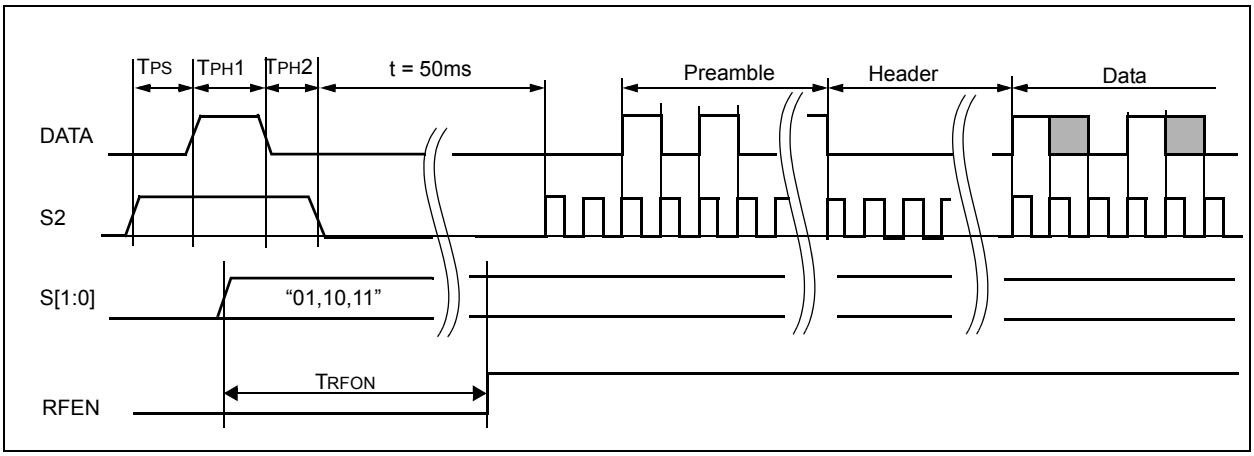
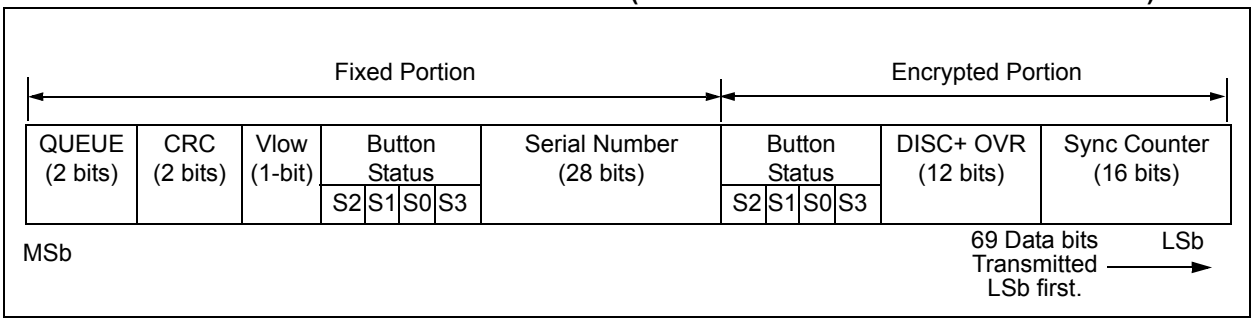


FIGURE 4-2: CODE WORD ORGANIZATION (SYNCHRONOUS TRANSMISSION MODE)



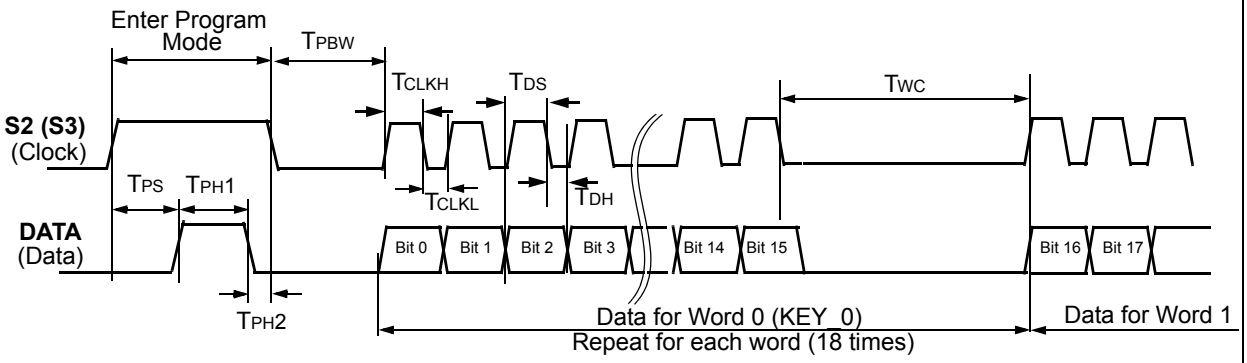
5.0 PROGRAMMING THE HCS362

When using the HCS362 in a system, the user will have to program some parameters into the device, including the serial number and the secret key before it can be used. The programming cycle allows the user to input all 288 bits in a serial data stream, which are then stored internally in EEPROM. Programming will be initiated by forcing the DATA line HIGH, after the S2 line has been held HIGH for the appropriate length of time (Table 5-1 and Figure 5-1). After the Program mode is entered, a delay must be provided to the device for the automatic bulk write cycle to complete. This will write all locations in the EEPROM to an all zeros pattern including the OSC calibration bits.

The device can then be programmed by clocking in 16 bits at a time, using S2 as the clock line and DATA as the data in-line. After each 16-bit word is loaded, a programming delay is required for the internal program cycle to complete. This delay can take up to Twc. At the end of the programming cycle, the device can be verified (Figure 5-2) by reading back the EEPROM. Reading is done by clocking the S2 line and reading the data bits on DATA. For security reasons, it is not possible to execute a verify function without first programming the EEPROM. **A Verify operation can only be done once, immediately following the Program cycle**.

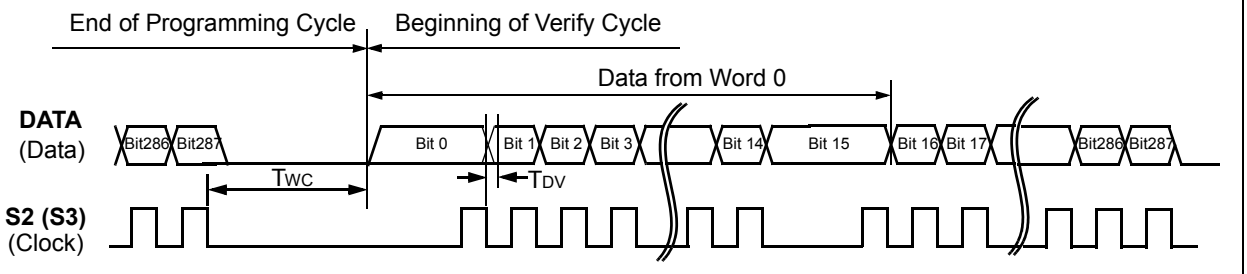
Note:	To ensure that the device does not accidentally enter Programming mode, PWM should never be pulled high by the circuit connected to it. Special care should be taken when driving PNP RF transistors.

FIGURE 5-1: PROGRAMMING WAVEFORMS



Note 1: Unused button inputs to be held to ground during the entire programming sequence.
2: The VDD pin must be taken to ground after a Program/Verify cycle.

FIGURE 5-2: VERIFY WAVEFORMS



Note: If a Verify operation is to be done, then it must immediately follow the Program cycle.

© 2011 Microchip Technology Inc.

TABLE 5-1: PROGRAMMING/VERIFY TIMING REQUIREMENTS

V_{DD} = 5.0V ± 10% 25 °C ± 5 °C				
Parameter	**Symbol**	**Min.**	**Max.**	**Units**
Program mode setup time	T_{PS}	3.5	4.5	ms
Hold time 1	T_{PH1}	3.5	—	ms
Hold time 2	T_{PH2}	50	—	µs
Bulk Write time	T_{PBW}	4.0	—	ms
Program delay time	T_{PROG}	4.0	—	ms
Program cycle time	T_{WC}	50	—	ms
Clock low time	T_{CLKL}	50	—	µs
Clock high time	T_{CLKH}	50	—	µs
Data setup time	T_{DS}	0	—	µs
Data hold time	T_{DH}	30	—	µs
Data out valid time	T_{DV}	—	30	µs

6.0 INTEGRATING THE HCS362 INTO A SYSTEM

Use of the HCS362 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a license agreement) firmware routines that accept transmissions from the HCS362 and decrypt the hopping code portion of the data stream. These routines provide system designers the means to develop their own decoding system.

6.1 Learning a Transmitter to a Receiver

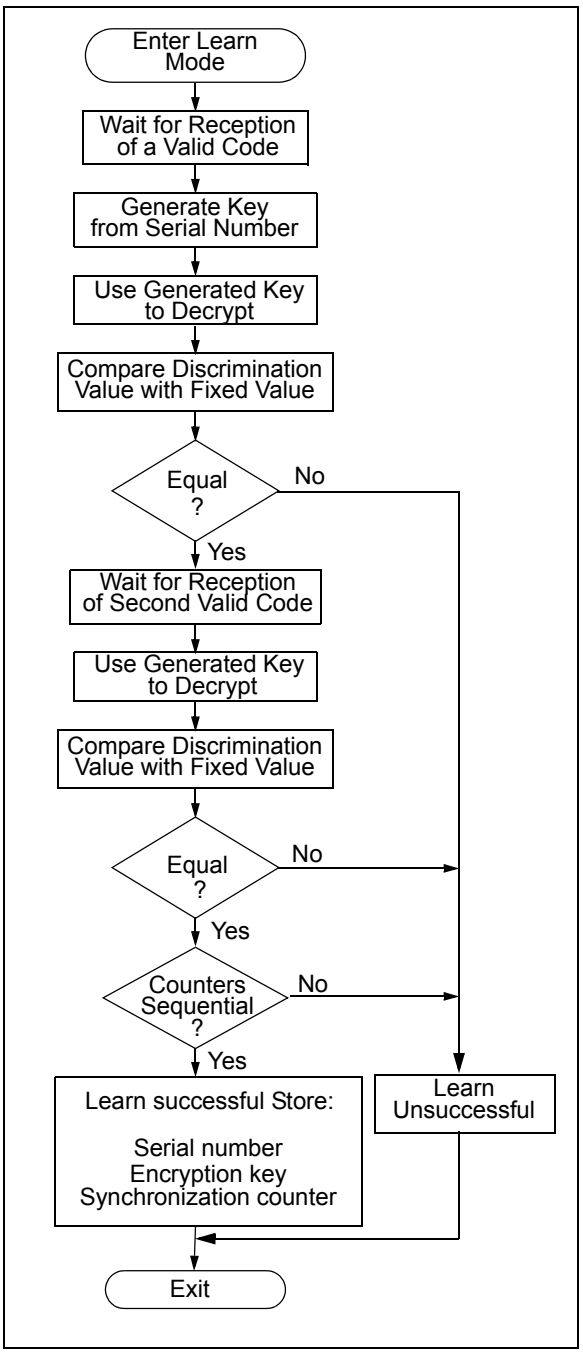
A transmitter must first be 'learned' by a decoder before its use is allowed in the system. Several learning strategies are possible, Figure 6-1 details a typical learn sequence. Core to each, the decoder must minimally store each learned transmitter's serial number and current synchronization counter value in EEPROM. Additionally, the decoder typically stores each transmitter's unique crypt key. The maximum number of learned transmitters will therefore be relative to the available EEPROM.

A transmitter's serial number is transmitted in the clear but the synchronization counter only exists in the code word's encrypted portion. The decoder obtains the counter value by decrypting using the same key used to encrypt the information. The KEELOQ algorithm is a symmetrical block cipher so the encryption and decryption keys are identical and referred to generally as the crypt key. The encoder receives its crypt key during manufacturing. The decoder is programmed with the ability to generate a crypt key as well as all but one required input to the key generation routine; typically the transmitter's serial number.

Figure 6-1 summarizes a typical learn sequence. The decoder receives and authenticates a first transmission; first button press. Authentication involves generating the appropriate crypt key, decrypting, validating the correct key usage via the discrimination bits and buffering the counter value. A second transmission is received and authenticated. A final check verifies the counter values were sequential; consecutive button presses. If the learn sequence is successfully complete, the decoder stores the learned transmitter's serial number, current synchronization counter value and appropriate crypt key. From now on the crypt key will be retrieved from EEPROM during normal operation instead of recalculating it for each transmission received.

Certain learning strategies have been patented and care must be taken not to infringe.

FIGURE 6-1: TYPICAL LEARN SEQUENCE

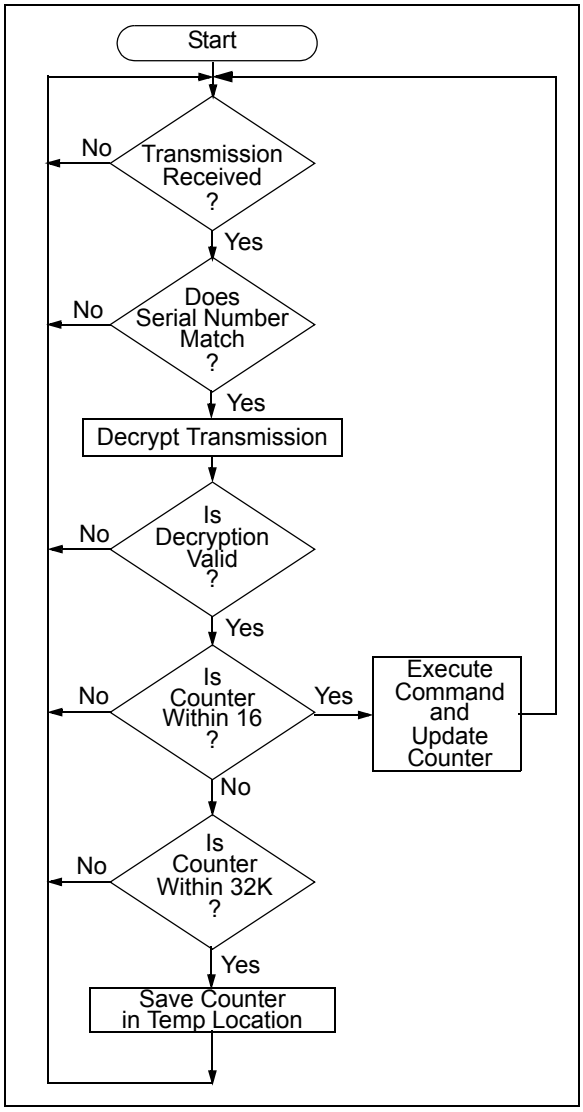


© 2011 Microchip Technology Inc.

6.2 Decoder Operation

Figure 6-2 summarizes normal decoder operation. The decoder waits until a transmission is received. The received serial number is compared to the EEPROM table of learned transmitters to first determine if this transmitter's use is allowed in the system. If from a learned transmitter, the transmission is decrypted using the stored crypt key and authenticated via the discrimination bits for appropriate crypt key usage. If the decryption was valid the synchronization value is evaluated.

FIGURE 6-2: TYPICAL DECODER OPERATION



6.3 Synchronization with Decoder (Evaluating the Counter)

The KEELOQ technology patent scope includes a sophisticated synchronization technique that does not require the calculation and storage of future codes. The technique securely blocks invalid transmissions while providing transparent resynchronization to transmitters inadvertently activated away from the receiver.

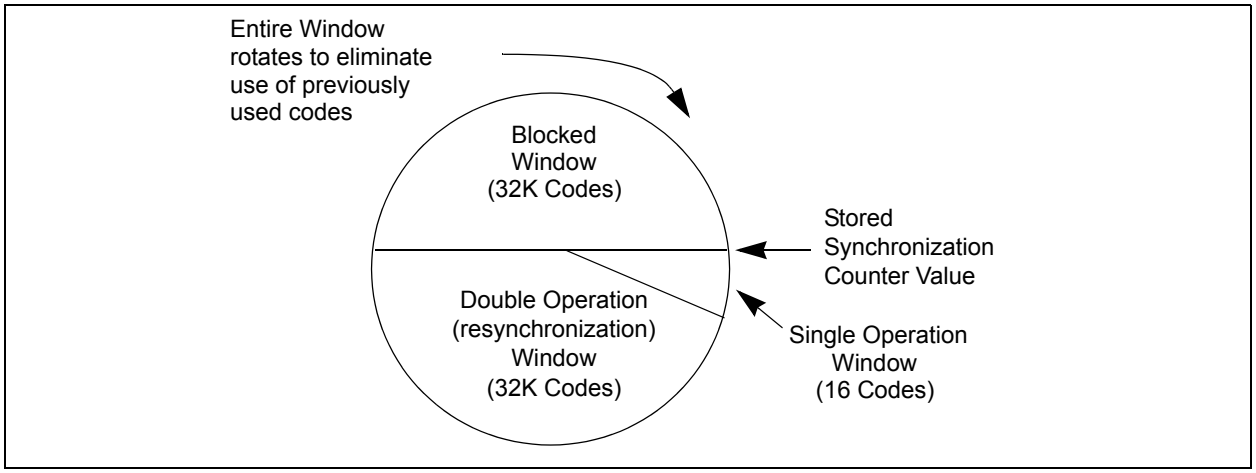
Figure 6-3 shows a 3-partition, rotating synchronization window. The size of each window is optional but the technique is fundamental. Each time a transmission is authenticated, the intended function is executed and the transmission's synchronization counter value is stored in EEPROM. From the currently stored counter value there is an initial "Single Operation" forward window of 16 codes. If the difference between a received synchronization counter and the last stored counter is within 16, the intended function will be executed on the single button press and the new synchronization counter will be stored. Storing the new synchronization counter value effectively rotates the entire synchronization window.

A "Double Operation" (resynchronization) window further exists from the Single Operation window up to 32K codes forward of the currently stored counter value. It is referred to as "Double Operation" because a transmission with synchronization counter value in this window will require an additional, sequential counter transmission prior to executing the intended function. Upon receiving the sequential transmission the decoder executes the intended function and stores the synchronization counter value. This resynchronization occurs transparently to the user as it is human nature to press the button a second time if the first was unsuccessful.

The third window is a "Blocked Window" ranging from the double operation window to the currently stored synchronization counter value. Any transmission with synchronization counter value within this window will be ignored. This window excludes previously used, perhaps code-grabbed transmissions from accessing the system.

Note:	The synchronization method described in this section is only a typical implementation and because it is usually implemented in firmware, it can be altered to fit the needs of a particular system.

FIGURE 6-3: SYNCHRONIZATION WINDOW



© 2011 Microchip Technology Inc.

7.0 DEVELOPMENT SUPPORT

The PIC® microcontrollers and dsPIC® digital signal controllers are supported with a full range of software and hardware development tools:

- Integrated Development Environment
  - MPLAB® IDE Software
- Compilers/Assemblers/Linkers
  - MPLAB C Compiler for Various Device Families
  - HI-TECH C for Various Device Families
  - MPASM™ Assembler
  - MPLINK™ Object Linker/ MPLIB™ Object Librarian
  - MPLAB Assembler/Linker/Librarian for Various Device Families
- Simulators
  - MPLAB SIM Software Simulator
- Emulators
  - MPLAB REAL ICE™ In-Circuit Emulator
- In-Circuit Debuggers
  - MPLAB ICD 3
  - PICkit™ 3 Debug Express
- Device Programmers
  - PICkit™ 2 Programmer
  - MPLAB PM3 Device Programmer
- Low-Cost Demonstration/Development Boards, Evaluation Kits, and Starter Kits

7.1 MPLAB Integrated Development Environment Software

The MPLAB IDE software brings an ease of software development previously unseen in the 8/16/32-bit microcontroller market. The MPLAB IDE is a Windows® operating system-based application that contains:

- A single graphical interface to all debugging tools
  - Simulator
  - Programmer (sold separately)
  - In-Circuit Emulator (sold separately)
  - In-Circuit Debugger (sold separately)
- A full-featured editor with color-coded context
- A multiple project manager
- Customizable data windows with direct edit of contents
- High-level source code debugging
- Mouse over variable inspection
- Drag and drop variables from source to watch windows
- Extensive on-line help
- Integration of select third party tools, such as IAR C Compilers

The MPLAB IDE allows you to:

- Edit your source files (either C or assembly)
- One-touch compile or assemble, and download to emulator and simulator tools (automatically updates all project information)
- Debug using:
  - Source files (C or assembly)
  - Mixed C and assembly
  - Machine code

MPLAB IDE supports multiple debugging tools in a single development paradigm, from the cost-effective simulators, through low-cost in-circuit debuggers, to full-featured emulators. This eliminates the learning curve when upgrading to tools with increased flexibility and power.

7.2 MPLAB C Compilers for Various Device Families

The MPLAB C Compiler code development systems are complete ANSI C compilers for Microchip's PIC18, PIC24 and PIC32 families of microcontrollers and the dsPIC30 and dsPIC33 families of digital signal controllers. These compilers provide powerful integration capabilities, superior code optimization and ease of use.

For easy source level debugging, the compilers provide symbol information that is optimized to the MPLAB IDE debugger.

7.3 HI-TECH C for Various Device Families

The HI-TECH C Compiler code development systems are complete ANSI C compilers for Microchip's PIC family of microcontrollers and the dsPIC family of digital signal controllers. These compilers provide powerful integration capabilities, omniscient code generation and ease of use.

For easy source level debugging, the compilers provide symbol information that is optimized to the MPLAB IDE debugger.

The compilers include a macro assembler, linker, preprocessor, and one-step driver, and can run on multiple platforms.

7.4 MPASM Assembler

The MPASM Assembler is a full-featured, universal macro assembler for PIC10/12/16/18 MCUs.

The MPASM Assembler generates relocatable object files for the MPLINK Object Linker, Intel® standard HEX files, MAP files to detail memory usage and symbol reference, absolute LST files that contain source lines and generated machine code and COFF files for debugging.

The MPASM Assembler features include:

- Integration into MPLAB IDE projects
- User-defined macros to streamline assembly code
- Conditional assembly for multi-purpose source files
- Directives that allow complete control over the assembly process

7.5 MPLINK Object Linker/ MPLIB Object Librarian

The MPLINK Object Linker combines relocatable objects created by the MPASM Assembler and the MPLAB C18 C Compiler. It can link relocatable objects from precompiled libraries, using directives from a linker script.

The MPLIB Object Librarian manages the creation and modification of library files of precompiled code. When a routine from a library is called from a source file, only the modules that contain that routine will be linked in with the application. This allows large libraries to be used efficiently in many different applications.

The object linker/library features include:

- Efficient linking of single libraries instead of many smaller files
- Enhanced code maintainability by grouping related modules together
- Flexible creation of libraries with easy module listing, replacement, deletion and extraction

7.6 MPLAB Assembler, Linker and Librarian for Various Device Families

MPLAB Assembler produces relocatable machine code from symbolic assembly language for PIC24, PIC32 and dsPIC devices. MPLAB C Compiler uses the assembler to produce its object file. The assembler generates relocatable object files that can then be archived or linked with other relocatable object files and archives to create an executable file. Notable features of the assembler include:

- Support for the entire device instruction set
- Support for fixed-point and floating-point data
- Command line interface
- Rich directive set
- Flexible macro language
- MPLAB IDE compatibility

© 2011 Microchip Technology Inc.

7.7 MPLAB SIM Software Simulator

The MPLAB SIM Software Simulator allows code development in a PC-hosted environment by simulating the PIC® MCUs and dsPIC® DSCs on an instruction level. On any given instruction, the data areas can be examined or modified and stimuli can be applied from a comprehensive stimulus controller. Registers can be logged to files for further run-time analysis. The trace buffer and logic analyzer display extend the power of the simulator to record and track program execution, actions on I/O, most peripherals and internal registers.

The MPLAB SIM Software Simulator fully supports symbolic debugging using the MPLAB C Compilers, and the MPASM and MPLAB Assemblers. The software simulator offers the flexibility to develop and debug code outside of the hardware laboratory environment, making it an excellent, economical software development tool.

7.8 MPLAB REAL ICE In-Circuit Emulator System

MPLAB REAL ICE In-Circuit Emulator System is Microchip's next generation high-speed emulator for Microchip Flash DSC and MCU devices. It debugs and programs PIC® Flash MCUs and dsPIC® Flash DSCs with the easy-to-use, powerful graphical user interface of the MPLAB Integrated Development Environment (IDE), included with each kit.

The emulator is connected to the design engineer's PC using a high-speed USB 2.0 interface and is connected to the target with either a connector compatible with in-circuit debugger systems (RJ11) or with the new high-speed, noise tolerant, Low-Voltage Differential Signal (LVDS) interconnection (CAT5).

The emulator is field upgradable through future firmware downloads in MPLAB IDE. In upcoming releases of MPLAB IDE, new devices will be supported, and new features will be added. MPLAB REAL ICE offers significant advantages over competitive emulators including low-cost, full-speed emulation, run-time variable watches, trace analysis, complex breakpoints, a ruggedized probe interface and long (up to three meters) interconnection cables.

7.9 MPLAB ICD 3 In-Circuit Debugger System

MPLAB ICD 3 In-Circuit Debugger System is Microchip's most cost effective high-speed hardware debugger/programmer for Microchip Flash Digital Signal Controller (DSC) and microcontroller (MCU) devices. It debugs and programs PIC® Flash microcontrollers and dsPIC® DSCs with the powerful, yet easy-to-use graphical user interface of MPLAB Integrated Development Environment (IDE).

The MPLAB ICD 3 In-Circuit Debugger probe is connected to the design engineer's PC using a high-speed USB 2.0 interface and is connected to the target with a connector compatible with the MPLAB ICD 2 or MPLAB REAL ICE systems (RJ-11). MPLAB ICD 3 supports all MPLAB ICD 2 headers.

7.10 PICkit 3 In-Circuit Debugger/ Programmer and PICkit 3 Debug Express

The MPLAB PICkit 3 allows debugging and programming of PIC® and dsPIC® Flash microcontrollers at a most affordable price point using the powerful graphical user interface of the MPLAB Integrated Development Environment (IDE). The MPLAB PICkit 3 is connected to the design engineer's PC using a full speed USB interface and can be connected to the target via an Microchip debug (RJ-11) connector (compatible with MPLAB ICD 3 and MPLAB REAL ICE). The connector uses two device I/O pins and the reset line to implement in-circuit debugging and In-Circuit Serial Programming™.

The PICkit 3 Debug Express include the PICkit 3, demo board and microcontroller, hookup cables and CDROM with user's guide, lessons, tutorial, compiler and MPLAB IDE software.

7.11 PICkit 2 Development Programmer/Debugger and PICkit 2 Debug Express

The PICkit™ 2 Development Programmer/Debugger is a low-cost development tool with an easy to use interface for programming and debugging Microchip's Flash families of microcontrollers. The full featured Windows® programming interface supports baseline (PIC10F, PIC12F5xx, PIC16F5xx), midrange (PIC12F6xx, PIC16F), PIC18F, PIC24, dsPIC30, dsPIC33, and PIC32 families of 8-bit, 16-bit, and 32-bit microcontrollers, and many Microchip Serial EEPROM products. With Microchip's powerful MPLAB Integrated Development Environment (IDE) the PICkit™ 2 enables in-circuit debugging on most PIC® microcontrollers. In-Circuit-Debugging runs, halts and single steps the program while the PIC microcontroller is embedded in the application. When halted at a breakpoint, the file registers can be examined and modified.

The PICkit 2 Debug Express include the PICkit 2, demo board and microcontroller, hookup cables and CDROM with user's guide, lessons, tutorial, compiler and MPLAB IDE software.

7.12 MPLAB PM3 Device Programmer

The MPLAB PM3 Device Programmer is a universal, CE compliant device programmer with programmable voltage verification at V_{DDMIN} and V_{DDMAX} for maximum reliability. It features a large LCD display (128 x 64) for menus and error messages and a modular, detachable socket assembly to support various package types. The ICSP™ cable assembly is included as a standard item. In Stand-Alone mode, the MPLAB PM3 Device Programmer can read, verify and program PIC devices without a PC connection. It can also set code protection in this mode. The MPLAB PM3 connects to the host PC via an RS-232 or USB cable. The MPLAB PM3 has high-speed communications and optimized algorithms for quick programming of large memory devices and incorporates an MMC card for file storage and data applications.

7.13 Demonstration/Development Boards, Evaluation Kits, and Starter Kits

A wide variety of demonstration, development and evaluation boards for various PIC MCUs and dsPIC DSCs allows quick application development on fully functional systems. Most boards include prototyping areas for adding custom circuitry and provide application firmware and source code for examination and modification.

The boards support a variety of features, including LEDs, temperature sensors, switches, speakers, RS-232 interfaces, LCD displays, potentiometers and additional EEPROM memory.

The demonstration and development boards can be used in teaching environments, for prototyping custom circuits and for learning about various microcontroller applications.

In addition to the PICDEM™ and dsPICDEM™ demonstration/development board series of circuits, Microchip has a line of evaluation kits and demonstration software for analog filter design, KEELOQ® security ICs, CAN, IrDA®, PowerSmart battery management, SEEVAL® evaluation system, Sigma-Delta ADC, flow rate sensing, plus many more.

Also available are starter kits that contain everything needed to experience the specified device. This usually includes a single application and debug capability, all on one board.

Check the Microchip web page (www.microchip.com) for the complete list of demonstration, development and evaluation kits.

© 2011 Microchip Technology Inc.

8.0 ELECTRICAL CHARACTERISTICS

TABLE 8-1: ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Units
V_{DD}	Supply voltage	-0.3 to 6.6	V
V_{IN}	Input voltage	-0.3 to V_{DD} + 0.3	V
V_{OUT}	Output voltage	-0.3 to V_{DD} + 0.3	V
I_{OUT}	Max output current	20	mA
T_{STG}	Storage temperature	-55 to +125	°C
T_{LSOL}	Lead soldering temperature	300	°C
V_{ESD}	ESD rating	4,000	V

Note: Stresses above those listed under “ABSOLUTE MAXIMUM RATINGS” may cause permanent damage to the device.

TABLE 8-2: DC CHARACTERISTICS

Industrial (I): T_{AMB} = -40 °C to +85 °C						
		2.0V < V_{DD} < 6.3				
Parameter	**Sym.**	**Min.**	**Typ.(1)**	**Max.**	**Unit**	**Conditions**
Operating current (avg.)	I_{CC}	—	0.3	1.2	mA	V_{DD} = 6.3V
Standby current	I_{CCS}	—	0.1	1.0	µA	V_{DD} = 6.3V
Auto-shutoff current(2,3)	I_{CCS}	—	40	75	µA	—
High level Input voltage	V_{IH}	0.65 V_{DD}	—	V_{DD} + 0.3	V	V_{DD} = 2.0V
Low level input voltage	V_{IL}	-0.3	—	0.15 V_{DD}	V	V_{DD} = 2.0V
High level output voltage	V_{OH}	0.7 V_{DD} 0.7 V_{DD}	—	—	V	I_{OH} = -1.0 mA, V_{DD} = 2.0V I_{OH} = -2.0 mA, V_{DD} = 6.3V
Low level output voltage	V_{OL}	—	—	0.15 V_{DD} 0.15 V_{DD}	V	I_{OL} = 1.0 mA, V_{DD} = 2.0V I_{OL} = 2.0 mA, V_{DD} = 6.3V
RFEN pin high drive	I_{RFEN}	0.5 1.0	1 2.5	3.0 5.0	mA	V_{RFEN} = 1.4V V_{DD} = 2.0V V_{RFEN} = 4.4V V_{DD} = 6.3V
$\overline{LED}$ sink current	I_{LEDL} I_{LEDH}	1.0 2.0	3.5 4.5	6.0 7.0	mA mA	V_{LED} = 1.5V, V_{DD} = 3.0V V_{LED} = 1.5V, V_{DD} = 6.3V
Pull-down Resistance; S0-S3	R_{S0-3}	40	60	80	KΩ	V_{DD} = 4.0V
Pull-down Resistance; PWM	R_{PWM}	80	120	160	KΩ	V_{DD} = 4.0V

Note 1: Typical values are at 25 °C.
2: Auto-shutoff current specification does not include the current through the input pull-down resistors.
3: These values are characterized but not tested.

FIGURE 8-1: POWER-UP AND TRANSMIT TIMING

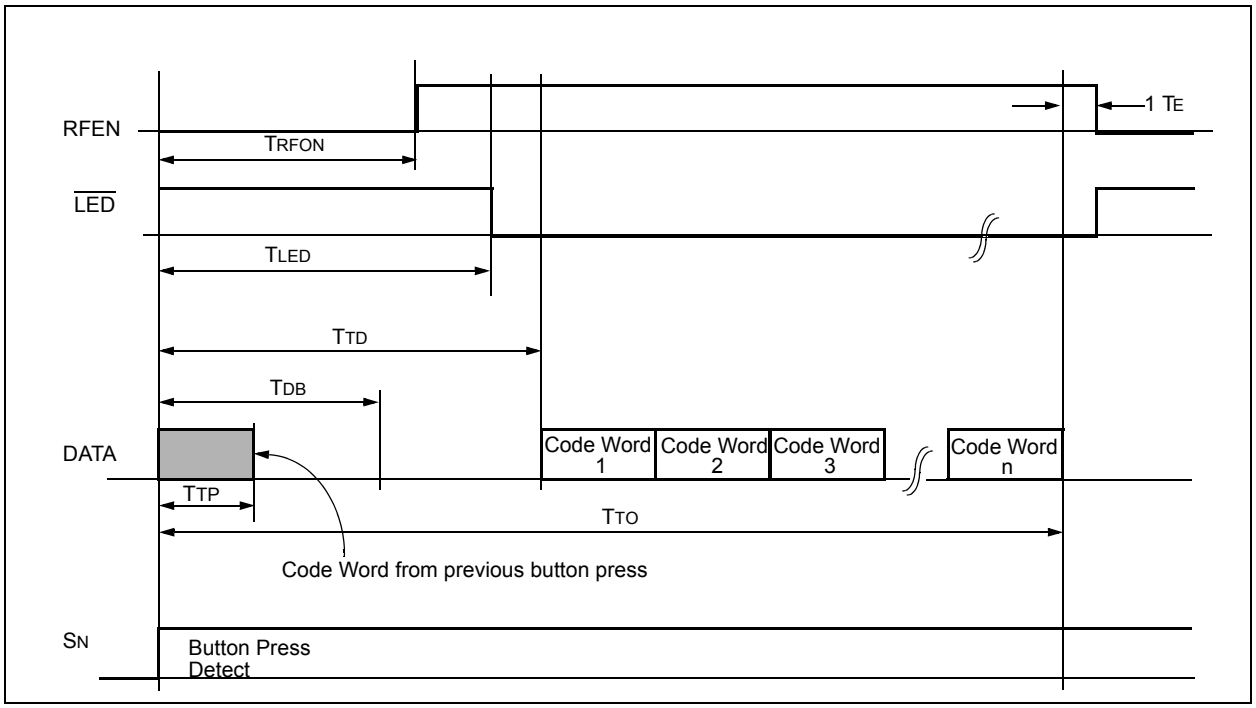


TABLE 8-3: POWER-UP AND TRANSMIT TIMING REQUIREMENTS(3)

VDD = +2.0 to 6.3V Industrial (I): TAMB = -40 °C to +85 °C						
Parameter	**Symbol**	**Min.**	**Typical**	**Max.**	**Unit**	**Remarks**
Transmit delay from button detect	TTD	26	30	40	ms	**(Note 1)**
Debounce delay	TDB	18	20	22	ms	—
Auto-shutoff time-out period (TIMO=10)	TTO	23.4	25.6	28.16	s	**(Note 2)**
RFEN after key press	TRFON	22	26	36	ms	—
LED on after key press	TLED	25	—	45	ms	—
Time to terminate code word from previous button press	TTP	—	—	10 ms	—	—

Note 1: Transmit delay maximum value if the previous transmission was successfully transmitted.
2: The Auto-shutoff time-out period is not tested.
3: These values are characterized but not tested

© 2011 Microchip Technology Inc.

FIGURE 8-2: PWM FORMAT SUMMARY (MOD=0)

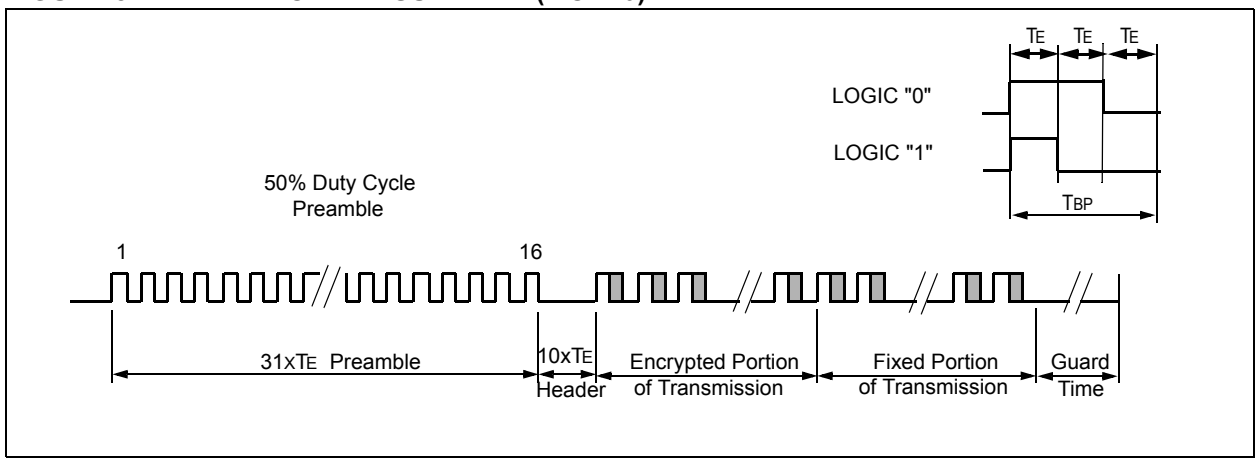


FIGURE 8-3: PWM PREAMBLE/HEADER FORMAT (MOD=0)

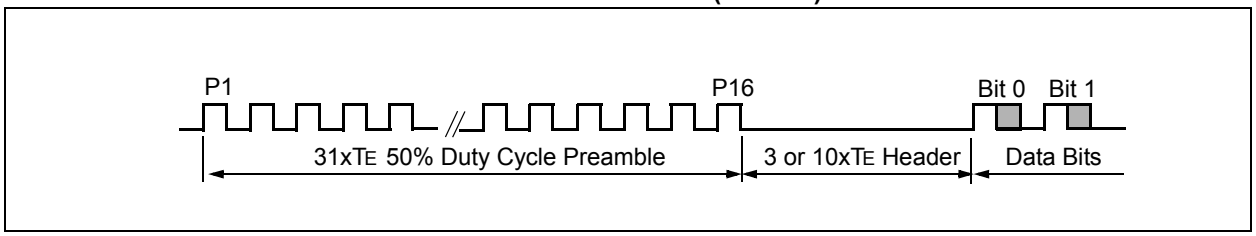


FIGURE 8-4: PWM DATA FORMAT (MOD = 0)

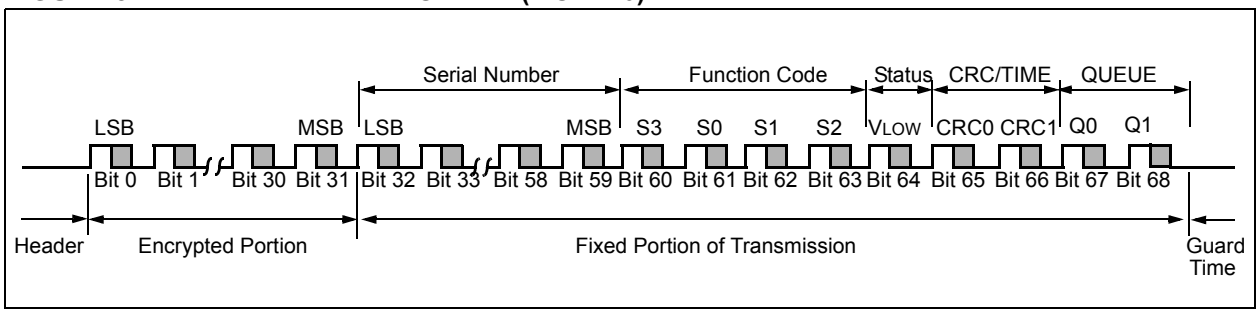


FIGURE 8-5: MANCHESTER FORMAT SUMMARY (MOD=1)

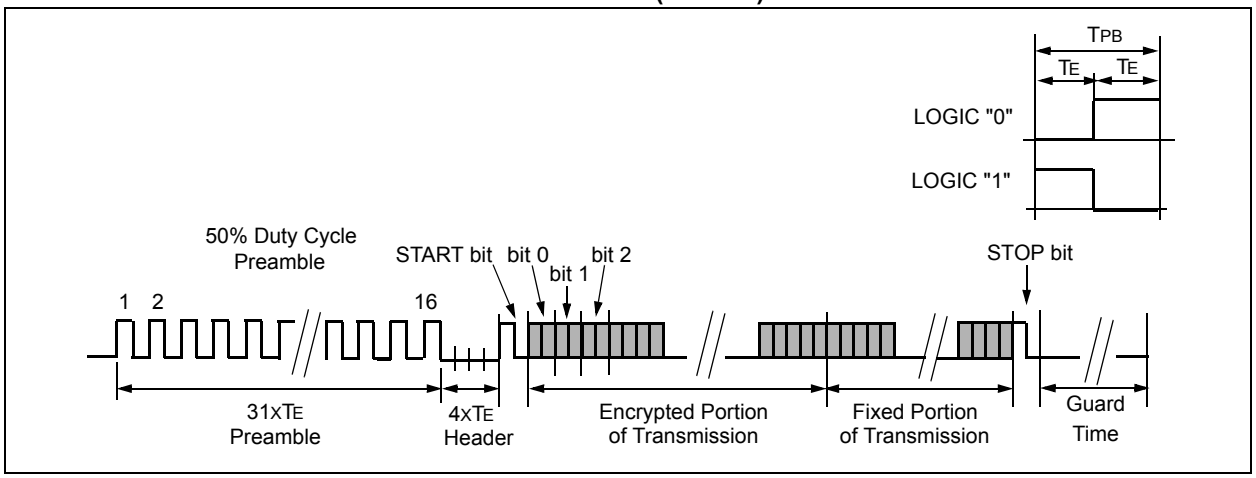
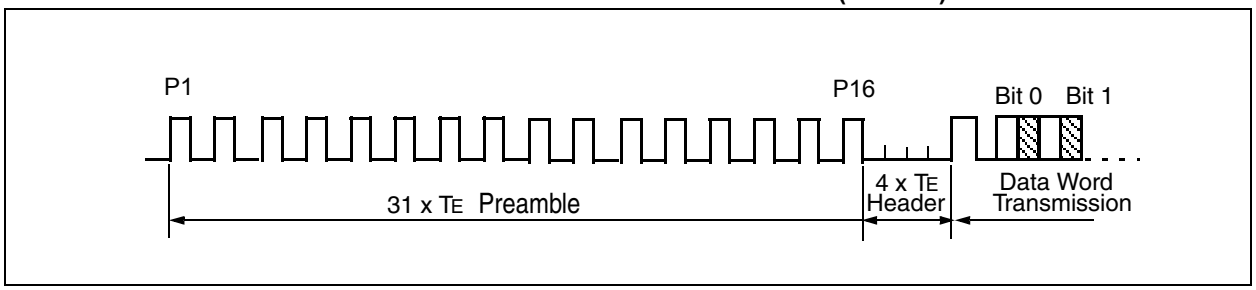


FIGURE 8-6: MANCHESTER PREAMBLE/HEADER FORMAT (MOD=1)



© 2011 Microchip Technology Inc.

TABLE 8-4: CODE WORD TRANSMISSION TIMING PARAMETERS – PWM MODE(1,3)

V_{DD} = +2.0V to 6.3V Commercial (C): T_{AMB} = 0 °C to +70 °C Industrial (I): T_{AMB} = -40 °C to +85 °C		BSEL Value				
		11	10	01	00	
Symbol	Characteristic	Typical	Typical	Typical	Typical	Units
T_E	Basic pulse element	800	400	200	100	µs
T_{BP}	Bit width	3	3	3	3	T_E
T_P	Preamble duration	31	31	31	31	T_E
T_H	Header duration(4)	10	10	10	10	T_E
T_C	Data duration	207	207	207	207	T_E
T_G	Guard time(2)	27.2	26.4	26	25.8	ms
—	Total transmit time	220	122	74	50	ms
—	Data Rate	417	833	1667	3334	bps

013001

Note 1: The timing parameters are not tested but derived from the oscillator clock.
2: Assuming `GUARD = 10` option selected in `CONFIG_0` Configuration Word.
3: Allow for a +/- 10% tolerance on the encoder internal oscillator after calibration.
4: Assuming `HEADER = 1` option selected in `SEED_3` Configuration Word.

TABLE 8-5: CODE WORD TRANSMISSION TIMING PARAMETERS—MANCHESTER MODE(1,3)

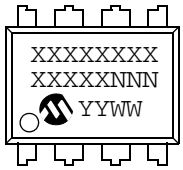
V_{DD} = +2.0V to 6.3V Commercial (C): T_{AMB} = 0 °C to +70 °C Industrial (I): T_{AMB} = -40 °C to +85 °C		BSEL Value				
		11	10	01	00	
Symbol	Characteristic	Typical	Typical	Typical	Typical	Units
T_E	Basic pulse element(3)	800	400	200	100	µs
T_{BP}	Bit width	2	2	2	2	T_E
T_P	Preamble duration	31	31	31	31	T_E
T_H	Header duration	4	4	4	4	T_E
T_C	Data duration	138	138	138	138	T_E
T_G	Guard time(2)	26.8	26.4	26	25.8	ms
—	Total transmit time	166	96	61	43	ms
—	Data Rate	625	1250	2500	5000	bps

Note 1: The timing parameters are not tested but derived from the oscillator clock.
2: Assuming `GUARD = 10` option selected in `CONFIG_0` Configuration Word.
3: Allow for a +/- 10% tolerance on the encoder internal oscillator after calibration.

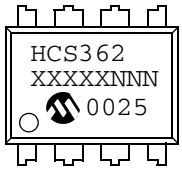
9.0 PACKAGING INFORMATION

9.1 Package Marking Information

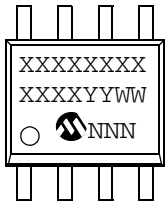
8-Lead PDIP



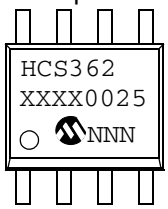
Example:



8-Lead SOIC



Example:



8-Lead TSSOP



Example:



Legend:	XX...X	Customer specific information*
	Y	Year code (last digit of calendar year)
	YY	Year code (last 2 digits of calendar year)
	WW	Week code (week of January 1 is week ‘01’)
	NNN	Alphanumeric traceability code

Note: In the event the full Microchip part number cannot be marked on one line, it will be carried over to the next line thus limiting the number of available characters for customer specific information.

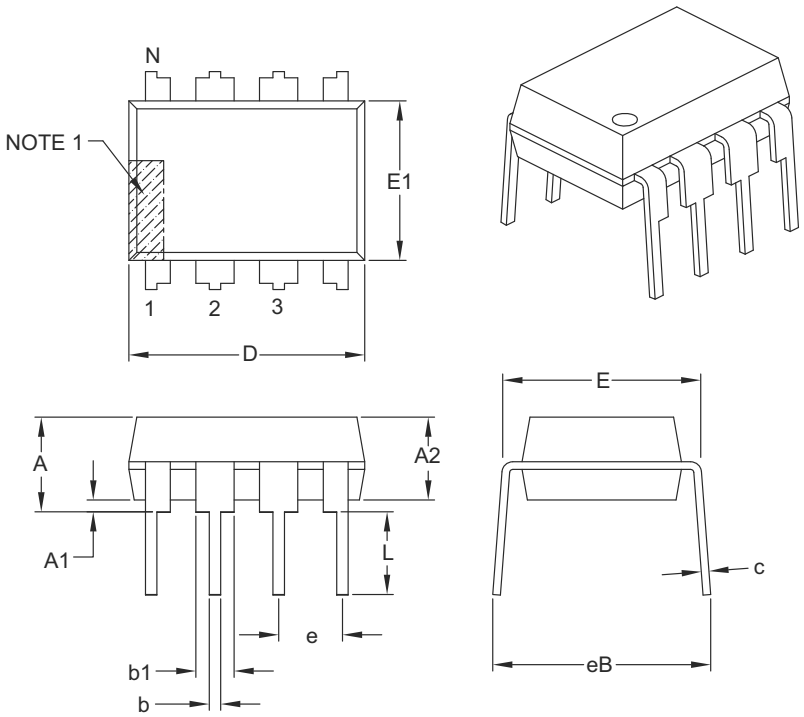
***** Standard PIC MCU device marking consists of Microchip part number, year code, week code, and traceability code. For PIC MCU device marking beyond this, certain price adders apply. Please check with your Microchip Sales Office. For SQTP devices, any special marking adders are included in SQTP price.

© 2011 Microchip Technology Inc.

9.2 Package Details

8-Lead Plastic Dual In-Line (P) – 300 mil Body [PDIP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		INCHES		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		.100 BSC	
Top to Seating Plane	A	–	–	.210
Molded Package Thickness	A2	.115	.130	.195
Base to Seating Plane	A1	.015	–	–
Shoulder to Shoulder Width	E	.290	.310	.325
Molded Package Width	E1	.240	.250	.280
Overall Length	D	.348	.365	.400
Tip to Seating Plane	L	.115	.130	.150
Lead Thickness	c	.008	.010	.015
Upper Lead Width	b1	.040	.060	.070
Lower Lead Width	b	.014	.018	.022
Overall Row Spacing §	eB	–	–	.430

Notes:

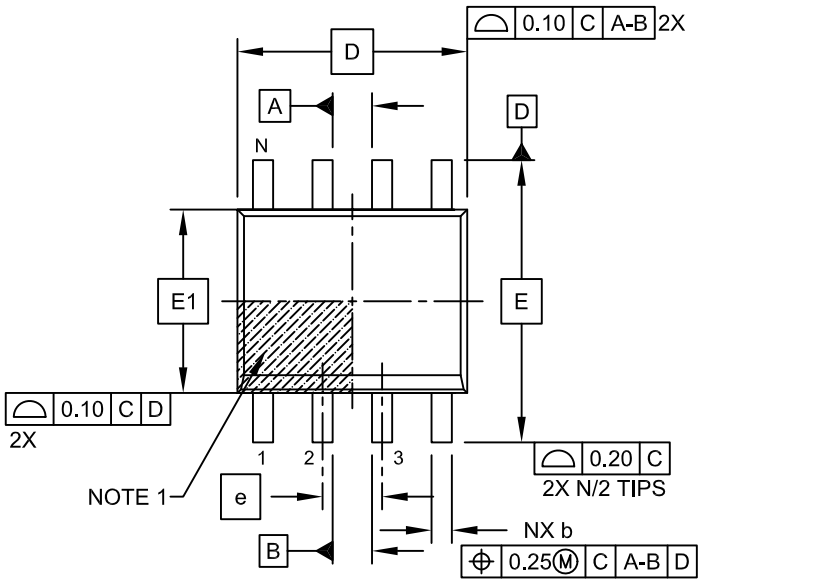
1. Pin 1 visual index feature may vary, but must be located with the hatched area.
2. § Significant Characteristic.
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .010" per side.
4. Dimensioning and tolerancing per ASME Y14.5M.

   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

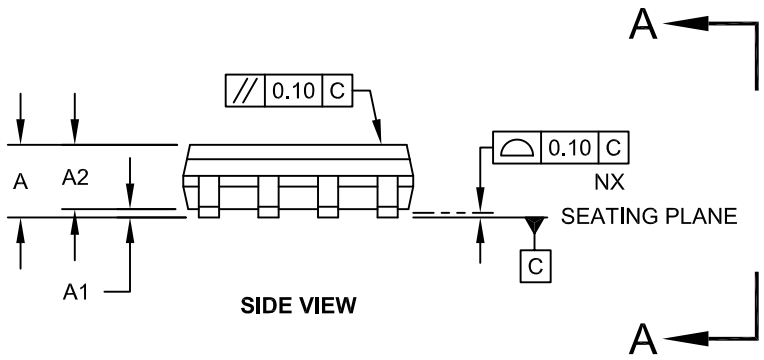
Microchip Technology Drawing C04-018B

8-Lead Plastic Small Outline (SN) - Narrow, 3.90 mm Body [SOIC]

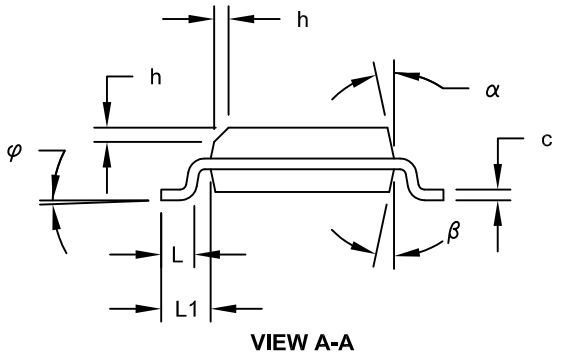
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW



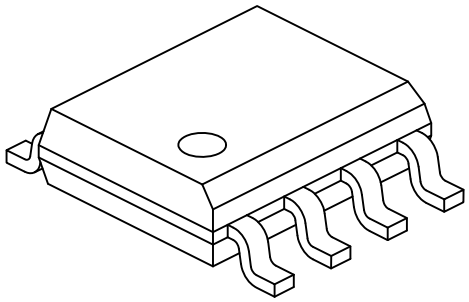
VIEW A-A

Microchip Technology Drawing No. C04-057C Sheet 1 of 2

© 2011 Microchip Technology Inc.

8-Lead Plastic Small Outline (SN) - Narrow, 3.90 mm Body [SOIC]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		1.27 BSC	
Overall Height	A	-	-	1.75
Molded Package Thickness	A2	1.25	-	-
Standoff §	A1	0.10	-	0.25
Overall Width	E		6.00 BSC	
Molded Package Width	E1		3.90 BSC	
Overall Length	D		4.90 BSC	
Chamfer (Optional)	h	0.25	-	0.50
Foot Length	L	0.40	-	1.27
Footprint	L1		1.04 REF	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M

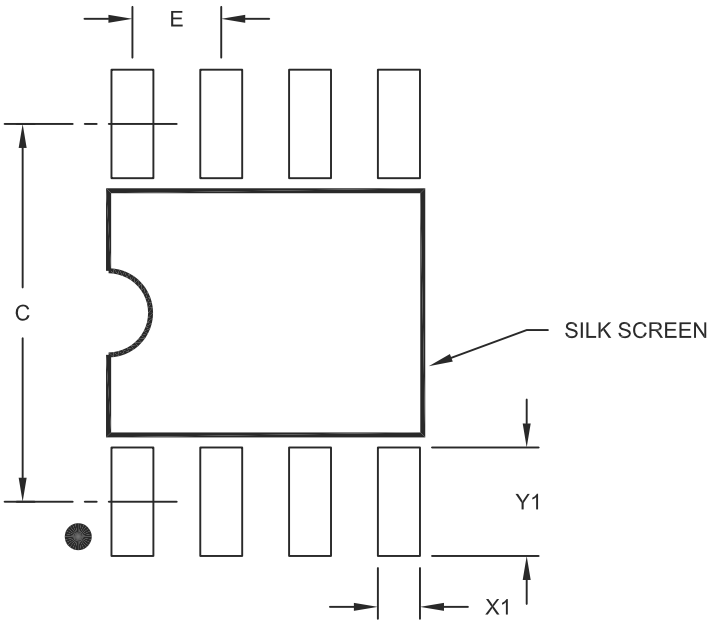
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

   REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing No. C04-057C Sheet 2 of 2

8-Lead Plastic Small Outline (SN) – Narrow, 3.90 mm Body [SOIC]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		1.27 BSC	
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

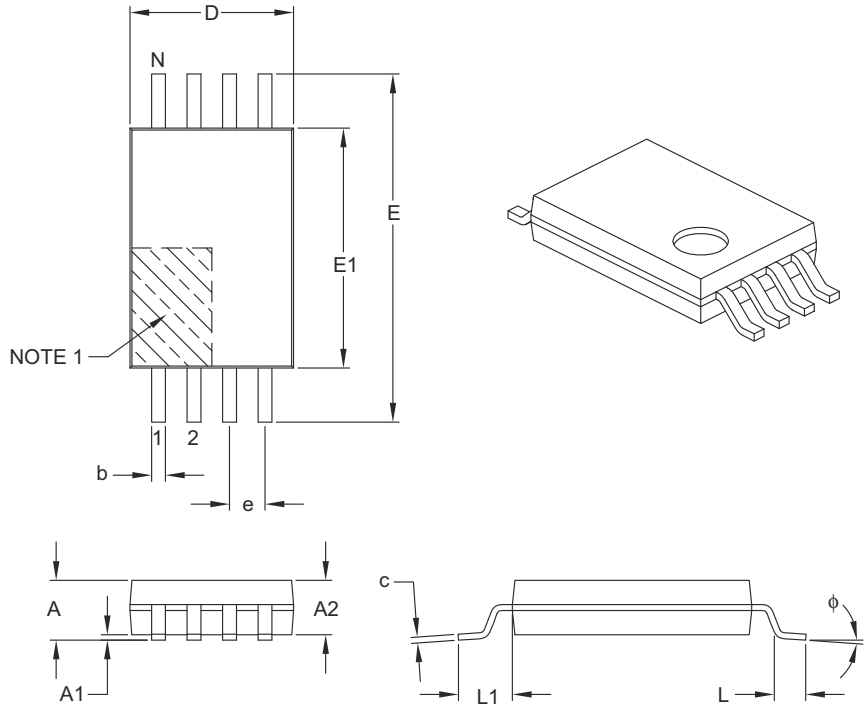
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2057A

© 2011 Microchip Technology Inc.

8-Lead Plastic Thin Shrink Small Outline (ST) – 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		0.65 BSC	
Overall Height	A	–	–	1.20
Molded Package Thickness	A2	0.80	1.00	1.05
Standoff	A1	0.05	–	0.15
Overall Width	E		6.40 BSC	
Molded Package Width	E1	4.30	4.40	4.50
Molded Package Length	D	2.90	3.00	3.10
Foot Length	L	0.45	0.60	0.75
Footprint	L1		1.00 REF	
Foot Angle	ϕ	0°	–	8°
Lead Thickness	c	0.09	–	0.20
Lead Width	b	0.19	–	0.30

Notes:

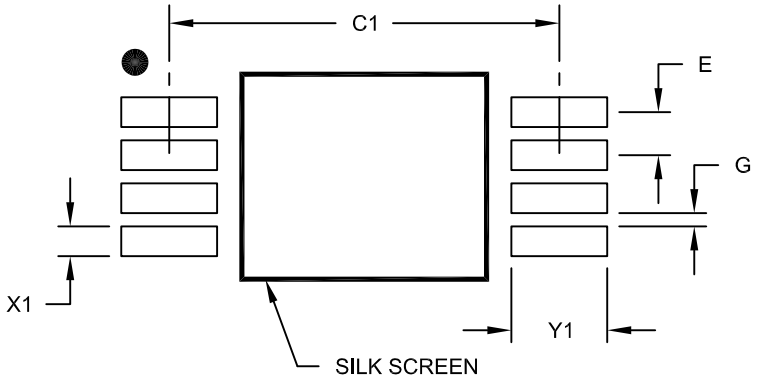
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15 mm per side.
3. Dimensioning and tolerancing per ASME Y14.5M.

BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-086B

8-Lead Plastic Thin Shrink Small Outline (ST) - 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.65 BSC	
Contact Pad Spacing	C1		5.90	
Contact Pad Width (X8)	X1			0.45
Contact Pad Length (X8)	Y1			1.45
Distance Between Pads	G	0.20		

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2086A

© 2011 Microchip Technology Inc.

APPENDIX A: ADDITIONAL INFORMATION

Microchip's Secure Data Products are covered by some or all of the following:

Code hopping encoder patents issued in European countries and U.S.A.

Secure learning patents issued in European countries, U.S.A. and R.S.A.

REVISION HISTORY

Revision E (June 2011)

- Updated the following sections: Development Support, The Microchip Web Site, Reader Response and HCS362 Product Identification System
- Added new section **Appendix A**
- Minor formatting and text changes were incorporated throughout the document

THE MICROCHIP WEB SITE

Microchip provides online support via our WWW site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support
- Development Systems Information Line

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://microchip.com/support

© 2011 Microchip Technology Inc.

READER RESPONSE

It is our intention to provide you with the best documentation possible to ensure successful use of your Microchip product. If you wish to provide your comments on organization, clarity, subject matter, and ways in which our documentation can better serve you, please FAX your comments to the Technical Publications Manager at (480) 792-4150.

Please list the following information, and use this outline to provide us with your comments about this document.

TO: Technical Publications Manager Total Pages Sent _____

RE: Reader Response

From: Name _____

Company _____

Address _____

City / State / ZIP / Country _____

Telephone: (_____) _____ - _____ FAX: (_____) _____ - _____

Application (optional):

Would you like a reply? ___Y ___N

Device: HCS362 Literature Number: DS40189E

Questions:

1. What are the best features of this document?

2. How does this document meet your hardware and software development needs?

3. Do you find the organization of this document easy to follow? If not, why?

4. What additions to the document do you think would enhance the structure and subject?

5. What deletions from the document could be made without affecting the overall usefulness?

6. Is there any incorrect or misleading information (what and where)?

7. How would you improve this document?

HCS362 PRODUCT IDENTIFICATION SYSTEM

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

HCS362 — X /X

Package:	P =	Plastic DIP (300 mil body), 8-lead
	SN =	Plastic SOIC (150 mil body), 8-lead
	ST =	Plastic TSSOP (4.4mm body), 8-lead
Temperature Range:	I =	–40 °C to +85 °C
Device:	HCS362	Code Hopping Encoder
	HCS362T	Code Hopping Encoder (Tape and Reel)

© 2011 Microchip Technology Inc.

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families 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 Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is 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 products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC^{32} logo, rfPIC and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MXDEV, MXLAB, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, Application Maestro, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rfLAB, Select Mode, Total Endurance, TSHARC, UniWinDriver, WiperLock and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

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.

© 2011, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

Printed on recycled paper.

ISBN: 978-1-61341-228-2

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2002

Microchip received ISO/TS-16949:2002 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

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:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-2819-3180
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-6578-300
Fax: 886-3-6578-370

Taiwan - Kaohsiung
Tel: 886-7-213-7830
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

05/02/11

© 2011 Microchip Technology Inc.