HCS412

KEELOQ® Code Hopping Encoder and Transponder

FEATURES

Security

- Programmable 64-bit encoder crypt key
- Two 64-bit IFF keys
- Keys are read protected
- 32-bit bi-directional challenge and response using one of two possible keys
- 69-bit transmission length
  - 32-bit hopping code,
  - 37-bit nonencrypted portion
- Programmable 28/32-bit serial number
- 60-bit, read protected seed for secure learning
- Two IFF encryption algorithms
- Delayed counter increment mechanism
- Asynchronous transponder communication
- Transmissions include button Queuing information

Operating

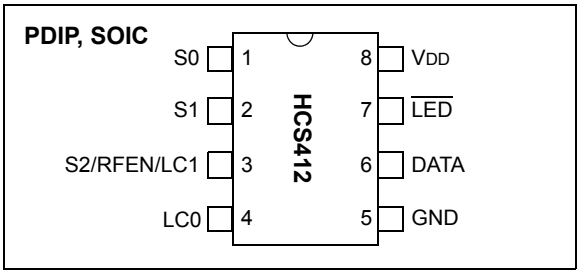
- 2.0V to 6.3V operation
- Three switch inputs: S2, S1, S0 – seven functions
- Battery-less bi-directional transponder capability
- Selectable baud rate and code word blanking
- Automatic code word completion
- Battery low detector
- PWM or Manchester data encoding
- Combined transmitter, transponder operation
- Anticollision of multiple transponders
- Passive proximity activation
- Device protected against reverse battery
- Intelligent damping for high Q LC-circuits
- 100 mVPP sensitive LC input

Typical Applications

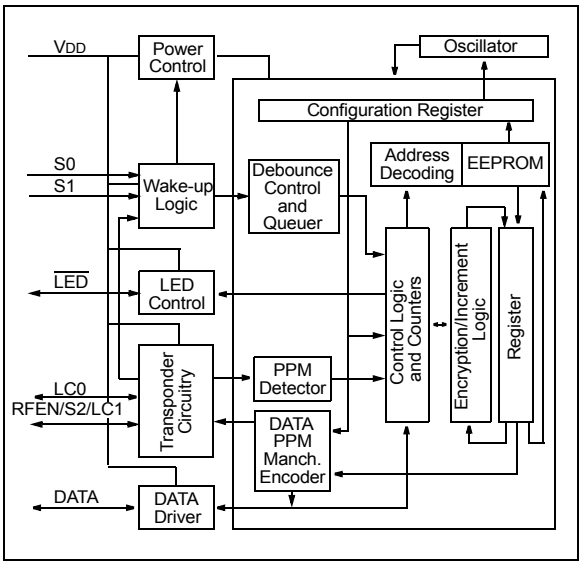
- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks (Home/Office/Hotel)
- Burglar alarm systems
- Proximity access control

PACKAGE TYPES

PDIP, SOIC



BLOCK DIAGRAM



Other

- Simple programming interface
- On-chip tunable RC oscillator, ± 10%
- On-chip EEPROM
- 64-bit user EEPROM in Transponder mode
- Battery-low LED indication
- Serialized Quick Turn Programming (SQTP℠)
- 8-pin PDIP/SOIC
- RF Enable output
- ASK and FSK PLL interface option
- Built in LC input amplifier

GENERAL DESCRIPTION

The HCS412 combines patented KEELOQ® code hopping technology with bi-directional transponder challenge-and-response security into a single chip solution for logical and physical access control.

When used as a code hopping encoder, the HCS412 is ideally suited to keyless entry systems; vehicle and garage door access in particular. The same HCS412 can also be used as a secure bi-directional transponder for contactless token verification. These capabilities make the HCS412 ideal for combined secure access control and identification applications, dramatically reducing the cost of hybrid transmitter/transponder solutions.

1.0 SYSTEM OVERVIEW

Key Terms

The following is a list of key terms used throughout this data sheet. For additional information on terminology, please refer to the KEELOQ introductory Technical Brief (TB003).

- **RKE -** Remote Keyless Entry.
- **PKE** - Passive Keyless Entry.
- **Button Status** - Indicates what transponder button input(s) activated the transmission. Encompasses the 4 button status bits LC0, S2, S1 and S0 (Figure 3-2).
- **Code Hopping** - A method by which a code, viewed externally to the system, appears to change unpredictably each time it is transmitted (Section 1.1.3).
- **Code word** - A block of data that is repeatedly transmitted upon button activation (Section 3.2).
- **Transmission** - A data stream consisting of repeating code words.
- **Crypt key** - A unique and secret 64-bit number used to encrypt and decrypt data. In a symmetrical block cipher such as the KEELOQ algorithm, the encryption and decryption keys are equal and will therefore be referred to generally as the crypt key.
- **Encoder** - A device that generates and encodes data.
- **Encryption Algorithm** - A recipe whereby data is scrambled using a crypt key. The data can only be interpreted by the respective decryption algorithm using the same crypt key.
- **Decoder** - A device that decodes data received from an encoder.
- **Transponder Reader (Reader, for short)** - A device that authenticates a token using bi-directional communication.
- **Decryption algorithm** - A recipe whereby data scrambled by an encryption algorithm can be unscrambled using the same crypt key.
- **Learn** – Learning involves the receiver calculating the transmitter's appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter value and crypt key in EEPROM (Section 6.1). The KEELOQ product family facilitates several learning strategies to be implemented on the decoder. The following are examples of what can be done.
  - **Simple Learning**
    The receiver uses a fixed crypt key, common to all components of all systems by the same manufacturer, to decrypt the received code word's encrypted portion.
  - **Normal Learning**
    The receiver uses information transmitted during normal operation to derive the crypt key and decrypt the received code word's encrypted portion.
  - **Secure Learn**
    The transmitter is activated through a special button combination to transmit a stored 60-bit seed value used to generate the transmitter's crypt key. The receiver uses this seed value to derive the same crypt key and decrypt the received code word's encrypted portion.
- **Manufacturer's code** - A unique and secret 64-bit number used to generate unique encoder crypt keys. Each encoder is programmed with a crypt key that is a function of the manufacturer's code. Each decoder is programmed with the manufacturer code itself.
- **Anticollision** - A scheme whereby transponders in the same field can be addressed individually preventing simultaneous response to a command (Section 4.3.1).
- **IFF** - Identify Friend or Foe (Section 1.2).
- **Proximity Activation** - A method whereby an encoder automatically initiates a transmission in response to detecting an inductive field (Section 4.4.1).
- **Transport code** - An access code, 'password' known only by the manufacturer, allowing program access to certain secure device memory areas (Section 4.3.3).
- **AGC** - Automatic Gain Control.

1.1 Encoder Overview

The HCS412 code hopping transcoder is designed specifically for passive entry systems; primarily vehicle access. The transcoder portion of a passive entry system is integrated into a transmitter, carried by the user and operated to gain access to a vehicle or restricted area. The HCS412 is meant to be a cost-effective yet secure solution to such systems, requiring very few external components (Figure 2-6).

1.1.1 LOW-END SYSTEM SECURITY RISKS

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

1.1.2 HCS412 SECURITY

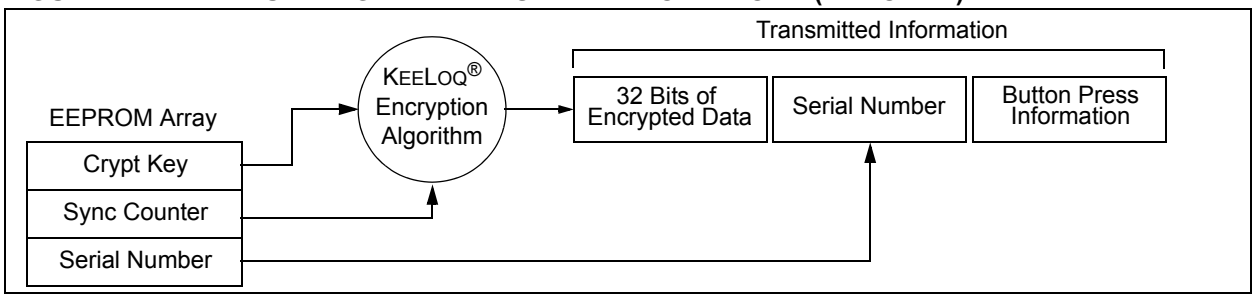
The HCS412, on the other hand, employs the KEELOQ code hopping technology coupled with a transmission length of 69 bits to virtually eliminate the use of code 'grabbing' or code 'scanning'. The high security level of the HCS412 is based on the patented KEELOQ technology. A block cipher based on a block length of 32 bits and a key length of 64 bits is used. The algorithm obscures the information in such a way that even if the transmission information (before coding) differs by only one bit from that of the previous transmission, statistically greater than 50 percent of the next transmission's encrypted bits will change.

1.1.3 HCS412 HOPPING CODE

The 16-bit synchronization counter is the basis behind the transmitted code word changing for each transmission; it increments each time a button is pressed.

Once the device detects a button press, it reads the button inputs and updates the synchronization counter. The synchronization counter and crypt key are input to the encryption algorithm and the output is 32 bits of encrypted information. This encrypted data will change with every button press, its value appearing externally to 'randomly hop around', hence it is referred to as the hopping portion of the code word. The 32-bit hopping code is combined with the button information and serial number to form the code word transmitted to the receiver. The code word format is explained in greater detail in Section 3.2.

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



1.2 Identify Friend or Foe (IFF) Overview

Validation of a token first involves an authentication device sending a random challenge to the token. The token then replies with a calculated response that is a function of the received challenge and the stored crypt key. The authentication device, transponder reader, performs the same calculation and compares it to the token's response. If they match, the token is identified as valid and the transponder reader can take appropriate action.

The HCS412's 32-bit IFF response is generated using one of two possible encryption algorithms and one of two possible crypt keys; four combinations total. The authenticating device precedes the challenge with a five bit command word dictating which algorithm and key to use in calculating the response.

The bi-directional communication path required for IFF is typically inductive for short range (<10cm) transponder applications and an inductive challenge, RF response for longer range (~1.5m) passive entry applications.

2.0 DEVICE DESCRIPTION

2.1 Pinout Description

The HCS412's footprint is identical to other encoders in the KEELOQ family, except for the two pins reserved for low frequency communication.

TABLE 2-1: PINOUT SUMMARY

Pin Name	Pin Number	Description
S0	1	Button input pin with Schmitt Trigger detector and internal 60 kΩ (nominal) pull-down resistor (Figure 2-1).
S1	2	Button input pin with Schmitt Trigger detector and internal 60 kΩ (nominal) pull-down resistor (Figure 2-1).
S2/RFEN/LC1	3	Multi-purpose input / output pin (Figure 2-2). • Button input pin with Schmitt Trigger detector and internal pull-down resistor. • RFEN output driver. • LC1 low frequency (LF) antenna output driver for inductive responses and LC bias. • Programming clock signal input.
LC0	4	Low frequency (LF) antenna input with automatic gain control for inductive reception and low frequency output driver for inductive responses (Figure 2-3).
GND	5	Ground reference.
DATA	6	Transmission data output driver. Programming input / output data signal (Figure 2-4).
LED	7	LED output driver (Figure 2-5).
VDD	8	Positive supply voltage.

FIGURE 2-1: S0/S1 PIN DIAGRAM

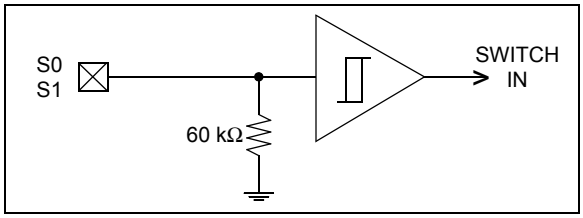


FIGURE 2-2: S2/RFEN/LC1 PIN DIAGRAM

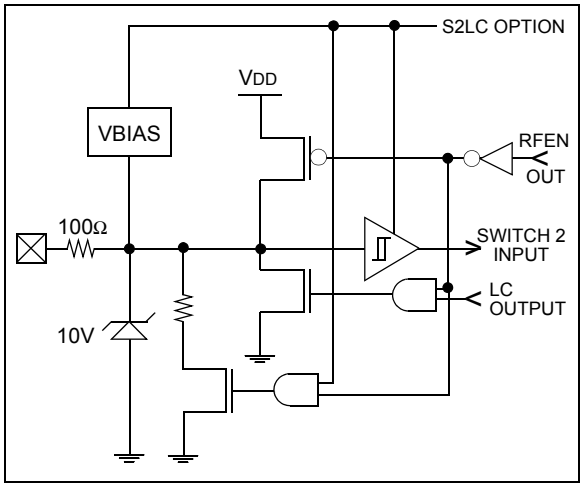


FIGURE 2-3: LC0 PIN DIAGRAM

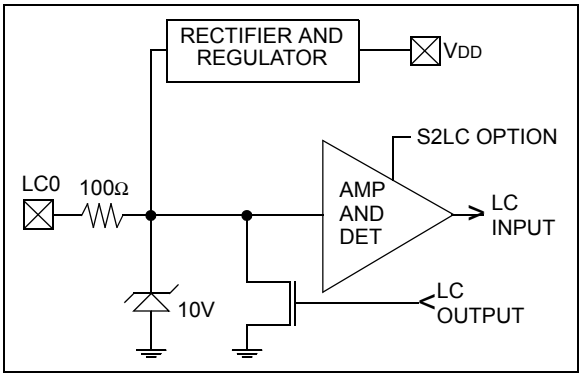


FIGURE 2-4: DATA PIN DIAGRAM

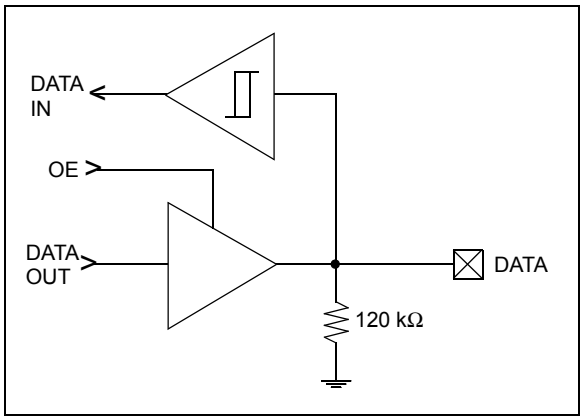


FIGURE 2-5: LED PIN DIAGRAM

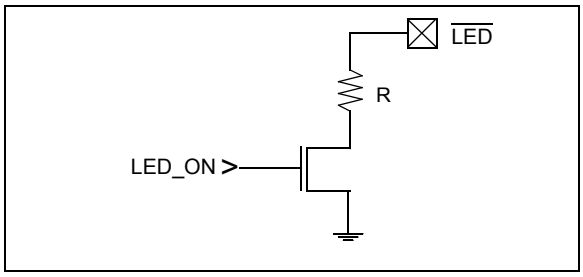
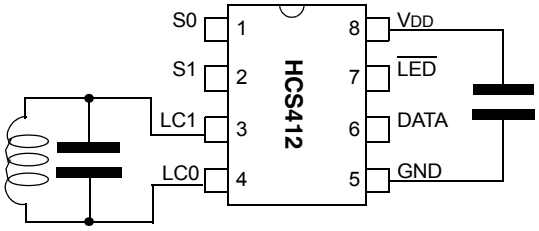
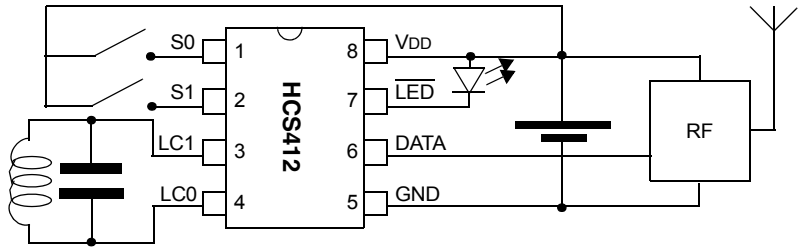


FIGURE 2-6: TYPICAL APPLICATION CIRCUITS

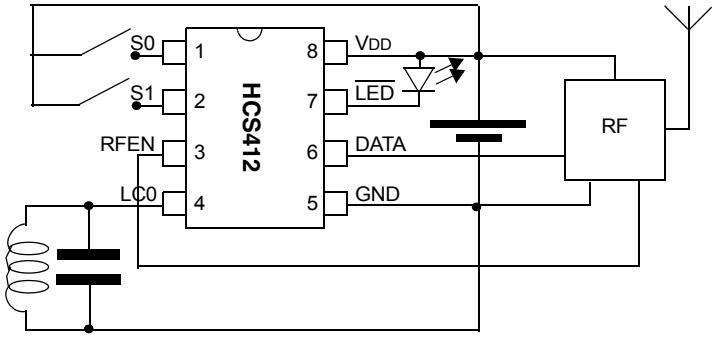
Battery-less Short Range Transponder



Long Range / Proximity Activated Transponder / Encoder



Short Range Transponder with RFEN Control / Long Range Encoder



2.2 Architecture Overview

2.2.1 WAKE-UP LOGIC AND POWER DISTRIBUTION

The HCS412 automatically goes into a low-power Standby mode once connected to the supply voltage. Power is supplied to the minimum circuitry required to detect a wake-up condition; button activation or LC signal detection.

The HCS412 will wake from Low-power mode when a button input is pulled high or a signal is detected on the LC0 LF antenna input pin. Waking involves powering the main logic circuitry that controls device operation. The button and transponder inputs are then sampled to determine which input activated the device.

A button input activation places the device into Encoder mode. A signal detected on the transponder input places the device into Transponder mode. Encoder mode has priority over Transponder mode so a signal on the transponder input would be ignored if it occurred simultaneously to a button activation; ignored until the button input is released.

2.2.2 CONTROL LOGIC

A dedicated state machine, timer and a 32-bit shift register perform the control, timing and data manipulation in the HCS412. This includes the data encryption, data output modulation and reading of and writing to the onboard EEPROM.

2.2.3 EEPROM

The HCS412 contains nonvolatile EEPROM to store configuration options, user data and the synchronization counter.

The configuration options are programmed during production and include the read protected security-related information such as crypt keys, serial number and discrimination value (Table 7-2).

The 64 bits (4x16-bit words) of user EEPROM are read/write accessible through the low frequency communication path as well as in-circuit, wire programmable during production.

The initial synchronization counter value is programmed during production. The counter is implemented in Grey code and updated using bit writes to minimize EEPROM writing over the life of the product. The user need not worry about counter format conversion as the transmitted counter value is in binary format.

Counter corruption is protected for by the use of a semaphore word as well as by the internal circuitry ensuring the EEPROM write voltage is at an acceptable level prior to each write.

The EEPROM is programmed during production by clocking (S2 pin) the data into the DATA pin (Section 7.0). Certain EEPROM locations can also be remotely read/written through the LF communication path (Section 4.3).

2.2.4 CONFIGURATION REGISTER

The first activation after connecting power to the HCS412, the device retrieves the configuration from EEPROM storage and buffers the information in a configuration register. The configuration register then dictates various device operation options including the RC oscillator tuning, the S2/RFEN/LC1 pin configuration, low voltage trip point, modulation format,...

2.2.5 ONBOARD RC OSCILLATOR AND OSCILLATOR TUNE VALUE (OSCT)

The HCS412 has an onboard RC oscillator. As the RC oscillator is susceptible to variations in process parameters, temperature and operating voltage, oscillator tuning is provided for more accurate timing characteristics.

The 4-bit Oscillator Tune Value (OSCT) (Table 2-2) allows tuning within ±4% of the optimal oscillator speed at the voltage and temperature used when tuning the device. A properly tuned oscillator is then accurate over temperature and voltage variations to within ±10% of the tuned value.

Oscillator speed is significantly affected by changes in the device supply voltage. It is therefore best to tune the HCS412 such that the variance in oscillator speed be symmetrical about an operating mid-point (Figure 2-7). ie...

- If the design is to run on a single lithium battery, tune the oscillator while supplying the HCS412 with ~2.5V (middle of the 3V to 2V usable battery life).
- If the design is to run on two lithium batteries, tune the oscillator while supplying the HCS412 with ~4V (middle of 6V to 2V battery life).
- If the design is to run on 5V, tune the oscillator while supplying the HCS412 with 5V.

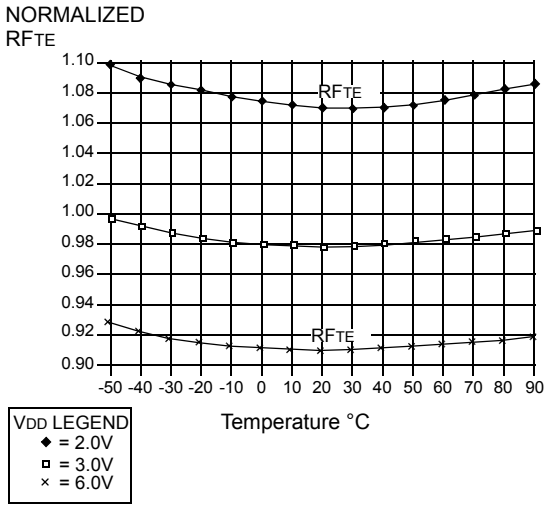
Say the HCS412's oscillator is tuned to be optimal at a 6V supply voltage but the device will operate on a single lithium battery. The resulting oscillator variance over temperature and voltage will not be ±4% but will be more like -7% to -15%.

Programming using a supply voltage other than 5V may not be practical. In these cases, adjust the oscillator tune value such that the device will run optimally at the target voltage. (i.e., If programming using 5V a device that will run at 3V, program the device to run slow at 5V such that it will run optimally at 3V).

TABLE 2-2: OSCILLATOR CALIBRATION VALUE (OSCT)

OSCT3:0	Description
0111b	Slowest Oscillator Setting (long TE)
+	:
0011b 0010b 0001b	: Slower (longer TE) :
0000b	Nominal Setting
1111b 1110b 1101b	: Faster (shorter TE) :
-	:
1000b	Fastest Oscillator Setting (short TE)

FIGURE 2-7: HCS412 NORMALIZED RFTE VERSUS TEMP



Note: Values are for calibrated oscillator.

2.2.6 LOW VOLTAGE DETECTOR

The HCS412's battery voltage detector detects when the supply voltage drops below a predetermined value. The value is selected by the Low Voltage Trip Point Select (VLOWSEL) configuration option.

The low voltage detector result is included in encoder transmissions (VLOW) allowing the receiver to indicate when the transmitter battery is low (Figure 3-2).

The HCS412 indicates a low battery condition by changing the LED operation (Figure 3-9).

FIGURE 2-8: TYPICAL VOLTAGE TRIP POINTS

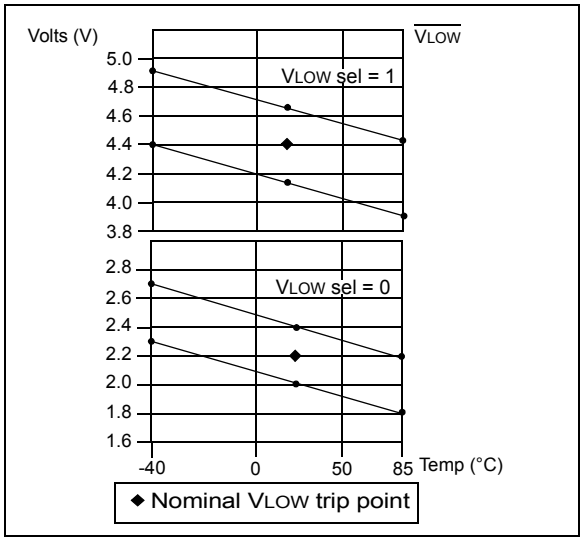


TABLE 2-3: VLOWSEL OPTIONS

VLOWSEL	Nominal Trip Point	Description
0	2.2V	for 3V battery applications
1	4.4V	for 6V battery applications

TABLE 2-4: VLOW STATUS BIT

VLOW	Description
0	VDD is above selected trip voltage
1	VDD is below selected trip voltage

2.2.7 THE S2/RFEN/LC1 PIN

The S2/RFEN/LC1 pin may be used as a button input, RF enable output or as an interface to the LF antenna. Select between LC1 antenna interface and S2/RFEN functionality with the button/transponder select (S2LC) configuration option (Table 2-2).

2.2.7.1 S2 BUTTON INPUT CONSIDERATIONS

The S2/RFEN/LC1 pin defaults to LF antenna output LC1 when the HCS412 is first connected to the supply voltage (i.e., battery replacement).

The configuration register controlling the pin's function is loaded on the first device activation after battery replacement. A desired S2 input state is therefore enabled only after the first activation of either S0, S1 or LC0. The transponder bias circuitry switches off and the internal pull-down resistor is enabled when the S2/RFEN/LC1 pin reaches button input configuration.

There will be an extra delay the first activation after connecting to the supply voltage while the HCS412 retrieves the configuration word and configures the pins accordingly.

2.2.7.2 TRANSPONDER INTERFACE

Connecting an LC resonant circuit between the LC0 and the LC1 pins creates the bi-directional low frequency communication path with the HCS412.

The internal circuitry on the HCS412 provides the following functions:

- LF input amplifier and envelope detector to detect and shape the incoming low frequency excitation signal.
- 10V zener input protection from excessive antenna voltage generated when proximate to very strong magnetic fields.
- LF antenna clamping transistors for inductive responses back to the transponder reader. The antenna ends are shorted together, 'clamped', dissipating the oscillatory energy. The reader detects this as a momentary load on its excitation antenna.
- Damping circuitry that improves communication when using high-Q LC antenna circuits.
- Incoming LF energy rectification and regulation for the supply voltage in battery-less or low battery transponder instances.

During normal transponder operation, the LC1 pin functions to bias the LC0 AGC amplifier input. The amplifier gain control sets the optimum level of amplification in respect to the incoming signal strength. The signal then passes through an envelope detector before interpretation in the logic circuit.

2.2.7.3 RF ENABLE OUTPUT

When the RF enable (RFEN) configuration option is enabled, the RFEN signal output is coordinated with the DATA output pin to provide typical ASK or FSK PLL activation.

TABLE 2-1: RFEN OPTION

RFEN	Description
0	RF Enable output is disabled.
1	RF Enable output is enabled.

TABLE 2-2: S2/RFEN/LC1 CONFIGURATION OPTION

S2LC	Resulting S2/RFEN/LC1 Configuration
0	• LC1 low frequency antenna output driver for inductive responses and LC bias. **Note:** LC0 low frequency antenna input is also enabled.
1	• S2 button input pin with Schmitt Trigger detector and internal pull-down resistor. • RFEN output driver. **Note:** LC0 and LC1 low frequency antenna interfaces are disabled and the transponder circuitry is switched off to reduce standby current.

3.0 ENCODER OPERATION

3.1 Encoder Activation

3.1.1 BUTTON ACTIVATION

The main way to enter Encoder mode is when the wake-up circuit detects a button input activation; button input transition from GND to VDD. The HCS412 control logic wakes and delays a switch debounce time prior to sampling the button inputs. The button input states, cumulatively called the button status, determine whether the HCS412 transmits a code hopping or seed transmission, Table 3-1.

Additional button activations added during a transmission will immediately RESET the HCS412, perhaps leaving the current code word incomplete. The device will start a new transmission which includes the updated button code value.

Buttons removed during a transmission will have no effect unless no buttons remain activated. If no button activations remain, the minimum number of compete code words will be completed (Section 3.4.1) and the device will return to Standby mode.

3.1.2 PROXIMITY ACTIVATION

The other way to enter Encoder mode is if the S2/LC option is configured for LC operation and the wake-up circuit detects a signal on the LC0 LF antenna input pin. This form of activation is called Proximity activation as a code hopping transmission would be initiated when the device was proximate to a LF field.

Refer to Section 4.4 for details on configuring the HCS412 for Proximity Activation.

TABLE 3-1: ENCODER MODE ACTIVATION

4-Bit Button Status				SEED	TMPSD	Resulting Transmission
LC0 (Note 1)	S2	S1	S0			
X	0	0	1	X	X	Code hopping transmission
X	0	1	0	X	X	Code hopping transmission
X	0	1	1	0	0	Code hopping transmission
				0	1	Code hopping code words until time = TDSD, then seed code words. SEED transmissions temporarily enabled until the 7lsb's of the synchronization counter wrap 7Fh to 00h. Then only code hopping code words.
				1	0	Code hopping code words until time = TDSD, then seed code words.
				1	1	Code hopping transmission (2 key IFF enabled)
X	1	0	1	X	X	Code hopping transmission
X	1	0	0	X	X	Code hopping transmission
X	1	1	0	X	X	Code hopping transmission
X	1	1	1	0	0	Code hopping transmission
				0	1	Limited SEED transmissions - temporarily enabled until the 7lsb's of the synchronization counter wrap 7Fh to 00h.
				1	0	SEED transmission
				1	1	Code hopping transmission (2 key IFF enabled)
1	0	0	0	X	X	Proximity activated code hopping transmission.

Note 1: The transmitted button status will reflect the state of the LC0 input when the button inputs are sampled.

3.2 Transmitted Code Word

The HCS412 transmits a 69-bit code word in response to a button or proximity activation (Figure 3-1). Each code word contains a 50% duty cycle preamble, header, 32 bits of encrypted data and 37 bits of fixed code data followed by a guard period before another code word can begin.

The 32 bits of **Encrypted Data** include 4 button bits, 2 counter overflow bits, 10 discrimination bits and the 16-bit synchronization counter value (Figure 3-2).

The content of the 37 bits of **Fixed Code Data** varies with the extended serial number (XSER) option (Figure 3-2).

- If the extended serial number option is disabled (XSER = 0), the 37 bits include 5 status bits, 4 button status bits and the 28-bit serial number.
- If the extended serial number option is enabled (XSER = 1), the 37 bits include 5 status bits and the 32-bit serial number.

FIGURE 3-1: CODE WORD FORMAT

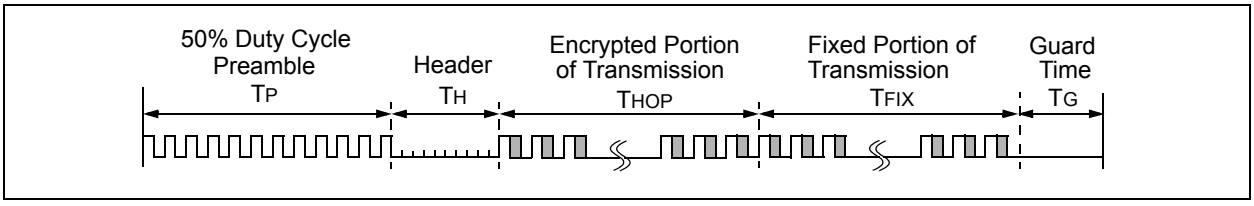
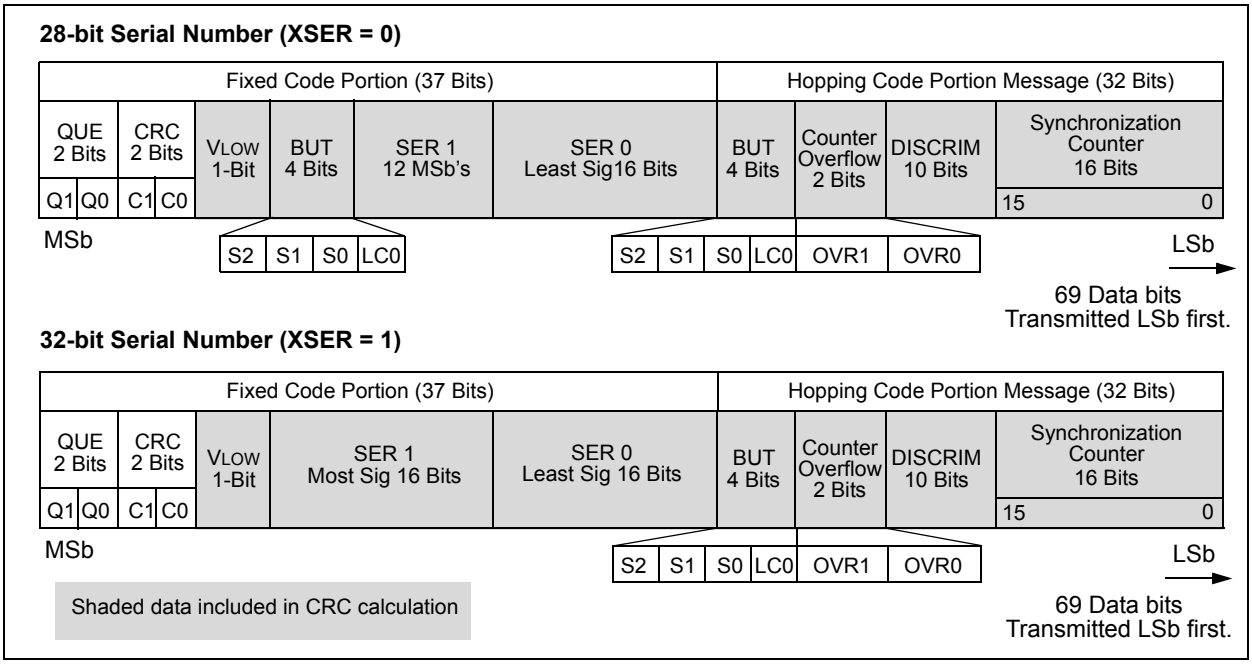


FIGURE 3-2: CODE WORD ORGANIZATION



3.2.1 QUEUE COUNTER (QUE)

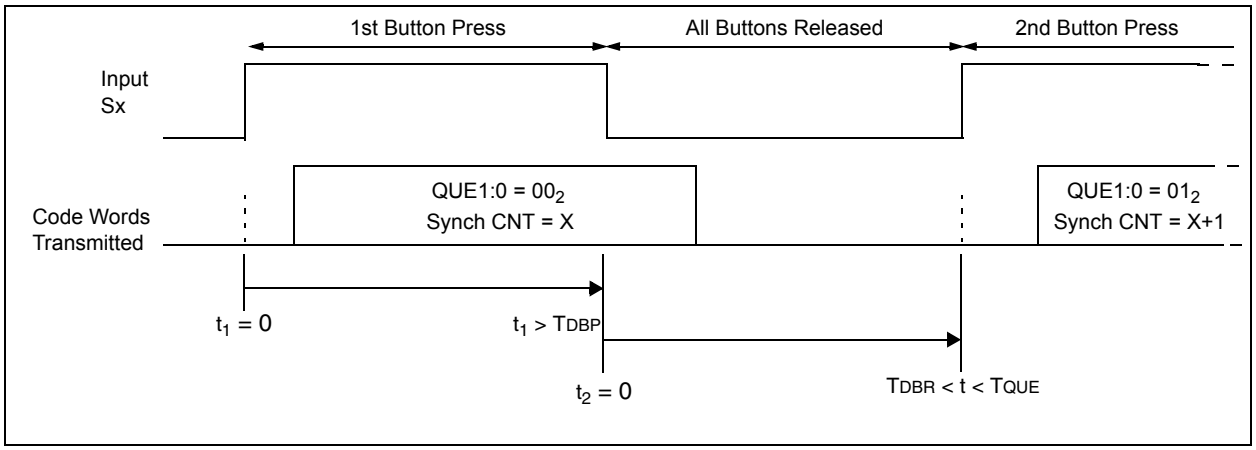
The QUE counter can be used to request secondary decoder functions using only a single transmitter button. Typically a decoder must keep track of incoming transmissions to determine when a double button press occurs, perhaps an unlock all doors request. The QUE counter removes this burden from the decoder by counting multiple button presses.

The 2-bit QUE counter is incremented each time an active button input is released for at least the Debounce Time (TDBR), then reactivated (button pressed again) within the Queue Time (TQUE). The counter increments up from 0 to a maximum of 3, returning to 0 only after a different button activation or after button activations spaced greater than the Queue Time (TQUE) apart.

The current transmission aborts, after completing the minimum number of code words (Section 3.4.1), when the active button input is released. A button re-activation within Queue Time (TQUE) then initiates a new transmission (new synchronization counter, encrypted data) using the updated QUE value.

Figure 3-3 shows the timing diagram to increment the queue counter value.

FIGURE 3-3: QUE COUNTER TIMING DIAGRAM



3.2.2 CYCLE REDUNDANCY CHECK (CRC)

The CRC bits may be used to check the received data integrity, but it is not recommended when operating near the low voltage trip point, see Note below.

The CRC is calculated on the 65 previously transmitted bits (Figure 3-2), detecting all single bit and 66% of all double bit errors.

EQUATION 3-1: CRC CALCULATION

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

and

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

with

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

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

Note: The CRC may be wrong when the operating voltage is near VLOW trip point. VLOW is sampled twice each transmission, once for the CRC calculation (DATA output is LOW) and once when the VLOW bit is transmitted (DATA output is HIGH). VDD varying slightly during a transmission could lead to a different VLOW status transmitted than that used in the CRC calculation.
Work around: If the CRC is incorrect, recalculate for the opposite value of VLOW.

3.2.3 LOW VOLTAGE DETECTOR STATUS (VLOW)

The low voltage detector result is included in every transmitted code word.

The HCS412 samples the voltage detector output at the onset of a transmission and just before the VLOW bit is transmitted in each code word. The first sample is used in the CRC calculation and the subsequent samples determine what VLOW value will be transmitted.

The transmitted VLOW status will be a '0' as long as VDD remains above the selected low voltage trip point. VLOW will change to a '1' if VDD drops below the selected low voltage trip point.

TABLE 3-2: LOW VOLTAGE STATUS BIT

VLOW	Description
0	VDD is above trip voltage (VLOWSEL)
1	VDD is below trip voltage (VLOWSEL)

TABLE 3-3: LOW VOLTAGE TRIP POINT SELECTION OPTIONS

VLOWSEL	Nominal Trip Point	Description
0	2.2V	for 3V battery applications
1	4.4V	for 6V battery applications

3.2.4 COUNTER OVERFLOW BITS (OVR1, OVR0)

The Counter Overflow Bits may be utilized to increase the synchronization counter range from the nominal 65,535 to 131,070 or 196,605.

The bits must be programmed during production as '1's to be utilized. OVR0 is cleared the first time the synchronization counter wraps from FFFFh to 0000h. OVR1 is cleared the second time the synchronization counter wraps to zero. The two bits remain at '0' after all subsequent counter wraps.

3.2.5 EXTENDED SERIAL NUMBER (XSER)

The Extended Serial Number option determines whether the serial number is 28 or 32 bits.

When configured for a 28-bit serial number, the most significant nibble of the 32 bits reserved for the serial number is replaced with a copy of the 4-bit button status, Figure 3-2.

3.2.6 DISCRIMINATION VALUE (DISC)

The Discrimination Value is a 10-bit fixed value typically used by the decoder in a post-decryption check. It may be any value, but in a typical system it will be programmed as the 10 Least Significant bits of the serial number.

The discrimination bits are part of the information that form the encrypted portion of the transmission (Figure 3-2). After the receiver has decrypted a transmission, the discrimination bits are checked against the receiver's stored value to verify that the decryption process was valid. If the discrimination value was programmed equal to the 10 LSb's of the serial number then it may merely be compared to the respective bits of the received serial number.

3.2.7 SEED CODE WORD DATA FORMAT

The Seed Code Word transmission allows for what is known as a secure learning function, increasing a system's security.

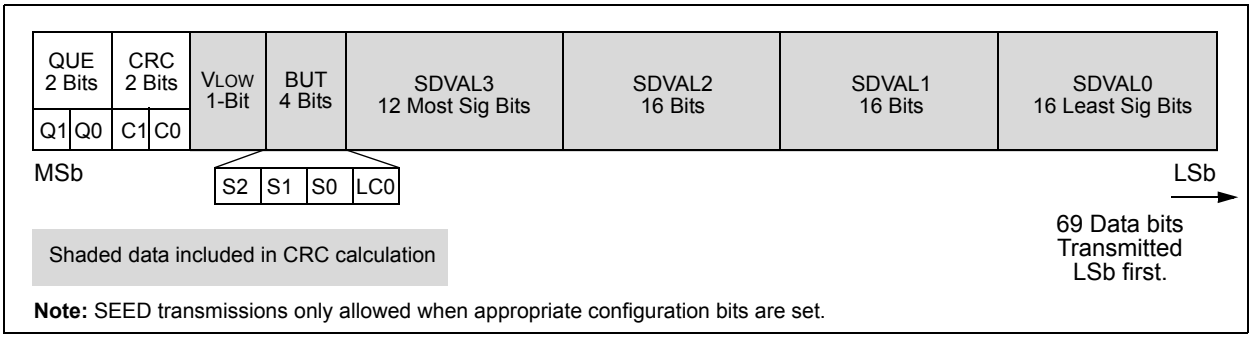
The seed code word also consists of 69 bits, but the 32 bits of code hopping data and the 28 bits of fixed data are replaced by a 60-bit seed value that was stored during production (Figure 3-4). Instead of using the normal key generation inputs to create the crypt key, this seed value is used.

Seed transmissions are either:

- permanently enabled
- permanently disabled
- temporarily enabled (limited) until the 7 Least Significant bits of the synchronization counter wrap from 7Fh to 00h.

The Seed Enable (SEED) and Temporary Seed Enable (TMPSD) configuration options control the function (Table 3-4).

FIGURE 3-4: SEED CODE WORD DATA FORMAT



Note: SEED transmissions only allowed when appropriate configuration bits are set.

TABLE 3-4: SEED TRANSMISSION OPTIONS

SEED	TMPSD	Description
0	0	SEED transmissions permanently disabled
0	1	Limited SEED transmissions **(Note 1)** - temporarily enabled until the 7 LSb's of the synchronization counter wrap from 7Fh to 00h
1	0	SEED transmissions permanently enabled **(Note 1)**
1	1	SEED transmissions permanently disabled (2 key IFF enabled)

Note 1: Refer to Table 3-1 for appropriate button activation of SEED transmissions.

3.3 Transmission Data Modulation

The data modulation format is selectable between Pulse Width Modulation (PWM) and Manchester using the Data Modulation (MOD) configuration option.

Regardless of the modulation format, each code word contains a leading 50% duty cycle preamble and a synchronization header to wake the receiver and provide synchronization events for the receive routine. Each code word also contains a trailing guard time, separating code words. Manchester encoding further includes a leading and closing '1' around each 69-bit data block.

The same code word repeats as long as the same input pins remain active, until a time-out occurs or a delayed seed transmission is activated.

The modulated data timing is typically referred to in multiples of a Basic Timing Element (RFTE). 'RF' TE because the DATA pin output is typically sent through a RF transmitter to the decoder or transponder reader.

RFTE may be selected using the Transmission Baud Rate (RFBSL) configuration option (Table 3-6).

TABLE 3-5: TRANSMISSION MODULATION TIMING

Period	PWM	Manchester	Units
Preamble	31*	31*	RFTE
Header	10	4	RFTE
Data	207	142	RFTE
Guard	46	31	RFTE

* Enabling long preambles extends the first code word's preamble to TLPRE milliseconds.

TABLE 3-6: BAUD RATE SELECTION (RFBSL)

RFBSL1:0	CWBE	PWM RFTE	Manchester RFTE	Transmit...
00b	X	400 µs	800 µs	All code words
01b	0	200 µs	400 µs	All code words
	1	200 µs	400 µs	Every other code word
10b	0	100 µs	200 µs	All code words
	1	100 µs	200 µs	Every other code word
11b	0	100 µs	200 µs	All code word
	1	100 µs	200 µs	Every fourth code word

FIGURE 3-5: PWM TRANSMISSION FORMAT—MOD = 0

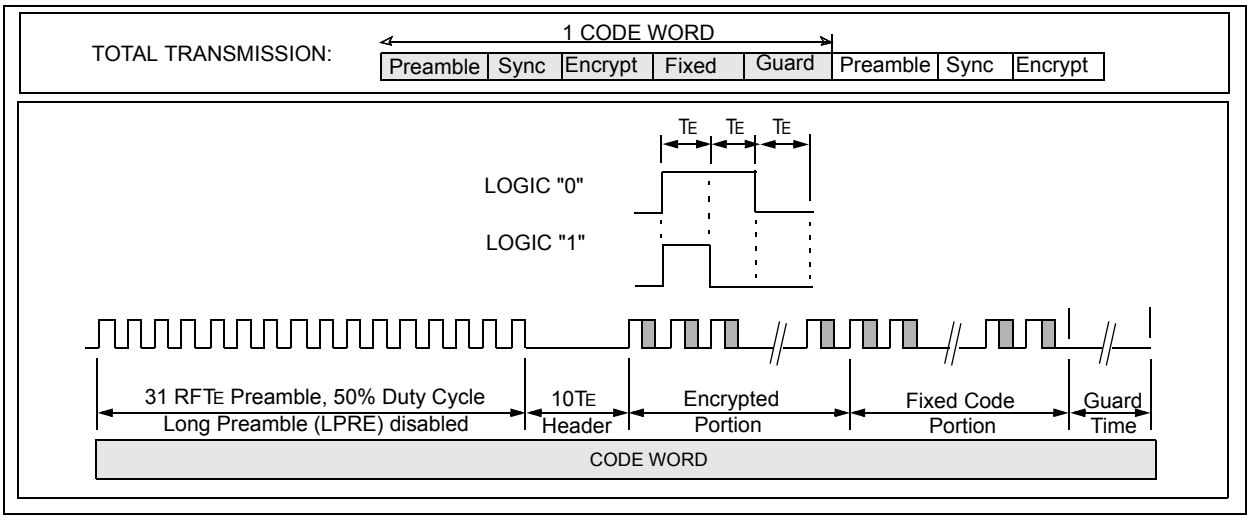
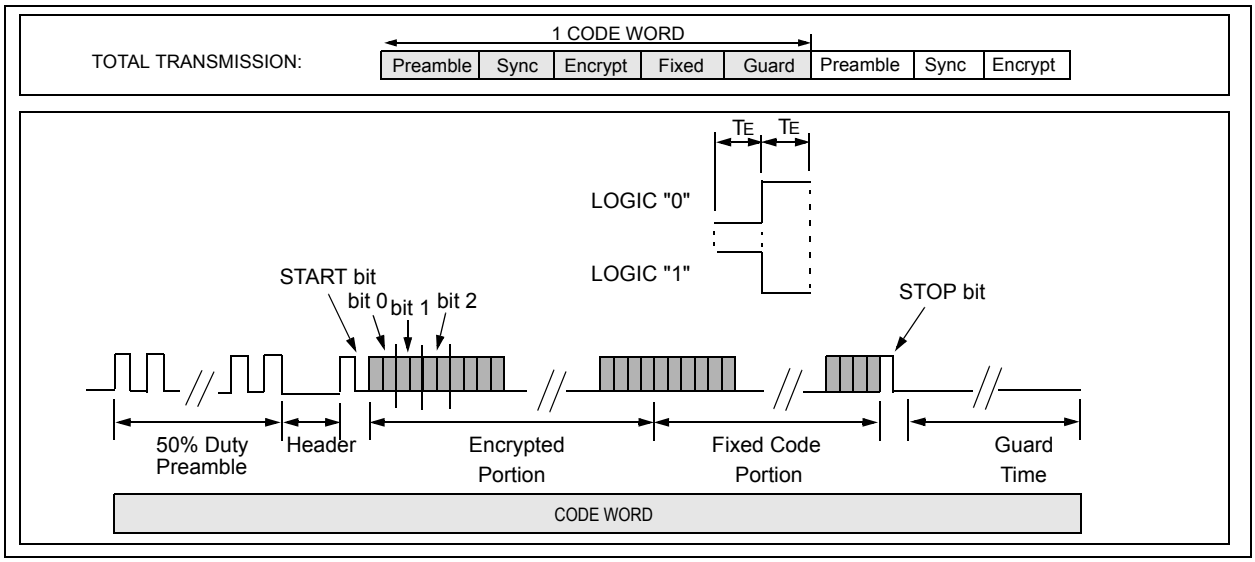


FIGURE 3-6: MANCHESTER TRANSMISSION FORMAT—MOD = 1



3.4 Encoder Special Features

3.4.1 CODE WORD COMPLETION AND MINIMUM CODE WORDS

The code word completion feature ensures that entire code words are transmitted, even if the active button is released before the code word transmission is complete. If the button is held down beyond the time for one code word, multiple complete code words will result.

The device default is that a momentary button press will transmit at least one complete code word. Enable the Minimum Four Code Words (MTX4) configuration option to extend this feature such that a minimum of 4 code words are completed on a momentary button activation.

3.4.2 AUTO-SHUTOFF

The Auto-shutoff function prevents battery drain should a button get stuck for a long period of time. The time period (TTO) is approximately 20 seconds, after which the device will enter Time-out mode.

The device will stop transmitting in Time-out mode but there will be leakage across the stuck button input's internal pull-down resistor. The current draw will therefore be higher than when in Standby mode.

3.4.3 CODE WORD BLANKING ENABLE

Federal Communications Commission (FCC) part 15 rules specify the limits on worst case average fundamental power and harmonics that can be transmitted in a 100 ms window. For FCC approval purposes, it may therefore be advantageous to minimize the transmission duty cycle. This can be achieved by minimizing the on-time of the individual bits as well as by blanking out consecutive code words.

The Code Word Blanking Enable (CWBE) option may be used to reduce the average power of a transmission by transmitting only every second or every fourth code word (Figure 3-7). This selectable feature is determined in conjunction with the baud rate selection bit RFBSL (Table 3-7).

Enabling the CWBE option may similarly allow the user to transmit a higher amplitude transmission as the time averaged power is reduced. CWBE effectively halves the RF on-time for a given transmission so the RF output power could theoretically be doubled while maintaining the same time averaged output power.

FIGURE 3-7: CODE WORD BLANKING

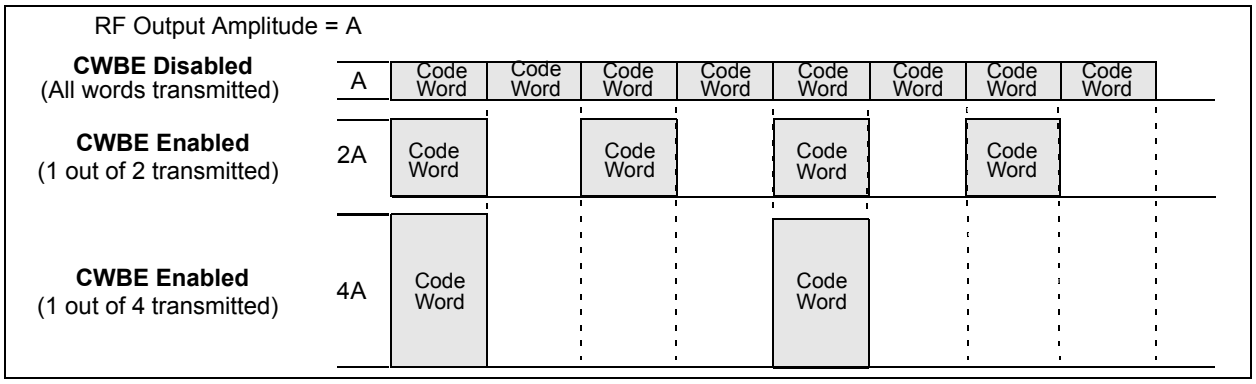


TABLE 3-7: CODE WORD BLANKING ENABLE (CWBE)

RFBSL1:0	CWBE	PWM RFTE	Manchester RFTE	Transmit...
00b	X	400 µs	800 µs	All code words
01b	0	200 µs	400 µs	All code words
	1	200 µs	400 µs	Every other code word
10b	0	100 µs	200 µs	All code words
	1	100 µs	200 µs	Every other code word
11b	0	100 µs	200 µs	All code word
	1	100 µs	200 µs	Every fourth code word

3.4.4 DELAYED INCREMENT (DINC)

The HCS412's Delayed Increment feature advances the synchronization counter by 12 a period of TTO after the encoder activation occurs, for additional security. The next activation will show a synchronization counter increase of 13, not 1.

If the active button is released before the time-out TTO has elapsed, the device stops transmitting but remains powered for the duration of the time-out period. The device will then advance the stored synchronization counter by 12 before powering down.

If the active button is released before the time-out TTO has elapsed and another activation occurs while waiting out the time-out period, the time-out counter will RESET and the resulting transmission will contain synchronization counter value +1.

Note: If delayed increment is enabled, the QUE counter will not reset to 0 until timeout TTO has elapsed.

3.4.5 PLL INTERFACE

If the RFEN/S2/LC1 pin is configured as an RF enable output, the pin's behavior is coordinated with the DATA pin to enable a typical PLL's ASK or FSK mode.

The PLL Interface (AFSK) configuration option controls the output as shown in Figure 3-8.

TABLE 3-8: PLL INTERFACE(AFSK)

AFSK	Description
0	ASK PLL Setup
1	FSK PLL Setup

3.4.6 LED OUTPUT

During normal operation (good battery), while transmitting data the device's LED pin will periodically be driven low as indicated in Figure 3-9.

If the supply voltage drops below the trip point specified by VLDWSEL, the LED pin will be driven low only once for a longer period of time.

3.4.7 LONG PREAMBLE (LPRE)

Enabling the Long Preamble configuration option extends the first code word's 50% duty cycle preamble to a 'long' preamble time TLPRE. The longer preamble will be a square wave at the selected RFTE (Figure 3-10).

FIGURE 3-8: RF ENABLE/ASK/FSK OPTIONS

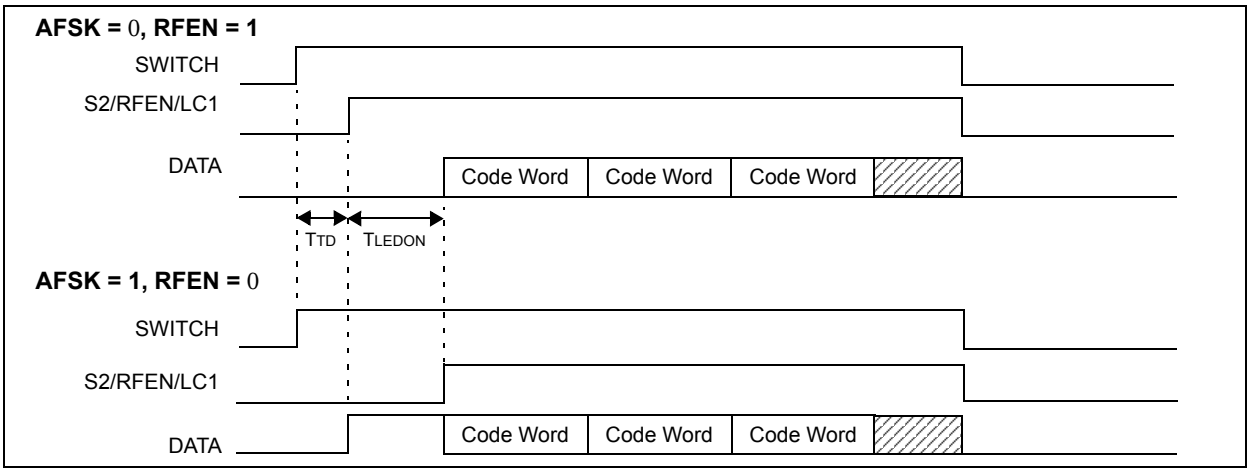


FIGURE 3-9: LED OPERATION

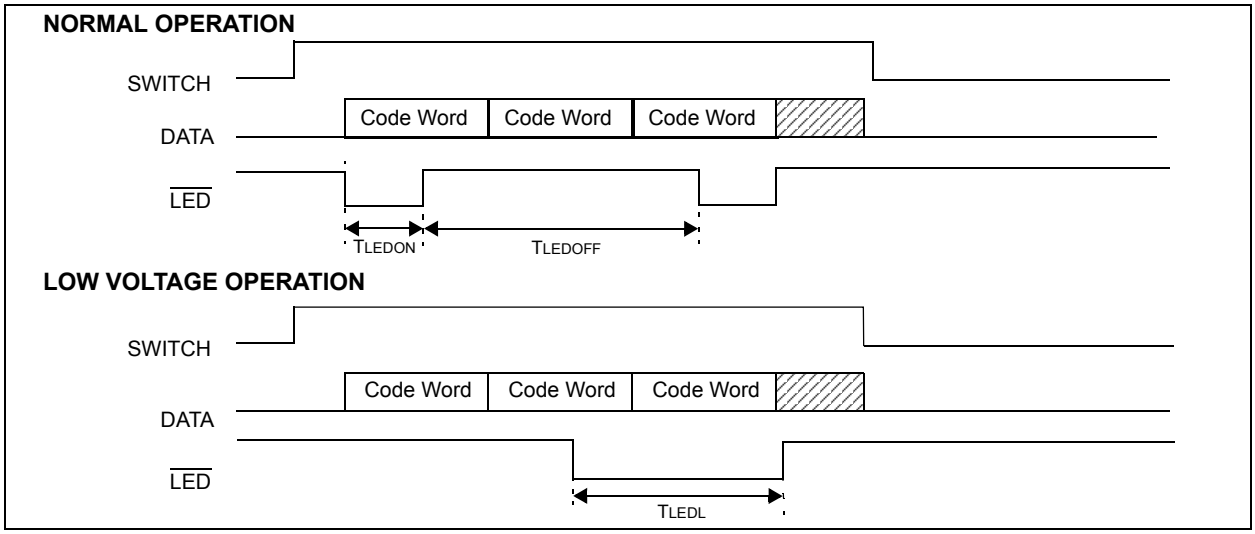
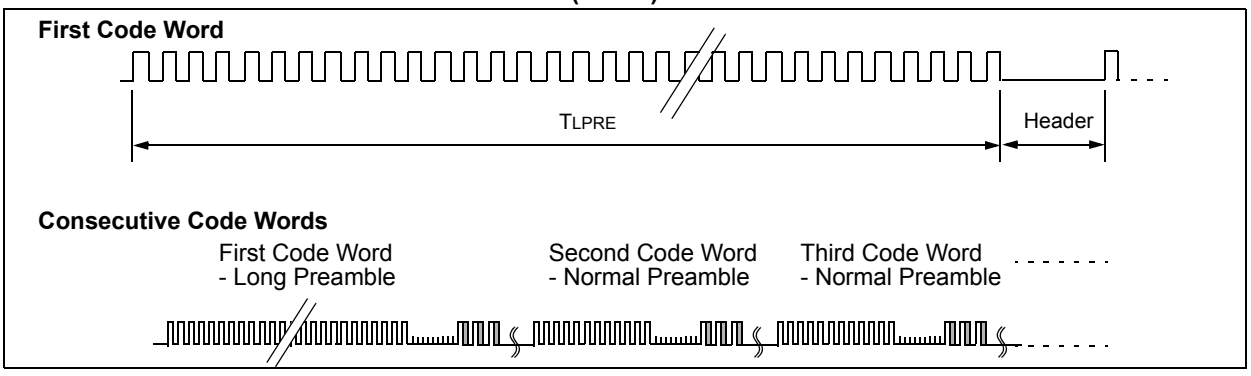


FIGURE 3-10: LONG PREAMBLE ENABLED (LPRE)



3.4.8 QLVS FEATURES

Setting the HCS412's special QLVS ('Quick Secure Learning') configuration option enables the following options:

- Reduces the time (T_{DSD}) before a delayed seed transmission begins.
- Disables DATA modulation when the LED pin is driven low (Figure 3-11).
  - If the PLL Interface option is set to ASK, the DATA pin will go low while the LED pin is low.
  - If the PLL Interface option is set to FSK, the DATA pin will go high and the RFEN output will go low while the LED pin is low. If the battery is low, the HCS412 transmits only until the LED goes on.
- If the Temporary Seed (TMPSD) option is enabled, seed transmission capability can be disabled by applying the button sequence shown in Figure 3-12

FIGURE 3-11: LED, DATA, RFEN INTERACTION WHEN QLVS IS SET

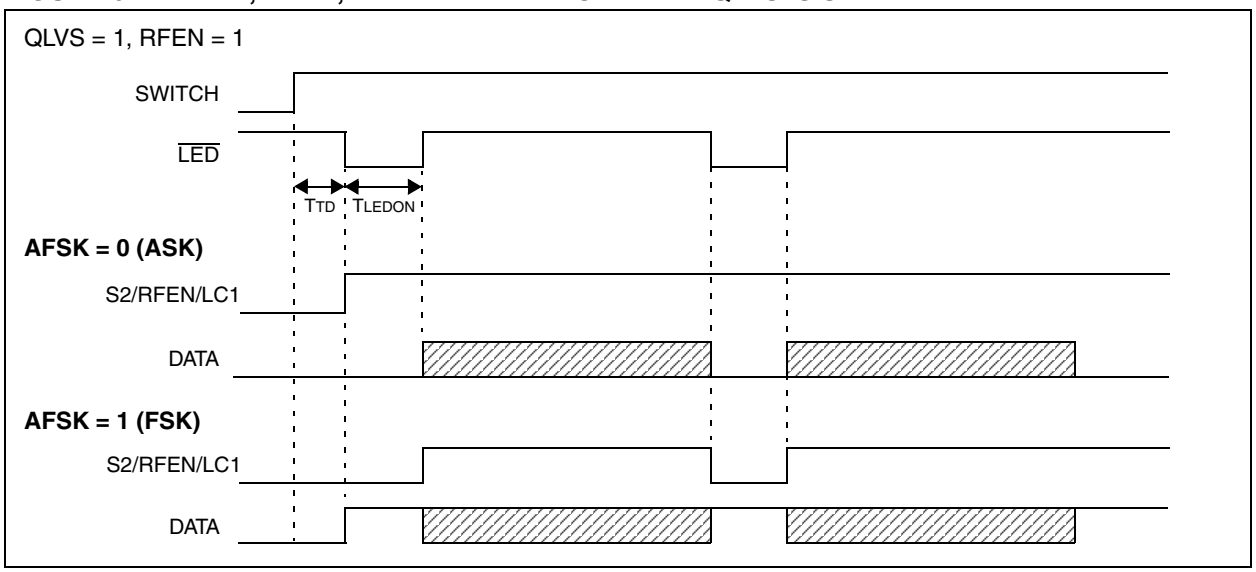


FIGURE 3-12: SEED DISABLE WAVEFORM

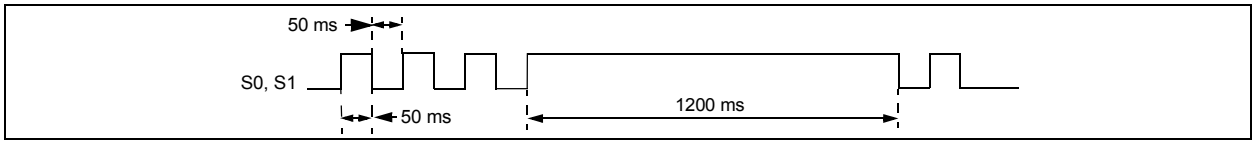


TABLE 3-9: ENCODER TIMING SPECIFICATIONS

V_{DD} = +2.0 to 6.6V Commercial (C): T_{AMB} = 0° C to +70° C Industrial (I): T_{AMB} = -40° C to +85° C						
Parameter	**Symbol**	**Min.**	**Typ.**	**Max.**	**Unit**	**Remarks**
Time to second button press	T_{BP}	44 + Code Word Time	58 + Code Word Time	63 + Code Word Time	ms	**Note 1**
Transmit delay from button detect	T_{TD}	20	30	40	ms	**Note 2**
Debounce delay on button press	T_{DBP}	14	20	26	ms	
Debounce delay on button release	T_{DBR}		20		ms	
Auto-shutoff time-out period	T_{TO}	18	20	22	s	**Note 3**
Long preamble	T_{LPRE}		64		ms	
LED on time	T_{LEDON}		32		ms	**Note 4**
LED off time	T_{LEDOFF}		480		ms	**Note 4**
LED on time (V_{DD} < V_{LOW} Trip Point)	T_{LEDL}		200		ms	**Note 5**
Time to delayed SEED transmission	T_{DSD}		3		s	
Queue Time	T_{QUE}		30		ms	

Note 1: T_{BP} is the time in which a second button can be pressed without completion of the first code word where 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 time-out period is not tested.

4: The LED times specified for V_{DD} > V_{TRIP} specified by V_{LOW} in the configuration word.

5: LED on time if V_{DD} < V_{TRIP} specified by V_{LOW} in the configuration word.

4.0 TRANSPONDER OPERATION

4.1 IFF Mode

The HCS412's IFF Mode allows it to function as a bi-directional token or transponder. IFF mode capabilities include the following.

- A bi-directional challenge and response sequence for IFF validation. HCS412 IFF responses may be directed to use one of two available encryption algorithms and one of two available crypt keys.
- Read selected EEPROM areas.
- Write selected EEPROM areas.
- Request a code hopping transmission.
- Proximity Activation of a code hopping transmission.

4.2 IFF Communication

The transponder reader initiates each communication by turning on the low frequency field, then waits for a HCS412 to Acknowledge the field.

The HCS412 enters IFF mode upon detecting a signal on the LC0 LF antenna input pin. Once the incoming signal has remained high for at least the power-up time T_{PU}, the device responds with a field Acknowledge sequence indicating that the it has detected the LF field, is in IFF Mode and is ready to receive commands (Figure 4-1). The HCS412 will repeat the field Acknowledge sequence every 255 LF_{TE}'s if the field remains but no command is received (Figure 4-1).

The transponder reader follows the HCS412's field Acknowledge by sending the desired 5-bit command and associated data. LF commands are always preceded by a 2 LF_{TE} low START pulse and are Pulse Position Modulated (PPM) as shown in Figure 4-2. The last command or data bit should be followed by leaving the field on for a minimum of 6 LF_{TE}.

HCS412 PPM data responses are preceded by a 1 LF_{TE} low pulse, followed by a 01b preamble before the data begins (Figure 4-4). The responses are sent either on the LC antenna output alone or on both the LC output and the DATA pin, depending on the device configuration (Section 4.4.2). This allows for short-range LF responses as well as long-range RF responses.

Data to and from the HCS412 is always sent Least Significant bit first. The data length and modulation format vary according to the command and the transmission path.

Data Length and Commands:

- Read and Write transfers 16 bits of data.
- Challenge and Response transfers 32 bits of data.

Modulation Format and Transmission Path:

- LF responses on the LC output are Pulse Position Modulated (PPM) according to Figure 4-2.
- RF responses on the DATA pin modulate according to standard encoder transmissions (Figure 3-5, Figure 3-6).

Communication with the HCS412 over the low frequency path (LC pins) uses a basic Timing Element, LF_{TE}. The Low Frequency Baud Rate Select option, LFBSL, sets LF_{TE} to either 100 µs or 200 µs (Table 4-1).

The response on the DATA pin uses the Encoder mode's RF Timing Element (RF_{TE}) and the modulation format set by the MOD configuration option (Table 3-6). The RF responses use the standard Encoder mode format with the 32-bit hopping portion replaced by the response data (Figure 4-19). If the response is only 16 bits, the 32 bits will contain 2 copies of the response (Figure 4-16).

TABLE 4-1: LOW FREQUENCY BAUD RATE SELECT BITS

LFBSL	LF_{TE}
0	200 µs
1	100 µs

4.2.1 CALCULATING COMMUNICATION TE

The HCS412's internal oscillator will vary ±10% over the device's rated voltage and temperature range. When the oscillator varies, both its transmitted T_E and expected T_E when receiving will vary.

Communication reliability with the token may be improved by calculating the HCS412's T_E from the field Acknowledge sequence and using this measured time element in communication to and in reception routines from the token.

Always begin and end the time measurement on rising edges. Whether LF or RF, the falling edge decay rates may vary but the rising edge relationships should remain consistent. A common T_E calculation method would be to time an 8 T_E sequence, then divide the value down to determine the single T_E value. An 8 T_E measurement will give good resolution and may be easily right-shifted (divide by 2) three times for the math portion of the calculation (Figure 4-1).

Accurately measuring T_E is important for communicating to an HCS412 as well as for inductive programming a device. The configuration word sent during programming contains the 4-bit oscillator tuning value. Accurately determining T_E allows the programmer to calculate the correct oscillator tuning bits to place in the configuration word, whether the device oscillator needs to be sped up or slowed down to meet its desired T_E.

FIGURE 4-1: FIELD ACKNOWLEDGE SEQUENCE

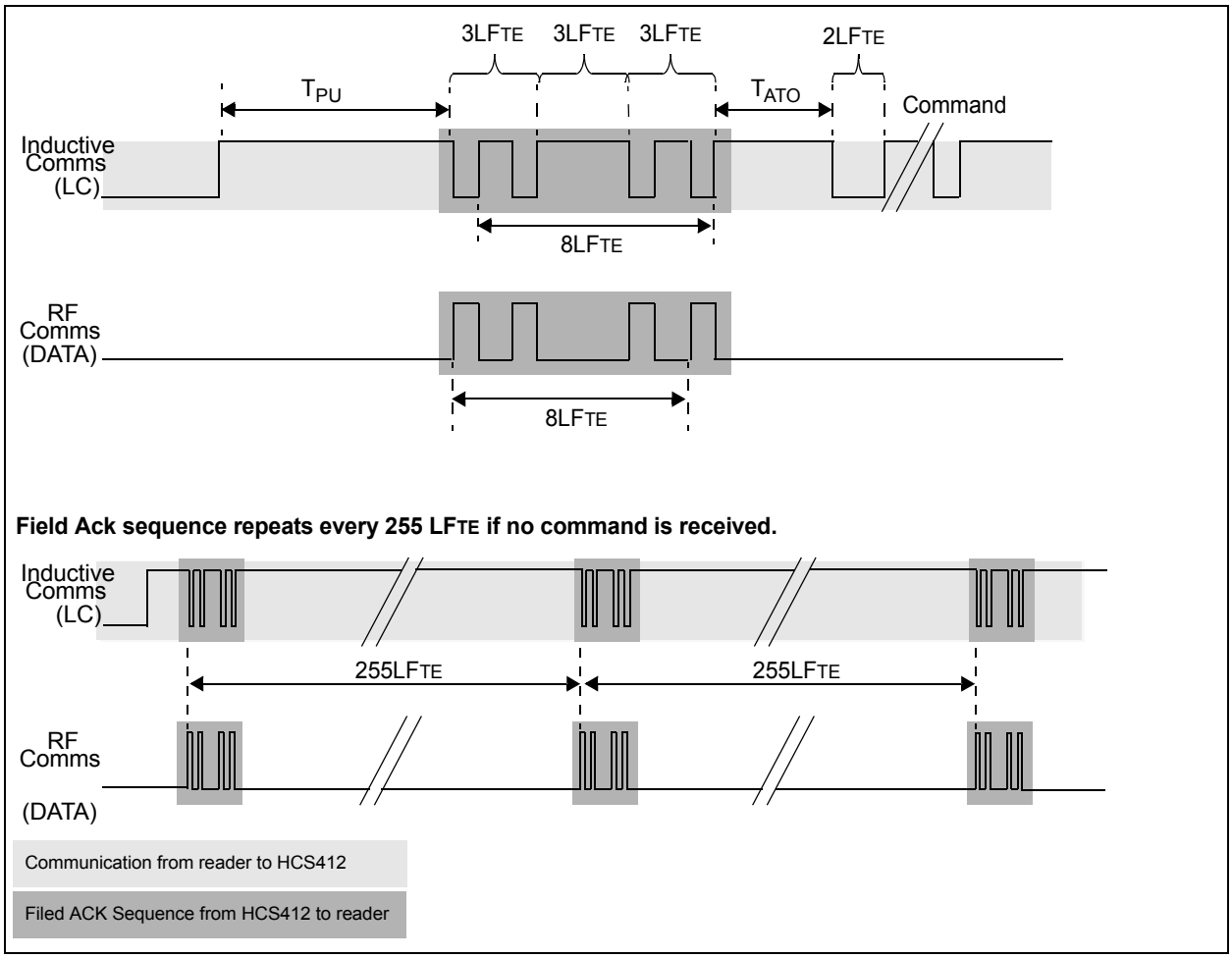
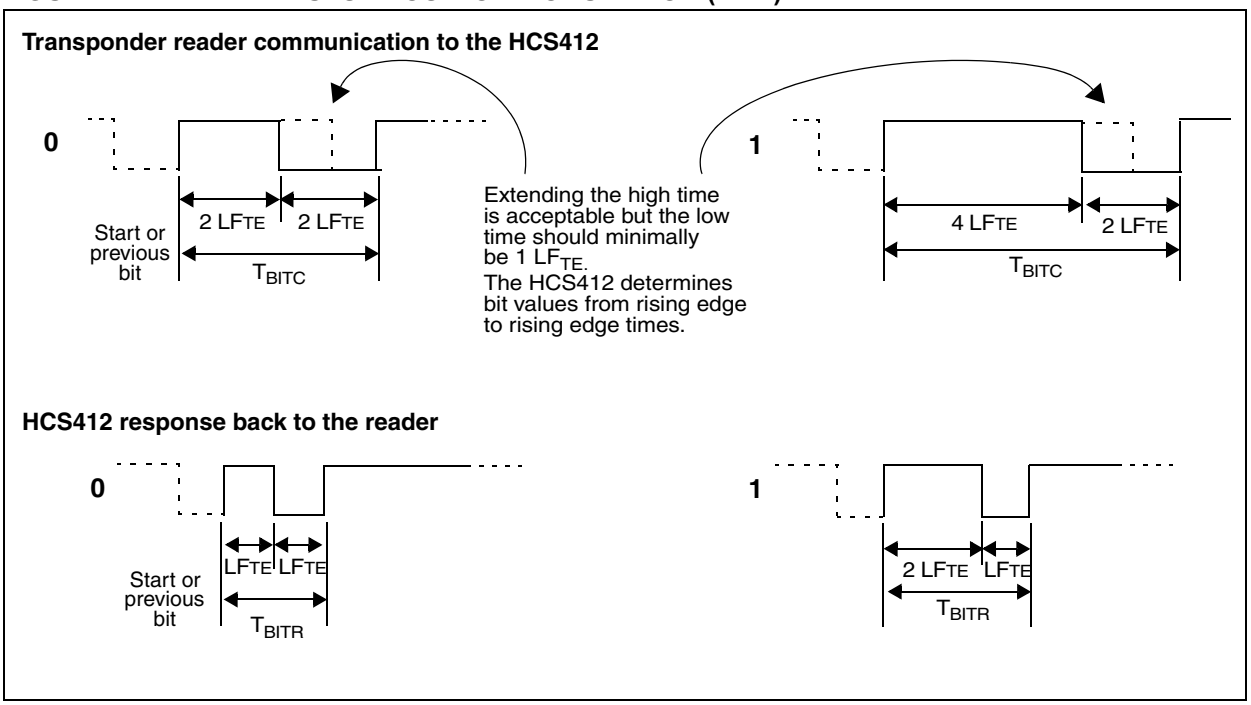


FIGURE 4-2: LC PIN PULSE POSITION MODULATION (PPM)



4.3 IFF Commands

TABLE 4-2: LIST OF AVAILABLE IFF COMMANDS

Opcode	Command
Anticollision Command (Section 4.3.1)	
00000	Select HCS412, used if Anticollision enabled
Read Commands (Section 4.3.2)	
00001	Read configuration word
00010	Read low serial number (least significant 16 bits)
00011	Read high serial number (most significant 16 bits)
00100	Read user EEPROM 0
00101	Read user EEPROM 1
00110	Read user EEPROM 2
00111	Read user EEPROM 3
Program Command (Section 4.3.5)	
01000	Program HCS412 EEPROM
Write Commands (Section 4.3.3)	
01001	Write configuration word
01010	Write low serial number (least significant 16 bits)
01011	Write high serial number (most significant 16 bits)
01100	Write user EEPROM 0
01101	Write user EEPROM 1
01110	Write user EEPROM 2
01111	Write user EEPROM 3
Challenge and Response Commands (Section 4.3.6)	
10000	Challenge and Response using key-1 and IFF algorithm
10001	Challenge and Response using key-1 and HOP algorithm
10100	Challenge and Response using key-2 and IFF algorithm
10101	Challenge and Response using key-2 and HOP algorithm
Request Hopping Code Command (Section 4.3.7)	
11000	Request Hopping Code transmission
Default IFF Command (Section 4.3.8)	
11100	Enable default IFF communication

4.3.1 ANTICOLLISION

Multiple tokens in the same inductive field will simultaneously respond to inductive commands. The responses will collide making token authentication impossible. Enabling anticollision allows addressing of an individual token, regardless how many tokens are in the field.

The HCS412 method is that all tokens trained to a given vehicle will have the same 25 MSb's of their serial number. The serial numbers of up to 8 tokens trained to access a given vehicle will differ only in the 3 LSb's. Think of the 25 MSb's of the HCS412's serial number as the vehicle ID and the 3 LSb's as the token ID. The vehicle ID associates the token with a given vehicle and the token ID makes it a uniquely addressable (selectable) 1 of 8 possible tokens authorized to access the vehicle.

The transponder reader addresses an individual token, HCS412, by sending a '`SELECT ENCODER`' command. The command is followed by from 1 to 25 bits of the HCS412's serial number, starting with bit 3 (Least Significant bit first) (Figure 4-3).

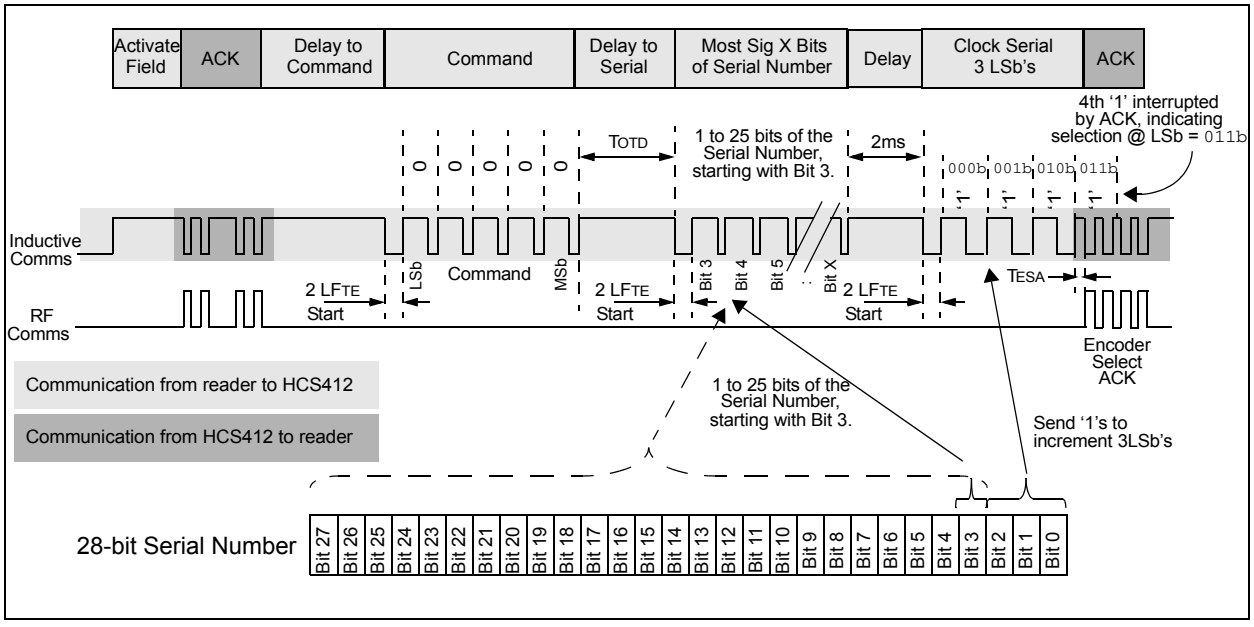
Clocking out '1's then increments the 3 LSb's, the first '1' setting the bits to `000b`. When the value matches the 3 LSb's of a token, the token responds with an Encoder Select Acknowledge. The reader must halt clocking out further '1's or risk selecting multiple tokens. Any remaining tokens in the field will be unselected, responding only if a new device selection sequence selects them. Removing the field will also RESET a selected/unselected state if removed long enough to result in a device RESET.

The ability to isolate a single HCS412 for communication greatly depends on the number of Most Significant serial number bits included in the device selection sequence. The more serial number bits sent, the more narrow the device selection. All bits not transmitted are treated as wildcards. Sending only 1 bit, bit 3 as a '0', will only narrow the number of tokens allowed to respond to all with bit 3 equal to '0'. When the transponder reader sends the full 25 MSb's of the serial number, it narrows all possible tokens down to only those trained to the vehicle - only those tokens whose serial number's 25 MSb's match.

TABLE 4-3: DEVICE SELECT COMMAND

Command	Description	Expected data In	Response
`00000`	Select HCS412, used if Anticollision enabled	The desired HCS412's serial number	Encoder select Acknowledge if serial number match

FIGURE 4-3: ANTICOLLISION - DEVICE SELECTION



4.3.2 READ

The transponder reader sends one of seven possible read commands indicating which 16-bit EEPROM word to retrieve (Table 4-4). The HCS412 retrieves the data and returns the 16-bit response.

Each Read response is preceded by a 1LFTE low START pulse and '01b' preamble (Figure 4-4).

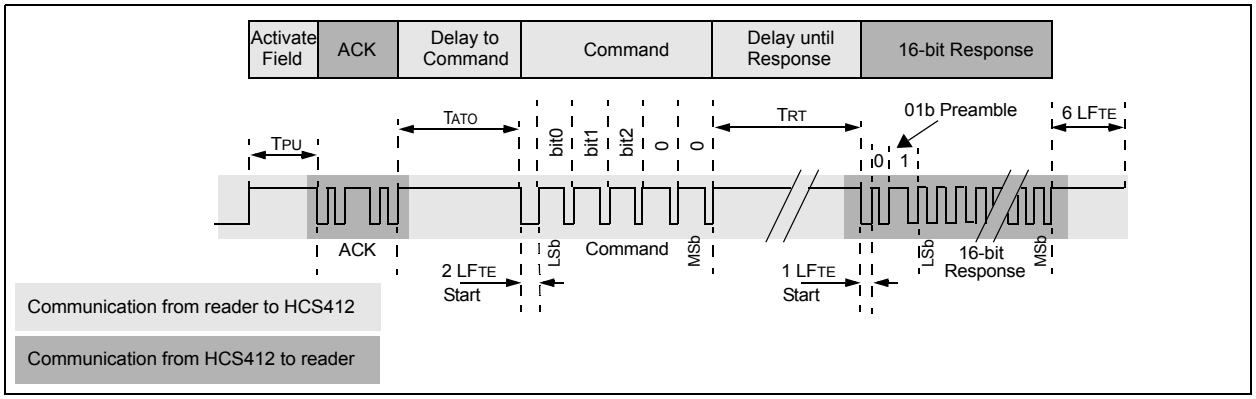
The following locations are available to read:

- The 64-bit general purpose user EEPROM. (USER[3:0]).
- The 32-bit serial number (SER[1:0]). The serial number is also transmitted in each code hopping transmission.
- The16-bit Configuration word containing all non-security related options.

TABLE 4-4: LIST OF READ COMMANDS

Command	Description	Expected data In	Response
00001	Read Configuration word	None	16-bit Configuration word
00010	Read low serial number	None	Lower 16 bits of serial number (SER0)
00011	Read high serial number	None	Higher 16 bits of serial number (SER1)
00100	Read user EEPROM 0	None	16 Bits of User EEPROM USR0
00101	Read user EEPROM 1	None	16 Bits of User EEPROM USR1
00110	Read user EEPROM 2	None	16 Bits of User EEPROM USR2
00111	Read user EEPROM 3	None	16 Bits of User EEPROM USR3

FIGURE 4-4: READ



4.3.3 WRITE

The transponder reader sends one of seven possible write commands (Table 4-5) indicating which 16-bit EEPROM word to write to. The 16-bit data to be written follows the command. The HCS412 will attempt to write the value into EEPROM and respond with an Acknowledge sequence if successful.

The following locations are available to write:

- The 64-bit general purpose user EEPROM. (USER[3:0]) (Figure 4-6).
- The 32-bit serial number (SER[1:0]). The serial number is also transmitted in each code hopping transmission (Figure 4-5).
- The16-bit Configuration word containing all non-security related configuration options. If the configuration is written, the device must be RESET before the new settings take effect (Figure 4-5).

A Transport Code, write access password, protects the serial number and configuration word from undesired modification. For these locations the reader must follow the WRITE command with the appropriate 28-bit transport code, then the 16 bits of data to write. Only a correct match with the transport code programmed during production will allow write access to the serial number and configuration word (Figure 4-5).

The delay to a successful write Acknowledge will vary depending on the number of bits changed.

TABLE 4-5: LIST OF WRITE COMMANDS

Command	Description	Expected data In	Response if Write is Successful
01001	Write Configuration word	28-bit Transport code; 16-Bit configuration word	Write Acknowledge pulse
01010	Write low serial number	28-bit Transport code; Least Significant 16 bits of the serial number (SER0)	Write Acknowledge pulse
01011	Write high serial number	28-bit Transport code; Most Significant 16 bits of the serial number (SER1)	Write Acknowledge pulse
01100	Write user EEPROM 0	16 Bit User EEPROM USR0	Write Acknowledge pulse
01101	Write user EEPROM 1	16 Bit User EEPROM USR1	Write Acknowledge pulse
01110	Write user EEPROM 2	16 Bit User EEPROM USR2	Write Acknowledge pulse
01111	Write user EEPROM 3	16 Bit User EEPROM USR3	Write Acknowledge pulse

FIGURE 4-5: WRITE TO SERIAL NUMBER OR CONFIGURATION

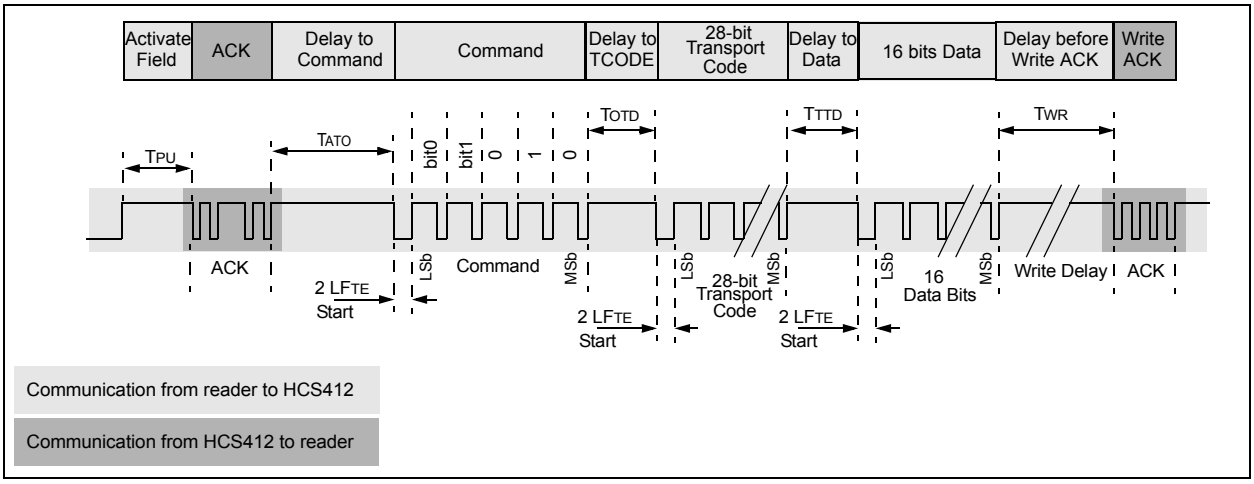
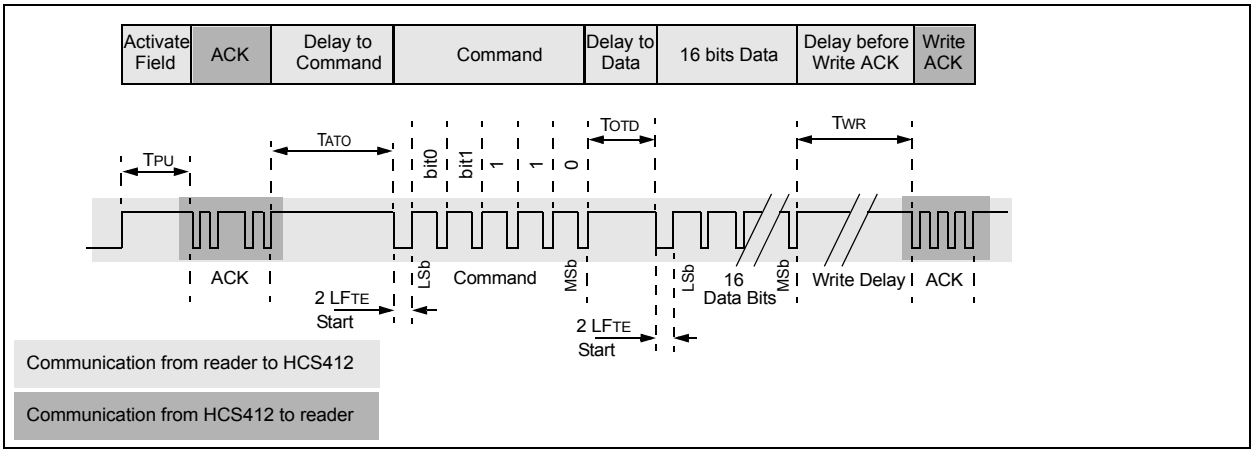


FIGURE 4-6: WRITE TO USER AREA

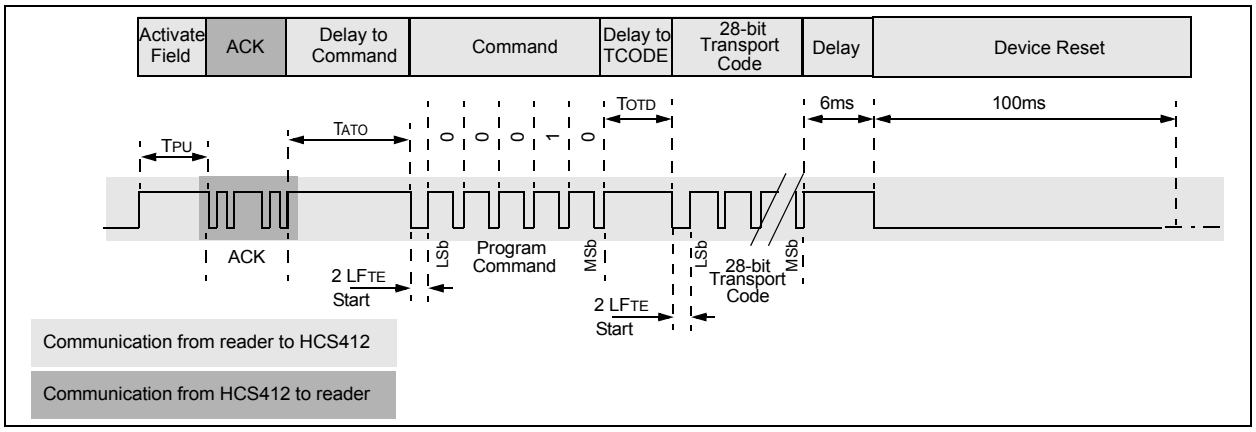


4.3.4 BULK ERASE

A Bulk Erase resets the HCS412's memory map to all zeros. The transponder reader selects the appropriate device through anticollision, as need be, issues the PROGRAM command followed by the device's 28-bit transport code, then resets the device by removing the field for 100 ms.

Resetting the device after the PROGRAM command results in a bulk erase, resetting the EEPROM memory map to all zeros. This is important to remember as the reader must now communicate to the device using the communication options resulting from a zero'd configuration word - baud rates, modulation format, etc. (Table 5-1).

FIGURE 4-7: BULK ERASE



4.3.5 PROGRAM

Inductive programming a HCS412 begins with a bulk erase sequence (Section 4.3.4), followed by issuing the PROGRAM command and the desired EEPROM memory map's 18x16-bit words (Section 5.0). The HCS412 will send a write Acknowledge after each word has been successfully written, indicating the device is ready to receive the next 16-bit word.

After a complete 18 word memory map has been received and written, the HCS412 PPM modulates 18 bursts of 16-bit words on the LC pins for write verification. Each word follows the standard HCS412 response format with a leading 1LFTE low START pulse and '01b' preamble (Figure 4-10).

Since the bulk erase resets the configuration options to all zeros, the oscillator tuning value will also be cleared. The correct tuning value is required when the programming sequence sends the new configuration word. The value may either be obtained by reading the configuration word prior to bulk erase to extract the value or by determining TE from the field Acknowledge sequence and calculating the tuning value appropriately (Section 4.2.1).

TABLE 4-6: PROGRAM COMMANDS

Command	Description	Expected data In	Response
01000	Program HCS412 EEPROM	Transport code (28 bits); Complete memory map: 18 x 16-bit words (288 bits)	Write Acknowledge pulse after each 16-bit word, 288 bits transmitted in 18 bursts of 16-bit words

FIGURE 4-8: PROGRAM SEQUENCE - FIRST WORD

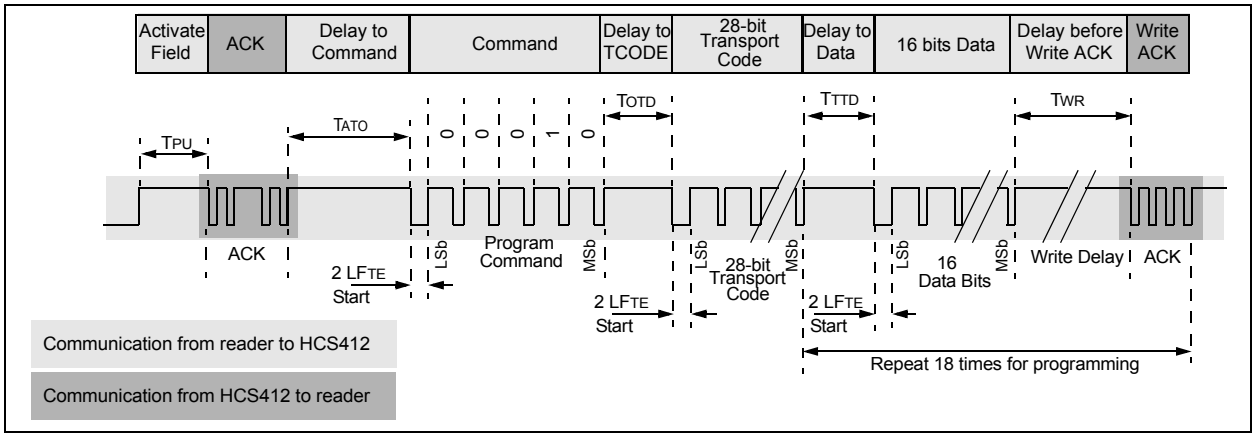


FIGURE 4-9: PROGRAM SEQUENCE - CONSECUTIVE WORDS

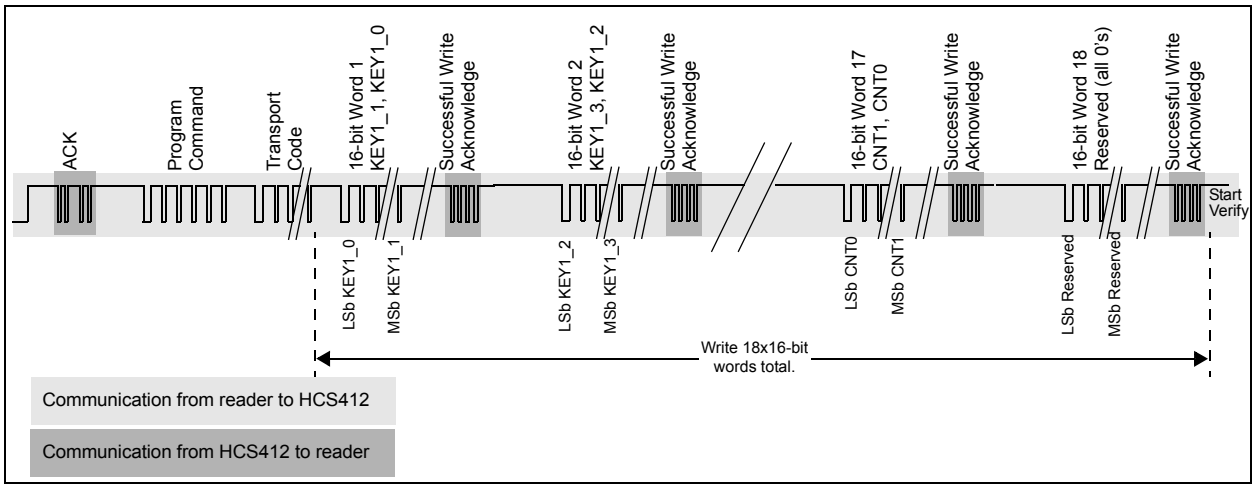
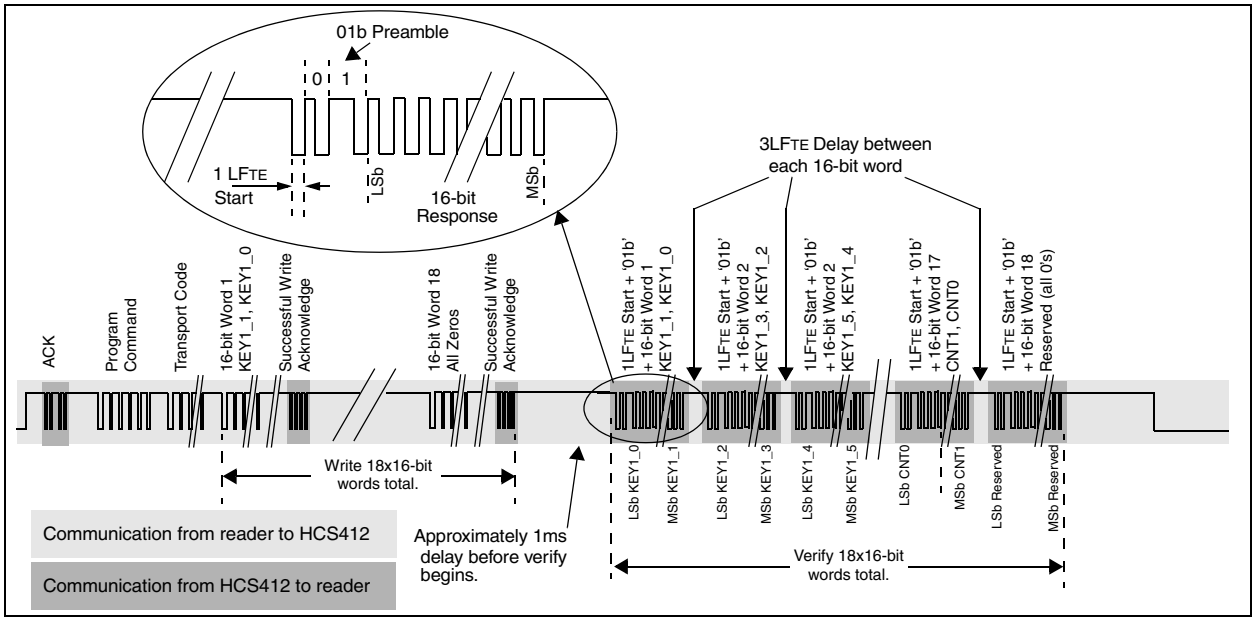


FIGURE 4-10: PROGRAMMING - VERIFICATION



4.3.6 IFF CHALLENGE AND RESPONSE

The transponder reader sends one of four possible IFF commands indicating which crypt key and which algorithm to use to encrypt the challenge (Table 4-7).

The command is followed by the 32-bit challenge, typically a random number. The HCS412 encrypts the challenge using the designated crypt key and algorithm and responds with the 32-bit encrypted result. The reader authenticates the response by comparing it to the expected value.

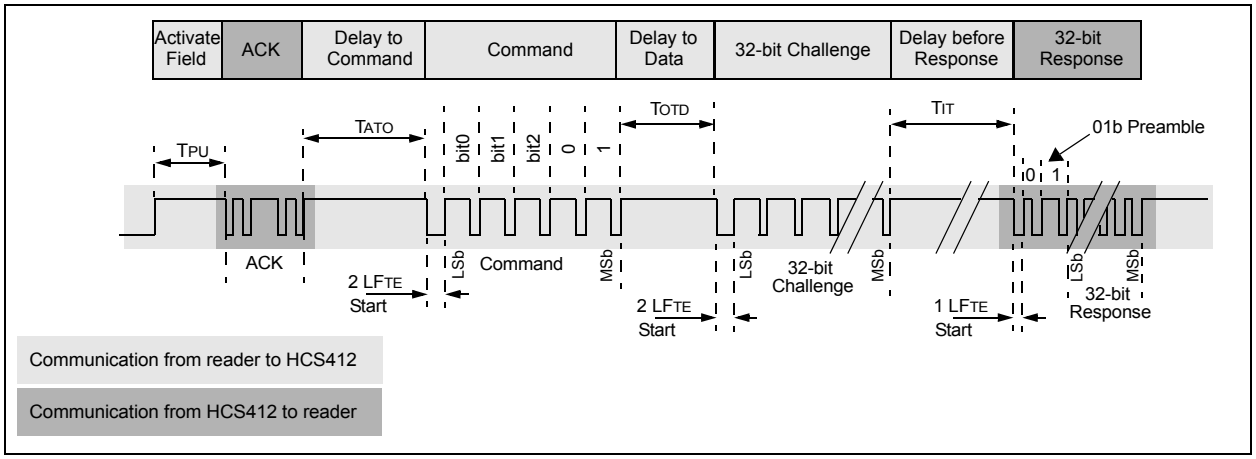
The second crypt key and the seed value occupy the same EEPROM storage area. To use the second crypt key for IFF, the Seed Enable (SEED) and the Temporary Seed Enable (TMPSD) configuration options must be disabled.

Note: If seed transmissions are not appropriately disabled, the HCS412 will default to using KEY1 for IFF.

TABLE 4-7: CHALLENGE AND RESPONSE COMMANDS

Command	Description	Expected data In	Response
10000	IFF using key-1 and IFF algorithm	32-Bit Challenge	32-Bit Response
10001	IFF using key-1 and HOP algorithm	32-Bit Challenge	32-Bit Response
10100	IFF using key-2 and IFF algorithm	32-Bit Challenge	32-Bit Response
10101	IFF using key-2 and HOP algorithm	32-Bit Challenge	32-Bit Response

FIGURE 4-11: IFF CHALLENGE AND RESPONSE



4.3.7 CODE HOPPING REQUEST

The command tells the HCS412 to increment the synchronization counter and build the 32-bit code hopping portion of the code word.

- If RF Echo is disabled, the data will be transmitted on the LC lines only (Figure 4-12).
- If RF Echo is enabled, the data will be transmitted in a code word on the DATA line followed by the data transmitted on the LC lines. The DATA line is transmitted first for passive entry support (Figure 4-13).

The data format will be the same as described in Section 3.2.

TABLE 4-8: REQUEST HOPPING CODE COMMANDS

Command	Description	Expected data In	Response
11000	Request Hopping Code transmission	None	32-Bit Hopping Code

FIGURE 4-12: CODE HOPPING REQUEST (RF ECHO DISABLED)

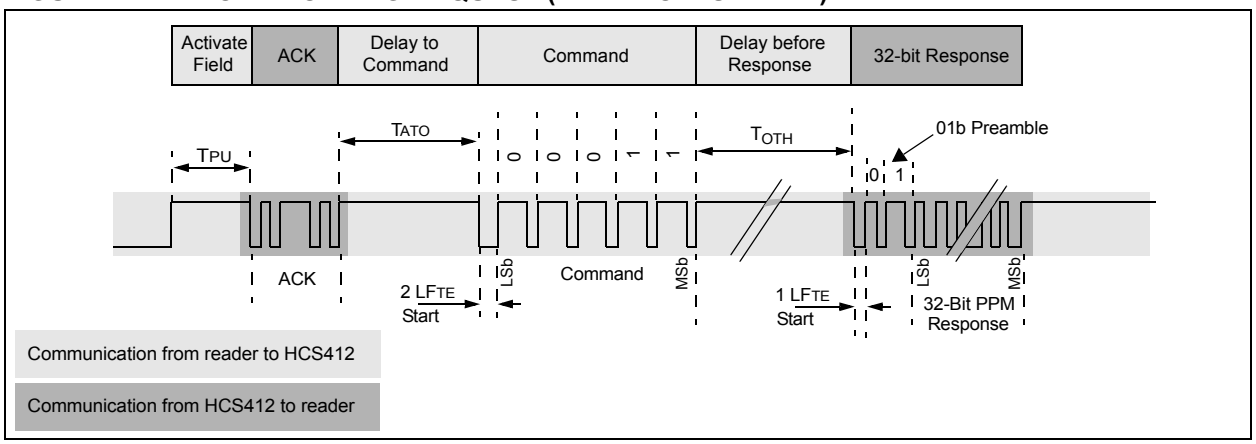
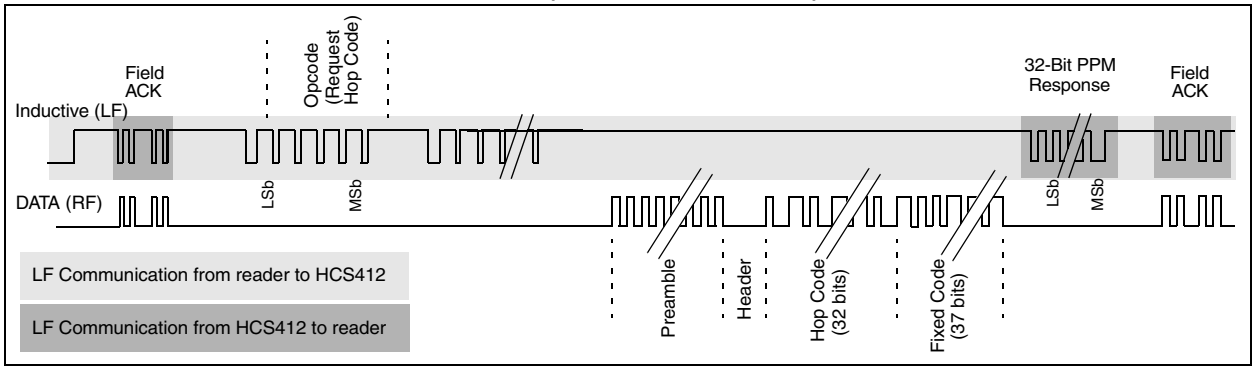


FIGURE 4-13: CODE HOPPING REQUEST (RF ECHO ENABLED)



4.3.8 ENABLE DEFAULT IFF COMMUNICATION

The ENABLE DEFAULT IFF COMMUNICATION command defaults certain HCS412 communication options such that the transponder reader may communicate to the device with a common (safe) protocol. The default setting remains for the duration of the communication, returning to normal only after a device RESET.

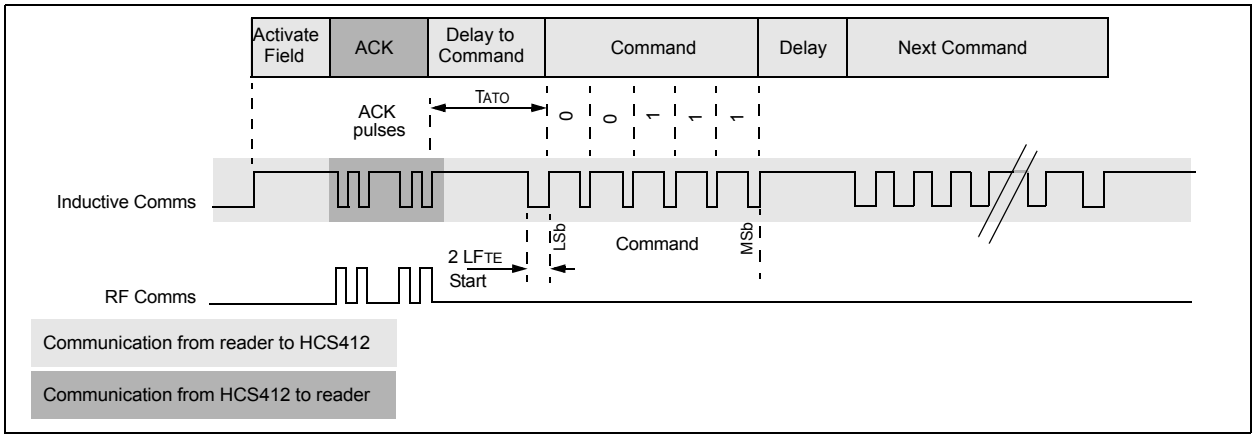
Default IFF communication settings:

- Anticollision disabled
- RF echo disabled
- 200 μs LF baud rate.

TABLE 4-9: DEFAULT IFF COMMUNICATION COMMANDS

Command	Description	Expected data In	Response
11100	Enable default IFF communication	None	None

FIGURE 4-14: ENABLE DEFAULT IFF COMMUNICATION



4.4 IFF Communication Special Features

TABLE 4-10: LF COMMUNICATION SPECIAL FEATURES (LFSP)

LFSP1:0	Description
00	No special options enabled
01	Anticollision enabled (Section 4.3.1)
10	Proximity Activation enabled
11	Anticollision and RF Echo enabled

4.4.1 PASSIVE PROXIMITY ACTIVATION (LFSP = 10)

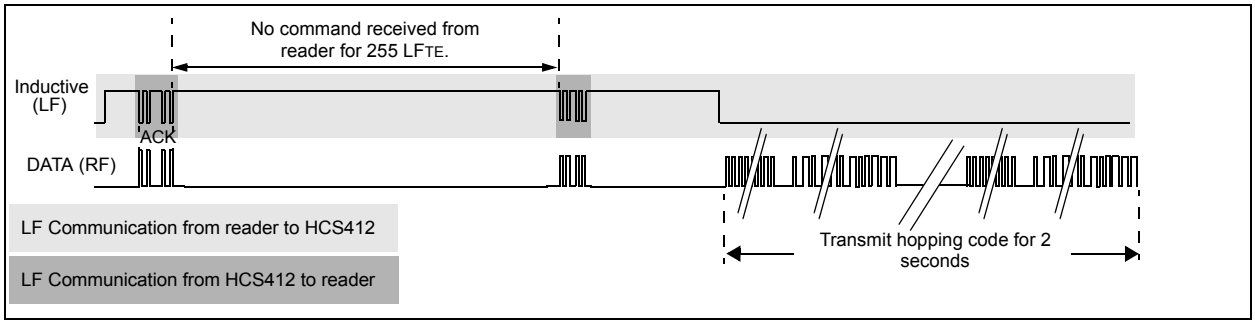
Enabling the Proximity Activation configuration option allows the HCS412 to transmit a hopping code transmission in response to a signal present on the LC0 pin.

The HCS412 sends out Field Acknowledge Sequence in response to detecting the LF field (Figure 4-1). If the HCS412 does not receive a command before the second field Acknowledge sequence [within 255 LFTE's], it will transmit a normal code hopping transmission for 2 seconds on the DATA pin. After 2 seconds the HCS412 reverts to normal transponder mode.

The 2 second transmission does not repeat when the device is in the presence of a continuous LF field. The HCS412 must be RESET, remove and reapply the LF field, to activate another transmission.

The button status used in the code hopping transmission indicates a proximity activation by clearing the S0, S1 and S2 button activation flags.

FIGURE 4-15: PROXIMITY ACTIVATION



4.4.2 ANTICOLLISION AND RF ECHO (LFSP = 11)

In addition to enabling anticollision, this mode adds that all HCS412 responses and Acknowledges are echoed on the DATA output line. Responses are first transmitted on the DATA line, followed by the equivalent data transmitted on the LF LC lines (Figure 4-16, Figure 4-17).

LF communication from the token to the transponder reader has much less range than LF communication from the reader to the token. Transmitting the information on the DATA line increases communication range by enabling longer range RF talk back.

The information is sent on the DATA line first to benefit longer range passive-entry authentication times.

FIGURE 4-16: RF ECHO OPTION AND READ COMMAND

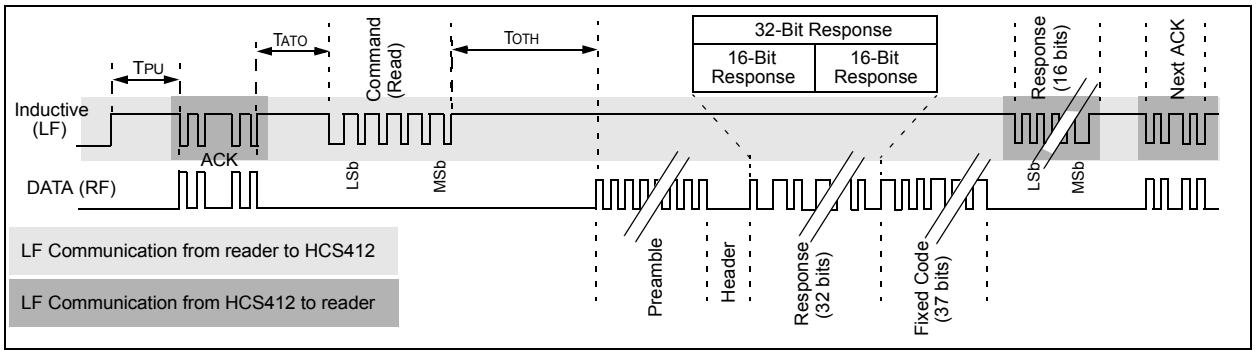


FIGURE 4-17: RF ECHO OPTION AND IFF COMMAND

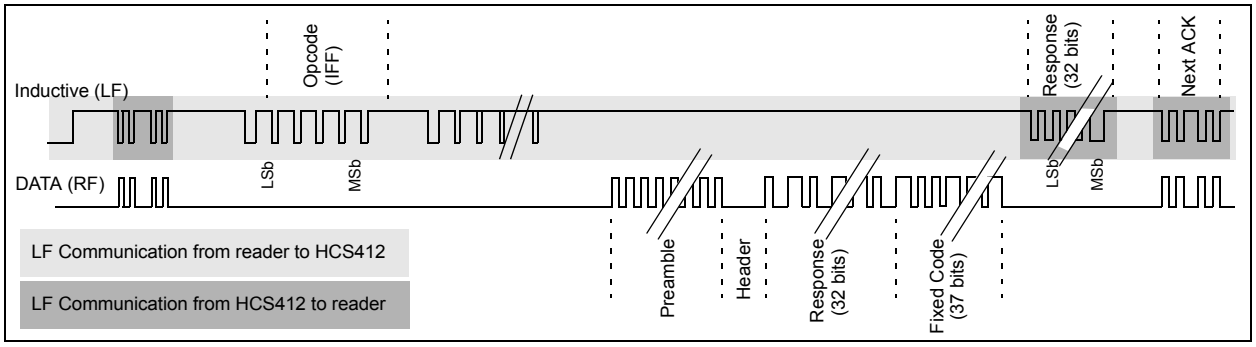
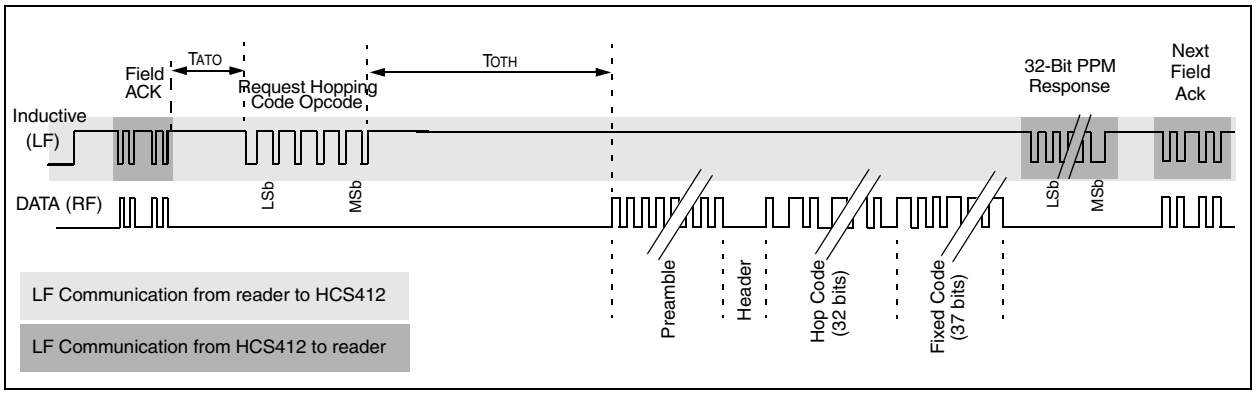


FIGURE 4-18: RF ECHO OPTION AND REQUEST HOPPING CODE COMMAND



4.4.3 INTELLIGENT DAMPING (IDAMP)

A high Q-factor LC antenna circuit connected to the HCS412 will continue to resonate after a strong LF field is removed, slowly decaying. The slow decay makes fast communication near the reader difficult as data bit low times disappear.

If the Intelligent Damping option is enabled, the HCS412 will clamp the LC pins through a 2 kΩ resistor for 5 µs every 1/4 LFTE, whenever the HCS412 is expecting data from the transponder reader. The intelligent damping pulses start 12.5 LFTE after the Acknowledge sequence is complete and continue for 12.5 LFTE. If the HCS412 detects data from the reader while sending out damping pulses, it will continue to send the damping pulses.

FIGURE 4-19: INTELLIGENT DAMPING

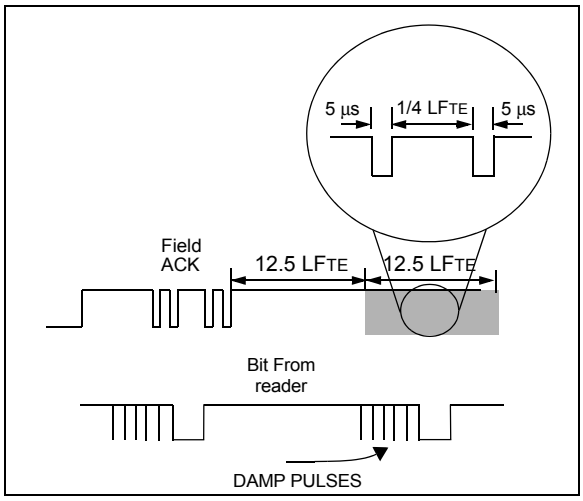


TABLE 4-11: INTELLIGENT DAMPING (IDAMP)

IDAMP	Description
0	Intelligent damping enabled
1	Intelligent damping disabled

TABLE 4-12: LF TIMING SPECIFICATIONS

Parameter		Symbol	Min.	Typ.	Max.	Units
Time Element	IFFB = 0 IFFB = 1	LFTE	180 90	200 100	220 110	µs
Power-up Time		TPU	4.2	6	7.8	ms
Acknowledge to Opcode Time		TATO	13			LFTE
PPM Command Bit Time	Data = 0 Data = 1	TBITC	— —	4 6	— —	LFTE
PPM Response Bit Time	Data = 0 Data = 1	TBITR	— —	2 3	— —	LFTE
Read Response Time		TRT	—	13	—	LFTE
IFF Response Time		TIT	3.87	4.3	4.73	ms
Opcode to Data Input Time		TOTD	2.6	—	—	ms
Transport Code to Data Input Time		TTTD	2.2	—	—	ms
Encoder Select Acknowledge Time		TESA	—	LFTE+100	—	µs
IFF EEPROM Write Time (16 bits)		TWR	—	30	—	ms
Op Code to Hop Code Response Time		TOTH	10.26	11.4	12.54	ms

5.0 CONFIGURATION SUMMARY

Table 5-1 summarizes the available HCS412 options.

TABLE 5-1: HCS412 CONFIGURATION SUMMARY

Symbol	Reference Section	Description			
KEY1		64-bit Encoder Key 1			
SDVAL	Section 3.2.7	60-bit seed value transmitted in CH Mode if (SEED = 1 AND TMPSD = 0) or if (SEED = 0 AND TMPSD = 1).			
KEY2		LSB 60 bits of Encoder Key 2. 4 MSb's set to XXXX. (**Note 1**)			
TCODE	Section 4.3.3	28-bit Transport Code			
AFSK	Section 3.4.5	PLL Interface Select.	0 = ASK	1 = FSK	
RFEN	Section 2.2.7	RF Enable output active.	0 = Disable	1 = Enable	
LPRE	Section 3.4.7	Long Preamble Enable.	0 = Disable	1 = Enable	
QLVS	Section 3.4.8	Special Features Enable.	0 = Disable	1 = Enable	
OSCT	Section 2.2.5	Oscillator Tune Value.	1000b	Fastest	
			0000b	Nominal	
			0111b	Slowest	
VLOWSEL	Section 2.2.6	Low Voltage Trip Point Select	0 = 2.2 Volt	1 = 4.4 Volt	
IDAMP	Section 4.4.3	Intelligent Damping Enable	0 = Enable	1 = Disable	
LFSP	Section 4.4	LF Communication Special Features	LFSP1:0	Active Feature	
			00b	None	
			01b	Anticollision	
			10b	Prox Activation	
			11b	RF Echo	
LFBSL	Section 4.2	IFF Baud Rate Select (LFTE)	0 = 200 us	1 = 100 us	
MOD	Section 3.3	DATA pin modulation format	0 = PWM	1 = Manch	
CWBE	Section 3.4.3	Code word Blanking Enable	0 = Disable	1 = Enable	
MTX4	Section 3.4.1	Minimum Four Code words	0 = Disable	1 = Enable	
RFBSL	Section 3.3	Transmission Baud Rate (RFTE)	RFBSL1:0	PWM	Manch
			00b	400 us	800 us
			01b	200 us	400 us
			10b	100 us	200 us
			11b	100 us	200 us
S2LC	Section 3.4.1	S2/RFEN/LC1 Pin Configuration bit.	0 = LC	1 = S Input	
—		Reserved, Set to 0	—	—	
TMPSD	Section 3.2.7	Temporary Seed Enable (**Note 1**)	0 = Disable	1 = Enable	
SEED	Section 3.2.7	Seed Transmission Enable (**Note 1**)	0 = Disable	1 = Enable	
XSER	Section 3.2.5	Extended Serial number	0 = Disable	1 = Enable	
DINC	Section 3.4.4	Delayed Increment	0 = Disable	1 = Enable	
DISC	Section 3.2.6	10-bit Discrimination value			
OVR	Section 3.2.4	Counter Overflow Value			
SER		32-bit Serial Number			
USR		64-bit user EEPROM area			
CNT		16-bit Synchronization counter			
—		Reserved set 0000h			

Note 1: If IFF with KEY2 is enabled only if TMPSD = 1 and SEED = 1.

6.0 INTEGRATING THE HCS412 INTO A SYSTEM

Use of the HCS412 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a free license agreement) firmware routines that accept transmissions from the HCS412 and decrypt the hopping code portion of the data stream. These routines provide system designers the means to develop their own decoding system.

6.1 Learning a Transmitter to a Receiver

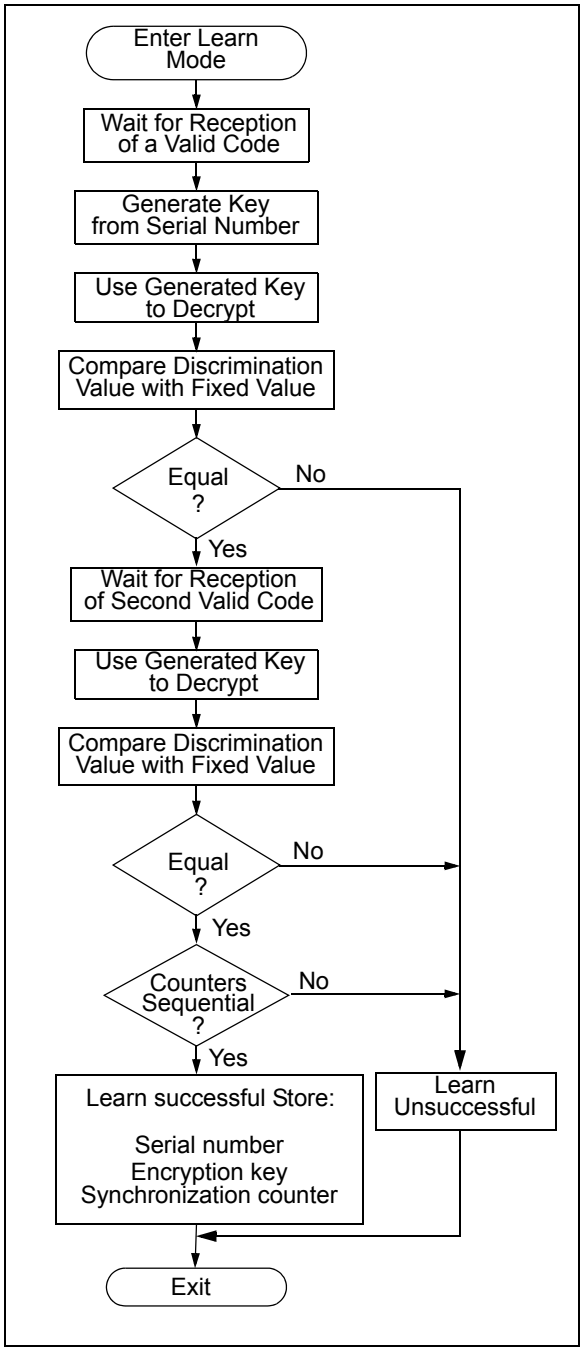
A transmitter must first be 'learned' by a decoder before its use is allowed in the system. Several learning strategies are possible, Figure 6-1 details a typical learn sequence. Core to each, the decoder must minimally store each learned transmitter's serial number and current synchronization counter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

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

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

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

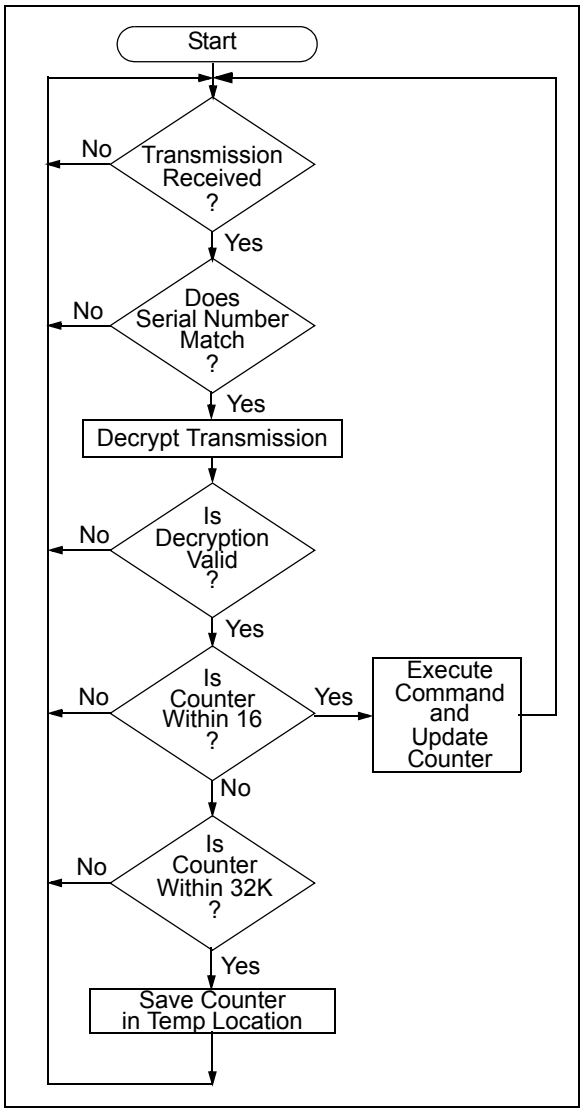
FIGURE 6-1: TYPICAL LEARN SEQUENCE



6.2 Decoder Operation

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

FIGURE 6-2: TYPICAL DECODER OPERATION



6.3 Synchronization with Decoder (Evaluating the Counter)

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

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

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

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

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

FIGURE 6-3: SYNCHRONIZATION WINDOW

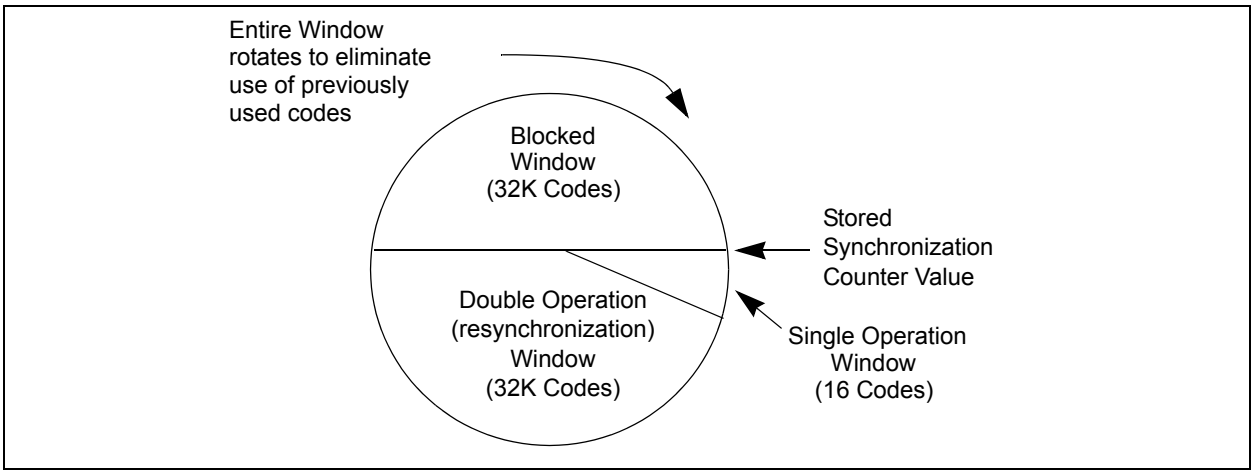
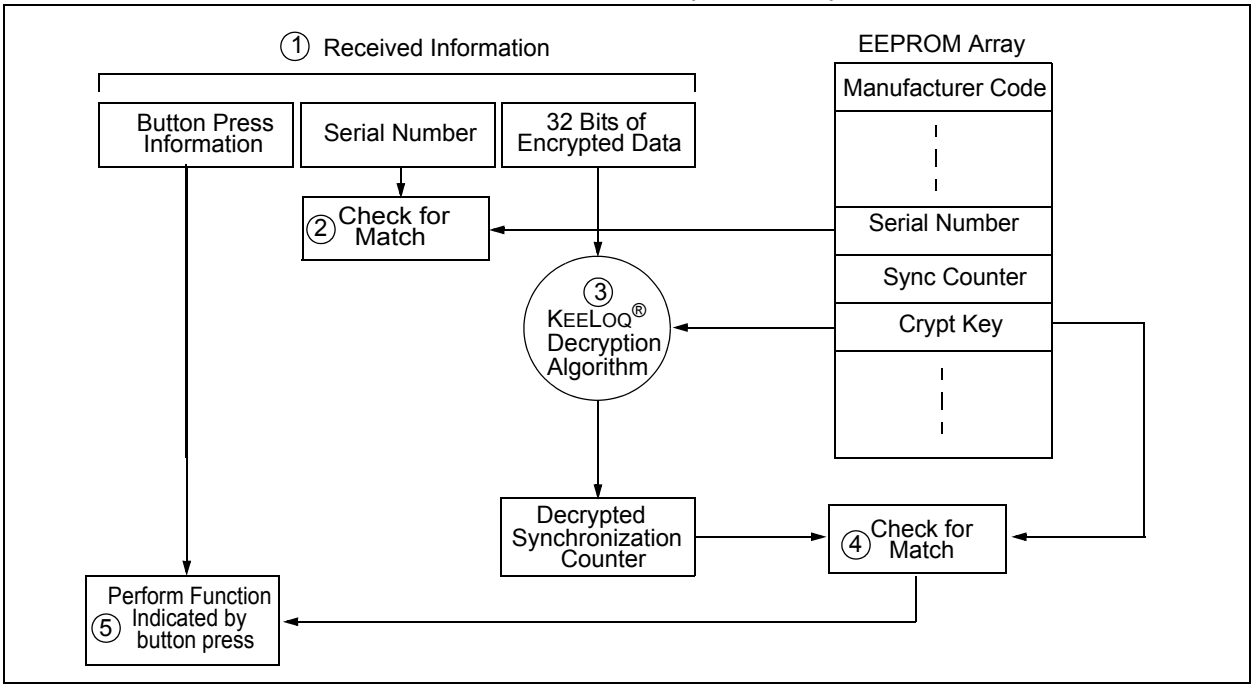


FIGURE 6-4: BASIC OPERATION OF RECEIVER (DECODER)



Note: Circled numbers indicate sequence of events.

7.0 PROGRAMMING THE HCS412

The HCS412 requires some parameters programmed into the device before it can be used. The programming cycle allows the user to input all 288 bits in a serial data stream, which are then stored internally in EEPROM.

Programming is initiated by forcing the DATA line high, after the S2 line has been held high for the appropriate length of time line (Table 7-1 and Figure 7-2).

A delay is required after entering Program mode while the automatic bulk erase cycle completes. The bulk erase writes all EEPROM locations to zeros.

The device is then programmed by clocking in the EEPROM memory map (Least Significant bit first) 16 bits at a time, using S2 as the clock line and DATA as the data-in line. After each 16-bit word is loaded, a programming delay is required for the internal program cycle to complete. This delay can take up to Twc.

The HCS412 will signal a 'write complete' after writing each 16-bit word by sending out a series of ACK pulses TACKH high, TACKL low on DATA. The ACK pulses continue until S2 is dropped.

Programming verification is allowed only once, after the programming cycle (Figure 7-3), by reading back the EEPROM memory map. Reading is done by clocking the S2 line and reading the data bits on DATA, again Least Significant bit first. For security reasons, it is not possible to execute a Verify function without first programming the EEPROM.

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

FIGURE 7-1: CREATION AND STORAGE OF CRYPT KEY DURING PRODUCTION

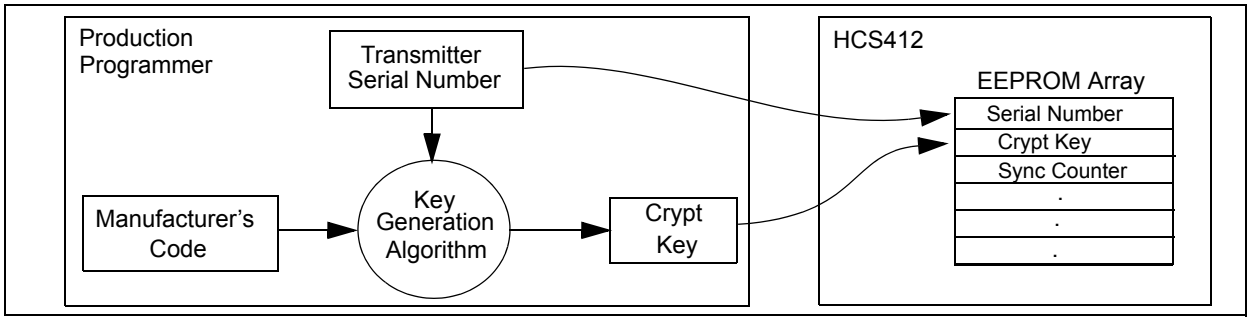
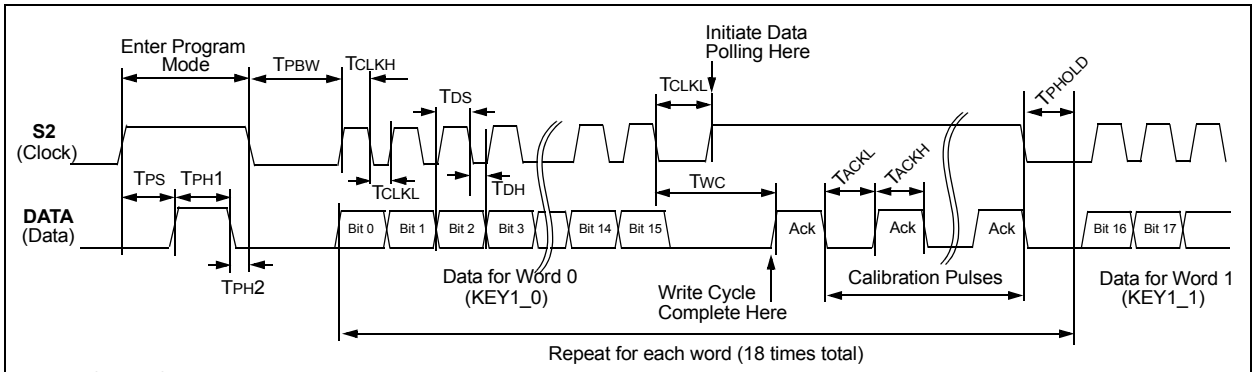
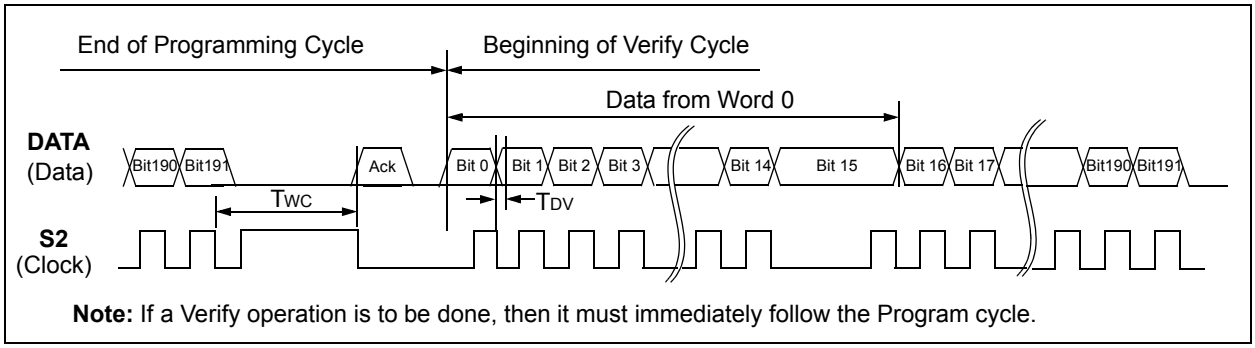


FIGURE 7-2: PROGRAMMING WAVEFORMS



Note 1: S0 and S1 button inputs to be held to ground during the entire programming sequence.

FIGURE 7-3: VERIFY WAVEFORMS



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

7.1 EEPROM Organization

TABLE 7-1: HCS412 EEPROM ORGANIZATION

16Bit Word	BITS															
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	KEY1_1								KEY1_0 (KEY1 LSB)							
2	KEY1_3								KEY1_2							
3	KEY1_5								KEY1_4							
4	KEY1_7 (KEY1 MSB)								KEY1_6							
5	SEED_1 / KEY2_1								SEED_0 / KEY2_0 (SEED AND KEY2 LSB)							
6	SEED_3 / KEY2_3								SEED_2 / KEY2_2							
7	SEED_5 / KEY2_5 / TCODE_1								SEED_4 / KEY2_4 / TCODE_0 (TCODE LSB)							
8	QLVS	LPRE	RFEN	AFSK	SEED_7 / KEY2_7 / TCODE_3 (MSB for all 3)				SEED_6 / KEY2_6 / TCODE_2							
9	Set to 0	S2LC	RFBSL 1	RFBSL 0	MTX4	CWBE	MOD	LFBSL	LFSP 1	LFSP 0	IDAMP	VLOWSEL	OSCT 3	OSCT 2	OSCT 1	OSCT 0
10	OVR 1	OVR 0	10bit Discrimination Value 9	8	7	6	5	4	3	2	1	0	DINC	XSER	SEED	TMPSD
11	SER1								SER0							
12	SER3								SER2							
13	USR0 MSB								USR0 LSB							
14	USR1 MSB								USR1 LSB							
15	USR2 MSB								USR2 LSB							
16	USR3 MSB								USR3 LSB							
17	CNT1 (Counter MSB)								CNT0 (Counter LSB)							
18	Reserved, set to 0								Reserved, set to 0							

TABLE 7-2: PROGRAMMING/VERIFY TIMING REQUIREMENTS

V_{DD} = 5.0V ± 10%, 25° C ± 5 °C				
Parameter	**Symbol**	**Min.**	**Max.**	**Units**
Program mode setup time	T_{PS}	2	5.0	ms
Hold time 1	T_{PH1}	4.0	—	ms
Hold time 2	T_{PH2}	50	—	µs
Bulk Write time	T_{PBW}	4.0	—	ms
Program delay time	T_{PROG}	4.0	—	ms
Program cycle time	T_{WC}	50	—	ms
Clock low time	T_{CLKL}	50	—	µs
Clock high time	T_{CLKH}	50	—	µs
Data setup time	T_{DS}	0	—	µs
Data hold time	T_{DH}	18	—	µs
Data out valid time	T_{DV}		30	µs
Hold time	T_{PHOLD}	100	—	µs
Acknowledge low time	T_{ACKL}	800	—	µs
Acknowledge high time	T_{ACKH}	800	—	µs

8.0 DEVELOPMENT SUPPORT

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

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

8.1 MPLAB Integrated Development Environment Software

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

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

The MPLAB IDE allows you to:

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

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

8.2 MPLAB C Compilers for Various Device Families

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

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

8.3 HI-TECH C for Various Device Families

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

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

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

8.4 MPASM Assembler

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

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

The MPASM Assembler features include:

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

8.5 MPLINK Object Linker/ MPLIB Object Librarian

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

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

The object linker/library features include:

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

8.6 MPLAB Assembler, Linker and Librarian for Various Device Families

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

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

8.7 MPLAB SIM Software Simulator

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

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

8.8 MPLAB REAL ICE In-Circuit Emulator System

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

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

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

8.9 MPLAB ICD 3 In-Circuit Debugger System

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

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

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

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

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

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

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

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

8.12 MPLAB PM3 Device Programmer

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

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

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

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

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

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

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

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

9.0 ELECTRICAL CHARACTERISTICS

TABLE 9-1: ABSOLUTE MAXIMUM RATING

Symbol	Item	Rating	Units
V_{DD}	Supply voltage	-0.3 to 6.6	V
V_{IN}*	Input voltage	-0.3 to V_{DD} + 0.3	V
V_{OUT}	Output voltage	-0.3 to V_{DD} + 0.3	V
I_{OUT}	Max output current	50	mA
T_{STG}	Storage temperature	-55 to +125	C **(Note)**
T_{LSOL}	Lead soldering temp	300	C **(Note)**
V_{ESD}	ESD rating (Human Body Model)	4000	V

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

* If a battery is inserted in reverse, the protection circuitry switches on, protecting the device and draining the battery.

TABLE 9-2: DC AND TRANSPONDER CHARACTERISTICS

Commercial (C): T_{AMB} = 0°C to 70°C
Industrial (I): T_{AMB} = -40°C to 85°C

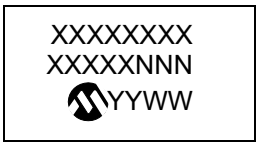
Parameter	Symbol	2.0V < V_{DD} < 6.3V			Unit	Conditions
		Min	Typ[1]	Max		
Average operating current **Note 2**	I_{DD} (avg)	—	200	500	µA	V_{DD} = 6.3V
Programming current	I_{DDP}		2.3	4.0	mA	V_{DD} = 6.3V
Standby current	I_{DDS}	—	0.1	500	nA	LC = off else < 5 µA
High level input voltage	V_{IH}	0.55 V_{DD}	—	V_{DD} + 0.3	V	
Low level input voltage	V_{IL}	-0.3	—	0.15 V_{DD}	V	
High level output voltage	V_{OH}	0.8 V_{DD} 0.8 V_{DD}	—	—	V	V_{DD} = 2V, I_{OH} =- .45 mA V_{DD} = 6.3V, I_{OH},= -2 mA
Low level output voltage	V_{OL}	— —	— —	0.08 V_{DD} 0.08 V_{DD}	V	V_{DD} = 2V, I_{OH} = 0.5 mA V_{DD} = 6.3V, I_{OH} = 5 mA
LED output current	I_{LED}	3.0	4.0	7.0	mA	V_{DD} = 3.0V, V_{LED} = 1.5V
Switch input resistor	R_S	40	60	80	kΩ	S0/S1 not S2
DATA input resistor	R_{DATA}	80	120	160	kΩ	
LC input current	I_{LC}	—	—	10.0	mA	V_{LCC}=10 V_{P-P}
LC input clamp voltage	V_{LCC}	—	10	—	V	I_{LC} <10 mA
LC induced output current	V_{DDI}	—		2.0	mA	V_{LCC} > 10V
LC induced output voltage	V_{DDV}	— —	4.5 4.0	— —	V	10 V < V_{LCC}, I_{DD} = 0 mA 10 V < V_{LCC}, I_{DD} = -1 mA
Carrier frequency	fc	—	125		kHz	
LC input sensitivity	V_{LCS}	—	100	—	mV_{PP}	**Note 3**

Note 1: Typical values at 25°C.
2: No load connected.
3: Not tested.

10.0 PACKAGING INFORMATION

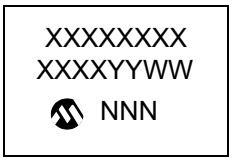
10.1 Package Marking Information

8-Lead PDIP



Example

8-Lead SOIC



Example

Legend:	MM...M	Microchip part number information
	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

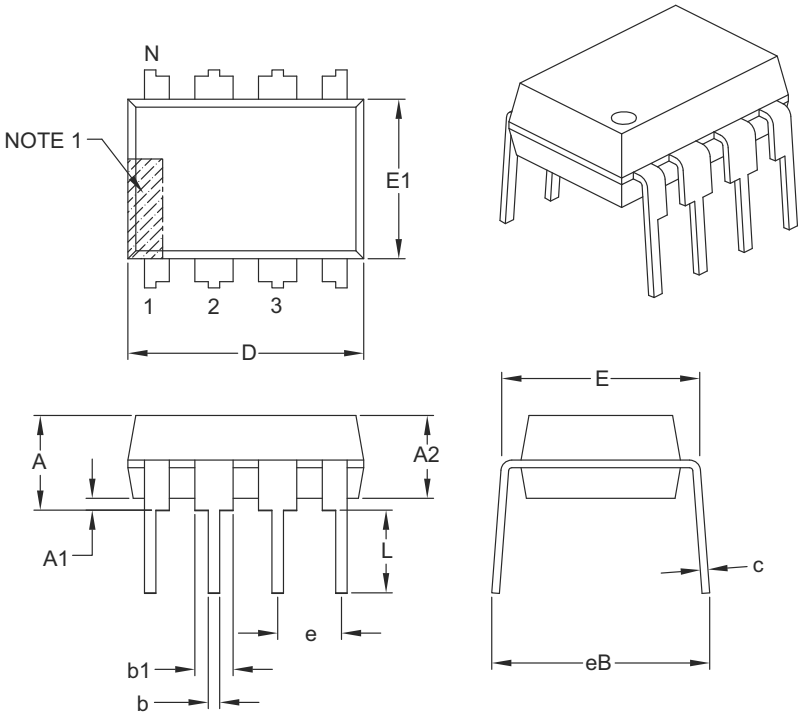
Note: In the event the full Microchip part number cannot be marked on one line, it will be carried over to the next line thus limiting the number of available characters for customer specific information.

***** Standard marking consists of Microchip part number, year code, week code and traceability 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.

10.2 Package Details

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

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



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

Notes:

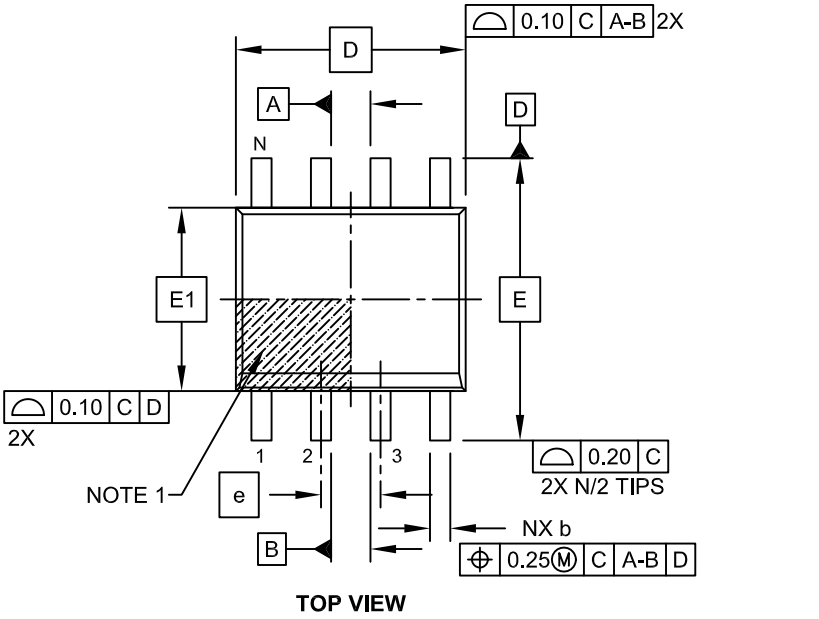
1. Pin 1 visual index feature may vary, but must be located with the hatched area.
2. § Significant Characteristic.
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .010" per side.
4. Dimensioning and tolerancing per ASME Y14.5M.

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

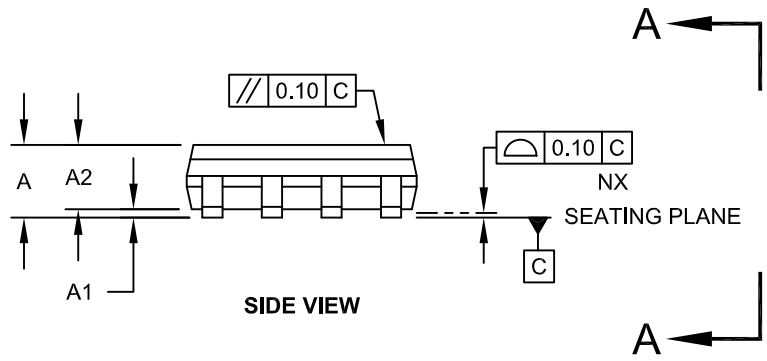
Microchip Technology Drawing C04-018B

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

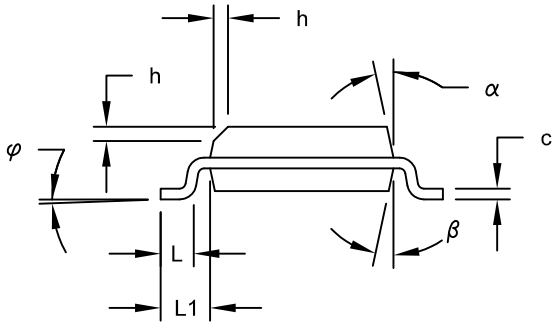
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



TOP VIEW



SIDE VIEW

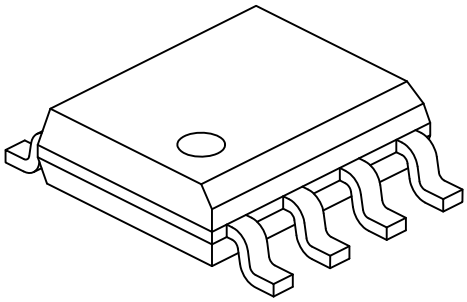


VIEW A-A

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

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

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



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

Notes:

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

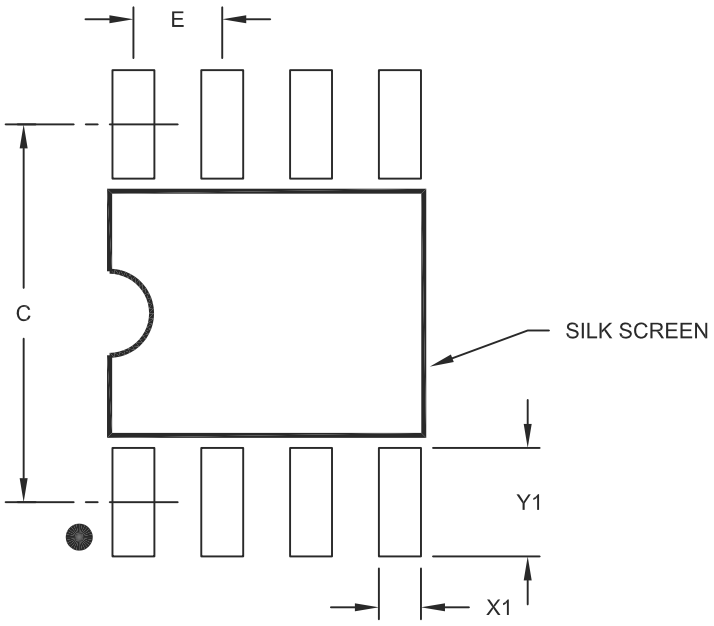
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

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

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

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

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



RECOMMENDED LAND PATTERN

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

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

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

Microchip Technology Drawing No. C04-2057A

APPENDIX A: ADDITIONAL INFORMATION

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

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

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

REVISION HISTORY

Revision D (June 2011)

- Updated the following sections: Development Support, The Microchip Web Site, Reader Response and HCS412 Product Identification System
- Added new section **Appendix A**
- Minor formatting and text changes were incorporated throughout the document

THE MICROCHIP WEB SITE

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

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

CUSTOMER CHANGE NOTIFICATION SERVICE

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

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

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

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

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

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

READER RESPONSE

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

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

TO: Technical Publications Manager Total Pages Sent _____

RE: Reader Response

From: Name _____

Company _____

Address _____

City / State / ZIP / Country _____

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

Application (optional):

Would you like a reply? ___Y ___N

Device: HCS412 Literature Number: DS41099D

Questions:

1. What are the best features of this document?

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

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

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

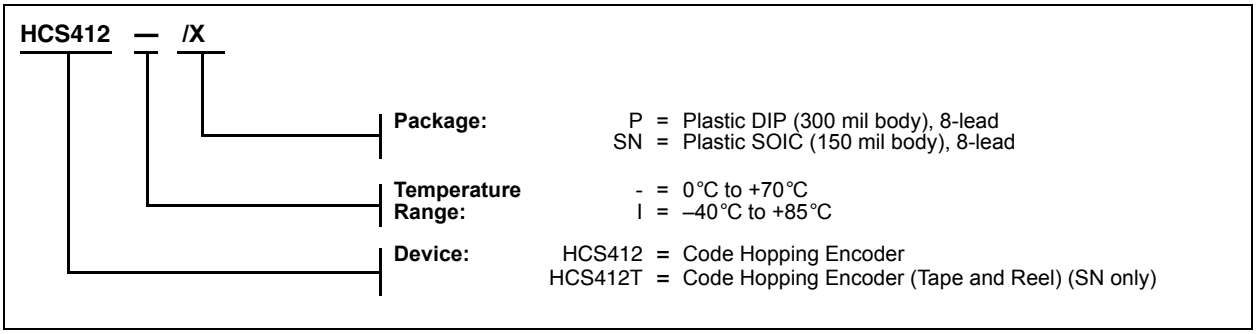
5. What deletions from the document could be made without affecting the overall usefulness?

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

7. How would you improve this document?

HCS412 PRODUCT IDENTIFICATION SYSTEM

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



NOTES:

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

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Trademarks

Printed on recycled paper.

ISBN: 978-1-61341-231-2

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

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

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

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

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

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

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

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

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

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

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

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

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

ASIA/PACIFIC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ASIA/PACIFIC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EUROPE

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

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

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

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

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

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

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

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

05/02/11