Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

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

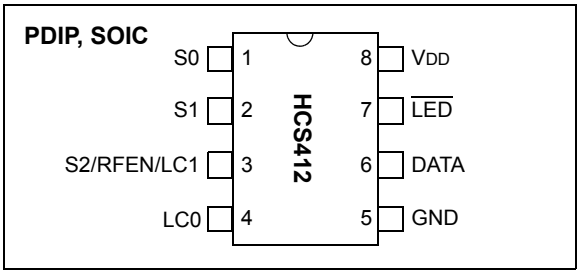
- 2.0V to 6.3V operation
- Three switch inputs: S2, S1, S0 – seven functions
- Battery-less bi-directional transponder capability
- Selectable baud rate and code word blanking
- Automatic code word completion
- Battery low detector
- PWM or Manchester data encoding
- Combined transmitter, transponder 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

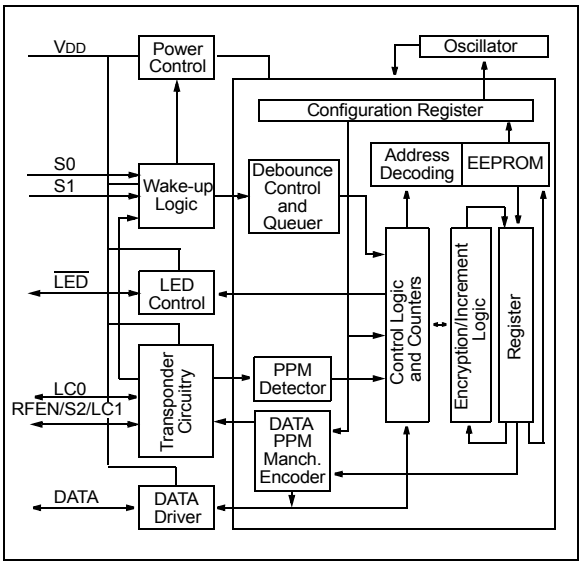
- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks (Home/Office/Hotel)
- Burglar alarm systems
- Proximity access control

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

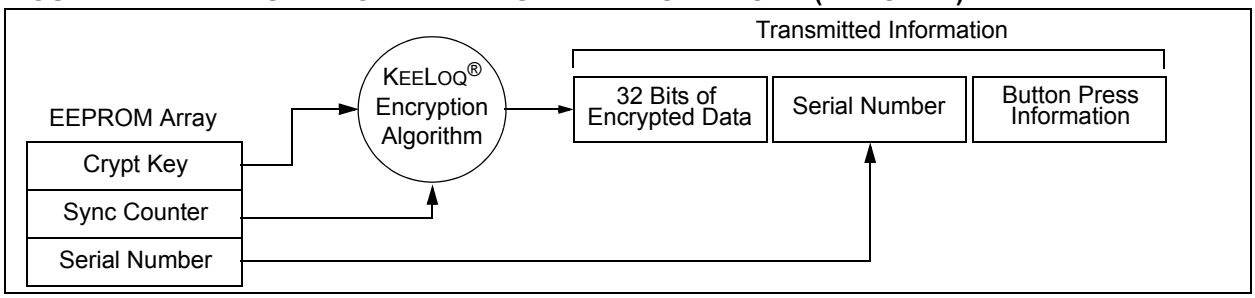
The HCS412, on the other hand, employs the KEELOQ code hopping technology coupled with a transmission length of 69 bits to virtually eliminate the use of code 'grabbing' or code 'scanning'. The high security level of the HCS412 is based on the patented KEELOQ technology. A block cipher based on a block 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

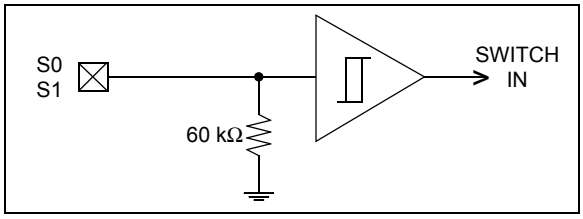


FIGURE 2-2: S2/RFEN/LC1 PIN DIAGRAM

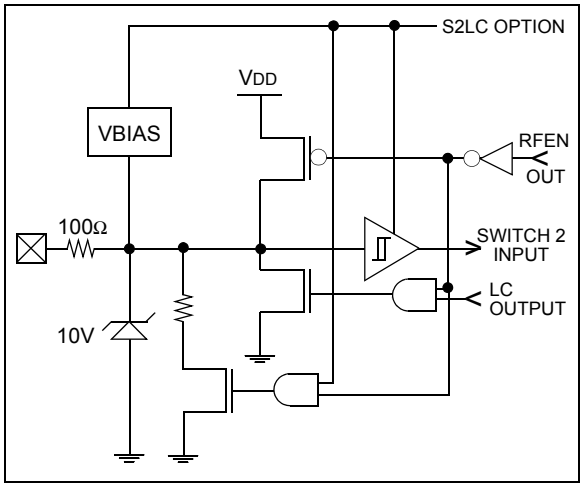


FIGURE 2-3: LC0 PIN DIAGRAM

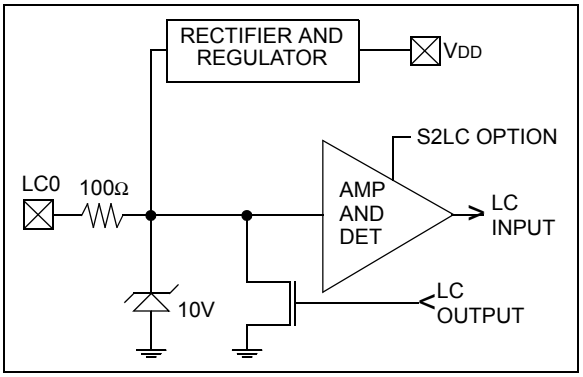


FIGURE 2-4: DATA PIN DIAGRAM

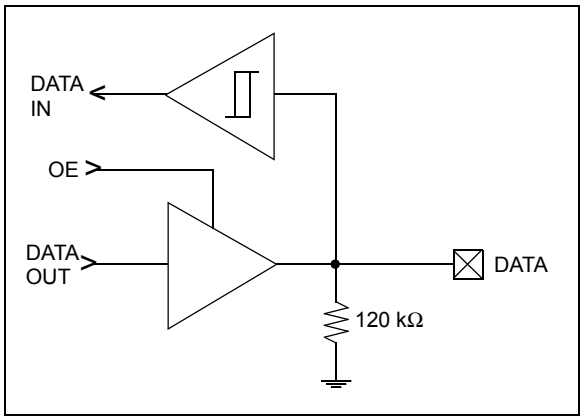


FIGURE 2-5: LED PIN DIAGRAM

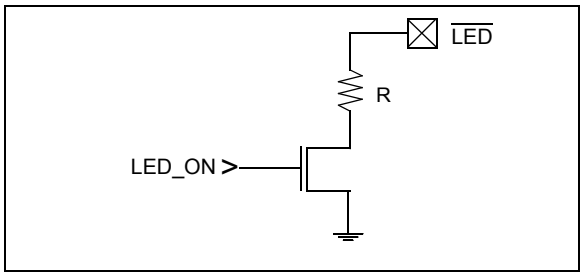
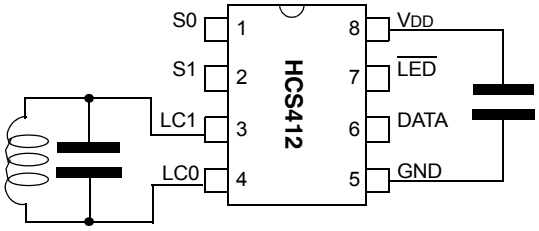
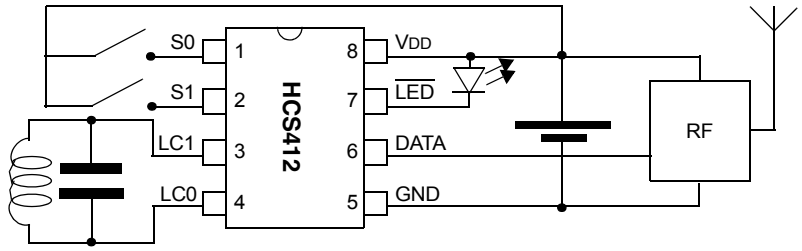


FIGURE 2-6: TYPICAL APPLICATION CIRCUITS

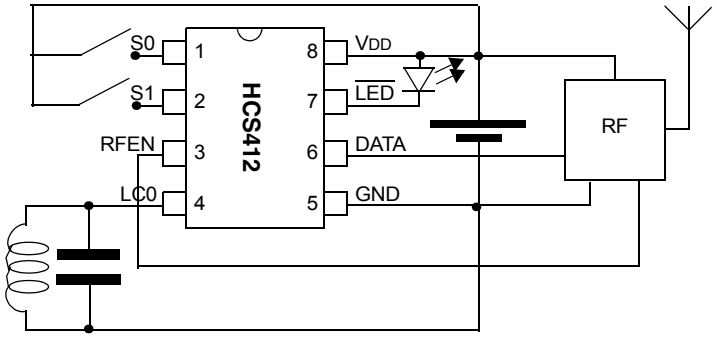
Battery-less Short Range Transponder



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.

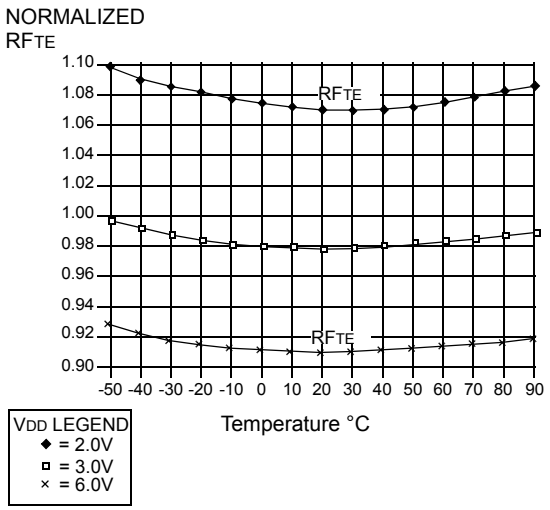
Say the HCS412's oscillator is tuned to be optimal at a 6V supply voltage but the device will operate on a single lithium battery. The resulting oscillator variance over temperature and voltage will not be ±4% but will be more like -7% to -15%.

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

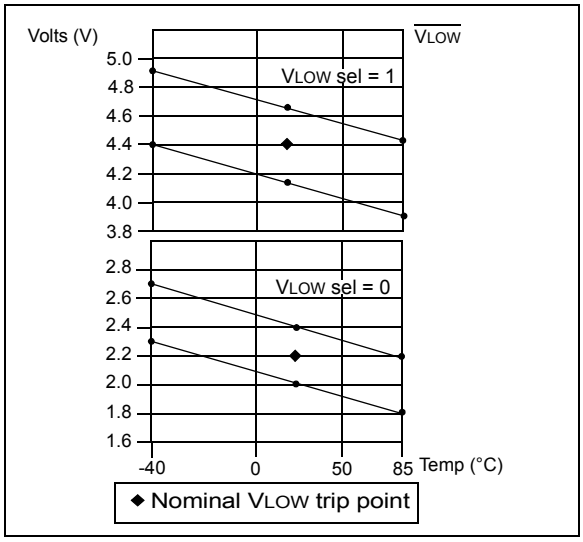


TABLE 2-3: VLOWSEL OPTIONS

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

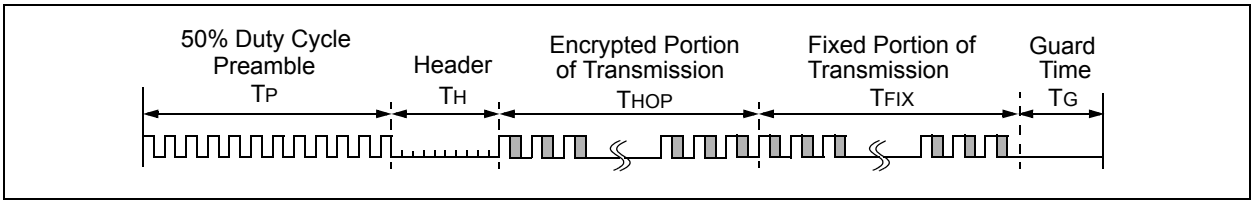
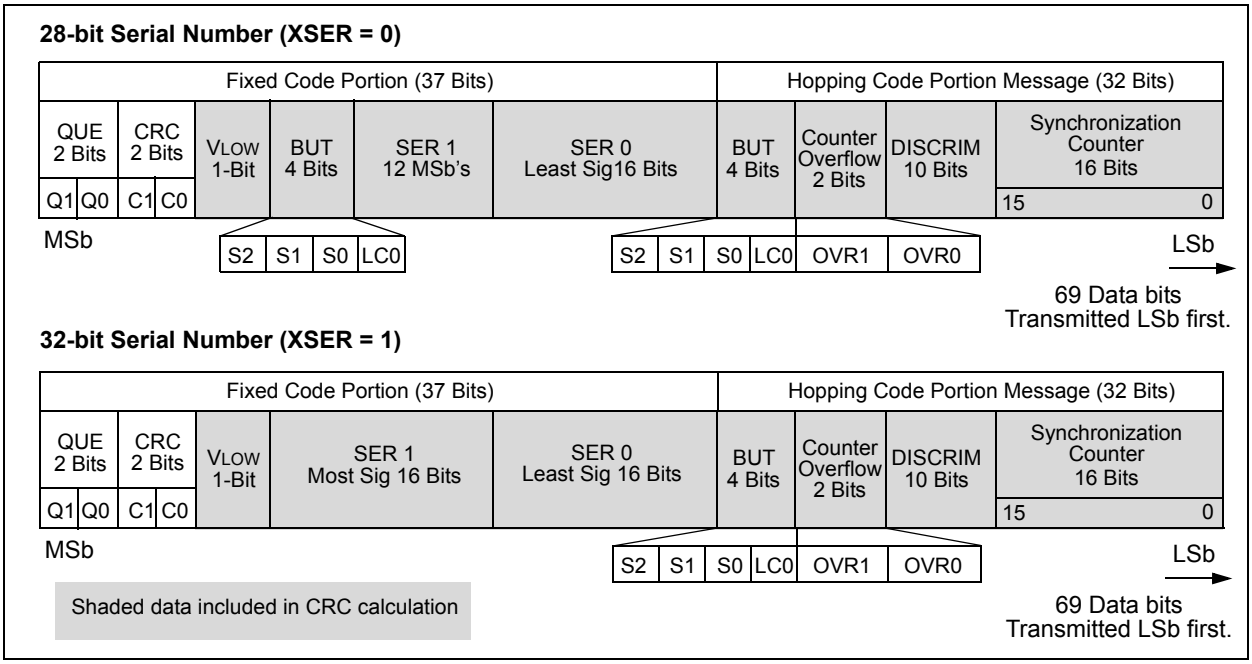


FIGURE 3-2: CODE WORD ORGANIZATION



3.2.1 QUEUE COUNTER (QUE)

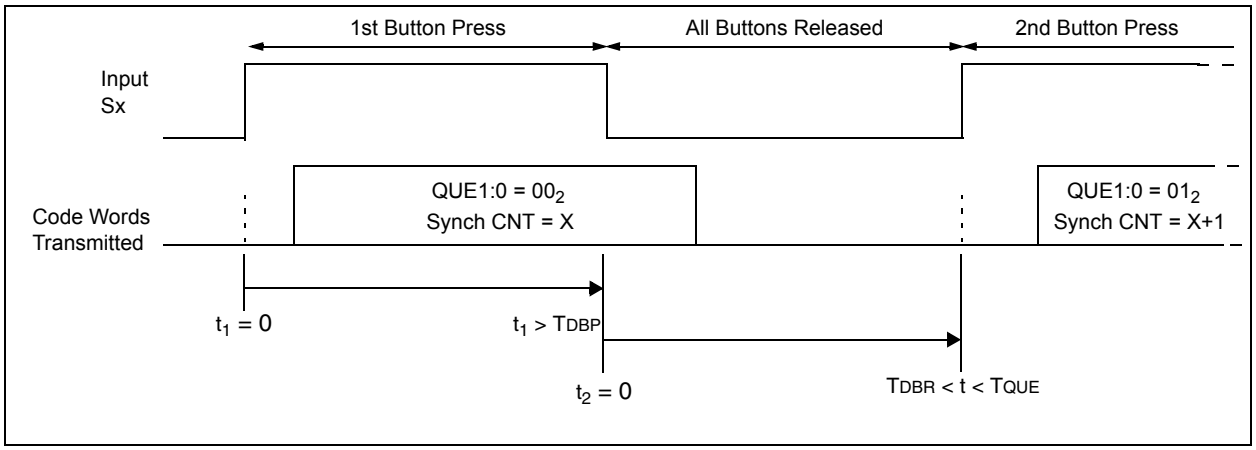
The QUE counter can be used to request secondary decoder functions using only a single transmitter button. Typically a decoder must keep track of incoming transmissions to determine when a double button press occurs, perhaps an unlock all doors request. The QUE counter removes this burden from the decoder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

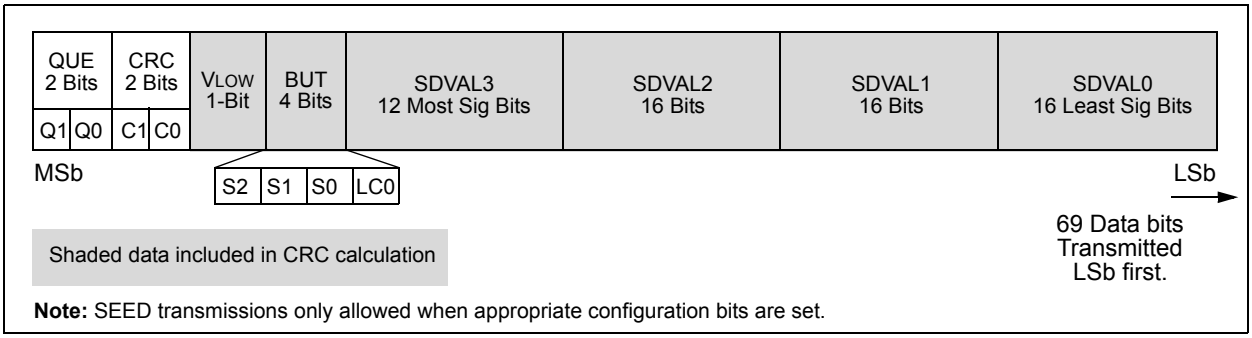
The seed code word also consists of 69 bits, but the 32 bits of code hopping data and the 28 bits of fixed data are replaced by a 60-bit seed value that was stored during production (Figure 3-4). Instead of using the normal key generation inputs to create the crypt key, this seed value is used.

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

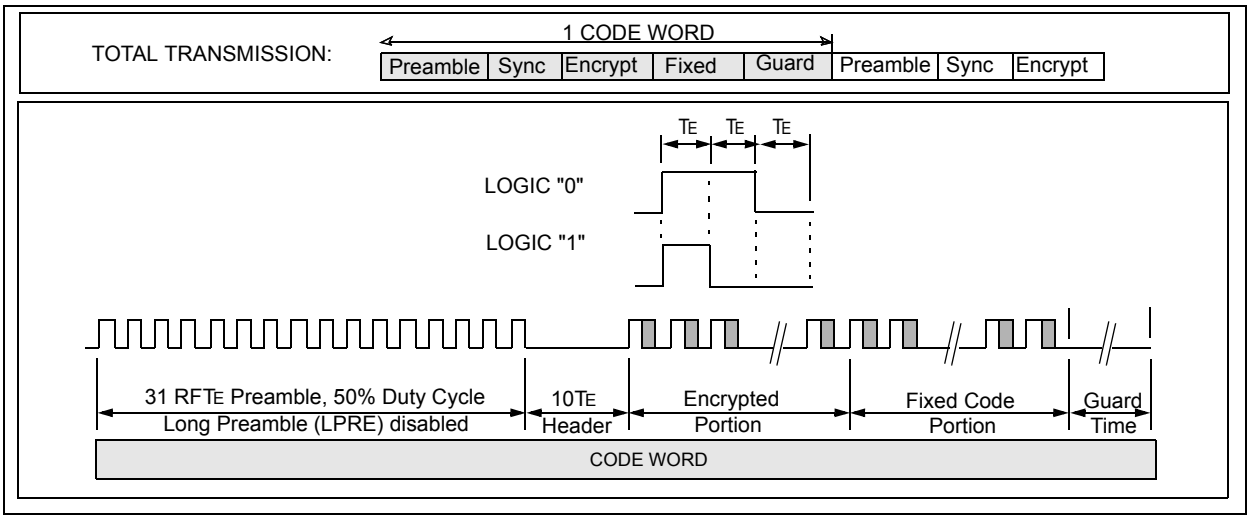
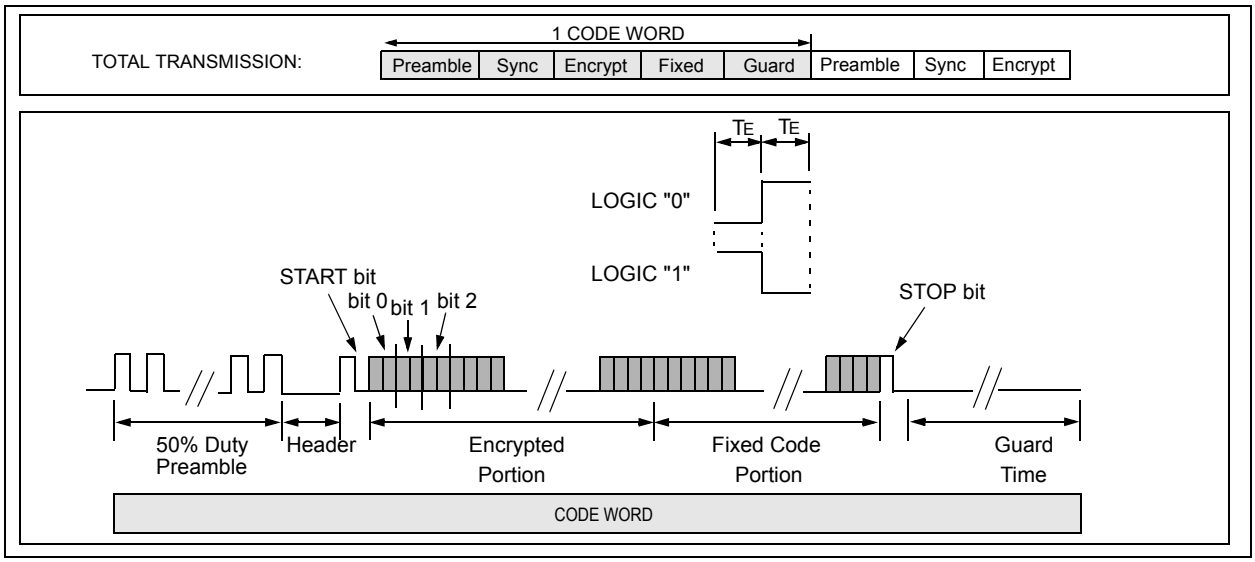


FIGURE 3-6: MANCHESTER TRANSMISSION FORMAT—MOD = 1



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

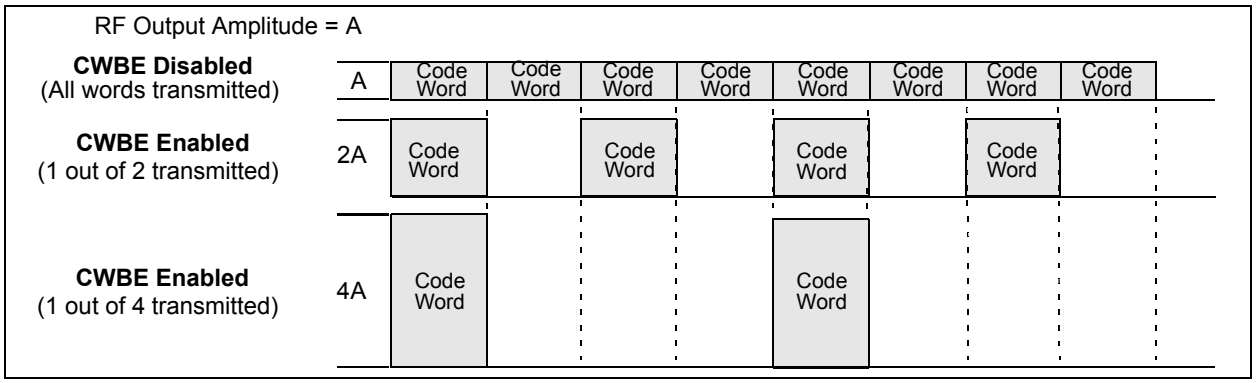


TABLE 3-7: CODE WORD BLANKING ENABLE (CWBE)

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

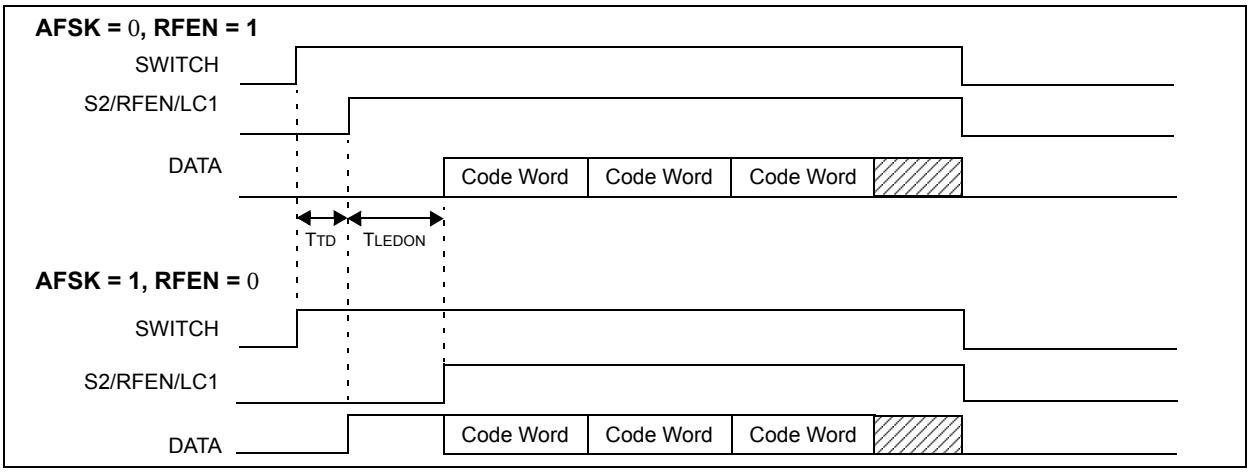


FIGURE 3-9: LED OPERATION

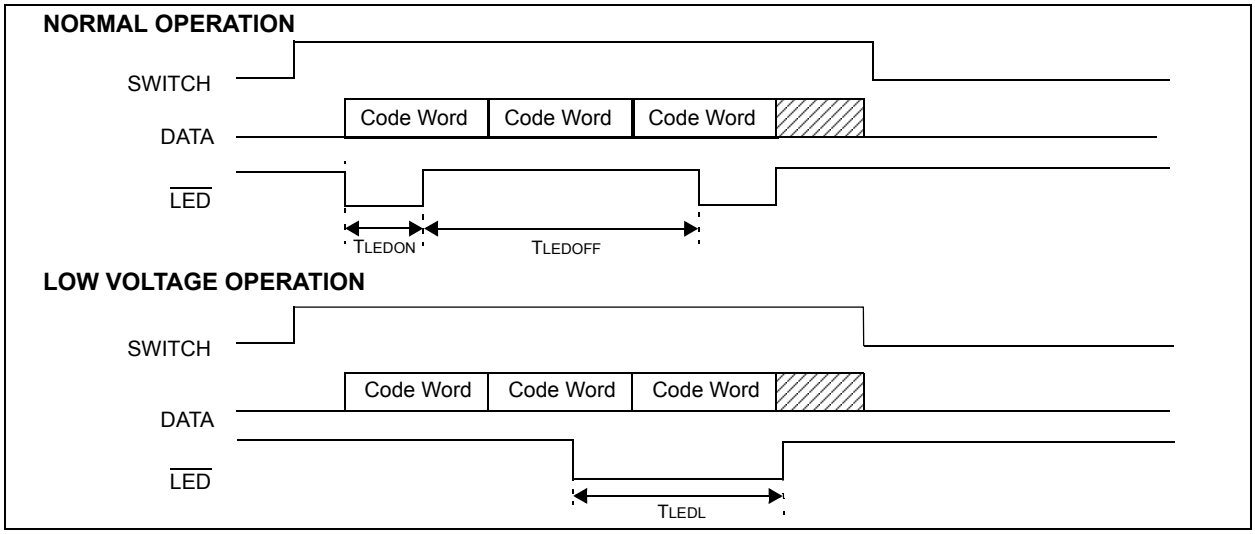
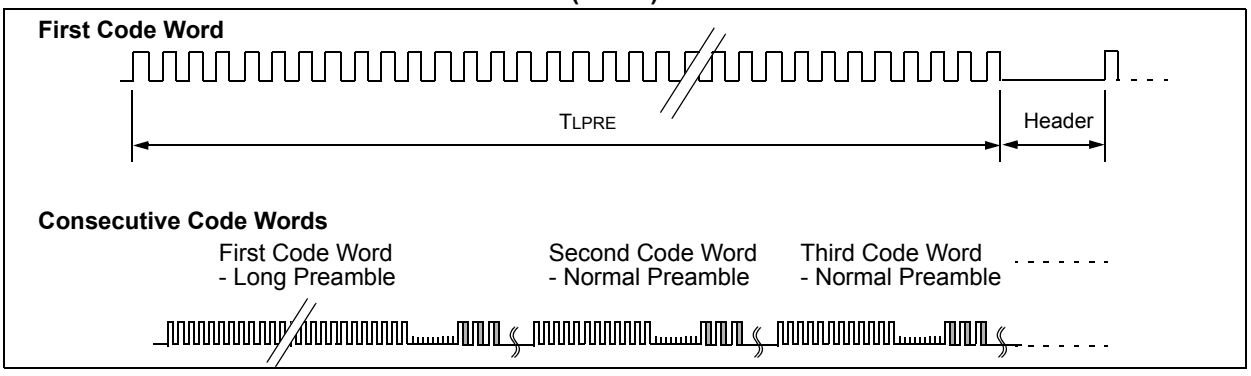


FIGURE 3-10: LONG PREAMBLE ENABLED (LPRE)



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

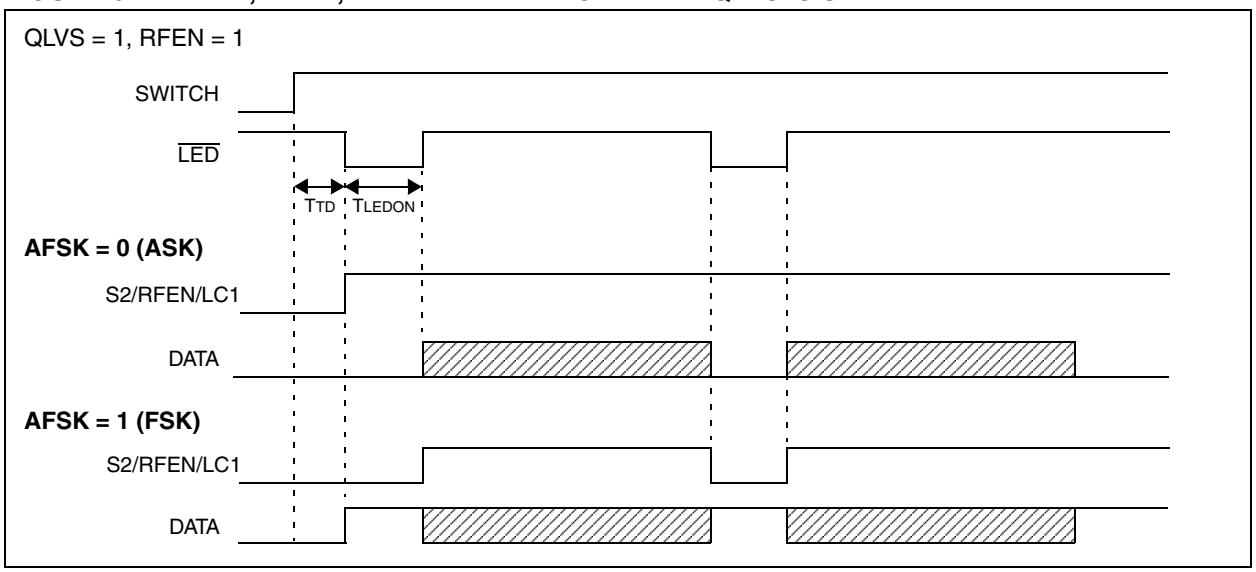


FIGURE 3-12: SEED DISABLE WAVEFORM

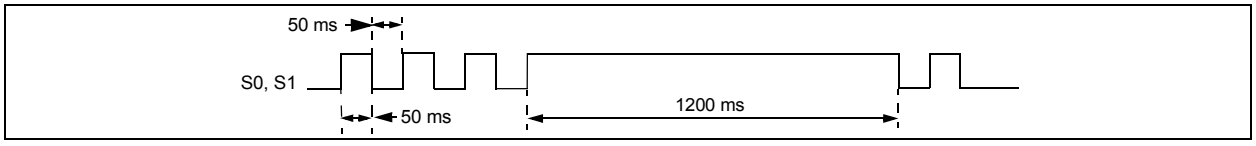


TABLE 3-9: ENCODER TIMING SPECIFICATIONS

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 TPU, 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 LFTE'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 LFTE 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 LFTE.

HCS412 PPM data responses are preceded by a 1 LFTE 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, LFTE. The Low Frequency Baud Rate Select option, LFBSL, sets LFTE to either 100 µs or 200 µs (Table 4-1).

The response on the DATA pin uses the Encoder mode's RF Timing Element (RFTE) 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	LFTE
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 TE and expected TE when receiving will vary.

Communication reliability with the token may be improved by calculating the HCS412's TE 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 TE calculation method would be to time an 8 TE sequence, then divide the value down to determine the single TE value. An 8 TE 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 TE 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 TE 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 TE.

FIGURE 4-1: FIELD ACKNOWLEDGE SEQUENCE

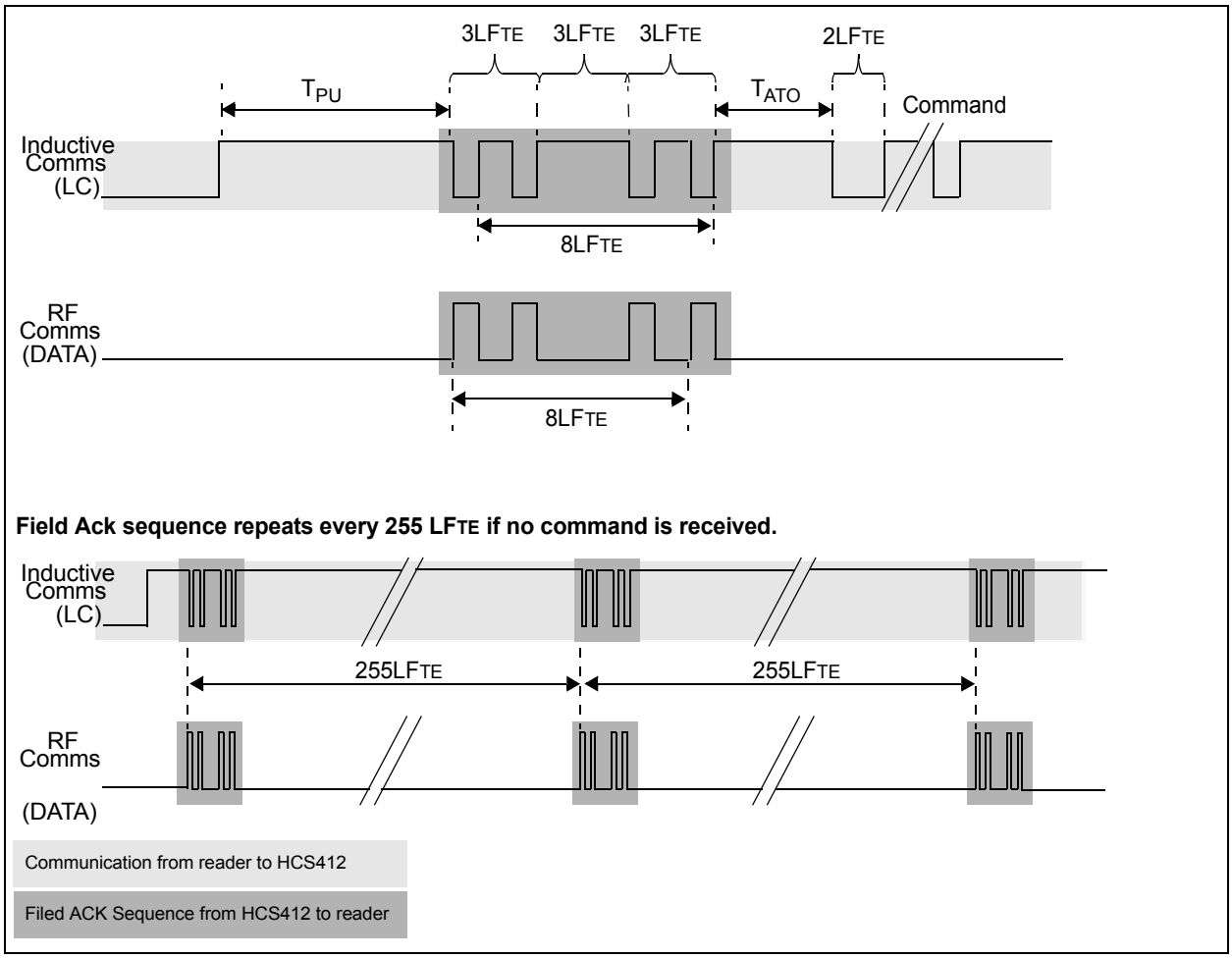
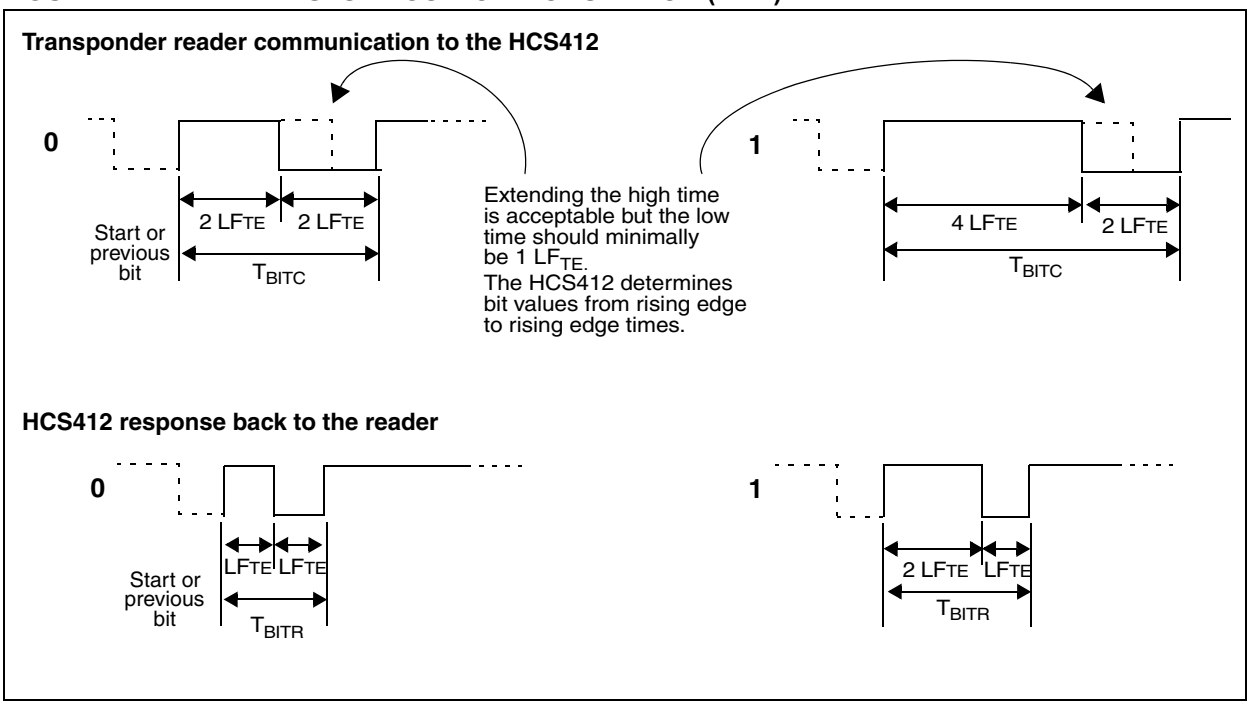


FIGURE 4-2: LC PIN PULSE POSITION MODULATION (PPM)



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).

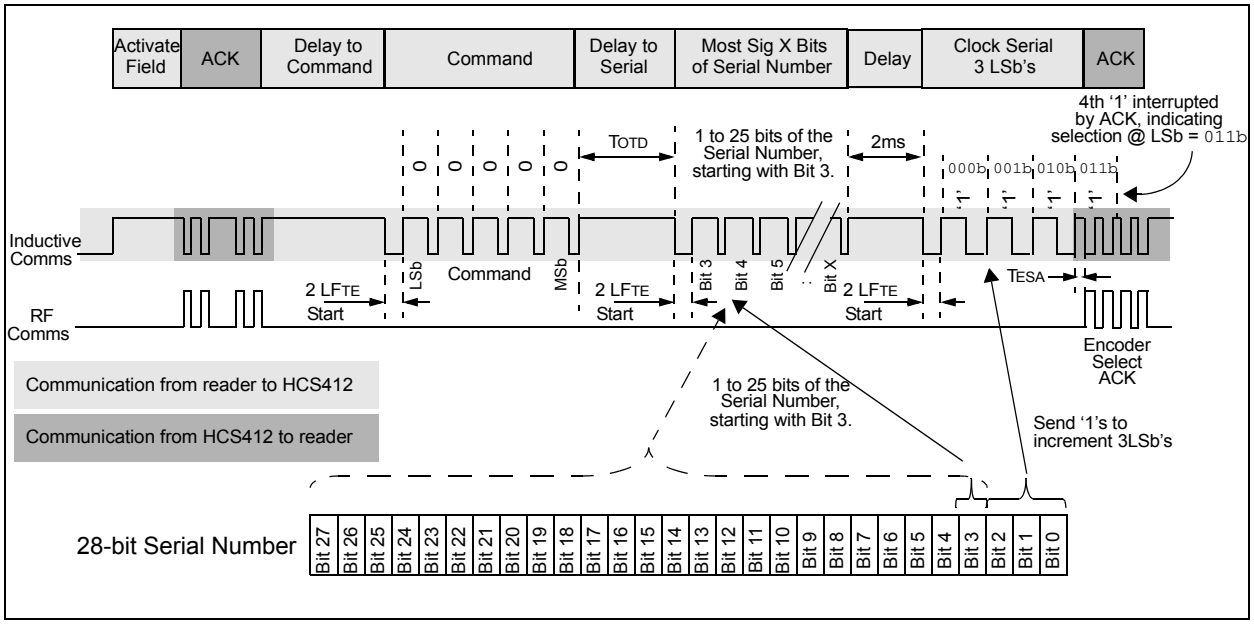
Clocking out '1's then increments the 3 LSb's, the first '1' setting the bits to `000b`. When the value matches the 3 LSb's of a token, the token responds with an Encoder Select Acknowledge. The reader must halt clocking out further '1's or risk selecting multiple tokens. Any remaining tokens in the 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).

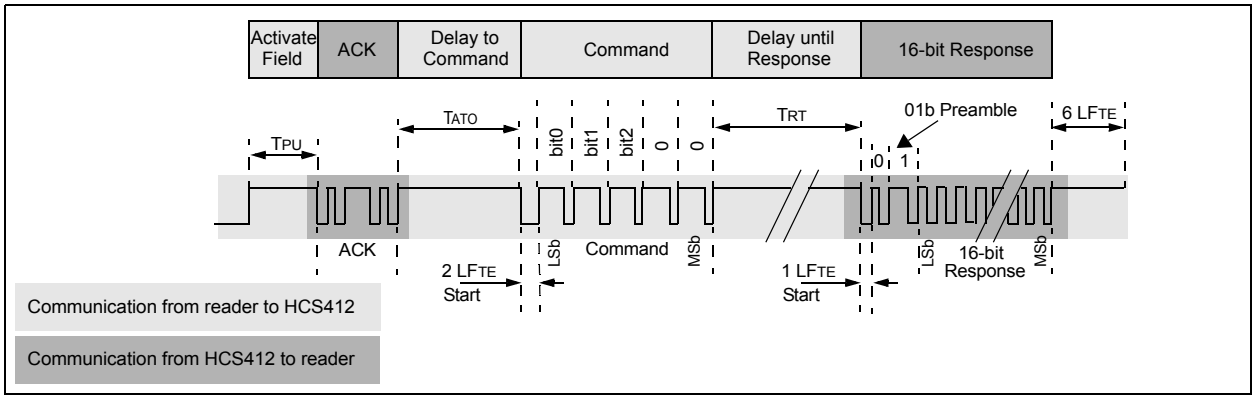
The following locations are available to read:

- 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

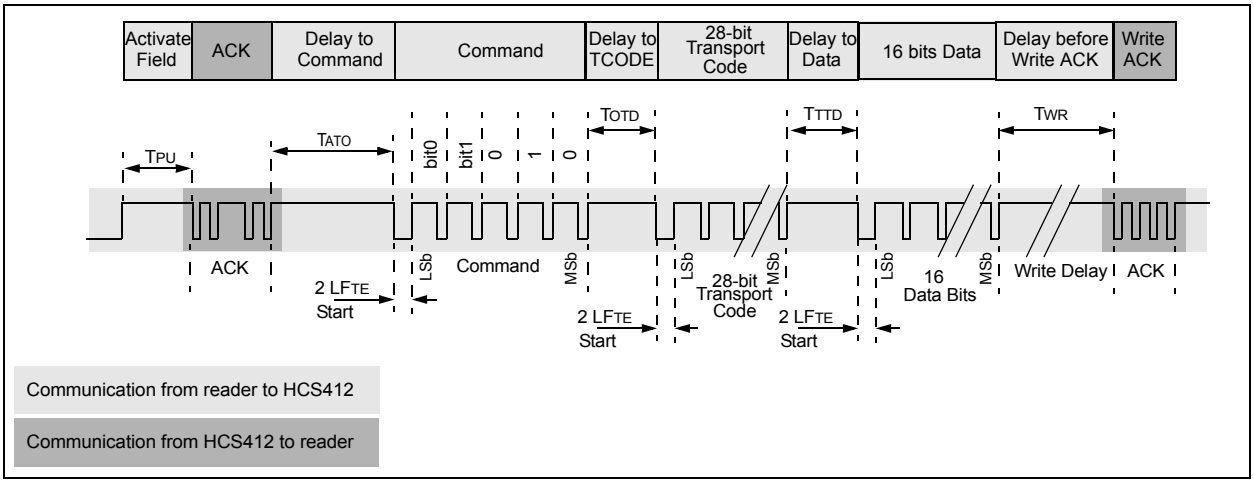
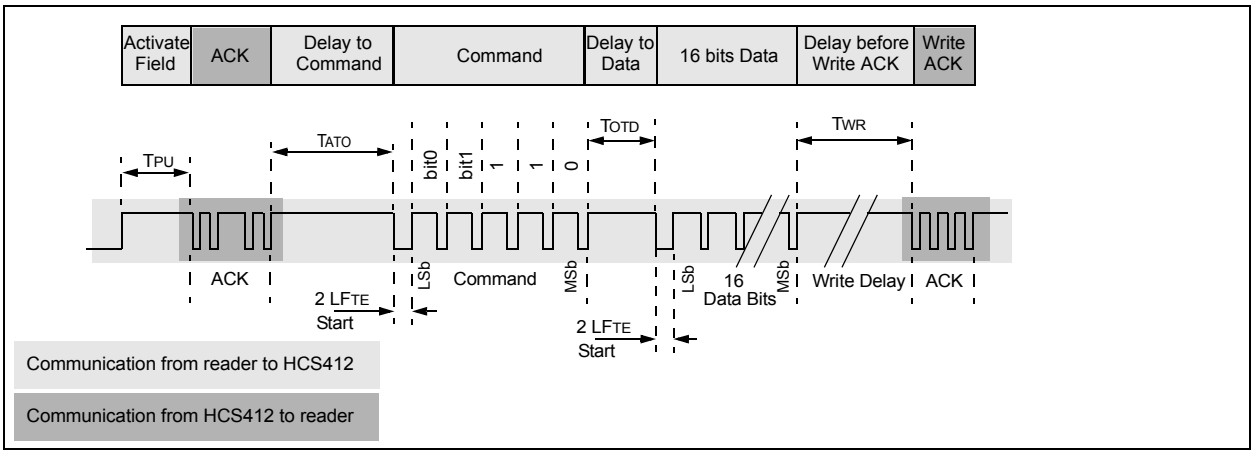


FIGURE 4-6: WRITE TO USER AREA

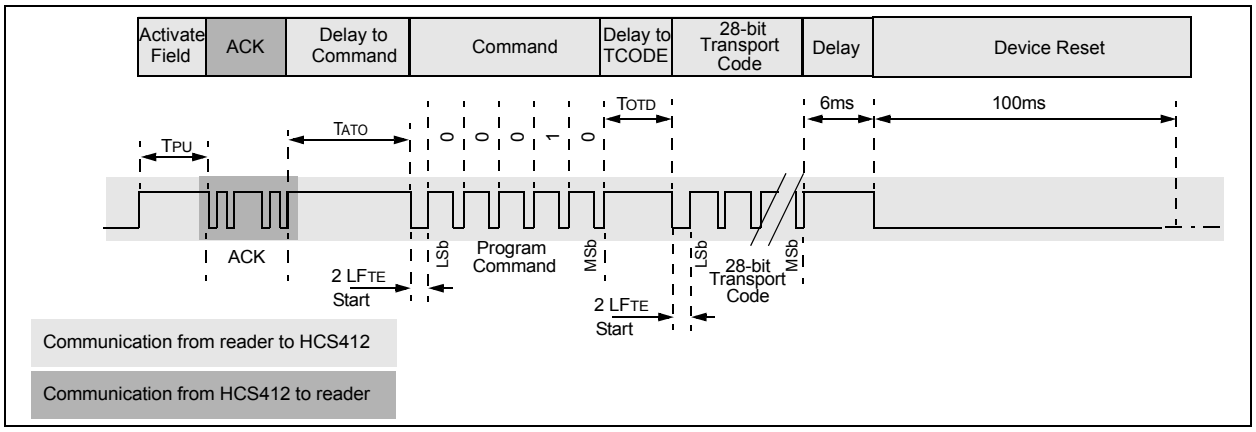


4.3.4 BULK ERASE

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

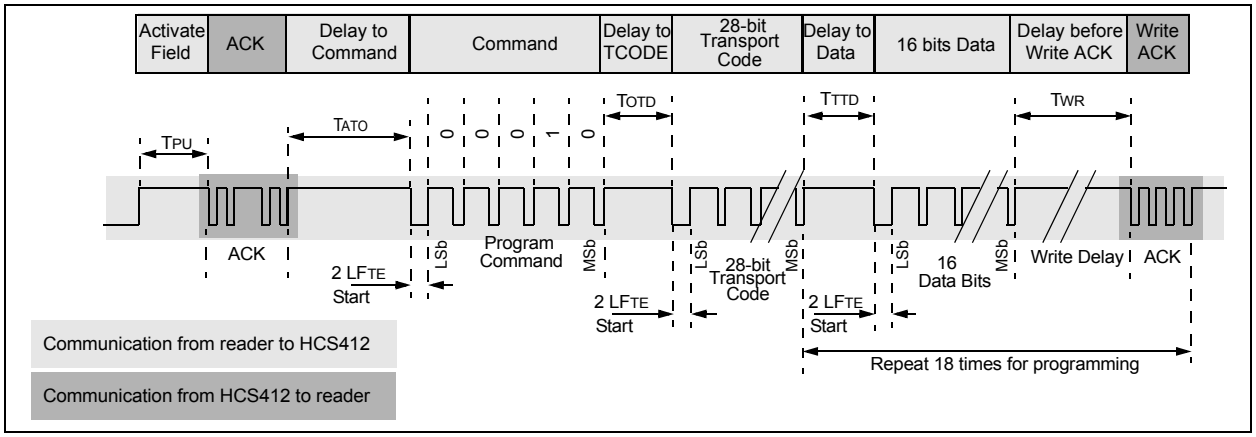


FIGURE 4-9: PROGRAM SEQUENCE - CONSECUTIVE WORDS

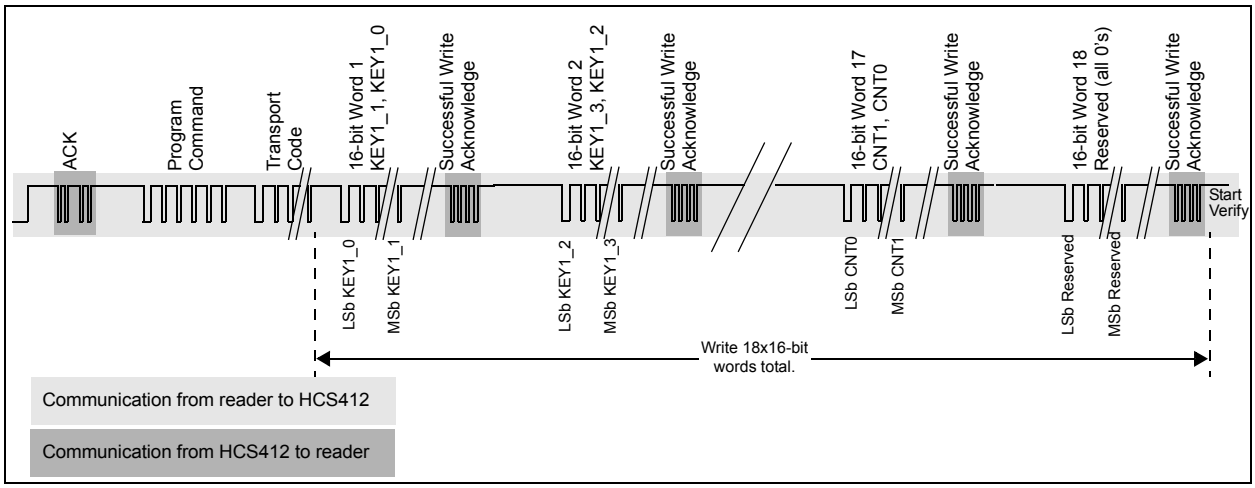
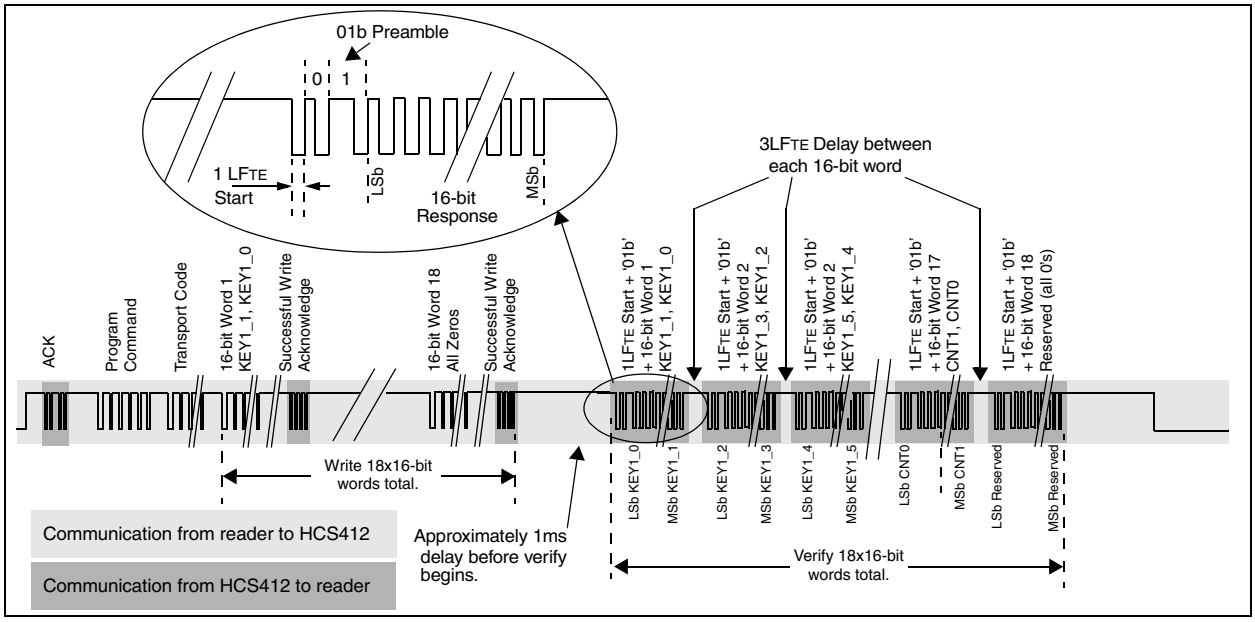


FIGURE 4-10: PROGRAMMING - VERIFICATION



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