HCS370

KEELOQ® Code Hopping Encoder

FEATURES

Security

- Two programmable 32-bit serial numbers
- Two programmable 64-bit encoder keys
- Two programmable 60-bit seed values
- Each transmission is unique
- 67/69-bit transmission code length
- 32-bit hopping code
- Encoder keys are read protected

Operating

- 2.0-5.5V operation
- Six button inputs
- 15 functions available
- Four selectable baud rates
- Selectable minimum code word completion
- Battery low signal transmitted to receiver
- Nonvolatile synchronization data
- PWM, VPWM, PPM and Manchester modulation
- Button queue information transmitted
- Dual Encoder functionality

Other

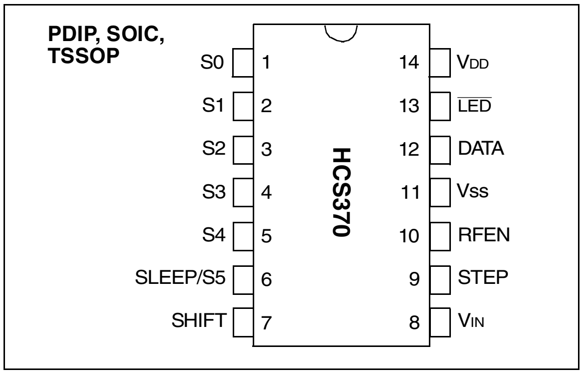
- On-chip EEPROM
- On-chip tuned oscillator (±10%)
- Button inputs have internal pull-down resistors
- $\overline{\text{LED}}$ output
- PLL control for ASK and FSK
- Low external component count
- Step-up voltage regulator

Typical Applications

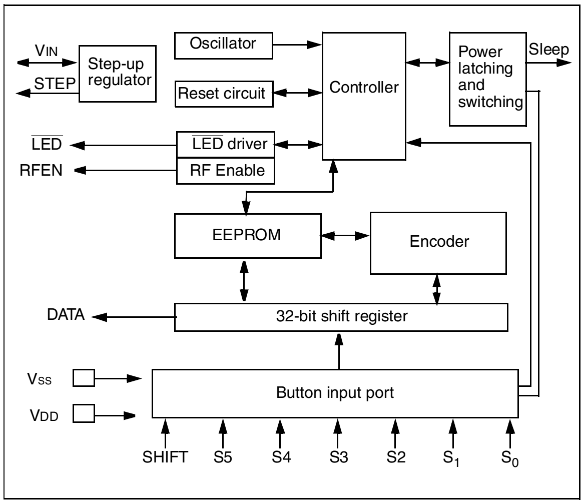
The HCS370 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

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

PACKAGE TYPES



HCS370 BLOCK DIAGRAM



GENERAL DESCRIPTION

The HCS370 is a code hopping encoder designed for secure Remote Keyless Entry (RKE) and secure remote control systems. The HCS370 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 authentication systems and access control systems.

The HCS370 combines a hopping code generated by a nonlinear encryption algorithm, with a serial number and status bits to create a secure transmission code. The length of the transmission effectively eliminates the threat of code scanning and the code hopping resists code grabbing access techniques.

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 encoder key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS370 a very secure unit. The HCS370 provides an easy to use serial interface for programming the necessary security keys, system parameters, and configuration data.

The HCS370 can be configured to function as two totally separate encoders allowing easy integration of two KEELOQ systems into a single transmitter. This, for example, enables the user to use the same transmitter to open a car and garage door.

The encoder 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 HCS370 operates over a wide voltage range of 2.0V to 5.5V 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.

The step-up voltage regulator switches an external transistor and inductor at 125 kHz to power the RF transmitter. A diode catches the inductor energy and stores it on the output capacitor. A voltage divider sets the output voltage by stopping the step-up pulses whenever V_{IN} > 1.2V.

1.0 SYSTEM OVERVIEW

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

- Code Hopping - A method by which a code changes in a predictable way each time it is transmitted.
- Code-word - A block of data that is repeatedly transmitted during a ***transmission***.
- Decoder - A device that can decode data sent by an ***encoder***.
- Decryption algorithm - A recipe whereby scrambled data can be unscrambled using the same ***encryption key*** used to scramble the data.
- Encoder - A device that can generate and encode data.
- Encoder key - A unique and secret digital number used to encrypt and decrypt data. (***encryption key***)
- Encryption Algorithm - A recipe whereby data is scrambled using an ***encryption key*** before it becomes public. The data can only be interpreted by using a ***decryption algorithm*** using the same ***encryption key***.
- Learn – The KEELOQ 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 encoder key, decrypt the discrimination value and the synchronization counter.
  - Secure Learn
    The transmitter is activated through a special button combination to transmit a stored 60-bit value (random seed) that can be used for key generation or be part of the key. Transmission of the seed can be disabled after learning is completed.
- Manufacturer's code – A unique and secret code used to generate unique ***encryption keys*** for each ***encoder***.
- RKE - Remote Keyless Entry
- Transmission - A stream of data consisting of repeating ***code-words***.

As indicated in the block diagram on page one, the HCS370 has a small EEPROM array which must be loaded with several parameters before use. The most important values for each encoder are:

- A 32-bit serial number which is meant to be unique for every encoder
- An encoder key
- A 16/20-bit synchronization value
- Configuration options

This information is programmed by the manufacturer at the time of production. The generation of the encoder keys is done using a key generation algorithm, as shown in 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 synchronization value is the basis for the transmitted code changing with 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. 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 encoder 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 3.2.

Any type of controller may be used as a decoder, but it is typically a microcontroller with compatible firmware that allows the decoder to operate in conjunction with a encoder, based on the HCS370.

Before an encoder can be used with a particular decoder, the encoder must be 'learned' by the decoder. Upon learning an encoder, information is stored by the decoder so that it may track the encoder, including the serial number of the encoder, the current synchronization value for that encoder and the same encoder key that is used on the encoder. If a decoder receives a message of valid format, the serial number is checked. If it is from a learned encoder, 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 decoder and the values received from the encoder.

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

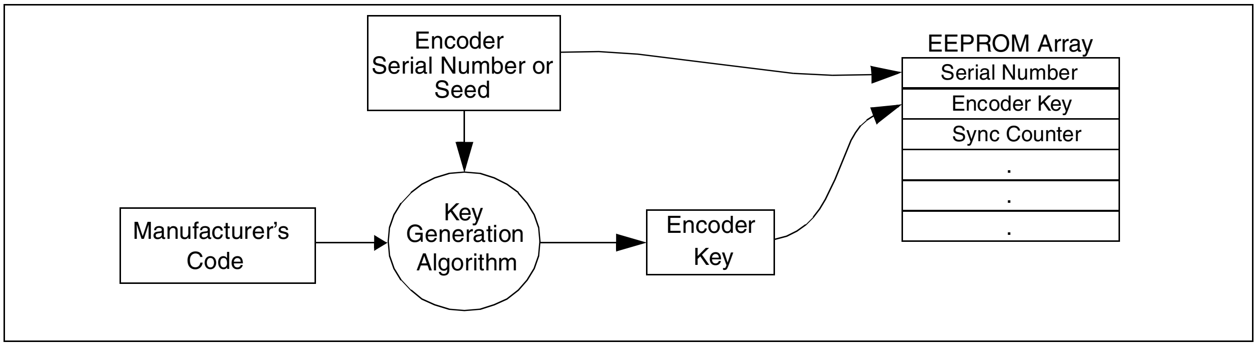


FIGURE 1-2: BASIC OPERATION OF ENCODER

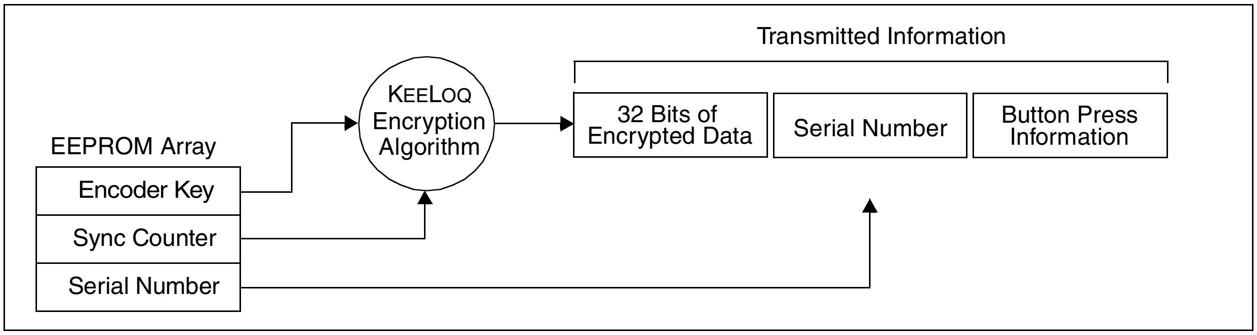
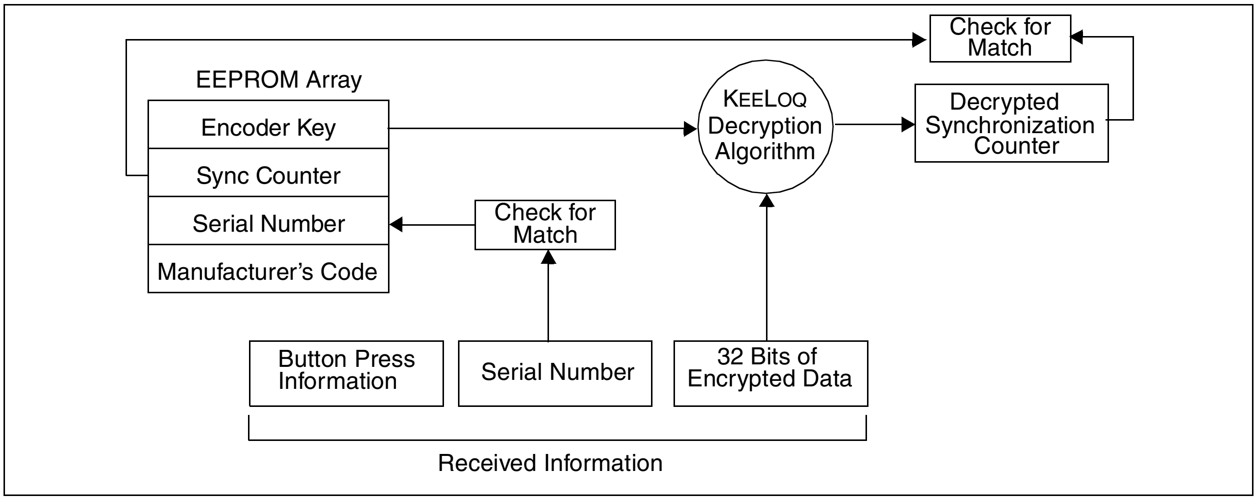


FIGURE 1-3: BASIC OPERATION OF DECODER



2.0 DEVICE DESCRIPTION

As shown in the typical application circuits (Figure 2-1), the HCS370 is an easy device to use. It requires only the addition of buttons and RF circuitry for use as the encoder in your security application. A description of each pin is described in Table 2-1. Refer to Figure 2-2 for information on the I/O pins.

> **Note:** S0-S4 have pulldown resistors and Vin, S5 and SHIFT must be externally tied to a supply rail.

TABLE 2-1 PIN DESCRIPTIONS

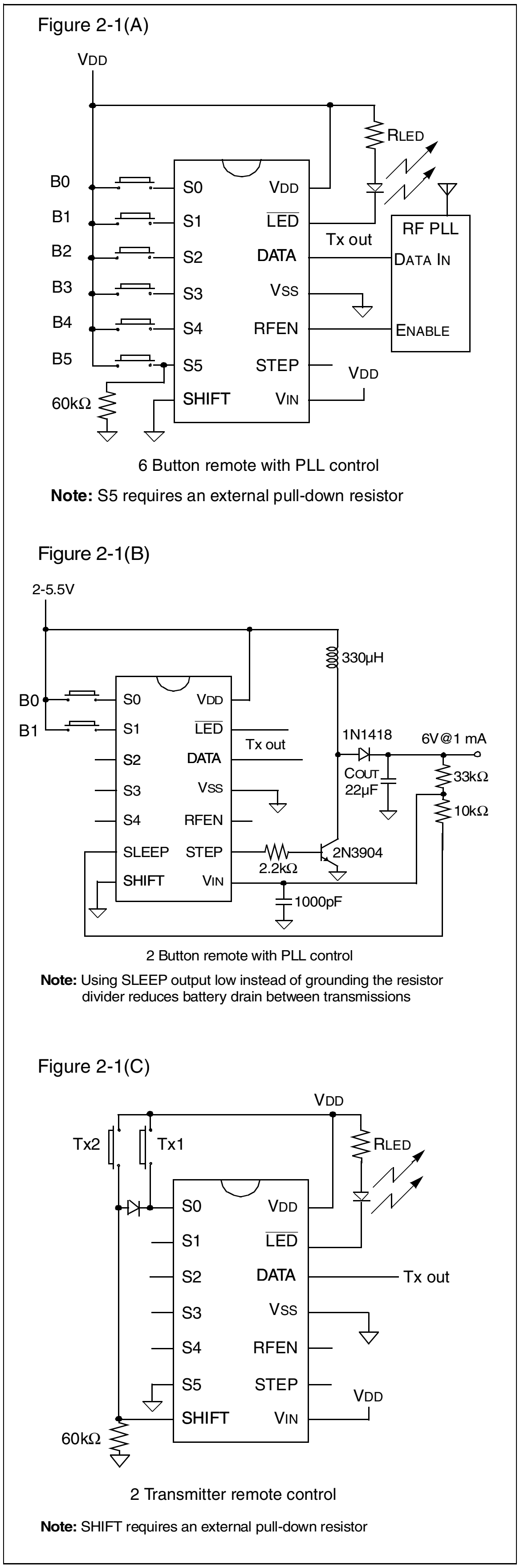
Name	Pin Number	Description
S0	1	Switch input S0
S1	2	Switch input S1
S2	3	Switch input S2
S3	4	Switch input S3
S4	5	Switch input S4
S5/SLEEP	6	Switch input S5, or SLEEP output
SHIFT	7	Shift input
VIN	8	Step-up regulator input
STEP	9	Step-up pulses output
RFEN	10	RF enable output
VSS	11	Ground reference
DATA	12	Transmission output pin
$\overline{\text{LED}}$	13	Open drain output for $\overline{\text{LED}}$ with pull-up resistor
VDD	14	Positive supply voltage

TABLE 2-2 FUNCTION CODES

Button	Function
S0	F[xx1x]
S1	F[x1xx]
S2	F[1xxx]
S3	F[xxx1]
S4	F[111x]
S5	F[11x1]

Note: The function code is repeated in the encrypted and unencrypted data of a transmission.

FIGURE 2-1: TYPICAL CIRCUITS



6 Button remote with PLL control

Note: S5 requires an external pull-down resistor

2 Button remote with PLL control

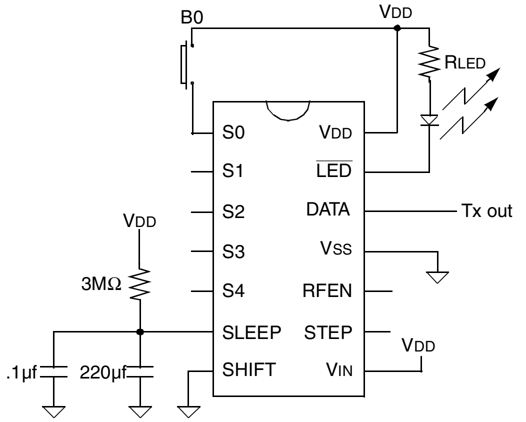
Note: Using SLEEP output low instead of grounding the resistor divider reduces battery drain between transmissions

2 Transmitter remote control

Note: SHIFT requires an external pull-down resistor

TYPICAL CIRCUITS (*Continued*)

Figure 2-1(D)



Incremental transmissions once per minute

Note: SHIFT must be tied low

FIGURE 2-2: I/O CIRCUITS

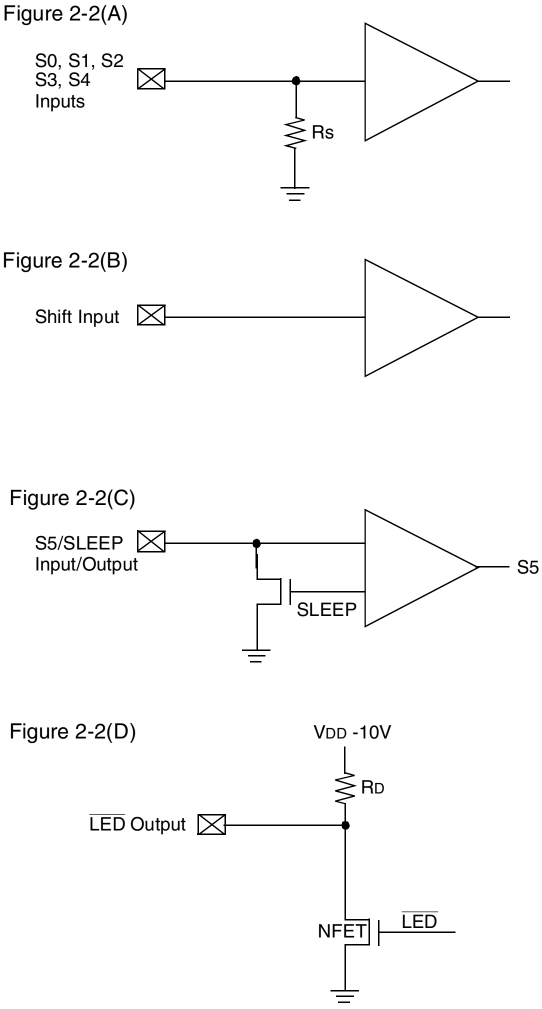


Figure 2-2(A)

Figure 2-2(B)

Figure 2-2(C)

Figure 2-2(D)

I/O CIRCUITS (*Continued*)

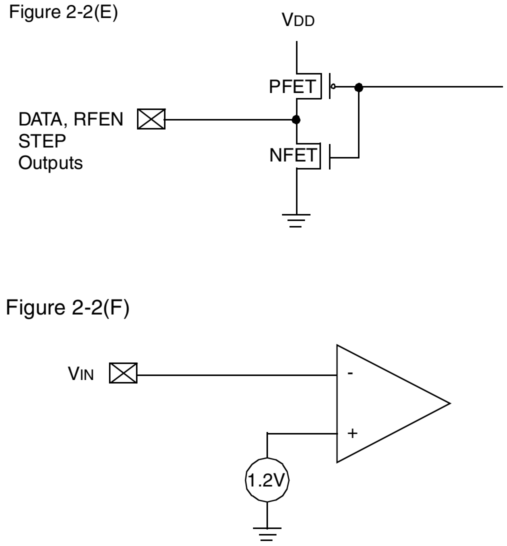


Figure 2-2(E)

Figure 2-2(F)

2.1 Architectural Overview

2.1.1 ONBOARD EEPROM

The HCS370 has an onboard nonvolatile EEPROM, which is used to store user programmable data and the synchronization counter. The data is 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 initial counter value is also programmed at the time of production. From then on the device maintains the counter itself. The HCS370 has built-in redundancy and protection against counter corruption. During every EEPROM write, the internal circuitry also ensures that the internal charge pump voltage required to write to the EEPROM is at an acceptable level.

2.1.2 INTERNAL RC OSCILLATOR

The HCS370 has an onboard RC oscillator that controls all the logic output timing characteristics. The oscillator frequency varies ±10% over voltage and temperature range from the factory calibrated value. All the timing values specified in this document are subject to this oscillator variation.

2.1.3 LOW VOLTAGE DETECTOR

A low battery voltage detector onboard the HCS370 can indicate when the operating voltage drops below a predetermined value. There are two options available depending on the Low Voltage Trip Point Select (VLOWSEL) configuration option. The two options provided are:

- A 2.2 V nominal level for 3V operation
- A 3.2 V nominal level for 5V operation

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 LED changes as well to further indicate that the battery is low and needs replacing.

The output of the Low Voltage Detector can also be latched once it has dropped below the selected value. The Low Voltage Latch (VLOWL) configuration option enables this option. If this option is enabled, the detector level is raised to 3V or 5V once a low battery voltage has been detected. The original value is reinstated, if the V_{DD} voltage is raised above this level, indicating that a new battery has been installed.

2.1.4 STEP-UP VOLTAGE REGULATOR

The step-up regulator samples V_{IN}, and if it is less than 1.2 volts, turns on the step-up pulses. Figure 2-1(B) shows a typical implementation to generate a higher voltage for the RF circuitry. The higher voltage increases transmitter range and the regulation holds that range as the battery discharges.

3.0 DEVICE OPERATION

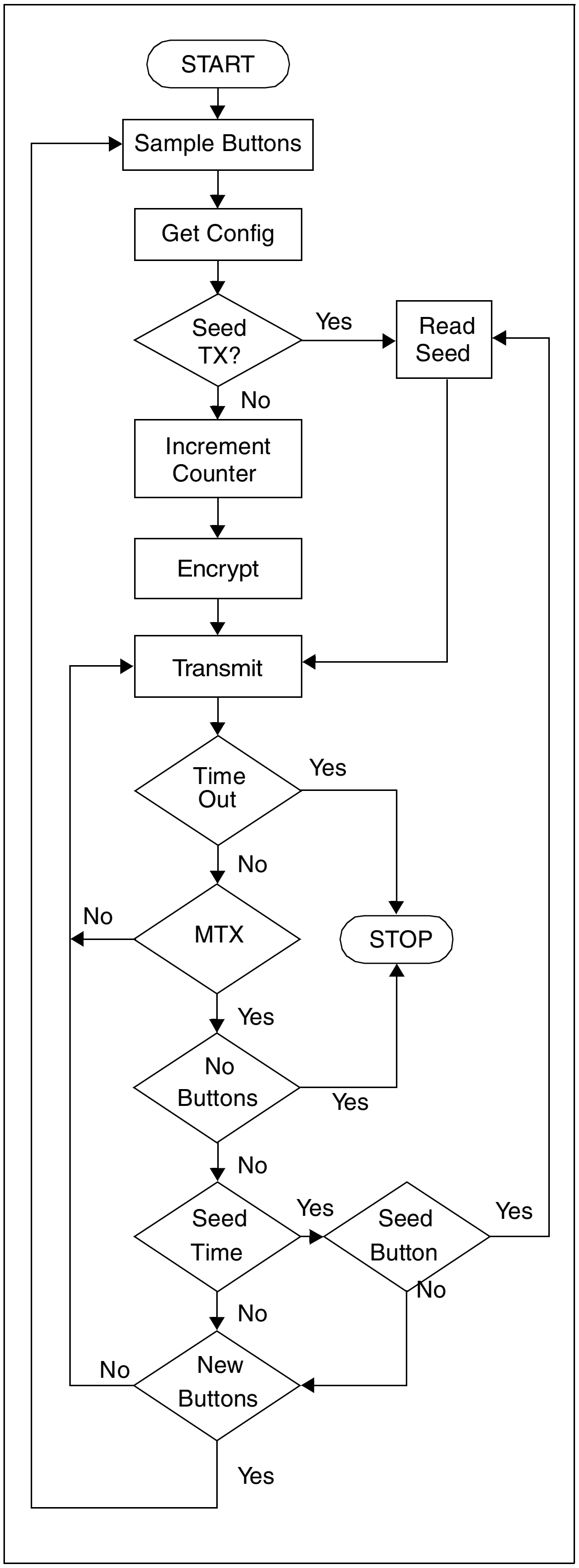
The HCS370 will normally be in a low power sleep mode. When a button input is taken high, the device will wakeup, start the step-up regulator and go through debounce delay of 20ms (TDB) before the button code is latched. The device will then read the configuration options and depending on the configuration options and the button code, it will determine what the data and modulation format will be for the transmission. The transmission will consist of a stream of code-words and will be transmitted TDU after the button is pressed and as long as the buttons are held down or a time-out occurs. The code-word format can be either a code hopping format or a seed format.

The time-out time can be selected with the Time-out Select (TSEL) configuration option. This option allows the time-out to be disabled or set to 0.8s, 3.2s or 25.6s. When a timeout 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, a minimum number of code-words will still be completed. The minimum code-words can be set to 1,2,4 or 8 using the minimum code words (MTX) 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.

A summary table of all the options is given in Section 5.0.

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



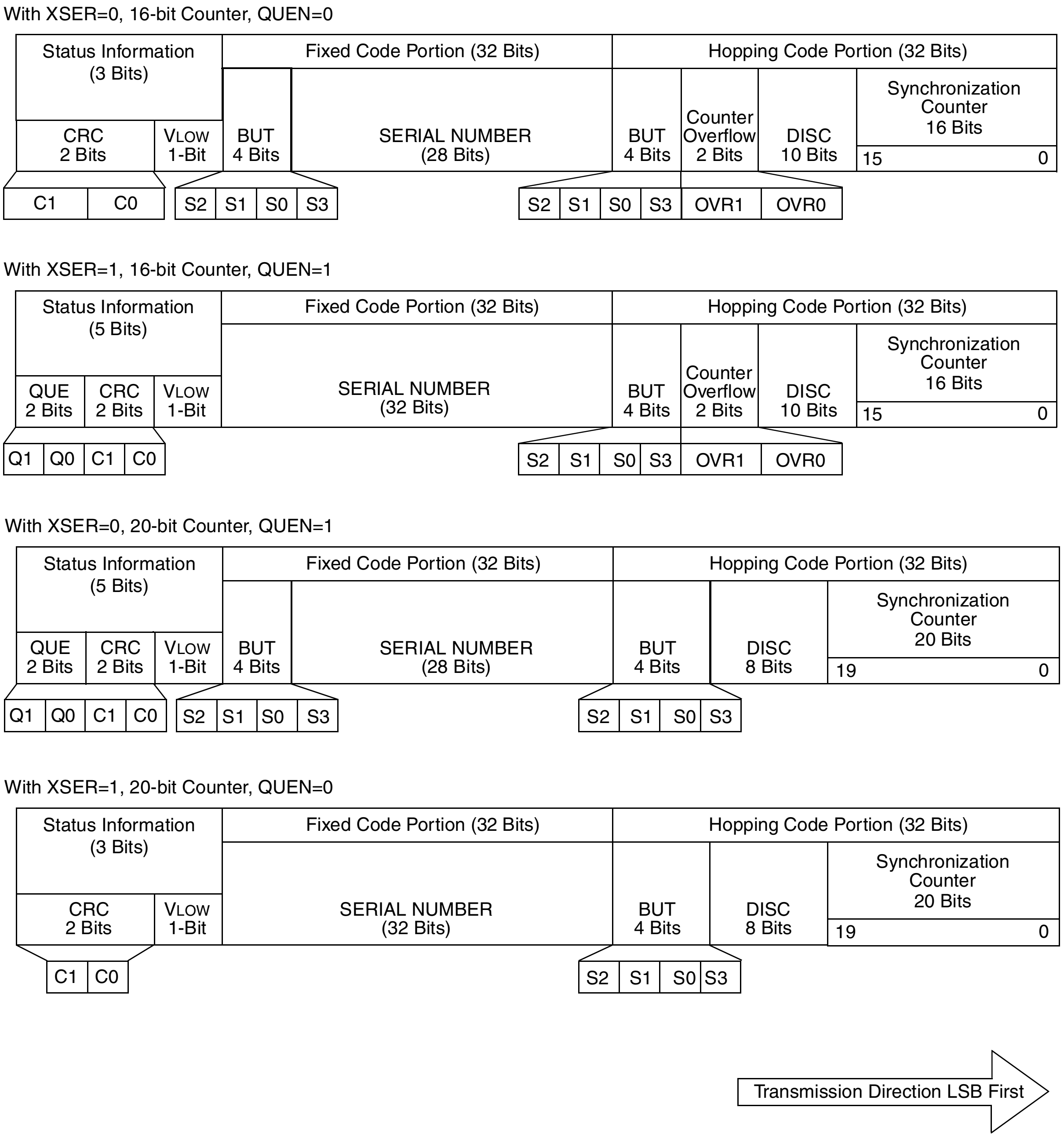
3.1 Dual Encoder Operation

The HCS370 contains two transmitter configuration words, serial numbers, encoder keys, discrimination values, counters and seed values. This means that the HCS370 can be used as two independent encoders. The code-word is calculated using one of two possible encoder configurations. Most options for code word and modulation formats can be different from Encoder 1 and Encoder 2, but LED and RF transmitter options have to be the same. The SHIFT input pin is used to select between the encoder configurations. A low on the SHIFT pin will select Encoder 1 and a high will select Encoder 2.

3.2 Code Hopping Code-Word Data Format

A Code hopping code-word consists of 32 bits of code hopping data, 32 bits of fixed code and between 3 and 5 bits of status information. Various code-word formats are shown in Figure 3-2.

FIGURE 3-2: CODE-WORD DATA FORMAT


With XSER=0, 16-bit Counter, QUEN=0
Status Information (3 Bits)
Fixed Code Portion (32 Bits)
Hopping Code Portion (32 Bits)
CRC 2 Bits
VLOW 1-Bit
BUT 4 Bits
SERIAL NUMBER (28 Bits)
BUT 4 Bits
Counter Overflow 2 Bits
DISC 10 Bits
Synchronization Counter 16 Bits
15
0
C1
C0
S2
S1
S0
S3
S2
S1
S0
S3
OVR1
OVR0
With XSER=1, 16-bit Counter, QUEN=1
Status Information (5 Bits)
Fixed Code Portion (32 Bits)
Hopping Code Portion (32 Bits)
QUE 2 Bits
CRC 2 Bits
VLOW 1-Bit
SERIAL NUMBER (32 Bits)
BUT 4 Bits
Counter Overflow 2 Bits
DISC 10 Bits
Synchronization Counter 16 Bits
15
0
Q1
Q0
C1
C0
S2
S1
S0
S3
OVR1
OVR0
With XSER=0, 20-bit Counter, QUEN=1
Status Information (5 Bits)
Fixed Code Portion (32 Bits)
Hopping Code Portion (32 Bits)
QUE 2 Bits
CRC 2 Bits
VLOW 1-Bit
BUT 4 Bits
SERIAL NUMBER (28 Bits)
BUT 4 Bits
DISC 8 Bits
Synchronization Counter 20 Bits
19
0
Q1
Q0
C1
C0
S2
S1
S0
S3
S2
S1
S0
S3
With XSER=1, 20-bit Counter, QUEN=0
Status Information (3 Bits)
Fixed Code Portion (32 Bits)
Hopping Code Portion (32 Bits)
CRC 2 Bits
VLOW 1-Bit
SERIAL NUMBER (32 Bits)
BUT 4 Bits
DISC 8 Bits
Synchronization Counter 20 Bits
19
0
C1
C0
S2
S1
S0
S3
Transmission Direction LSB First

3.2.1 CODE HOPPING PORTION

The hopping portion is calculated by encrypting the counter, discrimination value and function code with the Encoder Key (KEY). The hopping code is calculated when a button press is debounced and remains unchanged until the next button press.

The counter can be either a 16 or 20 bit counter, depending on the Counter select (CNTSEL) configuration option. The counter select option must be the same for both Encoder 1 and Encoder 2. If the 16 bit counter is selected, the discrimination value is 10 bits long and there are 2 counter overflow bits (OVR0, OVR1). Set both bits in production and OVR0 will be cleared on the first counter overflow and OVR1 on the second.

If the counter is 20 bits, the discrimination value is 8 bits long and there are no overflow bits. The rest of the 32 bits are made up of the function code also known as the button inputs.

The discrimination value can be programmed with any value to serve as a post decryption check on the decoder end. In a typical system, this will be programmed with the 8 or 10 least significant bits of the serial number, which will also be stored by the receiver system after a transmitter has been learned. The discrimination bits are part of the information that is to form the encrypted portion of the transmission. After the receiver has decrypted a transmission, the discrimination bits can be checked against the stored value to verify that the decryption process was valid.

3.2.2 FIXED CODE PORTION

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.

3.2.3 STATUS INFORMATION

The status bits will always contain the output of the Low Voltage detector (VLOW) and a Cyclic Redundancy Check (CRC). Button queue information can also be included in the code-words, if enabled.

3.2.3.1 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.

3.2.3.2 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 $0 \le n \le 64$

3.2.3.3 BUTTON QUEUE INFORMATION (QUEUE)

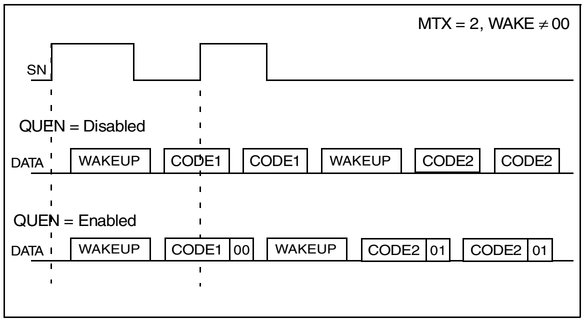
The queuing or repeated pressing of the same buttons can be handled in two ways on the HCS370. This is controlled with the Queue Counter Enable (QUEN) configuration option. This option can be different for Encoder 1 and Encoder 2.

When the QUEN option is disabled, the device will register up to two sequential button presses. In this case, the device will complete the minimum code words selected with the MTX option before the second code-word is calculated and transmitted. The code-word will be 67 bits in this case, with no additional queue bits transmitted.

If the QUEN option is enabled, the queue bits are added to 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 seconds from the start of the previous button press. The current code-word is terminated when a button is queued. This allows additional functionality for double or triple button presses.

Figure 3-3 shows code-word completion with the different QUEN settings.

FIGURE 3-3: CODE WORD COMPLETION WITH QUEN SETTINGS



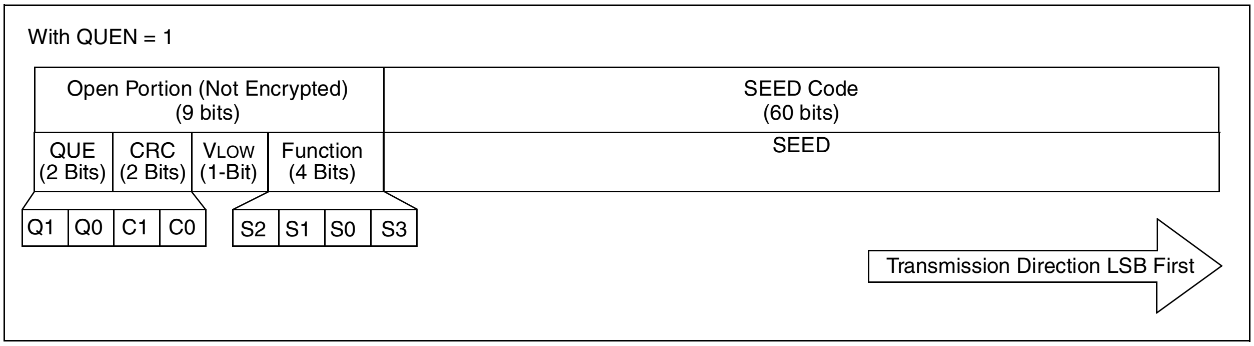
3.3 Seed Code-word Data Format

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 3-4. The function code for seed code-words is always 1111b.

Seed code-words for Encoder 1 and Encoder 2 can be configured as follows:

- Enabled or disabled with the Seed Enable (SDEN) configuration option.
- If the Limited Seed (SDLM) configuration option is set, then seed transmissions will be disabled when the synchronization counter is bigger than 127. Seed transmission remains disabled even if the 20/16 counter rolls over to 0.
- The delay before the seed transmission is transmitted can be set to 0.0s, 0.8s, 1.6s and 3.2s with the Seed Time (SDTM) configuration option. When it is set to a value other than 0.0s, the HCS370 will transmit a code-hopping transmission until the selected time expires, before the seed code-words are transmitted. This is useful for the decoder to learn the serial number and the seed from a single button press.
- The button code for transmitting a Seed code-word can be selected with the Seed Button (SDBT) configuration option. SDBT bits 0 to 3 correspond to button inputs S0 to S3. Set the bits high for the button combination that should trigger a seed transmission.
- The Seed mode can be changed between production and user mode with the Seed Mode (SDMD) configuration option. During user mode, the previous options directly control the Seed transmissions, as stated. However, Production mode overrides the Seed Time (SDTM) configuration option, if the synchronization counter is smaller than 128. In Production mode, the HCS370 will transmit normal hopping code code-words for the selected minimum code-words (MTX), and then transmit the same amount of seed code-words.

FIGURE 3-4: SEED CODE-WORD FORMAT



3.4 Transmission Modulation Format

The HCS370 transmission is made up of several code-words. Each code-word starts with a preamble and a header, followed by the data. The code-words are separated by a guard time that can be set to 0ms, 6.4ms, 51.2ms or 102.4ms with the Guard Time Select (GSEL) 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 100us, 200us, 400us or 800us with the Baud Rate Select (BSEL) configuration option. The Header time can be set to 4TE or 10TE with the Header Select (HSEL) Configuration option. These options can all be set individually for Encoder 1 and Encoder 2.

There are four different modulation formats available on the HCS370 that can be set individually for Encoder 1 or Encoder 2. The Modulation Select (MSEL) Configuration Option is used to select between:

- Pulse Width Modulation (PWM)
- Manchester Encoding
- Variable Pulse Width Modulation (VPWM)
- Pulse Position Modulation (PPM)

The various formats are shown in Figures 3-5 to 3-8.

FIGURE 3-5: PWM TRANSMISSION FORMAT

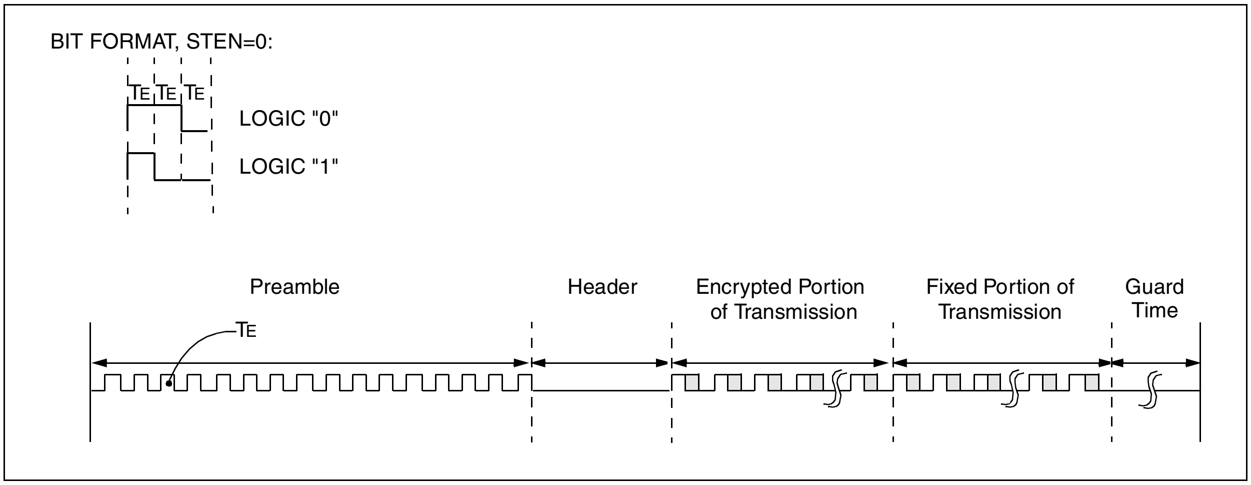


FIGURE 3-6: MANCHESTER FORMAT

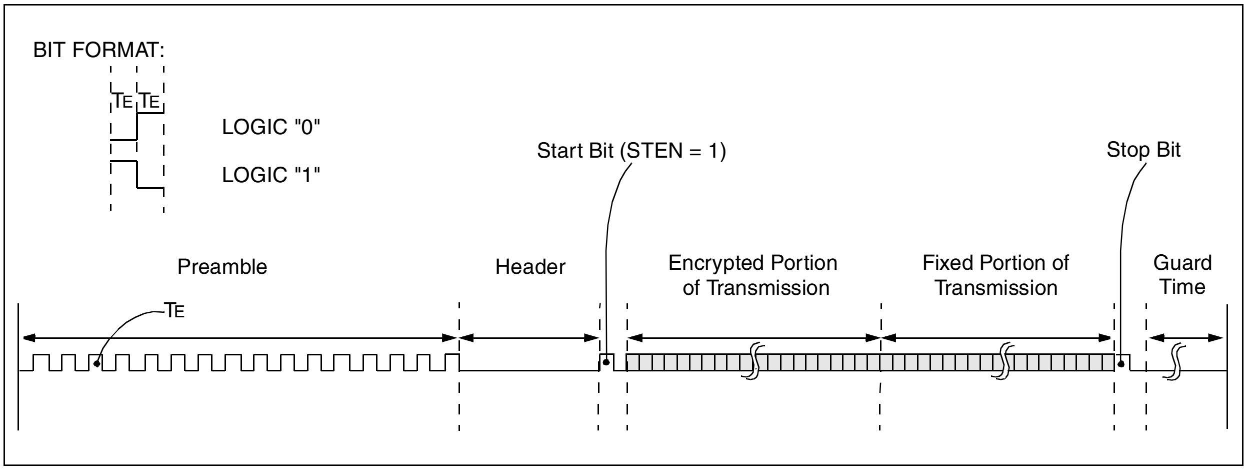


FIGURE 3-7: VPWM FORMAT SUMMARY

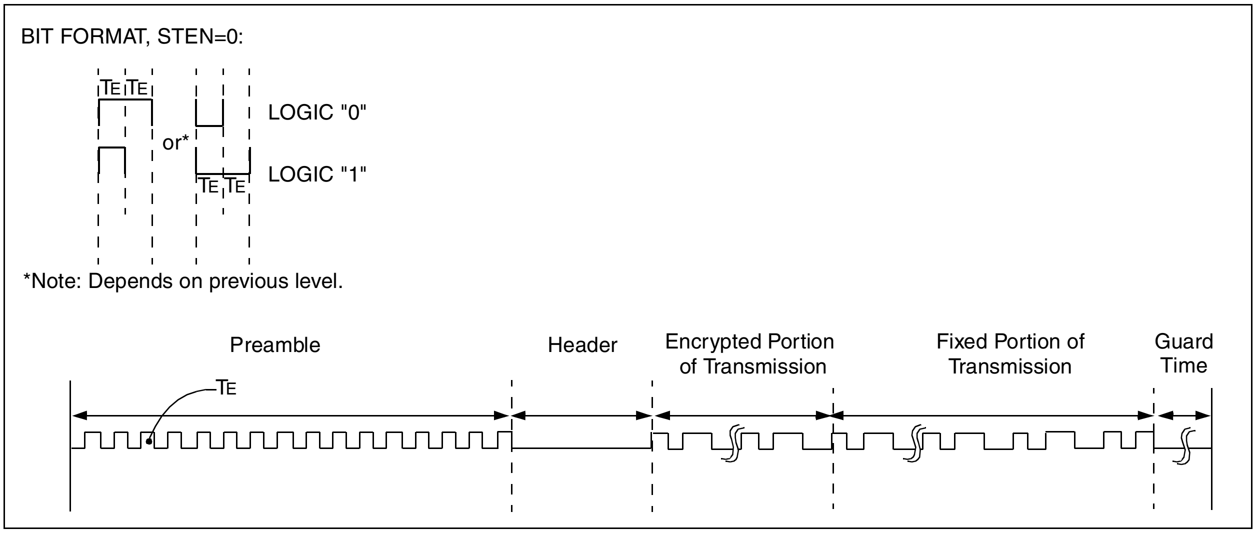
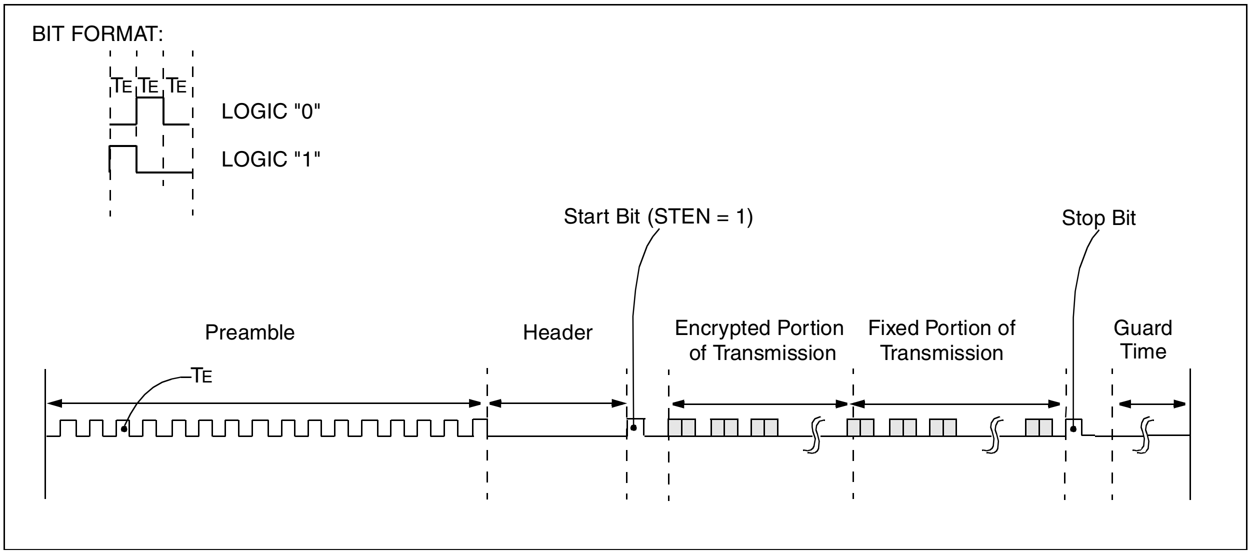

BIT FORMAT, STEN=0:
TE
TE
or*
LOGIC "0"
LOGIC "1"
TE
TE
*Note: Depends on previous level.
Preamble
Header
Encrypted Portion of Transmission
Fixed Portion of Transmission
Guard Time
TE

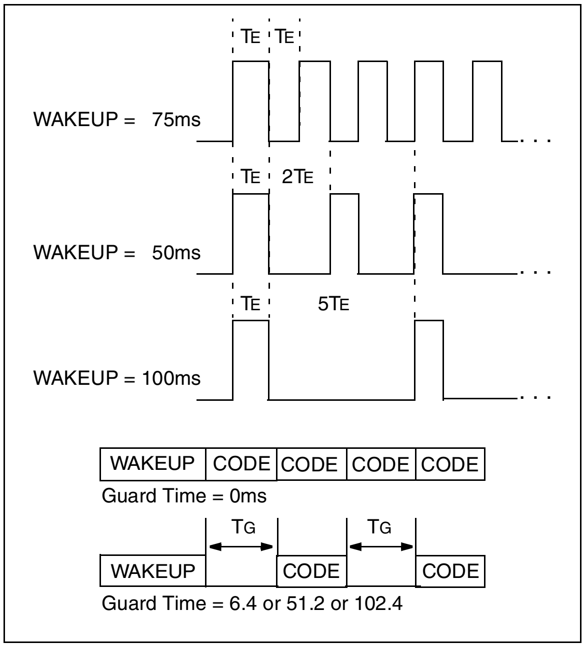
FIGURE 3-8: PPM TRANSMISSION FORMAT



In addition to the Modulation Format, Guard Time and Baud Rate, the following options are also available to change the Transmission Format:

- If the Start/Stop pulse Enable (STEN) configuration option is enabled, the HCS370 will place a leading and trailing ‘1’ on each code word. This is necessary for modulation formats such as Manchester and PPM Encoding to interpret the first and last data bit.
- A wakeup sequence can be transmitted before the transmission starts. The wakeup sequence is configured with the Wakeup (WAKE) configuration Option and can be disabled or set to 50ms, 75ms or 100ms of pulses as indicated in Figure 3-9.
- There will only be a guard time before the first code word when wakeup is enabled. The WAKE option is the same for both Encoder 1 and Encoder 2.

FIGURE 3-9: WAKEUP ENABLE

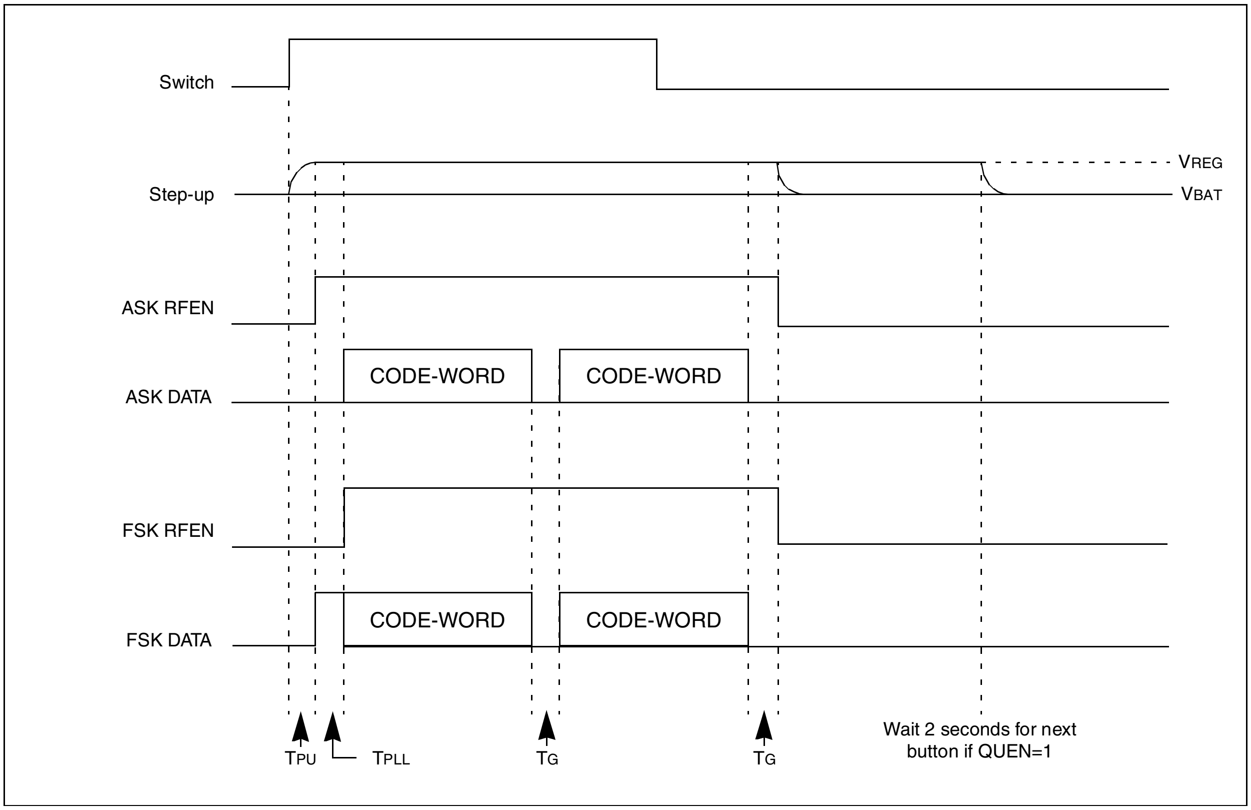


3.5 RF Enable and PLL Interface

The RFEN pin will be driven high whenever data is transmitted through the DATA pin.

The RF Enable and DATA outputs also interface with RF PLL’s. The PLL interface select (PLLSEL) configuration option selects between the ASK and FSK interface. Figure 3-10 show the startup sequence for both ASK and FSK interface options. The RFEN signal will go low at the end of the last code-word, including the guard time (TG). The power up time (TPU) is the debounce time plus the step-up regulator ramp up delay if WAIT=1. The PLL step-up time (TPLL) is also used to update the EEPROM counter and it will be twice the typical delay every 256 transmissions.

FIGURE 3-10: ASK/FSK INTERFACE

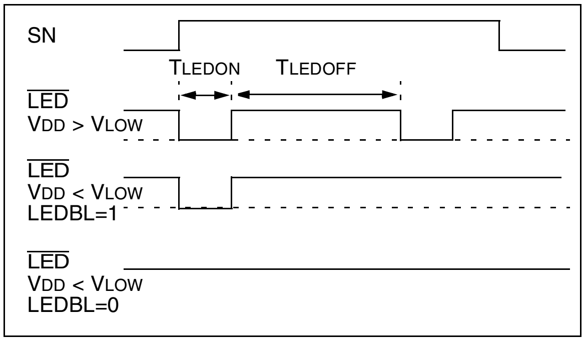


3.6 LED Output

The LED pin will be driven low while the HCS370 is transmitting data. The LED on time (TLEDON) can be selected between 50ms and 100ms with the LED on Time Select (LEDOS) configuration option. The LED off time (TLEDOFF) is fixed at 500ms. When the VDD Voltage drops below the selected VLOW trip point, the LED will not blink unless the LED Blink (LEDBL) option is set. If LEDBL is set and VDD is low, then the LED will only flash once. Waveforms of the LED behavior are shown in Figure 3-11.

For circuits with VDD greater than 3 volts, be sure to limit the LED circuit with a series resistor. The LED output can safely sink up to 25mA but adding an external resistor will conserve battery power. This is an open drain output but it does have a weak pull-up resistance capable of driving a CMOS input.

FIGURE 3-11: $\overline{\text{LED}}$ OPERATION



3.7 Step-Up Voltage Regulator

To create your own step-up regulator circuit, decide on an output voltage. Set the VIN resistor divider to drop it down to 1.2 volts. Keep the sum of the two resistors around 100kΩ. Put your maximum load on the output and increase the inductance until COUT charges from 0 to your output voltage in about 30ms from the minimum input voltage. Then test over your temperature and input voltage ranges.

The WAIT option will delay RF transmissions until COUT is charged. This permits a trade-off in slower button response times to save money on cheaper inductors. It can also optimize performance for good batteries and let response time drift for weak batteries. This option will also indicate failure to reach regulation voltage after 250 ms by not transmitting and not flashing the LED. If WAIT is disabled, the step-up regulator still operates and transmissions always start 30 ms after button press.

The SLEEP option can be enabled if S5 is not used. This reconfigures S5 to be an output high when the HCS370 is sleeping, and low when a button press wakes it up. One way to use this option is to save power on the step-up regulator. The problem is that the VIN resistor divider makes a DC path through the inductor and diode to discharge the battery. By tying the bottom of the divider to SLEEP as shown in Figure 2-1, the path is broken between transmissions.

4.0 INTEGRATING THE HCS370 INTO A SYSTEM

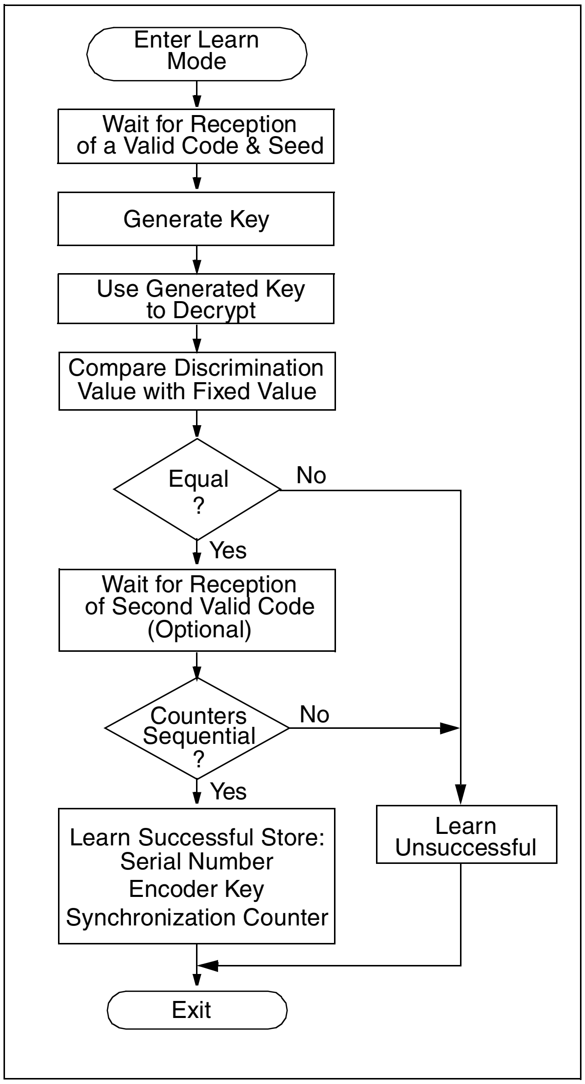
Use of the HCS370 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Example and Firmware routines that accept KEELOQ transmissions can be found in application notes.

4.1 Training the Receiver

In order for a transmitter to be used with a decoder, the transmitter must first be 'learned'. When a transmitter learns a decoder, it is suggested that the decoder stores the serial number and current synchronization value in EEPROM. Some learning strategies have been patented and care must be taken not to infringe. The decoder must keep track of these values for every transmitter that is learned (Figure 4-1).

The maximum number of transmitters that can be learned is only limited by available EEPROM memory. The decoder must also store the manufacturer's code in order to learn a transmitter. 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.

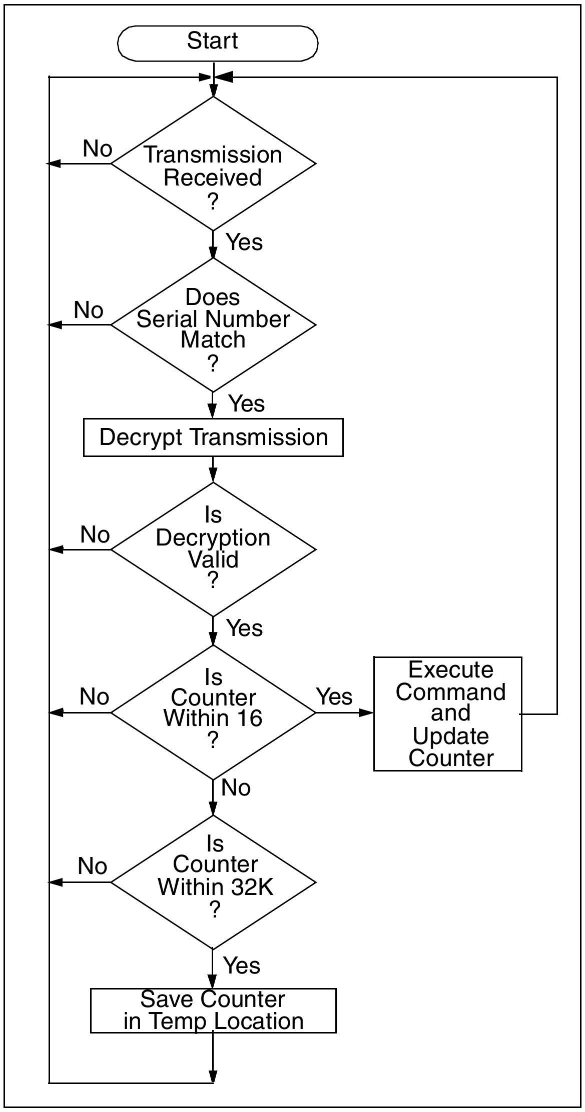
FIGURE 4-1: TYPICAL LEARN SEQUENCE


Enter Learn Mode
Wait for Reception of a Valid Code & Seed
Generate Key
Use Generated Key to Decrypt
Compare Discrimination Value with Fixed Value
Equal ?
No
Yes
Wait for Reception of Second Valid Code (Optional)
Counters Sequential ?
No
Yes
Learn Successful Store: Serial Number Encoder Key Synchronization Counter
Learn Unsuccessful
Exit

4.2 Decoder Operation

In a typical decoder operation (Figure 4-2), 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 4-2: TYPICAL DECODER OPERATION

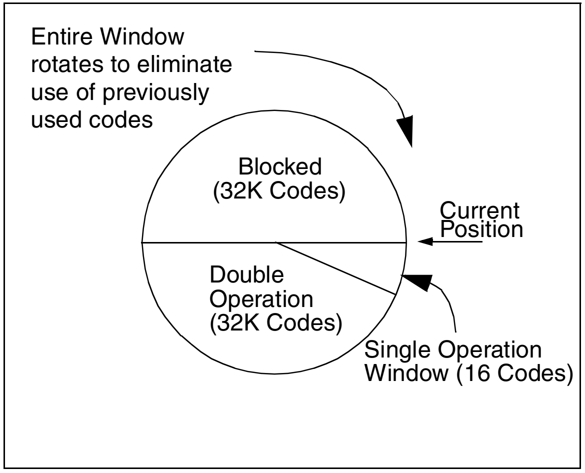


4.3 Synchronization with Decoder

The technology features a sophisticated synchronization technique (Figure 4-3) 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 (when using a 16-bit counter) 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 and because it is usually implemented in firmware, it can be altered to fit the needs of a particular system

FIGURE 4-3: SYNCHRONIZATION WINDOW (16-BIT COUNTER)


Entire Window rotates to eliminate use of previously used codes
Blocked (32K Codes)
Current Position
Double Operation (32K Codes)
Single Operation Window (16 Codes)

4.4 Security Considerations

The strength of this security is based on keeping a secret inside the transmitter that can be verified by encrypted transmissions to a trained receiver. The transmitter's secret is the manufacturer's key, not the encryption algorithm. If that key is compromised then a smart transceiver can capture any serial number, create a valid codeword, and trick all receivers trained with that serial number. The key cannot be read from the EEPROM without costly die probing but it can be calculated by brute force decryption attacks on transmitted codewords. The cost for these attacks should exceed what you would want to protect.

To protect the security of other receivers with the same manufacturer's code, you need to use the random seed for secure learn. It is a second secret that is unique for each transmitter. Its transmission on a special button press combination can be disabled if the receiver has another way to find it, or limited to the first 127 transmissions for the receiver to learn it. This way it is very unlikely to ever be captured. Now if a manufacturer's key is compromised new transmitters can be created, but without the unique seed they have to be relearned by the receiver. In the same way if the transmissions are decrypted by brute force on a computer, the random seed hides the manufacturer's key and prevents more than one transmitter from being compromised.

The length of the codeword at these baud rates makes brute force attacks that guess the hopping code take years. To make the receiver less susceptible to this attack make sure that you test all the bits in the decrypted code for the correct value. Do not just test low counter bits for sync and the bit for the button input of interest.

The main benefit of hopping codes is to prevent the retransmission of captured codewords. This works very well for codewords that the receiver decodes. Its weakness is if a code is captured when the receiver misses it, the code may trick the receiver once if it is used before the next valid transmission. To make the receiver more secure it could increment the counter on questionable codeword receptions. To make the transmitter more secure it could use separate buttons for lock and unlock functions. Another way would be to require two different buttons in sequence to gain access.

There are more ways to make KeeLoq systems more secure but these are all trade-offs. You need to find a balance between security, design effort, and usability, particularly in failure modes. For example if a button sticks or kids play with it, the counter should not end up in the blocked code window rendering the transmitter useless or requiring retraining.

5.0 EEPROM ORGANIZATION

A summary of the HCS370 EEPROM organization is shown in the table below. Data stored in the EEPROM can be classified as Encoder configuration (E) or Device specific (D). Two copies of the Encoder configuration must be stored for Encoder 1 and Encoder 2, unless the SHIFT input is tied to a logic level.

Symbol	Length (Bits)	Class	Description (Note 1)			Reference Section
KEY	64	E	Encoder Key			1.0, 3.2.1
SEED	60	E	Encoder Seed Value			1.0, 3.3
SYNC	20	E	Encoder Synchronization Counter (CNTSEL=1)			1.0, 2.1.1, 3.2, 3.2.1
	16	E	Encoder Synchronization Counter (CTNSEL=0)			
SER	32	E	Encoder Serial Number			1.0, 3.2, 3.2.2
DISC	10	E	Encoder Discrimination value			3.2, 3.2.1
OVR	2	E	Encoder Counter Overflow Bits			3.2, 3.2.1
MSEL	2	E	Transmission Modulation Format	Value	Format	3.4
				00b	PWM	
				01b	Manchester	
				10b	VPWM	
				11b	PPM	
HSEL	1	E	Header Select	4 TE = 0	10 TE = 1	3.4
XSER	1	E	Extended Serial Number	28 bits = 0	32 bits = 1	3.2
QUEN	1	E	Queue counter Enable	Disable = 0	Enable = 1	3.2.3.3
STEN	1	E	Start/Stop Pulse Enable	Disable = 0	Enable = 1	3.4
LEDBL	1	E	Low Voltage LED Blink	Never = 0	Once = 1	3.6
LEDOS	1	E	LED On Time Select(1)	50 ms = 0	100 ms = 1	3.6
SDLM	1	E	Limited Seed	Disable = 0	Enable = 1	3.3
SDEN	1	E	Seed Enable	Disable = 0	Enable = 1	3.3
SDMD	1	E	Seed Mode	User = 0	Production = 1	3.3
SDBT	4	E	Seed Button Code			3.3
SDTM	2	E	Time Before Seed codeword(1)	Value	Time (s)	3.3
				00b	0.0	
				01b	0.8	
				10b	1.6	
				11b	3.2	
BSEL	2	E	Transmission Baud Rate Select(1)	Value	TE (us)	3.4
				00b	100	
				01b	200	
				10b	400	
				11b	800	
GSEL	2	E	Guard Time Select(1)	Value	Time (ms)	3.4, 3.5
				00b	0.0	
				01b	6.4	
				10b	51.2	
				11b	102.4	
WAKE	2	D	Wakeup(1)	Value	Value	3.4
				00b	No Wakeup	
				01b	75ms 50%	
				10b	50ms 33.3%	
				11b	100ms 16.6%	
CNTSEL	1	D	Counter Select	16 bits = 0	20 bits = 1	3.2.1
VLOWL	1	D	Low Voltage Latch Enable	Disable = 0	Enable = 1	2.1.3

Symbol	Length (Bits)	Class	Description (Note 1)			Reference Section
VLOWSEL	1	D	Low Voltage Trip Point Select(2)	2.2 V = 0	3.2V = 1	2.1.3
PLLSEL	1	D	PLL Interface Select	ASK = 0	FSK = 1	3.5
MTX	2	D	Minimum Code-words	Value	Value	3.0; 3.2.3.3
				00b	1	
				01b	2	
				10b	4	
				11b	8	
SLEEP	1	D	SLEEP Output Enable	Disable = 0	Enable = 1	3.7
WAIT	1	D	Wait for Step-Up Regulator	Disable = 0	Enable = 1	3.5, 3.7
TSEL	2	D	Timeout Select(1)	Value	Time (s)	3.0
				00b	Disabled	
				01b	0.8	
				10b	3.2	
				11b	25.6	

Note 1: All Timing values vary ±10%.

2: Voltage thresholds are ±100mV.

6.0 ELECTRICAL CHARACTERISTICS

TABLE 6-1: ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Units
VDD	Supply voltage	-0.3 to 6.0	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
TLSOL	Lead soldering temp	300	°C

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

TABLE 6-2: DC CHARACTERISTICS

Commercial (C): TAMB = 0°C to +70°C **Industrial (I): TAMB = -40°C to +85°C**						
		2.0V < VDD < 5.5				
Parameter	**Sym.**	**Min.**	**Typ.**[1]	**Max.**	**Unit**	**Conditions**
Operating voltage	VDD	2.0	—	5.5	V	
Operating current (avg)	ICC	— —	1.5 0.8	4.5 1.6	mA mA	VDD = 5.5V VDD = 3.5V
Standby current	ICCS	—	—	1	µA	VDD = 5.5V
High level Input voltage	VIH	0.65VDD	—	VDD+0.3	V	
Low level input voltage	VIL	-0.3	—	0.15VDD	V	
High level output voltage	VOH	0.7Vdd	—	—	V	IOH = -1.0mA, VDD = 2.0V
Low level output voltage	VOL	—	—	0.08VDD	V	IOL = 1.0mA, VDD = 2.0V
RFEN pin high drive	IRFEN	—	3	—	mA	VRFEN = 0.7 VDD
$\overline{\text{LED}}$ sink current	ILED	—	—	10	mA	VDD = 5.5V
Pulldown Resistance; S0-S4	RS0-3	40	60	100	kΩ	VDD=4.0V
Low battery detect [2]	VLOW	2.1 3.1	2.2 3.2	2.3 3.3	V	VLOWSEL = 0 VLOWSEL= 1
Power on/off reset [2]	VPOR	—	1.9	—	V	

Note 1: Typical values are at 25°C.
2: This value is characterized and not tested

TABLE 6-3: AC CHARACTERISTICS

Commercial (C): TAMB = 0°C to +70°C **Industrial (I): TAMB = -40°C to +85°C**						
		2.0V < VDD < 5.5				
Parameter	**Sym.**	**Min.**	**Typ.**[1]	**Max.**	**Unit**	**Conditions**
Timing Element	TE	—	100	—	µs	BSEL = ‘00’
POwer Up Time	TPU	—	25	—	ms	
PLL Set-up Time	TPLL	10 —	15 —	30 285	ms ms	WAIT = 0 WAIT = 1
LED On Time	TLEDON	—	50	—	ms	LEDOS = ‘0’
LED Off Time	TLEDOFF	—	500	—	ms	
Guard Time	TG	—	102.4	—	ms	GSEL = ‘11’

Note 1: All Timing values are subject to the oscillator variance.

7.0 PACKAGING INFORMATION

7.1 Package Marking Information

14-Lead PDIP (300 mil)

```
XXXXXXXXXXXXXX
XXXXXXXXXXXXXX
   YYWWNNN
```

Example

```
    HCS370
XXXXXXXXXXXXXX
   9904NNN
```

14-Lead SOIC (150 mil)

```
XXXXXXXXXX
XXXXXXXXXX
  YYWWNNN
```

Example

```
  HCS370
XXXXXXXXXX
  9904NNN
```

14-Lead TSSOP (4.4 mm)

```
XXXXXX
  YYWW
   NNN
```

Example

```
HCS370
  9904
   NNN
```

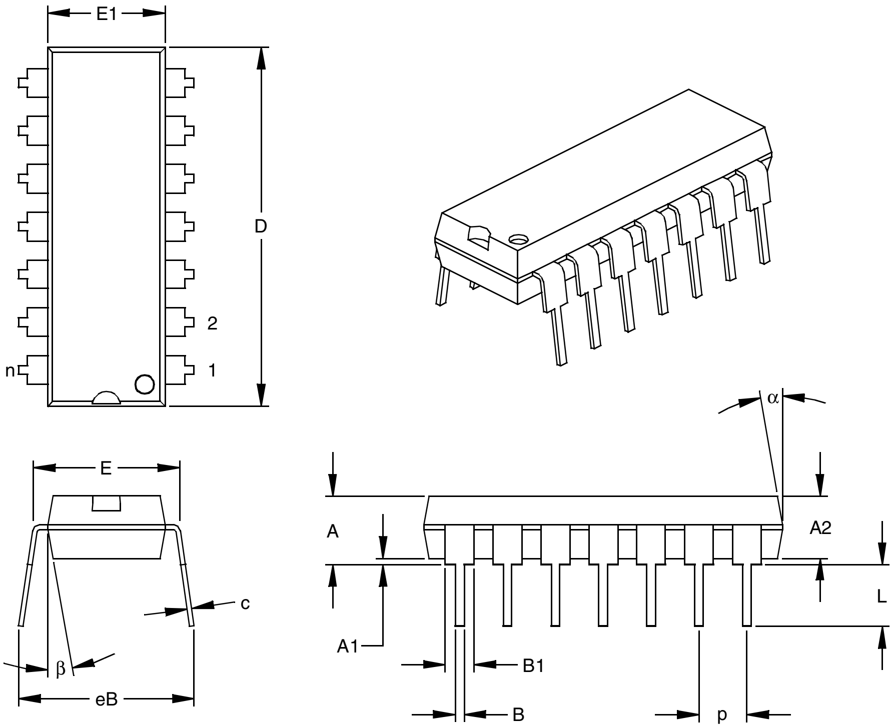
Legend:	XX...X	Customer specific information*
	YY	Year code (last 2 digits of calendar year)
	WW	Week code (week of January 1 is week ‘01’)
	NNN	Alphanumeric traceability code

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 marking consists of Microchip part number, year code, week code, facility code, mask rev#, and assembly code. For 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.

7.2 Package Details

14-Lead Plastic Dual In-line (P) – 300 mil (PDIP)



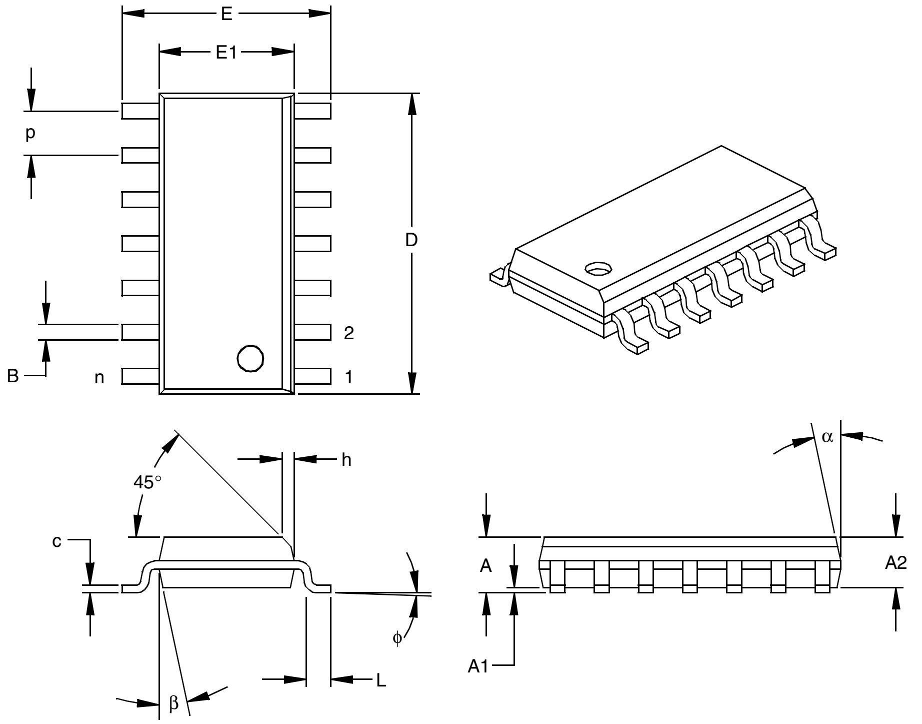
Units		INCHES*			MILLIMETERS		
Dimension Limits		MIN	NOM	MAX	MIN	NOM	MAX
Number of Pins	n		14			14	
Pitch	p		.100			2.54	
Top to Seating Plane	A	.140	.155	.170	3.56	3.94	4.32
Molded Package Thickness	A2	.115	.130	.145	2.92	3.30	3.68
Base to Seating Plane	A1	.015			0.38		
Shoulder to Shoulder Width	E	.300	.313	.325	7.62	7.94	8.26
Molded Package Width	E1	.240	.250	.260	6.10	6.35	6.60
Overall Length	D	.740	.750	.760	18.80	19.05	19.30
Tip to Seating Plane	L	.125	.130	.135	3.18	3.30	3.43
Lead Thickness	c	.008	.012	.015	0.20	0.29	0.38
Upper Lead Width	B1	.045	.058	.070	1.14	1.46	1.78
Lower Lead Width	B	.014	.018	.022	0.36	0.46	0.56
Overall Row Spacing §	eB	.310	.370	.430	7.87	9.40	10.92
Mold Draft Angle Top	α	5	10	15	5	10	15
Mold Draft Angle Bottom	β	5	10	15	5	10	15

* Controlling Parameter

§ Significant Characteristic

Notes:
Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .010” (0.254mm) per side.
JEDEC Equivalent: MS-001
Drawing No. C04-005

14-Lead Plastic Small Outline (SL) – Narrow, 150 mil (SOIC)

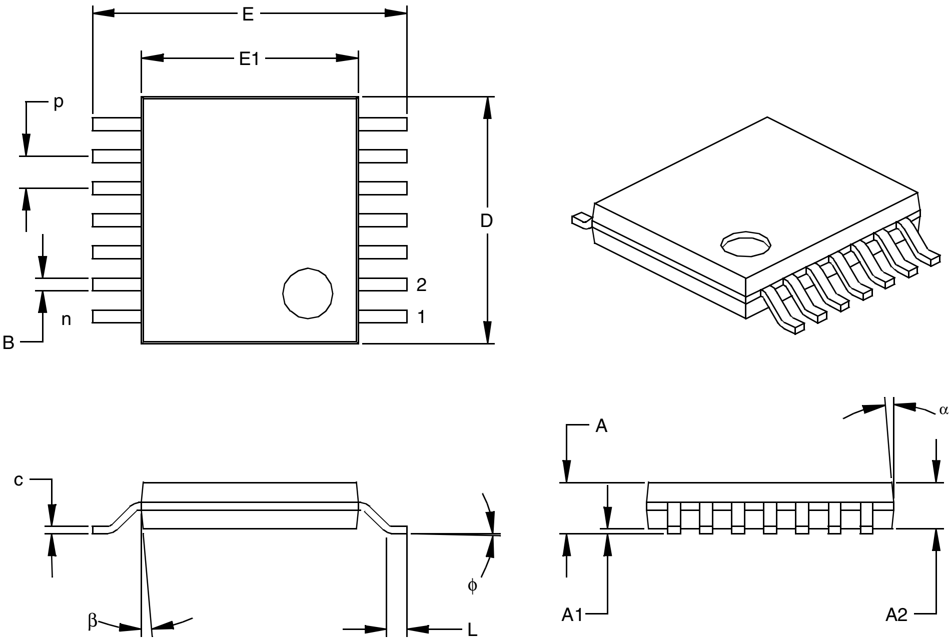


Units		INCHES*			MILLIMETERS		
Dimension Limits		MIN	NOM	MAX	MIN	NOM	MAX
Number of Pins	n		14			14	
Pitch	p		.050			1.27	
Overall Height	A	.053	.061	.069	1.35	1.55	1.75
Molded Package Thickness	A2	.052	.056	.061	1.32	1.42	1.55
Standoff §	A1	.004	.007	.010	0.10	0.18	0.25
Overall Width	E	.228	.236	.244	5.79	5.99	6.20
Molded Package Width	E1	.150	.154	.157	3.81	3.90	3.99
Overall Length	D	.337	.342	.347	8.56	8.69	8.81
Chamfer Distance	h	.010	.015	.020	0.25	0.38	0.51
Foot Length	L	.016	.033	.050	0.41	0.84	1.27
Foot Angle	φ	0	4	8	0	4	8
Lead Thickness	c	.008	.009	.010	0.20	0.23	0.25
Lead Width	B	.014	.017	.020	0.36	0.42	0.51
Mold Draft Angle Top	α	0	12	15	0	12	15
Mold Draft Angle Bottom	β	0	12	15	0	12	15

* Controlling Parameter
§ Significant Characteristic

Notes:
Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .010” (0.254mm) per side.
JEDEC Equivalent: MS-012
Drawing No. C04-065

14-Lead Plastic Thin Shrink Small Outline (ST) – 4.4 mm (TSSOP)



Units		INCHES			MILLIMETERS*		
Dimension Limits		MIN	NOM	MAX	MIN	NOM	MAX
Number of Pins	n		14			14	
Pitch	p		.026			0.65	
Overall Height	A			.043			1.10
Molded Package Thickness	A2	.033	.035	.037	0.85	0.90	0.95
Standoff §	A1	.002	.004	.006	0.05	0.10	0.15
Overall Width	E	.246	.251	.256	6.25	6.38	6.50
Molded Package Width	E1	.169	.173	.177	4.30	4.40	4.50
Molded Package Length	D	.193	.197	.201	4.90	5.00	5.10
Foot Length	L	.020	.024	.028	0.50	0.60	0.70
Foot Angle	φ	0	4	8	0	4	8
Lead Thickness	c	.004	.006	.008	0.09	0.15	0.20
Lead Width	B1	.007	.010	.012	0.19	0.25	0.30
Mold Draft Angle Top	α	0	5	10	0	5	10
Mold Draft Angle Bottom	β	0	5	10	0	5	10

* Controlling Parameter
§ Significant Characteristic

Notes:
Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .005" (0.127mm) per side.
JEDEC Equivalent: MO-153
Drawing No. C04-087

ON-LINE SUPPORT

Microchip provides on-line support on the Microchip World Wide Web (WWW) site.

The web site is used by Microchip as a means to make files and information easily available to customers. To view the site, the user must have access to the Internet and a web browser, such as Netscape or Microsoft Explorer. Files are also available for FTP download from our FTP site.

Connecting to the Microchip Internet Web Site

The Microchip web site is available by using your favorite Internet browser to attach to:

www.microchip.com

The file transfer site is available by using an FTP service to connect to:

ftp://ftp.microchip.com

The web site and file transfer site provide a variety of services. Users may download files for the latest Development Tools, Data Sheets, Application Notes, User's Guides, Articles and Sample Programs. A variety of Microchip specific business information is also available, including listings of Microchip sales offices, distributors and factory representatives. Other data available for consideration is:

- Latest Microchip Press Releases
- Technical Support Section with Frequently Asked Questions
- Design Tips
- Device Errata
- Job Postings
- Microchip Consultant Program Member Listing
- Links to other useful web sites related to Microchip Products
- Conferences for products, Development Systems, technical information and more
- Listing of seminars and events

Systems Information and Upgrade Hot Line

The Systems Information and Upgrade Line provides system users a listing of the latest versions of all of Microchip's development systems software products. Plus, this line provides information on how customers can receive any currently available upgrade kits.The Hot Line Numbers are:

1-800-755-2345 for U.S. and most of Canada, and

1-480-786-7302 for the rest of the world.

991103

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) 786-7578.

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

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: **HCS370** Literature Number: **DS41111B**

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 data sheet easy to follow? If not, why?

____

____

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

____

____

5. What deletions from the data sheet 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?

____

____

8. How would you improve our software, systems, and silicon products?

____

____

NOTES:

8.0 HCS370 PRODUCT IDENTIFICATION SYSTEM

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

HCS370 X /X

Package:	P	=	Plastic DIP (300 mil body), 14-lead
	SL	=	Plastic SOIC (150 mil body), 14-lead
	ST	=	Plastic TSSOP (4.4mm body), 14-lead
Temperature Range:	-	=	0°C to +70°C
	I	=	–40°C to +85°C
Device:	HCS370	=	Code Hopping Encoder
	HCS370T	=	Code Hopping Encoder (Tape and Reel - SL only)

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: (480) 786-7277.
3. The Microchip Worldwide Site (www.microchip.com)

Please specify which device, revision of silicon and Data Sheet (include Literature #) you are using.

New Customer Notification System
Register on our web site (www.microchip.com/cn) to receive the most current information on our products.

MICROCHIP

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.
2 LAN Drive, Suite 120
Westford, MA 01886
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 75001
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

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

China - Shanghai
Microchip Technology
Unit B701, Far East International Plaza,
No. 317, Xianxia Road
Shanghai, 200051, P.R.C.
Tel: 86-21-6275-5700 Fax: 86-21-6275-5060

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

India
Microchip Technology Inc.
India Liaison Office
Divyasree Chambers
I Floor, Wing A (A3/A4)
No. 11, O'Shaugnessey Road
Bangalore, 560 027, India
Tel: 91-80-207-2165 Fax: 91-80-207-2171

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

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
Microchip Technology Taiwan
11F-3, No. 207
Tung Hua North Road
Taipei, 105, Taiwan
Tel: 886-2-2717-7175 Fax: 886-2-2545-0139

EUROPE

Denmark
Microchip Technology Denmark ApS
Regus Business Centre
Lautrup hoj 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 - ler 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

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

8/01/00

DNV Certification, Inc.
USA

ANSI • RAB
QMS
ACCREDITED

DNV

DNV MSC
The Netherlands
Accredited by the RvA

ISO 9001 / QS-9000
REGISTERED FIRM

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, KEELOQ® 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.

Information contained in this publication regarding device applications and the like is intended through suggestion only and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. 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, except as maybe explicitly expressed herein, 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.