

## KEELOQ Code Hopping Encoder

### FEATURES

#### Security

- Programmable 28/32-bit serial number
- Programmable 64-bit encryption key
- Each transmission is unique
- 67-bit transmission code length
- 32-bit hopping code
- 35-bit fixed code (28/32-bit serial number, 4/0-bit function code, 1-bit status, 2-bit CRC)
- Encryption keys are read protected

#### Operating

- 2.0-6.6V operation
- Four button inputs
  - 15 functions available
- Selectable baud rate
- Automatic code word completion
- Battery low signal transmitted to receiver
- Nonvolatile synchronization data
- PWM and VPWM modulation

#### Other

- Easy to use programming interface
- On-chip EEPROM
- On-chip oscillator and timing components
- Button inputs have internal pulldown resistors
- Current limiting on LED output
- Minimum component count

#### Enhanced Features Over HCS300

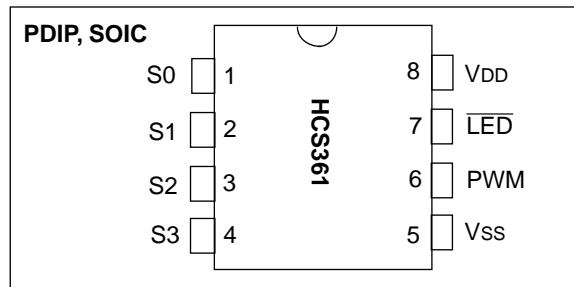
- 48-bit seed vs. 32-bit seed
- 2-bit CRC for error detection
- 28/32-bit serial number select
- Two seed transmission methods
- PWM and VPWM modulation
- Wake-up signal in VPWM mode
- IR modulation mode

#### Typical Applications

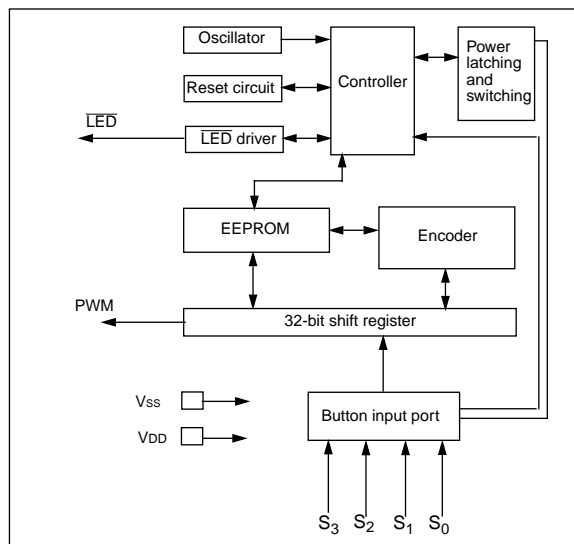
The HCS361 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

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

### PACKAGE TYPES



### HCS361 BLOCK DIAGRAM



### DESCRIPTION

The HCS361 is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS361 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 HCS361 combines a 32-bit hopping code generated by a nonlinear encryption algorithm, with a 28/32-bit serial number and 7/3 status bits to create a 67-bit transmission stream.

KEELOQ is a registered trademark of Microchip Technology, Inc.

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

Code hopping encoder patents issued in Europe, U.S.A., and R.S.A. — U.S.A.: 5,517,187; Europe: 0459781; R.S.A.: ZA93/4726

Secure learning patents issued in the U.S.A. and R.S.A. — U.S.A.: 5,686,904; R.S.A.: 95/5429

The length of the transmission eliminates the threat of code scanning and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend (code grabbing) schemes useless.

The encryption key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS361 a very secure unit. The HCS361 provides an easy to use serial interface for programming the necessary security keys, system parameters, and configuration data.

The encryption keys and code combinations are programmable but read-protected. The keys can only be verified after an automatic erase and programming operation. This protects against attempts to gain access to keys and manipulate synchronization values.

The HCS361 operates over a wide voltage range of 2.0V to 6.6V and has four button inputs in an 8-pin configuration. This allows the system designer the freedom to utilize up to 15 functions. The only components required for device operation are the buttons and RF circuitry, allowing a very low system cost.

## 1.0 SYSTEM OVERVIEW

### 1.1 Key Terms

- **Manufacturer's Code** – a 64-bit word, unique to each manufacturer, used to produce a unique encryption key in each transmitter (encoder).
- **Encryption Key** – a unique 64-bit key generated and programmed into the encoder during the manufacturing process. The encryption key controls the encryption algorithm and is stored in EEPROM on the encoder device.
- **Learn** – The HCS product family facilitates several learning strategies to be implemented on the decoder. The following are examples of what can be done.

#### Normal Learning

The receiver uses the same information that is transmitted during normal operation to derive the transmitter's secret key, decrypt the discrimination value and the synchronization counter.

#### Secure Learn

The transmitter is activated through a special button combination to transmit a stored 48-bit value (random seed) that can be used for key generation or be part of the key. Transmission of the random seed can be disabled after learning is completed.

The HCS361 is a code hopping encoder device that is designed specifically for keyless entry systems, primarily for vehicles and home garage door openers. It is meant to be a cost-effective, yet secure solution to such systems. The encoder portion of a keyless entry system is meant to be held by the user and operated to gain access to a vehicle or restricted area. The HCS361 requires very few external components (Figure 2-1).

Most keyless entry systems transmit the same code from a transmitter every time a button is pushed. The relative number of code combinations for a low end system is also a relatively small number. These shortcomings provide the means for a sophisticated thief to create a device that 'grabs' a transmission and retransmits it later or a device that scans all possible combinations until the correct one is found.

The HCS361 employs the KEELQ code hopping technology and an encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 67 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

As indicated in the block diagram on page one, the HCS361 has a small EEPROM array which must be loaded with several parameters before use. The most important of these values are:

- A 28/32-bit serial number which is meant to be unique for every encoder
- An encryption key that is generated at the time of production
- A 16-bit synchronization value

The serial number for each transmitter is programmed by the manufacturer at the time of production. The generation of the encryption key is done using a key generation algorithm (Figure 1-1). Typically, inputs to the key generation algorithm are the serial number of the transmitter or seed value, and a 64-bit manufacturer's code. The manufacturer's code is chosen by the system manufacturer and must be carefully controlled. The manufacturer's code is a pivotal part of the overall system security.

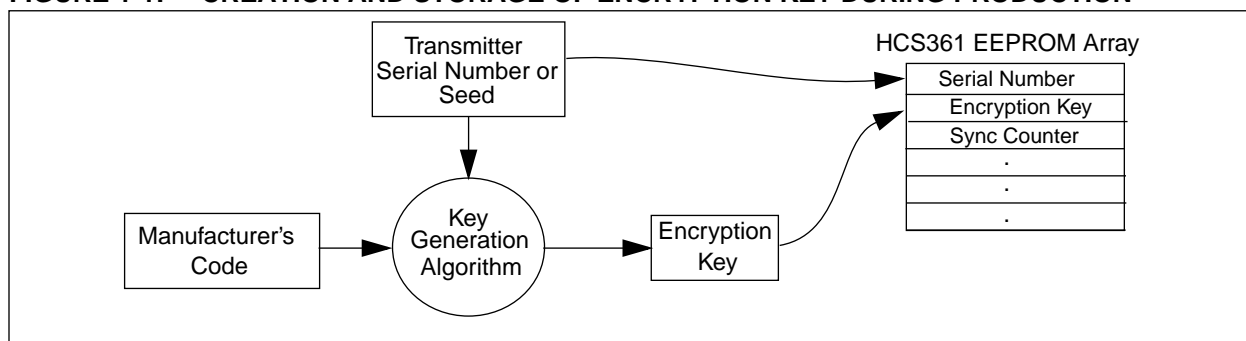
The 16-bit synchronization value is the basis for the transmitted code changing for each transmission, and is updated each time a button is pressed. Because of the complexity of the code hopping encryption algorithm, a change in one bit of the synchronization value will result in a large change in the actual transmitted code. There is a relationship (Figure 1-2) between the key values in EEPROM and how they are used in the encoder. Once the encoder detects that a button has been pressed, the encoder reads the button and updates the synchronization counter. The synchronization value is then combined with the encryption key in the encryption algorithm and the output is 32 bits of encrypted information. This data will change with every button press, 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 the serial number to form the code word transmitted to the receiver. The code word format is explained in detail in Section 4.2.

Any type of controller may be used as a receiver, but it is typically a microcontroller with compatible firmware that allows the receiver to operate in conjunction with a transmitter, based on the HCS361. Section 7.0 provides more detail on integrating the HCS361 into a total system.

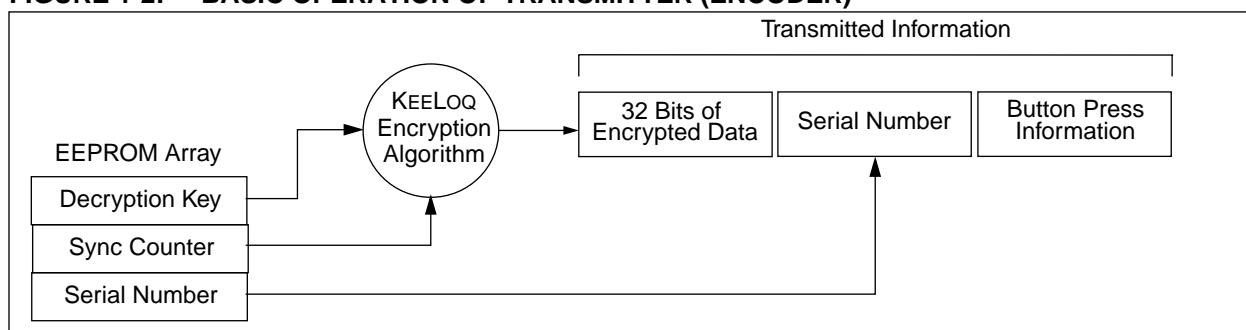
Before a transmitter can be used with a particular receiver, the transmitter must be 'learned' by the receiver. Upon learning a transmitter, information is stored by the receiver so that it may track the transmitter, including the serial number of the transmitter, the current synchronization value for that transmitter and the same encryption key that is used on the transmitter. If a receiver receives a message of valid

format, the serial number is checked and, if it is from a learned transmitter, the message is decrypted and the decrypted synchronization counter is checked against what is stored. If the synchronization value is verified, then the button status is checked to see what operation is needed. Figure 1-3 shows the relationship between some of the values stored by the receiver and the values received from the transmitter.

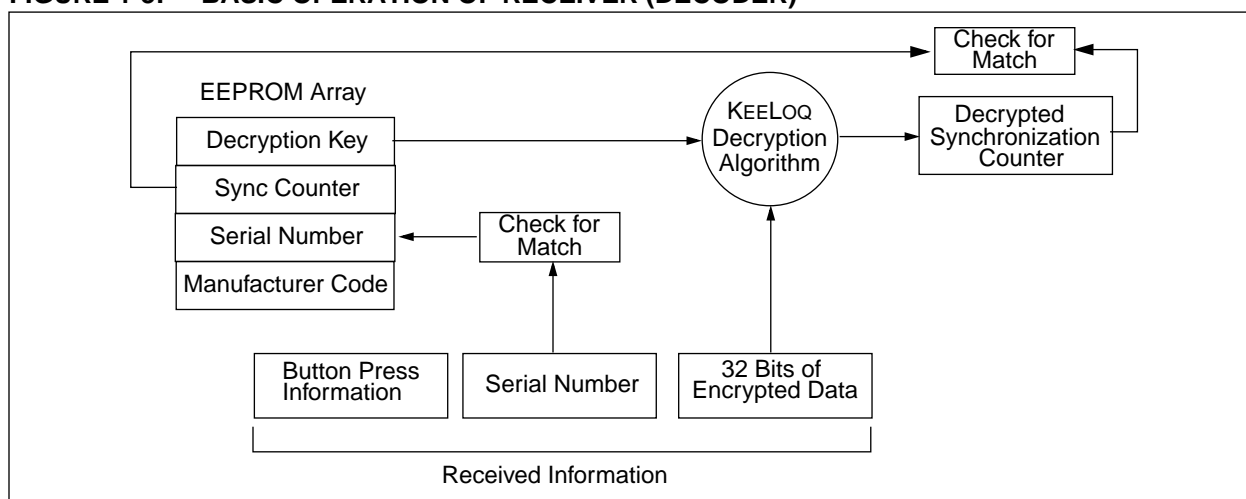
**FIGURE 1-1: CREATION AND STORAGE OF ENCRYPTION KEY DURING PRODUCTION**



**FIGURE 1-2: BASIC OPERATION OF TRANSMITTER (ENCODER)**



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



2.0 DEVICE OPERATION

As shown in the typical application circuits (Figure 2-1), the HCS361 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. A description of each pin is described in Table 2-1.

FIGURE 2-1: TYPICAL CIRCUITS

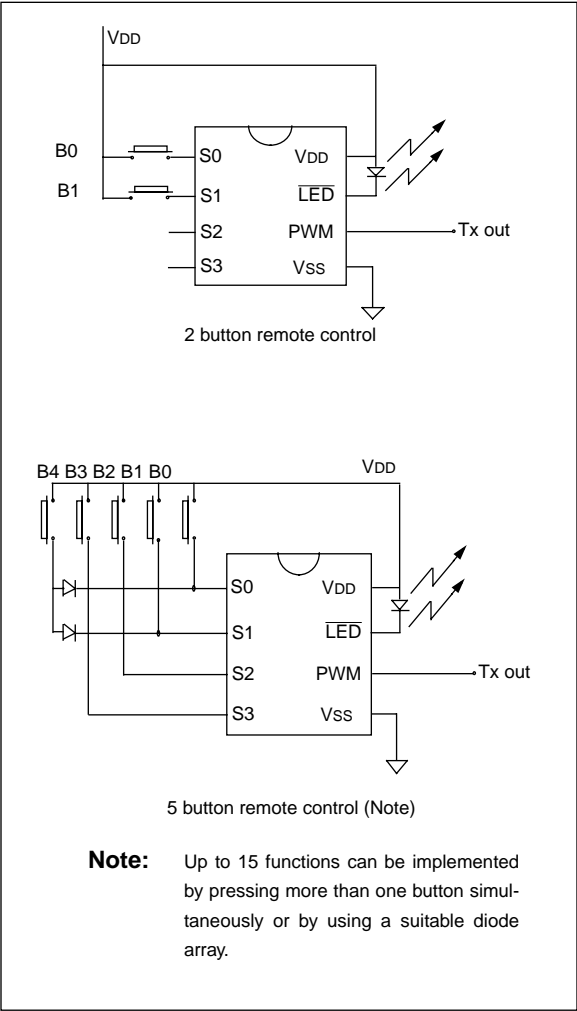


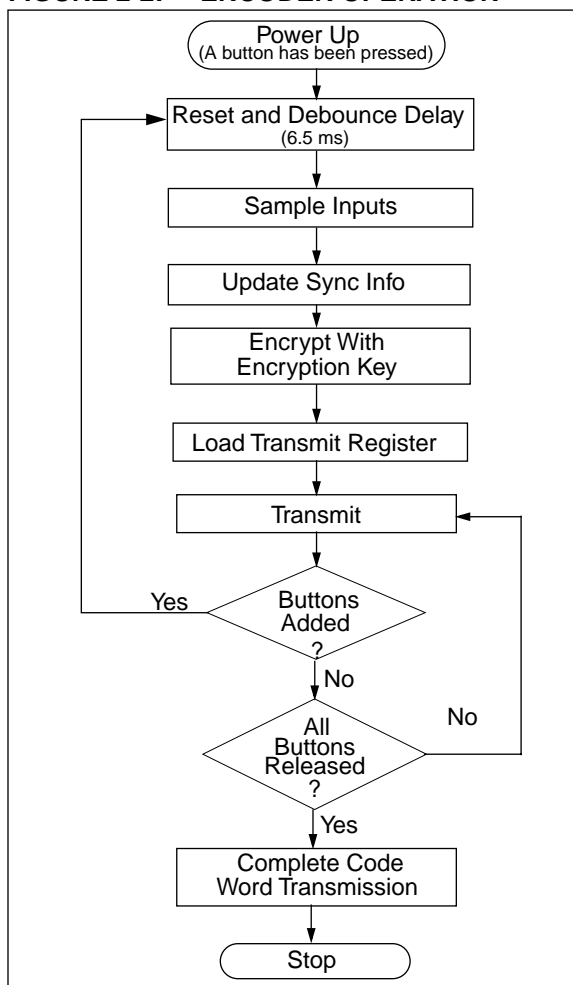
TABLE 2-1 PIN DESCRIPTIONS

Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2/Can also be clock pin when in programming mode
S3	4	Switch input 3/Clock pin when in programming mode
VSS	5	Ground reference connection
PWM	6	Pulse width modulation (PWM) output pin/Data pin for programming mode
LED	7	Cathode connection for directly driving LED during transmission
VDD	8	Positive supply voltage connection

The high security level of the HCS361 is based on the patented KEELQ technology. A block cipher type of encryption algorithm 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 the information in the previous transmission, the next coded transmission will be totally different. Statistically, if only one bit in the 32-bit string of information changes, approximately 50 percent of the coded transmission will change. The HCS361 will wake up upon detecting a switch closure and then delay approximately 6.5 ms for switch debounce (Figure 2-2). 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. 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 128K.

If in the transmit process it is detected that a new button(s) has been pressed, a reset will immediately be forced and the code word will not be completed. Please note that 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.

FIGURE 2-2: ENCODER OPERATION



### 3.0 EEPROM MEMORY ORGANIZATION

The HCS361 contains 192 bits (12 x 16-bit words) of EEPROM memory (Table 3-1). This EEPROM array is used to store the encryption key information, synchronization value, etc. Further descriptions of the memory array is given in the following sections.

TABLE 3-1 EEPROM MEMORY MAP

WORD ADDRESS	MNEMONIC	DESCRIPTION
0	KEY_0	64-bit encryption key (word 0)
1	KEY_1	64-bit encryption key (word 1)
2	KEY_2	64-bit encryption key (word 2)
3	KEY_3	64-bit encryption key (word 3)
4	SYNC_A	16-bit synchronization value
5	SYNC_B/SEED_2	16-bit synchronization or seed value (word 2)
6	RESERVED	Set to 0000H
7	SEED_0	Seed Value (word 0)
8	SEED_1	Seed Value (word 1)
9	SER_0	Device Serial Number (word 0)
10	SER_1	Device Serial Number (word 1)
11	CONFIG	Configuration Word

#### 3.1 Key 0 - Key 3 (64-Bit Encryption Key)

The 64-bit encryption key is used by the transmitter to create the encrypted message transmitted to the receiver. This key is created and programmed at the time of production using a key generation algorithm. Inputs to the key generation algorithm are the serial number for the particular transmitter being used and a secret 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. If a seed is used, the seed will also form part of the input to the key generation algorithm.

## 3.2 SYNC A, SYNC B (Synchronization Counter)

This is the 16-bit synchronization value that is used to create the hopping code for transmission. This value will be changed after every transmission. A second synchronization value can be used to stay synchronized with a second receiver.

## 3.3 SEED 0, SEED 1, and SEED 2 (Seed Word)

This is the three word (48 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.

## 3.4 SER 0, SER 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.

## 3.5 CONFIG (Configuration Word)

The configuration word is a 16-bit word stored in EEPROM array that is used by the device to store information used during the encryption process, as well as the status of option configurations. Further explanations of each of the bits are described in the following sections.

**TABLE 3-2 CONFIGURATION WORD**

Bit Number	Symbol	Bit Description
0	BACW	Blank Alternate Code Word
1	FAST	Baud Rate Selection
2	TXWAK	PWM mode: 1/6, 2/6 or 1/3, 2/3 select VPWM mode: Wakeup enable
3	SPM	Sync Pulse Modulation
4	SEED	Seed Transmission enable
5	DELM	Delay mode enable
6	TIMO	Time out enable
7	IND	Independent mode enable
8	USRA0	User bit
9	USRA1	User bit
10	USRB0	User bit
11	USRB1	User bit
12	XSER	Extended serial number enable
13	TMPSD	Temporary seed transmission enable
14	VPWM	VPWM select
15	OVR	Overflow bit

### 3.5.1 BACW: BLANK ALTERNATE CODE WORD

BACW = 1 selects the encoder to transmit every second code word. This can be used to reduce the average power transmitted over a 100ms window and thereby transmit a higher peak power.

### 3.5.2 FAST: SELECT FAST TRANSMISSION

FAST selects the baud rate. If FAST = 1, the baud rate is nominally 1667 bits per second and with FAST = 0, 833 bits per second.

### 3.5.3 TXWAK: BIT FORMAT SELECT OR WAKEUP

In PWM mode, this bit selects the bit format. If TXWAK = 1, the PWM pulse is 1/6;2/6 and for TXWAK = 0, 1/3;2/3 (Figure 4-1, VPWM = 0).

In VPWM mode, this bit enables the wake-up signal. With TXWAK = 1, transmission of the wake-up and dead time sequence is enabled (Figure 4-2, VPWM = 1). Wakeup is transmitted before the first code word of each transmission only. For TXWAK = 0, the transmission will skip wake-up and start transmitting the preamble portion of the code word (Figure 4-2, VPWM = 1).

### 3.5.4 SPM: SYNC PULSE MODULATION

Select modulation mode of Sync Pulse. If SPM = 1, the sync pulse is modulated (Figure 4-1 and Figure 4-2).

### 3.5.5 SEED: ENABLE SEED TRANSMISSION

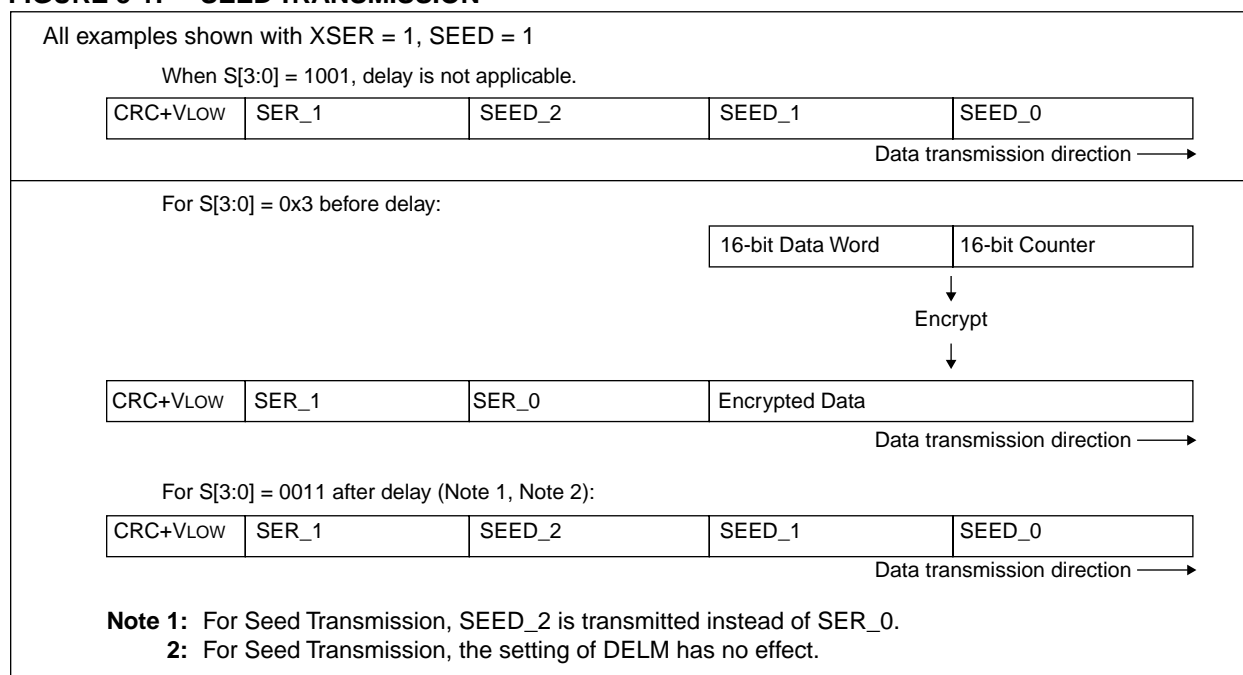
If SEED = 0, seed transmission is disabled. The independent counter mode can only be used with seed transmission disabled since SEED\_2 is shared with the second synchronization counter.

With SEED = 1, seed transmission is enabled. The appropriate button code(s) must be activated to transmit the seed information. In this mode, the seed infor-

mation (SEED\_0, SEED\_1, and SEED\_2) and the upper 12- or 16-bits of the serial number (SER\_1) are transmitted instead of the hop code.

Seed transmission is available for function codes (Table 3-7) S[3:0] = 1001 and S[3:0] = 0011 (delayed). This takes place regardless of the setting of the IND bit. The two seed transmissions are shown in Figure 3-1.

**FIGURE 3-1: SEED TRANSMISSION**



## 3.5.6 DELM: DELAY MODE

If DELM = 1, delay transmission is enabled. A delayed transmission is indicated by inverting the lower nibble of the discrimination value. The delay mode is primarily for compatibility with previous KEELOQ devices. If DELM = 0, delay transmission is disabled (Table 3-3).

**TABLE 3-3 TYPICAL DELAY TIMES**

TXWAK	FAST	Number of Code Words before Delay Mode	Time Before Delay Mode (VPWM = 0)
0	0	28	≈ 2.8s
0	1	56	≈ 2.9s
1	0	28	≈ 2.6s
1	1	56	≈ 2.8s

## 3.5.7 TIMO: TIME-OUT

If TIMO = 1, the time-out is enabled. Time-out can be used to terminate accidental continuous transmissions. When time-out occurs, the PWM output is set low and the LED is turned off. Current consumption will be higher than in standby mode since current will flow through the activated input resistors. This state can be exited only after all inputs are taken low. TIMO = 0, will enable continuous transmission (Table 3-4).

**TABLE 3-4 TYPICAL TIME-OUT TIMES**

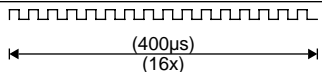
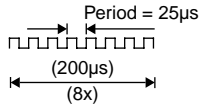

TXWAK	FAST	Maximum Number of Code Words Transmitted	Time Before Time-out (VPWM = 0)
0	0	256	≈ 25.6s
0	1	512	≈ 27.2s
1	0	256	≈ 23.8s
1	1	512	≈ 25.4s

## 3.5.8 IND: INDEPENDENT MODE

The independent mode can be used where one encoder is used to control two receivers. Two counters (SYNC\_A and SYNC\_B) are used in independent mode. As indicated in Table 3-7, function codes 1 to 7 use SYNC\_A and 8 to 15 SYNC\_B. The independent mode also selects IR mode. In IR mode function codes 12 to 15 will use counter B. The PWM output signal is modulated with a 40 kHz carrier. It must be pointed out the 40 kHz is derived from the internal clock and will therefore vary with the same percentage as the baud rate. If IND = 0, SYNC\_A is used for all function codes. If IND = 1, independent mode is enabled and counters for functions are used according to Table 3-7.

For IND = 1 and S[3:0] = 0xC, 0xD, 0xE, 0xF, Basic Pulse Width modulation becomes:

**TABLE 3-5 IR MODULATION**

TXWAK	FAST	Basic Pulse
0	0	
0 1	1 0	
1	1	

## 3.5.9 USRA,B: USER BITS

User bits form part of the discrimination value. The user bits together with the IND bit can be used to identify the counter that is used in independent mode.

## 3.5.10 XSER: EXTENDED SERIAL NUMBER

If XSER = 1, the full 32-bit serial number [SER\_1, SER\_0] is transmitted. If XSER = 0, the four most significant bits of the serial number are substituted by S[3:0] and is compatible with the HCS200/300/301.

## 3.5.11 TMPSD: TEMPORARY SEED TRANSMISSION

The temporary seed transmission can be used to disable learning after the transmitter has been used for a programmable number of operations. This feature can be used to implement very secure systems. After learning is disabled, the seed information cannot be accessed even if physical access to the transmitter is possible. If TMPSD = 1 the seed transmission will be disabled after a number of code hopping transmissions. The number of transmissions before seed transmission is disabled, can be programmed by setting the synchronization counter (SYNC\_A or SYNC\_B) to a value as shown in Table 3-6.

**TABLE 3-6 SYNCHRONOUS COUNTER INITIALIZATION VALUES**

Synchronous Counter Values	Number of Transmissions
0000H	128
0060H	64
0050H	32
0048H	16



TABLE 3-7 FUNCTION CODES

	S3	S2	S1	S0	IND = 0	IND = 1	Comments
					Counter		
1	0	0	0	1	A	A	
2	0	0	1	0	A	A	
3	0	0	1	1	A	A	If SEED = 1, transmit seed after delay.
4	0	1	0	0	A	A	
5	0	1	0	1	A	A	
6	0	1	1	0	A	A	
7	0	1	1	1	A	A	
8	1	0	0	0	A	B	
9	1	0	0	1	A	B	If SEED = 1, transmit seed immediately.
10	1	0	1	0	A	B	
11	1	0	1	1	A	B	
12	1	1	0	0	A	B IR mode	
13	1	1	0	1	A	B IR mode	
14	1	1	1	0	A	B IR mode	
15	1	1	1	1	A	B IR mode	

### 3.5.12 VPWM: VARIABLE PULSE WIDTH MODULATION

VPWM selects between VPWM modulation and PWM modulation. If VPWM = 1, VPWM modulation is selected as well as the following:

1. Enables the TXWAK bit to select the WAKEUP transmission.
2. Extends the Guard Time.

If VPWM = 0, PWM modulation is selected.

### 3.5.13 OVR: OVERFLOW

The overflow bit is used to extend the number of possible synchronization values. The synchronization counter is 16 bits in length, yielding 65,536 values before the cycle repeats. Under typical use of 10 operations a day, this will provide nearly 18 years of use before a repeated value will be used. Should the system designer conclude that is not adequate, then the overflow bit can be utilized to extend the number of unique values. This can be done by programming OVR to 1 at the time of production. The encoder will automatically clear OVR the first time that the transmitted synchronization value wraps from 0xFFFF to 0x0000. Once cleared, OVR cannot be set again, thereby creating a permanent record of the counter overflow. This prevents fast cycling of 64K counter. If the decoder system is programmed to track the overflow bits, then the effective number of unique synchronization values can be extended to 128K. If programmed to zero, the system will be compatible with the NTQ104/5/6 devices (i.e., no overflow with discrimination bits set to zero).

## 4.0 TRANSMITTED WORD

### 4.1 Transmission Format (PWM)

The HCS361 transmission is made up of several parts (Figure 4-1 and Figure 4-2). Each transmission is begun with a preamble and a header, followed by the encrypted and then the fixed data. The actual data is 67 bits which consists of 32 bits of encrypted data and 35 bits of fixed data. Each transmission is followed by a guard period before another transmission can begin. Refer to Table and Table for transmission timing specifications. The encrypted portion provides up to four billion changing code combinations and includes the function bits (based on which buttons were activated) along with the synchronization counter value and discrimination value. The non-encrypted portion is comprised of the CRC bits, VLOW bits, the function bits and the 28/32-bit serial number. The encrypted and non-encrypted sections combined increase the number of combinations to  $1.47 \times 10^{20}$ .

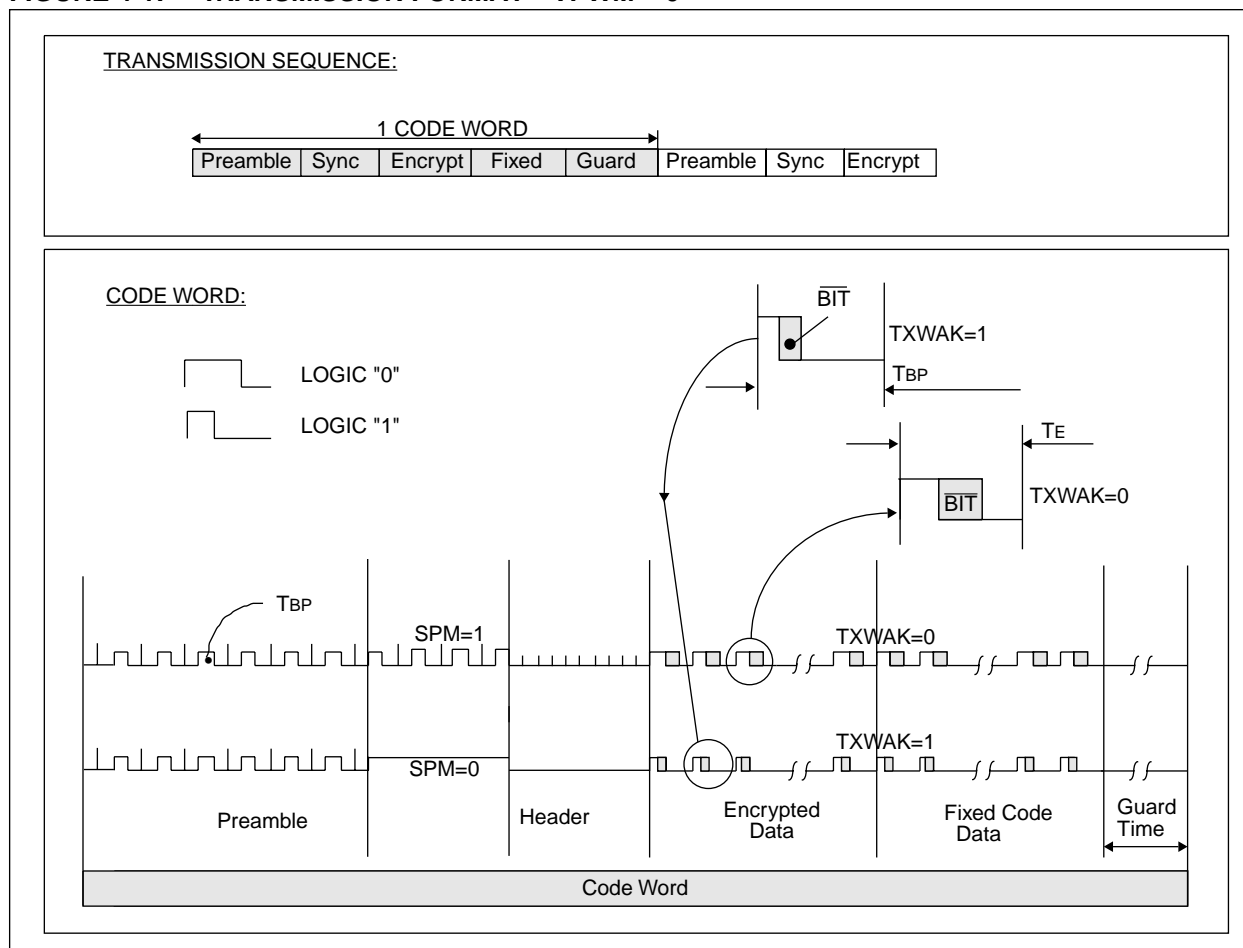
### 4.2 Code Word Organization

The HCS361 transmits a 67-bit code word when a button is pressed. The 67-bit word is constructed from a Fixed Code portion and an Encrypted Code portion (Figure 4-3).

The **Encrypted Data** is generated from 4 function bits, 2 user bits, overflow bit, independent mode bit, and 8 serial number bits, and the 16-bit synchronization value (Figure 8-4).

The **Non-encrypted Code Data** is made up of VLOW bit, 2 CRC bits, 4 function bits, and the 28-bit serial number. If the extended serial number (32 bits) is selected, the 4 function code bits will not be transmitted.

**FIGURE 4-1: TRANSMISSION FORMAT—VPWM = 0**



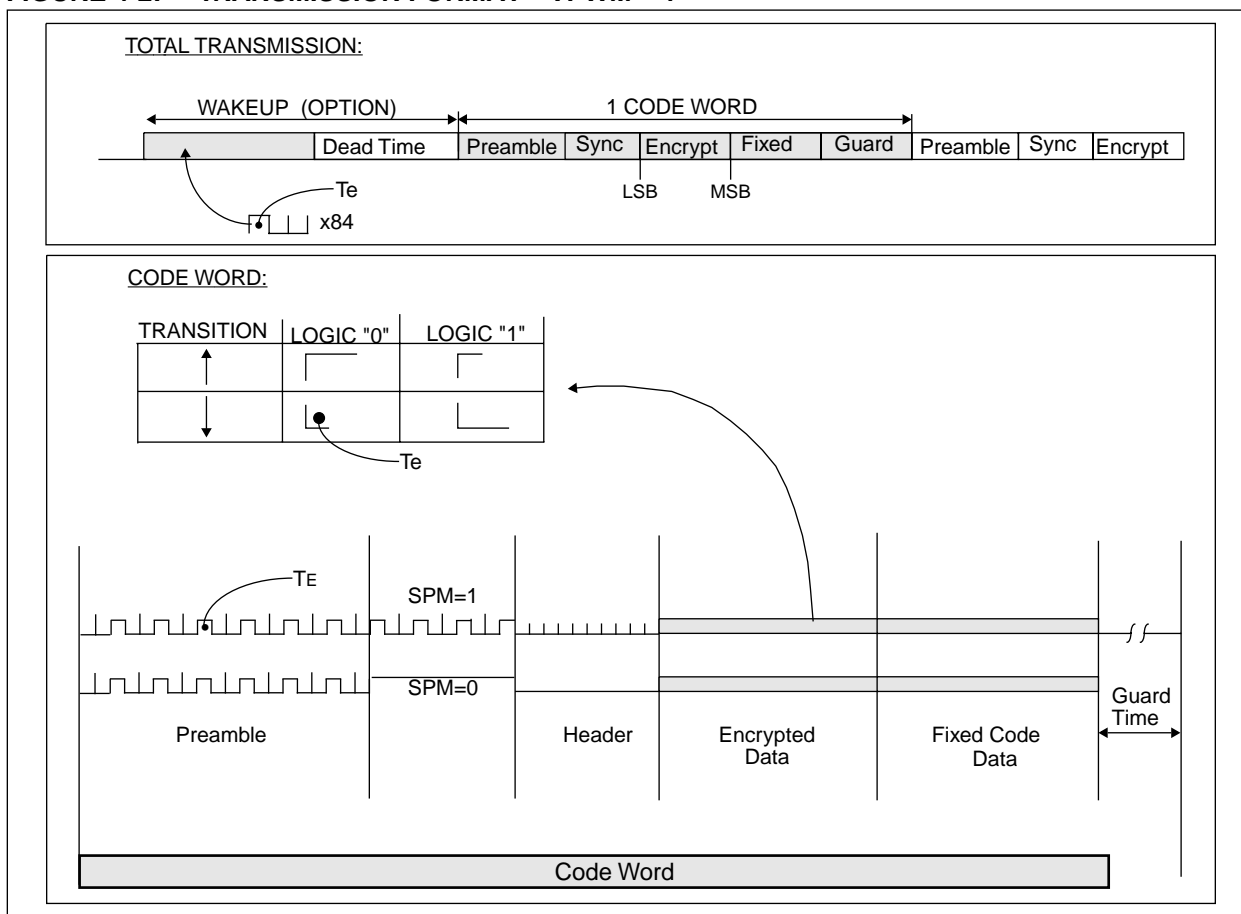
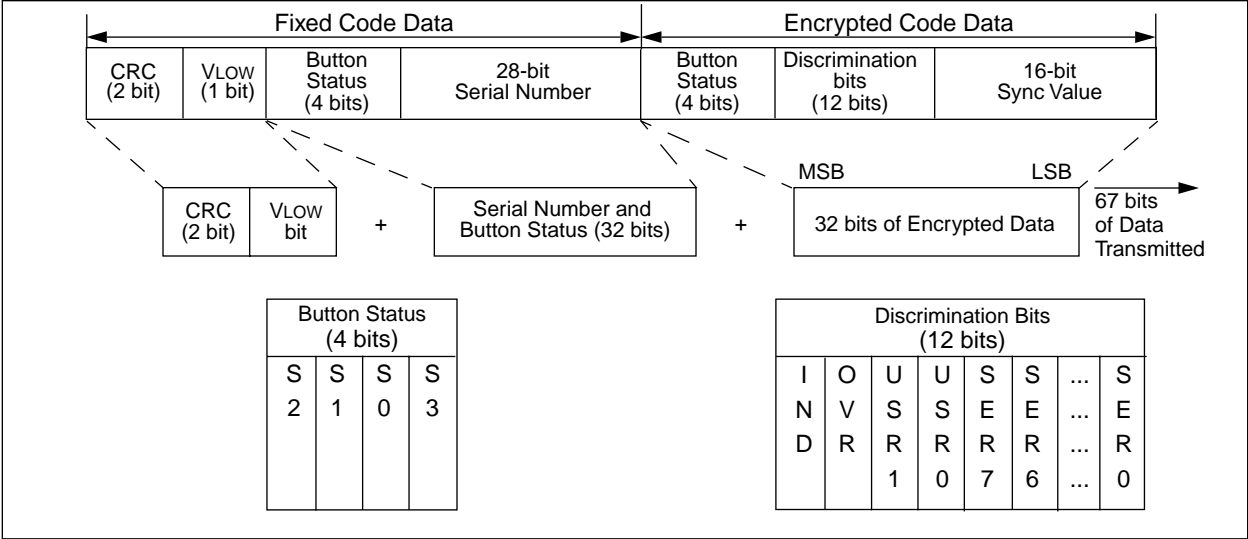
**FIGURE 4-2: TRANSMISSION FORMAT—VPWM = 1**

FIGURE 4-3: CODE WORD ORGANIZATION (RIGHT-MOST BIT IS CLOCKED OUT FIRST)



## 5.0 SPECIAL FEATURES

### 5.1 Code Word Completion

Code word completion is an automatic feature that ensures that the entire code word is transmitted, even if the button is released before the transmission is complete and that a minimum of two words are completed. The HCS361 encoder powers itself up when a button is pushed and powers itself down after the current transmission is finished, if the user has already released the button. If the button is held down beyond the time for two transmissions, then multiple transmissions will result. The HCS361 transmits at least two transmissions before powering down. If another button is activated during a transmission, the active transmission will be aborted and the new code will be generated using the new button information.

### 5.2 Blank Alternate Code Word

Federal Communications Commission (FCC) part 15 rules specify the limits on fundamental power and harmonics that can be transmitted. Power is calculated on the worst case average power transmitted in a 100ms window. It is therefore advantageous to minimize the duty cycle of the transmitted word. This can be achieved by minimizing the duty cycle of the individual bits and by blanking out consecutive words. Blank Alternate Code Word (BACW) is used for reducing the average power of a transmission (Figure 5-2). This is a selectable feature. Using the BACW allows the user to transmit a higher amplitude transmission if the transmission length is shorter. The FCC puts constraints on the average power that can be transmitted by a device, and BACW effectively prevents continuous transmission by only allowing the transmission of every second word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

### 5.3 CRC (Cycle Redundancy Check) Bits

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

#### EQUATION 5-1: CRC CALCULATION

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

and

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

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 calculation is incorrect, recalculate for the opposite value of VLOW.

### 5.4 Secure Learning

In order to increase the level of security in a system, it is possible for the receiver to implement what is known as a secure learning function. This can be done by utilizing the seed value on the HCS361 which is stored in EEPROM. Instead of the normal key generation method being used to create the encryption key, this seed value is used and there should not be any mathematical relationship between serial numbers and seeds for the best security.

### 5.5 Auto-shutoff

The Auto-shutoff function automatically stops the device from transmitting if a button inadvertently gets pressed for a long period of time. This will prevent the device from draining the battery if a button gets pressed while the transmitter is in a pocket or purse. This function can be enabled or disabled and is selected by setting or clearing the time-out bit (Section 3.5.7). Setting this bit will enable the function (turn Auto-shutoff function on) and clearing the bit will disable the function. Time-out period is approximately 25 seconds.

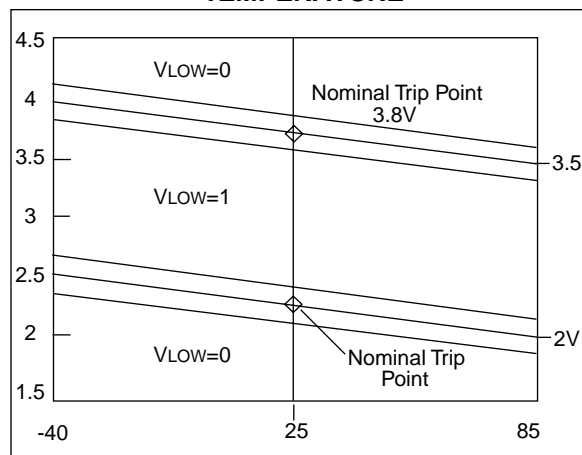
### 5.6 VLOW: Voltage LOW Indicator

The VLOW bit is transmitted with every transmission (Figure 4-3) and will be transmitted as a one if the operating voltage has dropped below the low voltage trip point, typically 3.8V at 25°C. This VLOW signal is transmitted so the receiver can give an indication to the user that the transmitter battery is low.

## 5.7 $\overline{\text{LED}}$ Output Operation

During normal transmission the  $\overline{\text{LED}}$  output is LOW while the data is being transmitted and high during the guard time. Two voltage indications are combined into one bit: VLOW. Table 5-1 indicates the operation value of VLOW while data is being transmitted.

**FIGURE 5-1: VLOW TRIP POINT VS. TEMPERATURE**



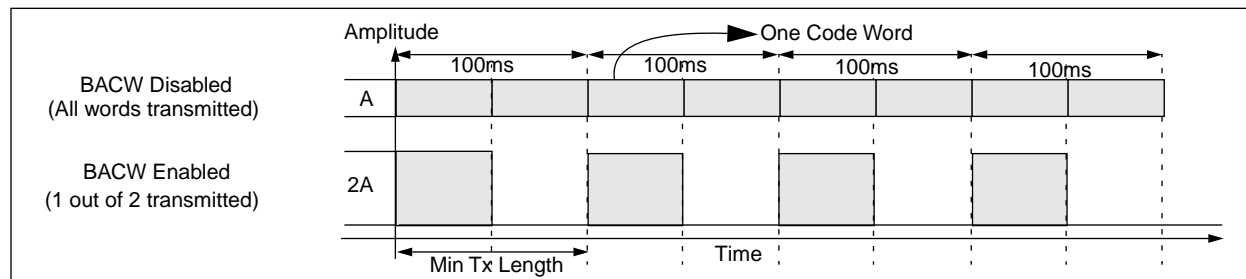
If the supply voltage drops below the low voltage trip point, the LED output will be toggled at approximately 1Hz during the transmission.

**TABLE 5-1 VLOW AND LED VS. VDD**

Approximate Supply Voltage	Vlow Bit	LED Operation*
Max → 3.8V	0	Normal
3.8V → 2.2V	1	Flashing
2.2V → Min	0	Normal

\*See also Flash operating modes.

**FIGURE 5-2: BLANK ALTERNATE CODE WORD**

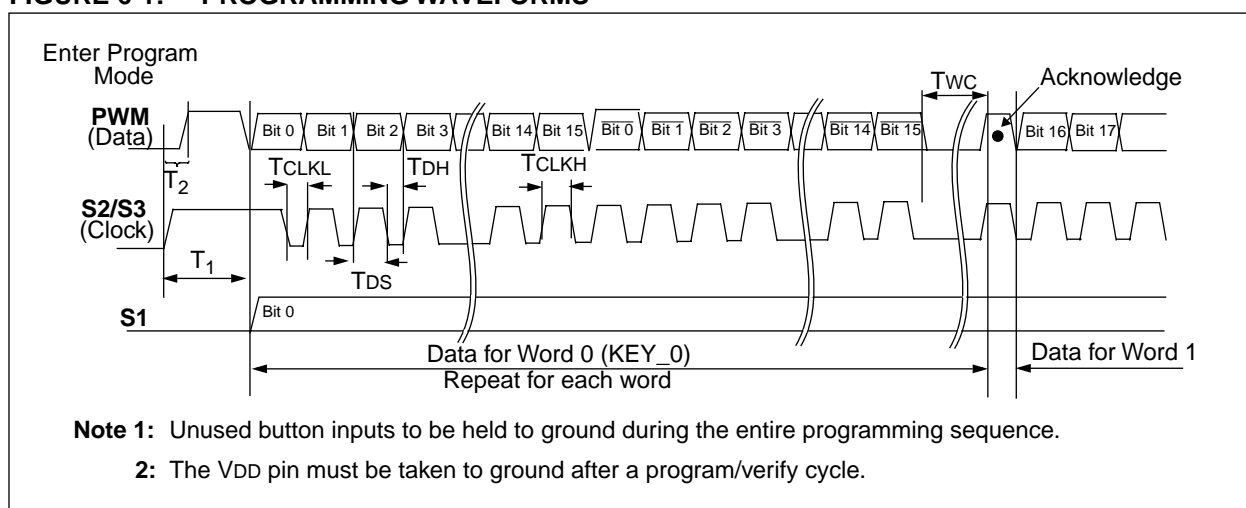


## 6.0 PROGRAMMING THE HCS361

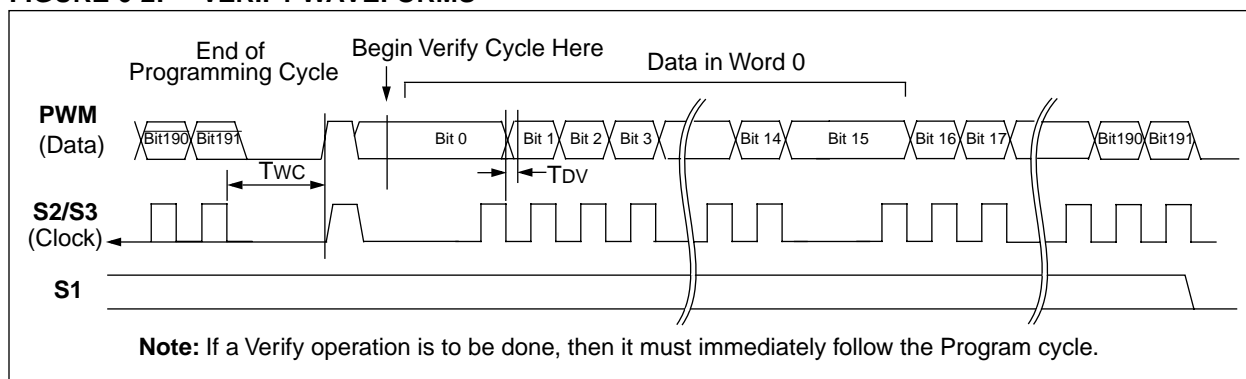
When using the HCS361 in a system, the user will have to program some parameters into the device including the serial number and the secret key before it can be used. The programming cycle allows the user to input all 192 bits in a serial data stream, which are then stored internally in EEPROM. Programming will be initiated by forcing the PWM line high, after the S3 line has been held high for the appropriate length of time. S0 should be held low during the entire program cycle. The S1 line on the HCS361 part needs to be set or cleared depending on the LS bit of the memory map (Key 0) before the key is clocked in to the HCS361. S1 must remain at this level for the duration of the programming cycle. The device can then be programmed by clocking in 16 bits at a time, followed by the word's

complement using S3 or S2 as the clock line and PWM as the data in line. After each 16-bit word is loaded, a programming delay is required for the internal program cycle to complete. An acknowledge bit can be read back after the programming delay (Twc). After the first word and its complement have been downloaded, an automatic bulk write is performed. This delay can take up to Twc. At the end of the programming cycle, the device can be verified (Figure 6-1) by reading back the EEPROM. Reading is done by clocking the S3 line and reading the data bits on PWM. 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.**

**FIGURE 6-1: PROGRAMMING WAVEFORMS**



**FIGURE 6-2: VERIFY WAVEFORMS**



**TABLE 6-1 PROGRAMMING/VERIFY TIMING REQUIREMENTS**

VDD = 5.0V ± 10% 25° C ± 5 °C				
Parameter	Symbol	Min.	Max.	Units
Program mode setup time	T <sub>2</sub>	0	4.9	ms
Hold time 1	T <sub>1</sub>	9.0	—	ms
Programming delay	TWC	—	30	ms
Clock low time	TCLKL	25	—	µs
Clock high time	TCLKH	25	—	µs
Data setup time	TDS	0	—	µs
Data hold time	TDH	18	—	µs
Data out valid time	TDV	—	24	µs



## 7.0 INTEGRATING THE HCS361 INTO A SYSTEM

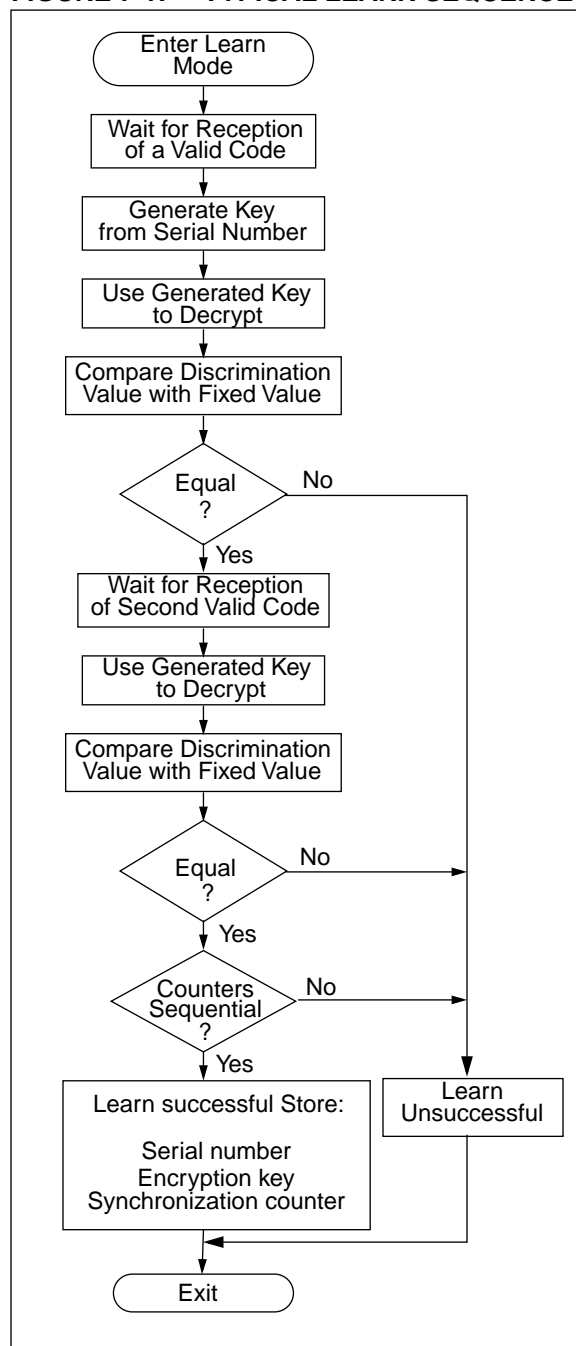
Use of the HCS361 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Firmware routines that accept transmissions from the HCS361 and decrypt the hopping code portion of the data stream are available. These routines provide system designers the means to develop their own decoding system.

### 7.1 Learning a Transmitter to a Receiver

In order for a transmitter to be used with a decoder, the transmitter must first be 'learned'. Several learning strategies can be followed in the decoder implementation. When a transmitter is learned to a decoder, it is suggested that the decoder stores the serial number and current synchronization value in EEPROM. The decoder must keep track of these values for every transmitter that is learned (Figure 7-1). The maximum number of transmitters that can be learned is only a function of how much EEPROM memory storage is available. The decoder must also store the manufacturer's code in order to learn a transmission transmitter, although this value will not change in a typical system so it is usually stored as part of the microcontroller ROM code. Storing the manufacturer's code as part of the ROM code is also better for security reasons.

It must be stated that some learning strategies have been patented and care must be taken not to infringe.

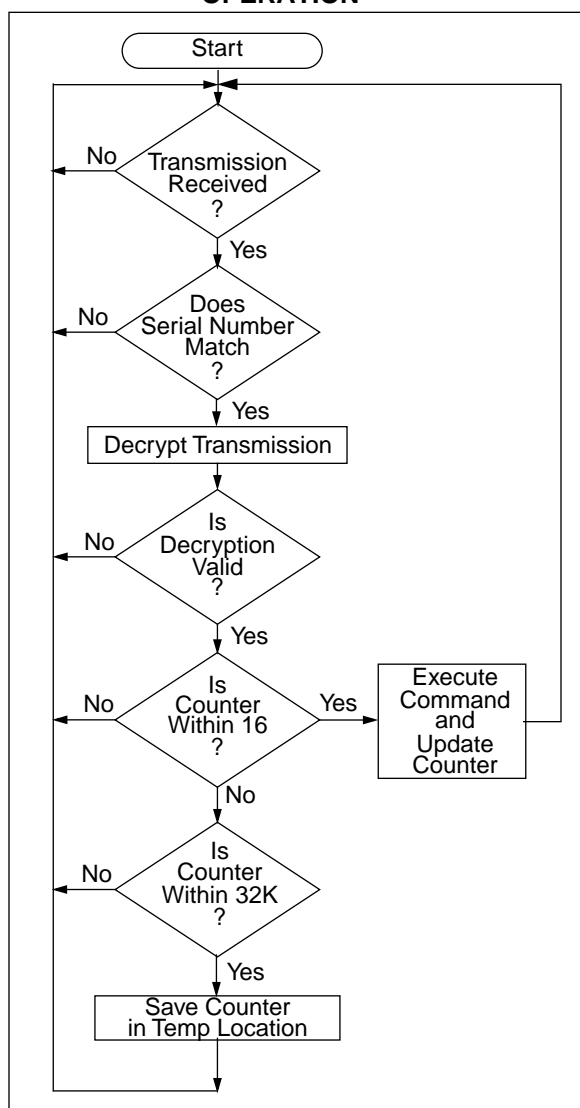
FIGURE 7-1: TYPICAL LEARN SEQUENCE



## 7.2 Decoder Operation

In a typical decoder operation (Figure 7-2), the key generation on the decoder side is done by taking the serial number from a transmission and combining that with the manufacturer's code to create the same secret key that was used by the transmitter. Once the secret key is obtained, the rest of the transmission can be decrypted. The decoder waits for a transmission and immediately can check the serial number to determine if it is a learned transmitter. If it is, it takes the encrypted portion of the transmission and decrypts it using the stored key. It uses the discrimination bits to determine if the decryption was valid. If everything up to this point is valid, the synchronization value is evaluated.

**FIGURE 7-2: TYPICAL DECODER OPERATION**

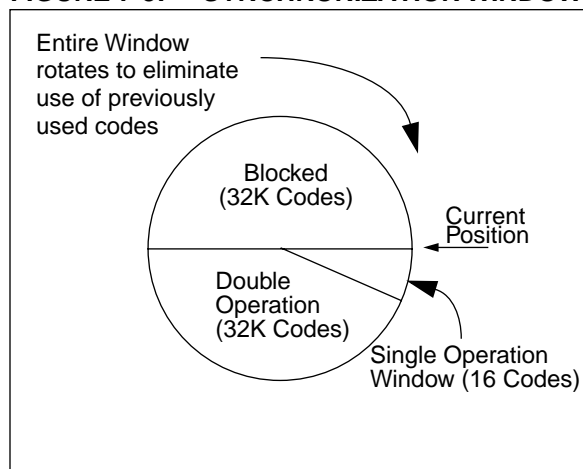


## 7.3 Synchronization with Decoder

The KEELOQ technology features a sophisticated synchronization technique (Figure 7-3) which does not require the calculation and storage of future codes. If the stored counter value for that particular transmitter and the counter value that was just decrypted are within a formatted window of say 16, the counter is stored and the command is executed. If the counter value was not within the single operation window, but is within the double operation window of say 32K window, the transmitted synchronization value is stored in temporary location and it goes back to waiting for another transmission. When the next valid transmission is received, it will check the new value with the one in temporary storage. If the two values are sequential, it is assumed that the counter had just gotten out of the single operation 'window', but is now back in sync, so the new synchronization value is stored and the command executed. If a transmitter has somehow gotten out of the double operation window, the transmitter will not work and must be relearned. Since the entire window rotates after each valid transmission, codes that have been used are part of the 'blocked' (32K) codes and are no longer valid. This eliminates the possibility of grabbing a previous code and retransmitting to gain entry.

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

**FIGURE 7-3: SYNCHRONIZATION WINDOW**



## 8.0 ELECTRICAL CHARACTERISTICS

**TABLE 8-1 ABSOLUTE MAXIMUM RATINGS**

Symbol	Item	Rating	Units
VDD	Supply voltage	-0.3 to 6.9	V
VIN	Input voltage	-0.3 to VDD + 0.3	V
VOUT	Output voltage	-0.3 to VDD + 0.3	V
IOUT	Max output current	25	mA
TSTG	Storage temperature	-55 to +125	°C (Note)
TLSOL	Lead soldering temp	300	°C (Note)
VESD	ESD rating	4000	V

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

**TABLE 8-2 DC CHARACTERISTICS**

Commercial (C): Tamb = 0°C to +70°C									
Industrial (I): Tamb = -40°C to +85°C									
		2.0V < VDD < 3.3			3.0 < VDD < 6.6				
Parameter	Sym.	Min	Typ <sup>1</sup>	Max	Min	Typ <sup>1</sup>	Max	Unit	Conditions
Operating current (avg)	ICC		0.3	1.2		0.7	1.6	mA	VDD = 3.3V VDD = 6.6V
Standby current	ICCS		0.1	1.0		0.1	1.0	µA	
Auto-shutoff current <sup>2,3</sup>	ICCS		40	75		160	350	µA	
High level Input voltage	VIH	0.55VDD		VDD+0.3	0.55VDD		VDD+0.3	V	
Low level input voltage	VIL	-0.3		0.15VDD	-0.3		0.15VDD	V	
High level output voltage	VOH	0.7VDD			0.7VDD			V	IOH = -1.0mA, VDD = 2.0V IOH = -2.0mA, VDD = 6.6V
Low level output voltage	VOL			0.08VDD			0.08VDD	V	IOL = 1.0mA, VDD = 2.0V IOL = 2.0mA, VDD = 6.6V
LED sink current	ILED	0.15	1.0	4.0	0.15	1.0	4.0	mA	VLED <sup>4</sup> = 1.5V, VDD = 6.6V
Resistance; S0-S3	RS0-3	40	60	80	40	60	80	KΩ	VDD = 4.0V
Resistance; PWM	RPWM	80	120	160	80	120	160	KΩ	VDD = 4.0V

**Note 1:** Typical values are at 25°C.

**2:** Auto-shutoff current specification does not include the current through the input pulldown resistors.

**3:** Auto-shutoff current is periodically sampled and not 100% tested

**4:** VLED is the voltage between the VDD pin and the LED pin.

FIGURE 8-1: POWER UP AND TRANSMIT TIMING

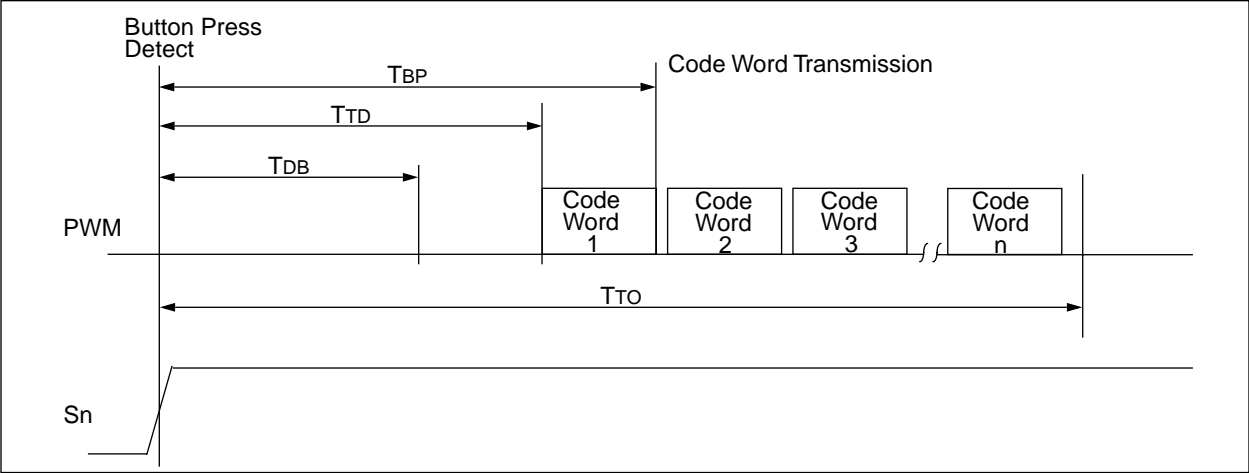
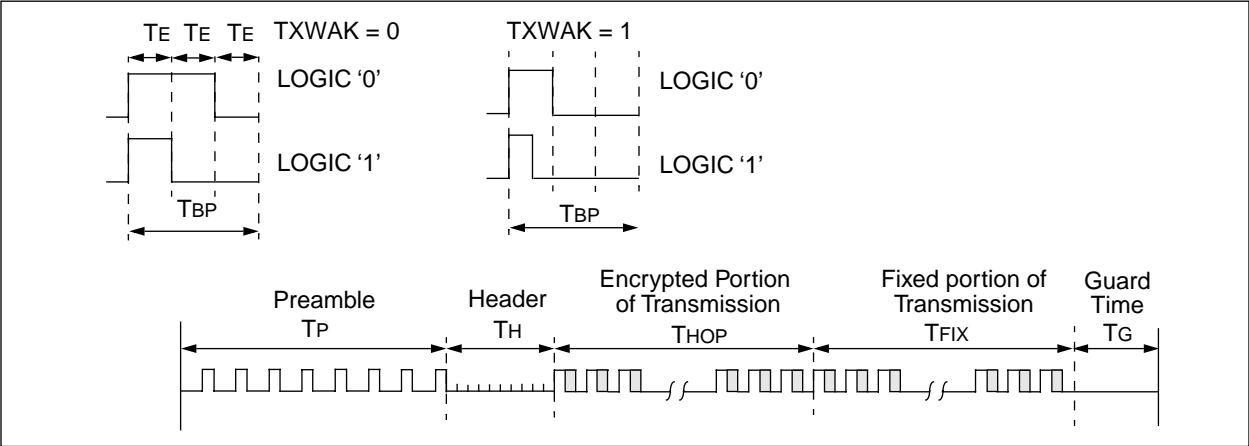


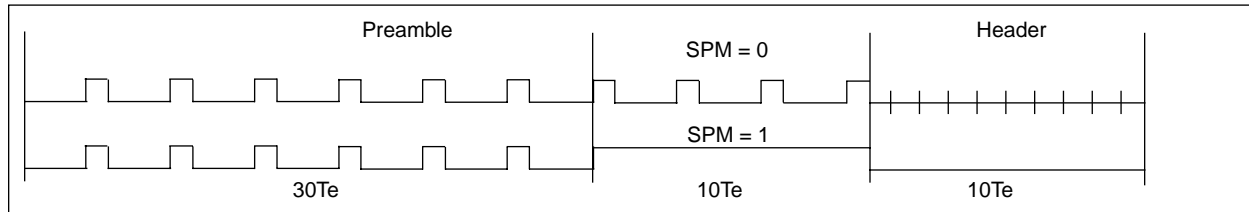
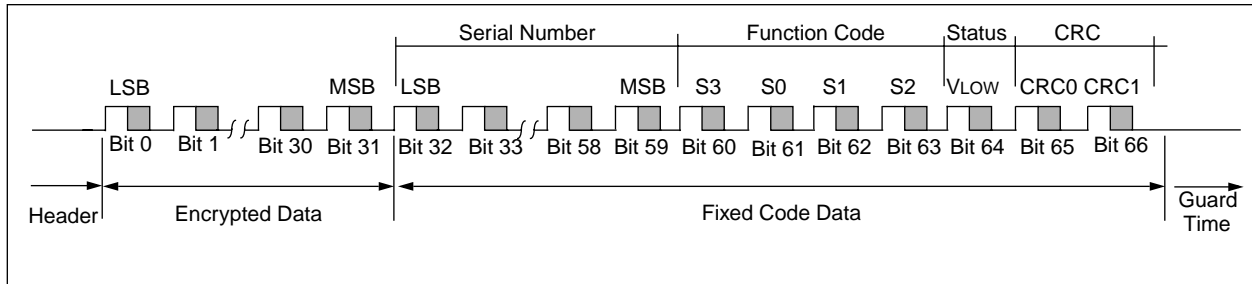
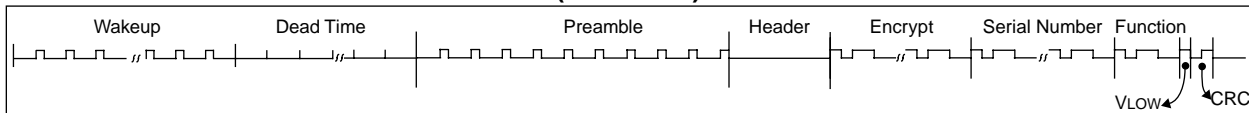
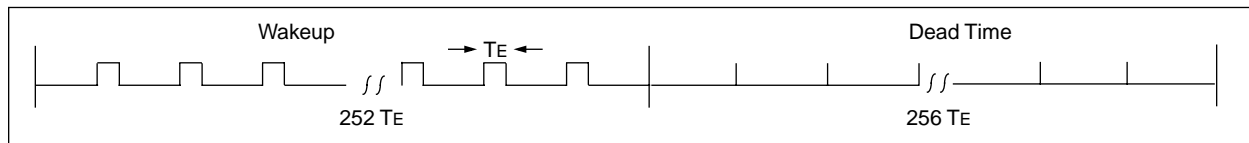
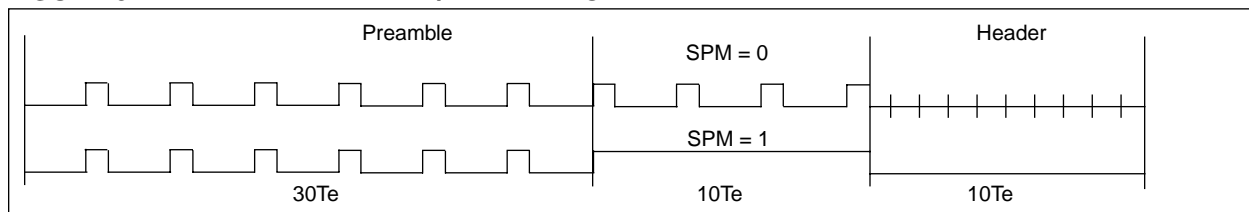
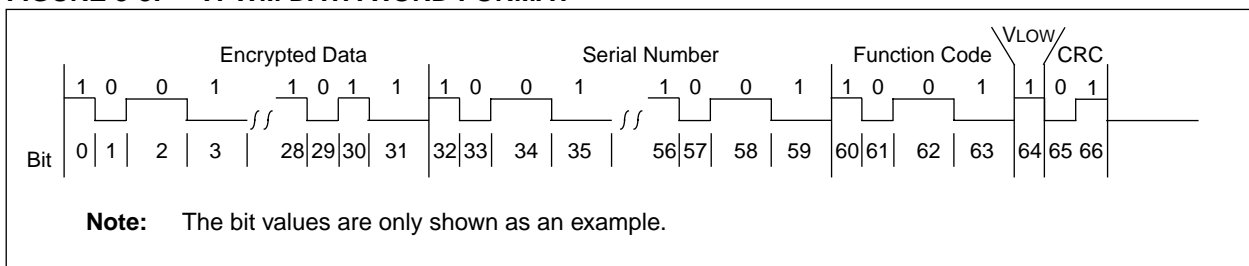
TABLE 8-3 POWER UP AND TRANSMIT TIMING REQUIREMENTS

VDD = +2.0 to 6.6V					
Commercial (C): Tamb = 0°C to +70°C					
Industrial (I): Tamb = -40°C to +85°C					
Parameter	Symbol	Min	Max	Unit	Remarks
Time to second button press	TBP	10 + Code Word Time	26 + Code Word Time	ms	(Note 1)
Transmit delay from button detect	TTD	4.5	26	ms	(Note 2)
Debounce delay	TDB	4	13	ms	
Auto-shutoff time-out period	TTO	15	35	s	(Note 3)

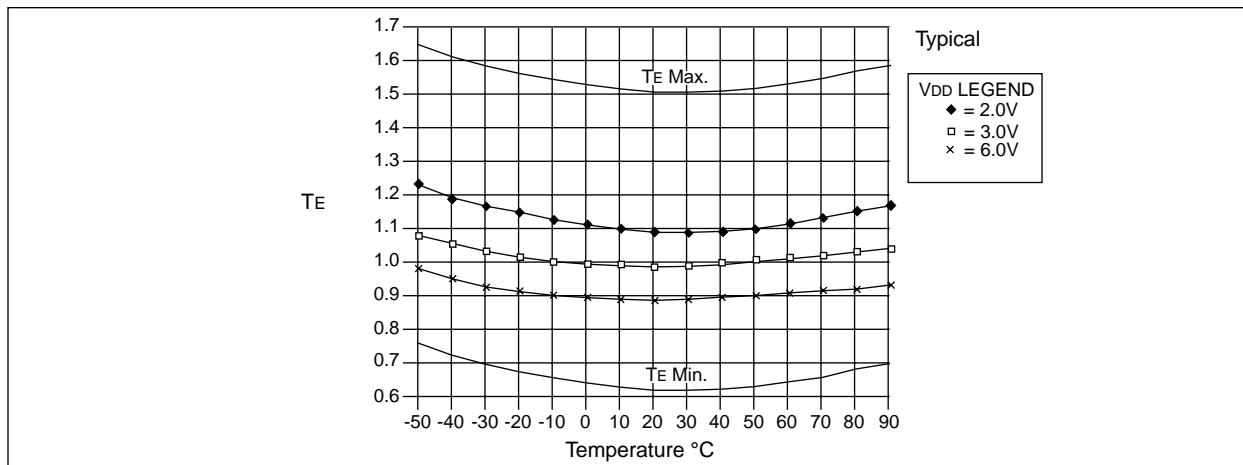
- Note 1:** TBP is the time in which a second button can be pressed without completion of the first code word and the intention was to press the combination of buttons.
- 2:** Transmit delay maximum value if the previous transmission was successfully transmitted.
- 3:** The auto shutoff timeout period is not tested.

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



**FIGURE 8-3: PWM PREAMBLE/HEADER FORMAT****FIGURE 8-4: PWM DATA WORD FORMAT****FIGURE 8-5: VPWM FORMAT SUMMARY (VPWM = 1)****FIGURE 8-6: VPWM WAKEUP FORMAT****FIGURE 8-7: VPWM PREAMBLE/HEADER FORMAT****FIGURE 8-8: VPWM DATA WORD FORMAT**

**FIGURE 8-9: HCS361 NORMALIZED TE VS. TEMP**



**TABLE 8-4 CODE WORD TRANSMISSION TIMING PARAMETERS**

**PWM Mode (TXWAK = 0)**

VDD = +2.0 to 6.6V Commercial (C):Tamb = 0°C to +70°C Industrial (I):Tamb = -40°C to +85°C			Code Words Transmitted							
			FAST = 0, TXWAK = 0			FAST = 1, TXWAK = 0				
Symbol	Characteristic	Number of TE	Min	Typ.	Max.	Number of TE	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	260	400	620	1	130	200	310	μs
TBP	PWM bit pulse width	3	780	1200	1860	3	390	600	930	μs
TP	Preamble duration	30	7.8	12.0	18.6	30	3.9	6.0	9.3	ms
TH	Header duration	10	2.6	4.0	6.2	10	1.3	2.0	3.1	ms
THOP	Hopping code duration	96	25.0	38.4	59.5	96	12.5	19.2	29.8	ms
TFIX	Fixed code duration	105	27.3	42.0	65.1	105	13.7	21.0	32.6	ms
TG	Guard Time	16	4.2	6.4	9.9	32	4.2	6.4	9.9	ms
—	Total Transmit Time	257	66.8	102.8	159.3	273	35.5	54.6	84.6	ms
—	PWM data rate	—	1282	833	538	—	2564	1667	1075	bps

**Note:** The timing parameters are not tested but derived from the oscillator clock.

**PWM Mode (TXWAK = 1)**

VDD = +2.0 to 6.6V Commercial (C):Tamb = 0°C to +70°C Industrial (I):Tamb = -40°C to +85°C			Code Words Transmitted							
			FAST = 0, TXWAK = 1			FAST = 1, TXWAK = 1				
Symbol	Characteristic	Number of TE	Min	Typ.	Max.	Number of TE	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	130	200	310	1	65	100	155	μs
TBP	PWM bit pulse width	6	780	1200	1860	6	390	600	930	μs
TP	Preamble duration	30	3.9	6.0	9.3	30	2.0	3.0	4.7	ms
TH	Header duration	10	1.3	2.0	3.1	10	0.7	1.0	1.6	ms
THOP	Hopping code duration	192	25.0	38.4	59.5	192	12.5	19.2	29.8	ms
TFIX	Fixed code duration	210	27.3	42.0	65.1	210	13.7	21.0	32.6	ms
TG	Guard Time	32	4.2	6.4	9.9	64	4.2	6.4	9.9	ms
—	Total Transmit Time	474	61.6	94.8	146.9	506	32.9	50.6	78.4	ms
—	PWM data rate	—	1282	833	538	—	2564	1667	1075	bps

**Note:** The timing parameters are not tested but derived from the oscillator clock.

**TABLE 8-5 CODE WORD TRANSMISSION TIMING PARAMETERS****VPWM Mode (FAST = 0)**

VDD = +2.0 to 6.6V Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C			Code Words Transmitted							
			FAST = 0, Shortest			FAST = 0, Longest				
Symbol	Characteristic	Number of TE	Min	Typ.	Max.	Number of TE	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	260	400	620	1	260	400	620	μs
TP	Preamble duration	30	7.8	12.0	18.6	30	7.8	12.0	18.6	ms
TH	Header duration	10	2.6	4.0	6.2	10	2.6	4.0	6.2	ms
THOP	Hopping code duration	32	8.3	12.8	19.8	64	16.6	25.6	39.7	ms
TFIX	Fixed code duration	35	9.1	14.0	21.7	70	18.2	28.0	43.4	ms
TG	Guard Time	112	29.1	44.8	69.4	112	29.1	44.8	69.4	ms
—	Total Transmit Time	219	56.9	87.6	135.8	286	74.4	114.4	177.3	ms
—	VPWM data rate	—	3846	2500	1613	—	3846	2500	1613	bps

**Note:** The timing parameters are not tested but derived from the oscillator clock.

**VPWM Mode (FAST = 1)**

VDD = +2.0 to 6.6V Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C			Code Words Transmitted							
			FAST = 1, Shortest			FAST = 1, Longest				
Symbol	Characteristic	Number of TE	Min	Typ.	Max.	Number of TE	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	130	200	310	1	130	200	310	μs
TP	Preamble duration	30	3.9	6.0	9.3	30	3.9	6.0	9.3	ms
TH	Header duration	10	1.3	2.0	3.1	10	1.3	2.0	3.1	ms
THOP	Hopping code duration	32	4.2	6.4	9.9	64	8.3	12.8	19.8	ms
TFIX	Fixed code duration	35	4.6	7.0	10.9	70	9.1	14.0	21.7	ms
TG	Guard Time	224	29.1	44.8	69.4	224	29.1	44.8	69.4	ms
—	Total Transmit Time	331	43.3	66.2	102.6	398	51.7	79.6	123.4	ms
—	VPWM data rate	—	7692	5000	3226	—	7692	5000	3226	bps

**Note:** The timing parameters are not tested but derived from the oscillator clock.

NOTES:



**NOTES:**

NOTES:

## HCS361 PRODUCT IDENTIFICATION SYSTEM

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

<b>HCS361</b>	—	<b>/P</b>	
			<b>Package:</b>
			P = Plastic DIP (300 mil Body), 8-lead
			SN = Plastic SOIC (150 mil Body), 8-lead
			<b>Temperature Range:</b>
			Blank = 0°C to +70°C
			I = -40°C to +85°C
			<b>Device:</b>
			HCS361 Code Hopping Encoder
			HCS361T Code Hopping Encoder (Tape and Reel)

### Sales and Support

#### Data Sheets

Products supported by a preliminary Data Sheet may have an errata sheet describing minor operational differences and recommended workarounds. To determine if an errata sheet exists for a particular device, please contact one of the following:

1. Your local Microchip sales office
2. The Microchip Corporate Literature Center U.S. FAX: (602) 786-7277
3. The Microchip Worldwide Web Site ([www.microchip.com](http://www.microchip.com))



## WORLDWIDE SALES AND SERVICE

### AMERICAS

#### Corporate Office

Microchip Technology Inc.  
2355 West Chandler Blvd.  
Chandler, AZ 85224-6199  
Tel: 480-786-7200 Fax: 480-786-7277  
Technical Support: 480-786-7627  
Web Address: <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: 630-285-0071 Fax: 630-285-0075

#### Dallas

Microchip Technology Inc.  
4570 Westgrove Drive, Suite 160  
Addison, TX 75248  
Tel: 972-818-7423 Fax: 972-818-2924

#### Dayton

Microchip Technology Inc.  
Two Prestige Place, Suite 150  
Miamisburg, OH 45342  
Tel: 937-291-1654 Fax: 937-291-9175

#### Detroit

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

#### Los Angeles

Microchip Technology Inc.  
18201 Von Karman, Suite 1090  
Irvine, CA 92612  
Tel: 949-263-1888 Fax: 949-263-1338

#### New York

Microchip Technology Inc.  
150 Motor Parkway, Suite 202  
Hauppauge, NY 11788  
Tel: 631-273-5305 Fax: 631-273-5335

#### San Jose

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

### AMERICAS (continued)

#### 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 Asia Pacific  
Unit 2101, Tower 2  
Metroplaza  
223 Hing Fong Road  
Kwai Fong, N.T., Hong Kong  
Tel: 852-2-401-1200 Fax: 852-2-401-3431

#### Beijing

Microchip Technology, Beijing  
Unit 915, 6 Chaoyangmen Bei Dajie  
Dong Erhuan Road, Dongcheng District  
New China Hong Kong Manhattan Building  
Beijing 100027 PRC  
Tel: 86-10-85282100 Fax: 86-10-85282104

#### India

Microchip Technology Inc.  
India Liaison Office  
No. 6, Legacy, Convent Road  
Bangalore 560 025, India  
Tel: 91-80-229-0061 Fax: 91-80-229-0062

#### Japan

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

#### Korea

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

#### Shanghai

Microchip Technology  
RM 406 Shanghai Golden Bridge Bldg.  
2077 Yan'an Road West, Hong Qiao District  
Shanghai, PRC 200335  
Tel: 86-21-6275-5700 Fax: 86 21-6275-5060

### ASIA/PACIFIC (continued)

#### Singapore

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

#### Taiwan, R.O.C

Microchip Technology Taiwan  
10F-1C 207  
Tung Hua North Road  
Taipei, Taiwan, ROC  
Tel: 886-2-2717-7175 Fax: 886-2-2545-0139

### EUROPE

#### United Kingdom

Arizona Microchip Technology Ltd.  
505 Eskdale Road  
Wokingham  
Berkshire, England RG41 5TU  
Tel: 44 118 921 5858 Fax: 44-118 921-5835

#### Denmark

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

#### France

Arizona Microchip Technology SARL  
Parc d'Activite du Moulin de Massy  
43 Rue du Saule Trapu  
Batiment A - 1er Etage  
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 München, Germany  
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

#### Italy

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

11/15/99



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

All rights reserved. © 1999 Microchip Technology Incorporated. Printed in the USA. 11/99 Printed on recycled paper.

Information contained in this publication regarding device applications and the like is intended for suggestion only and may be superseded by updates. No representation or warranty is given and no liability is assumed by Microchip Technology Incorporated with respect to the accuracy or use of such information, or infringement of patents or other intellectual property rights arising from such use or otherwise. Use of Microchip's products as critical components in life support systems is not authorized except with express written approval by Microchip. No licenses are conveyed, implicitly or otherwise, under any intellectual property rights. The Microchip logo and name are registered trademarks of Microchip Technology Inc. in the U.S.A. and other countries. All rights reserved. All other trademarks mentioned herein are the property of their respective companies.