HCS412

KEELOQ® Code Hopping Encoder and Transponder

FEATURES

Security

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

Operating

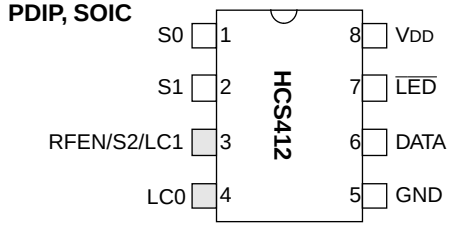
- 2.0V to 6.6V operation, 13V encoder only operation
- Three switch inputs [S2, S1, S0]—seven functions
- Batteryless bi-directional transponder
- Selectable baud rate and code word blanking
- Automatic code word completion
- Battery low signal transmitted
- Nonvolatile synchronization
- PWM or Manchester RF encoding
- Combined transmitter, transponder operation
- Anti-collision of multiple transponders
- Passive proximity activation
- Device protected against reverse battery
- Intelligent damping for high Q LC-circuits

Typical Applications

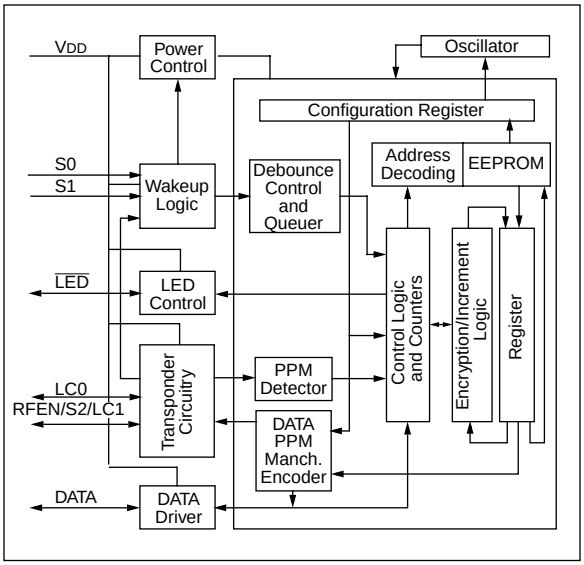
- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks (Home/Office/Hotel)
- Burglar alarm systems
- Proximity access control

PACKAGE TYPES

PDIP, SOIC



BLOCK DIAGRAM



Other

- 37-bit nonencrypted part contains 28/32-bit serial number, 4/0-bit function code, 1-bit battery low, 2-bit CRC, 2-bit queue
- Simple programming interface
- On-chip tunable RC oscillator (±10%)
- On-chip EEPROM
- 64-bit user EEPROM in transponder mode
- Battery-low LED indication
- SQTP serialization quick-time programming
- 8-pin PDIP/SOIC and die
- ASK and FSK PLL control
- RF Enable output
- Built in amplifier on LC inputs

KEELOQ is a registered trademark of Microchip Technology, Inc.
Microchip's Secure Data Products are covered by some or all of the following patents:
Code hopping encoder patents issued in Europe, U.S.A., and R.S.A. — U.S.A.: 5,517,187; Europe: 0459781; R.S.A.: ZA93/4726
Secure learning patents issued in the U.S.A. and R.S.A. — U.S.A.: 5,686,904; R.S.A.: 95/5429

DESCRIPTION

The HCS412 is a code hopping transponder device designed for secure entry systems. The HCS412 utilizes the patented KEELOQ® code hopping system and bi-directional challenge-and-response for logical and physical access control. High security learning mechanisms make this a turnkey solution when used with the KEELOQ decoders. The encoder keys and synchronization information are stored in protected on-chip EEPROM.

A low cost batteryless transponder can be implemented with the addition of an inductor and two capacitors.

A single HCS412 can be used as an encoder for Remote Keyless Entry (RKE) and a transponder for immobilization in the same circuit and thereby dramatically reducing the cost of hybrid transmitter/transponder circuits.

1.0 SYSTEM OVERVIEW

1.1 Key Terms

- Anticollision – Allows multiple transponders to be in the files simultaneously and be verified individually.
- CH Mode – Code Hopping Mode. The HCS412 transmits a 69-bit transmission each time it is activated, with at least 32-bits changing each time the encoder is activated.
- Encoder Key – A unique 64-bit key generated and programmed into the encoder during the manufacturing process. The encoder key controls the encryption algorithm and is stored in EEPROM on the encoder device.
- IFF – Identify friend or foe is a means of validating a token. A decoder sends a random challenge to the token and checks that the response of the token is a valid response.
- KEELOQ Encryption Algorithm – The high security level of the HCS412 is based on the patented KEELOQ technology. A block cipher encryption algorithm based on a block length of 32 bits and a key length of 64 bits is used. The algorithm obscures the information in such a way that even if the unencrypted/challenge information differs by only one bit from the information in the previous transmission/challenge, the next coded transmission/response will be totally different. Statistically, if only one bit in the 32-bit string of information changes, approximately 50 percent of the coded transmission will change.
- Learn – The KEELOQ product family facilitates several learning strategies to be implemented on the decoder. The following are examples of what can be done.

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

  Secure Learn – The transmitter is activated through a special button combination to transmit a stored 60-bit value (random seed) that can be used for key generation or be part of the key. Transmission of the random seed can be disabled after learning is completed.
- Manufacturer's Code – A 64-bit word, unique to each manufacturer, used to produce a unique encoder key in each transmitter (encoder).
- Passive Proximity Activation – When the HCS412 is brought into in a magnetic field without a command given by the base station, the HCS412 can be programmed to give an RF transmission.
- Transport Code – A 28-bit transport code needs to be given before the HCS412 can be inductively programmed. This prevents accidental programming of the HCS412.

1.2 KEELOQ Code Hopping Encoders

When the HCS412 is used as a code hopping encoder device, it is ideally suited to keyless entry systems, primarily for vehicles and home garage door openers. It is meant to be a cost-effective, yet secure solution to such systems. The encoder portion of a keyless entry system is meant to be carried by the user and operated to gain access to a vehicle or restricted area.

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

The HCS412 employs the KEELOQ code hopping technology and an encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 69 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

The HCS412 has a small EEPROM array which must be loaded with several parameters before use. The most important of these values are:

- A 28/32-bit serial number which is meant to be unique for every encoder
- 60-bit seed value
- A 64-bit encoder key that is generated at the time of production
- A 16-bit synchronization counter value
- Configuration options

The 16-bit synchronization counter value is the basis for the transmitted code changing for each transmission, and is updated each time a button is pressed. Because of the complexity of the code hopping encryption algorithm, a change in one bit of the synchronization counter value will result in a large change in the actual transmitted code.

Once the encoder detects that a button has been pressed, the encoder reads the button and updates the synchronization counter. The synchronization counter value, the function bits, and the discrimination value are then combined with the encoder key in the encryption algorithm, and the output is 32 bits of encrypted information (Figure 1-1). The code hopping portion provides up to four billion changing code combinations. This data will change with every button press, hence, it is referred to as the code hopping portion of the code word.

The 32-bit code hopping portion is combined with the button information and the serial number to form the code word transmitted to the receiver. The code word format is explained in detail in Section 2.2.

1.3 KEELOQ IFF

The HCS412 can be used as an IFF transponder for verification of a token. In IFF mode the HCS412 is ideally suited for authentication of a key before disarming a vehicle immobilizer. Once the key has been inserted in the car's ignition the decoder would inductively poll the key validating it before disarming the immobilizer.

IFF validation of the token involves a random challenge being sent by a decoder to a token. The token then generates a response to the challenge and sends this response to the decoder (Figure 1-2). The decoder calculates an expected response using the same challenge. The expected response is compared to the response received from the token. If the responses match, the token is identified as a valid token and the decoder can take appropriate action.

The HCS412 can do a 32-bit IFF. The HCS412 has two encryption algorithms that can be used to generate a response to a challenge. In addition there are up to two encoder keys that can be used by the HCS412. Typically each HCS412 will be programmed with a unique encoder key(s).

In IFF mode, the HCS412 will wait for a command from the base station and respond to the command. The command can either request a read/write from user EEPROM or an IFF challenge response. A given 32-bit challenge will produce a unique 32-bit response, based on the IFF key and IFF algorithm used.

FIGURE 1-1: BASIC OPERATION OF A CODE HOPPING TRANSMITTER (ENCODER)

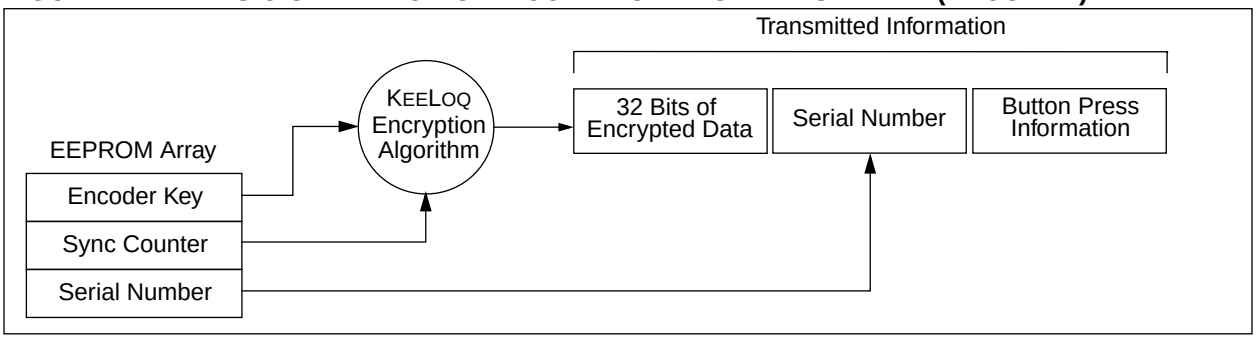
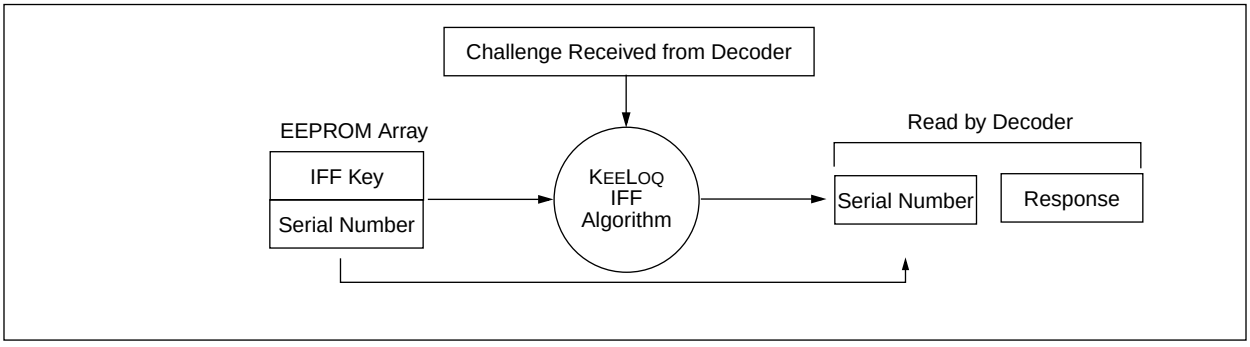


FIGURE 1-2: BASIC OPERATION OF AN IFF TOKEN



2.0 DEVICE OPERATION

The HCS412 can either operate as a normal code hopping transmitter with one or two IFF keys (Figure 2-1) or as purely an IFF token with two IFF keys (Figure 2-2 and Figure 2-3). When used as a code hopping transmitter the HCS412 only needs the addition of buttons and RF circuitry for use as a transmitter. Adding the transponder function to the transmitter requires the addition of an inductor and two capacitors as shown in Figure 2-1 and Figure 2-2. A description of each pin is given in Table 2-1. Table 2-2 shows the function codes for using the HCS412.

Figure 2-4 shows how to use the HCS412 with a 12V battery as a code hopping transmitter. The circuit uses the internal regulator, normally used for charging a capacitor/battery in LC mode, to generate a 6V supply for the HCS412.

FIGURE 2-1: COMBINED TRANSMITTER/ TRANSPONDER CIRCUIT

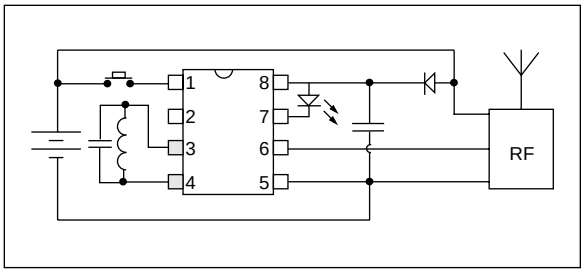


FIGURE 2-2: TRANSPONDER CIRCUIT

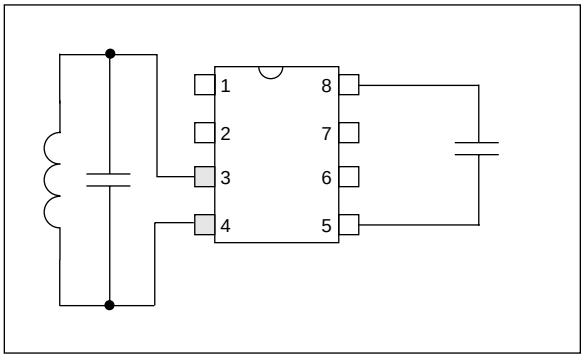


FIGURE 2-3: 2-WIRE, 1 OR 2-KEY IFF TOKEN

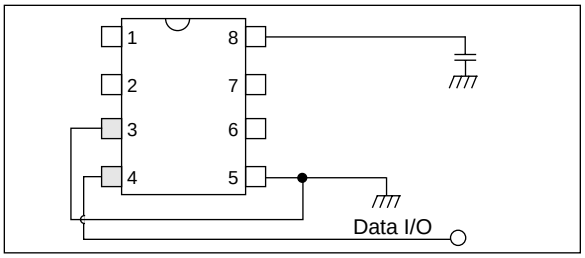


FIGURE 2-4: HCS412 ENCODER WITH 12V BATTERY

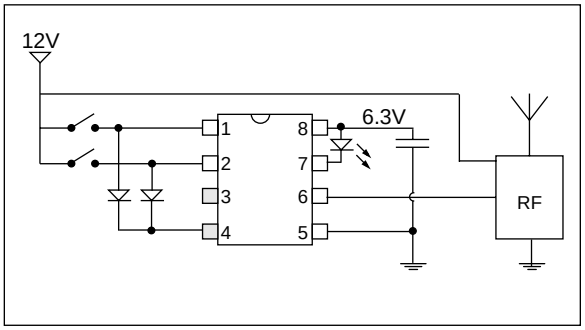
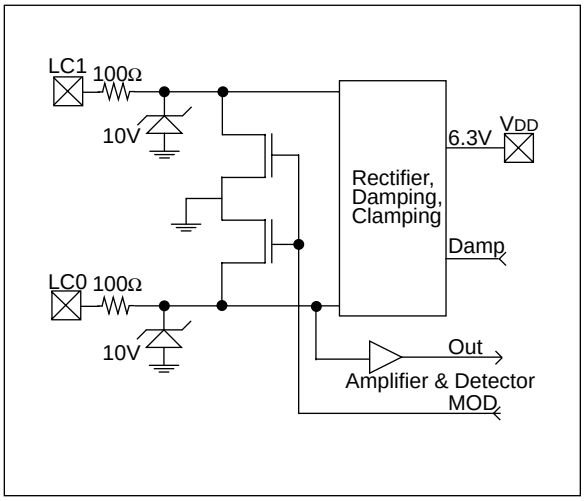


FIGURE 2-5: LC PIN BLOCK DIAGRAM



2.1 Pinout Description

The HCS412 has the same footprint as all of the other devices in the KEELOQ family, except for the two pins that are reserved for transponder operations.

- S[0:1] – are inputs with Schmitt Trigger detectors and an internal 60kΩ (nominal) pull-down resistors.
- S2/RFEN/LC1 – is an input with a Schmitt Trigger detector and internal pulldown. It is also an RF Enable line when configured as an output, and can be used as a transponder interface pin.
- LC0 is the second transponder interface pin to be connected to an LC circuit for inductive communication. LC0 is connected to an automatic gain controlled amplifier and a detector for data input. Data output is achieved by clamping LC0 and LC1 to GND through two NMOS transistors. These pins are also connected to a rectifier and a regulator, providing power to the rest of the logic and for charging an external power source (Battery/ Capacitor) through VDD.

The input impedance of the LC pins is a function of input voltage. At low voltages, the input impedance is in the order of mega-ohms. **When laying out a PC board, care should be taken to ensure that there is no cross coupling between the LC pins and other traces on the board.**

TABLE 2-1: PINOUT DESCRIPTION

Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2/LC1/RFEN	3	Switch input 2, RF Enable output, clock for programming and a transponder interface pin
LC0	4	Transponder interface pin
VSS	5	Ground reference connection
DATA	6	RF transmission output pin, data pin for programming mode
$\overline{\text{LED}}$	7	$\overline{\text{LED}}$ output pin
VDD	8	Positive supply voltage connection

TABLE 2-2: FUNCTION CODES

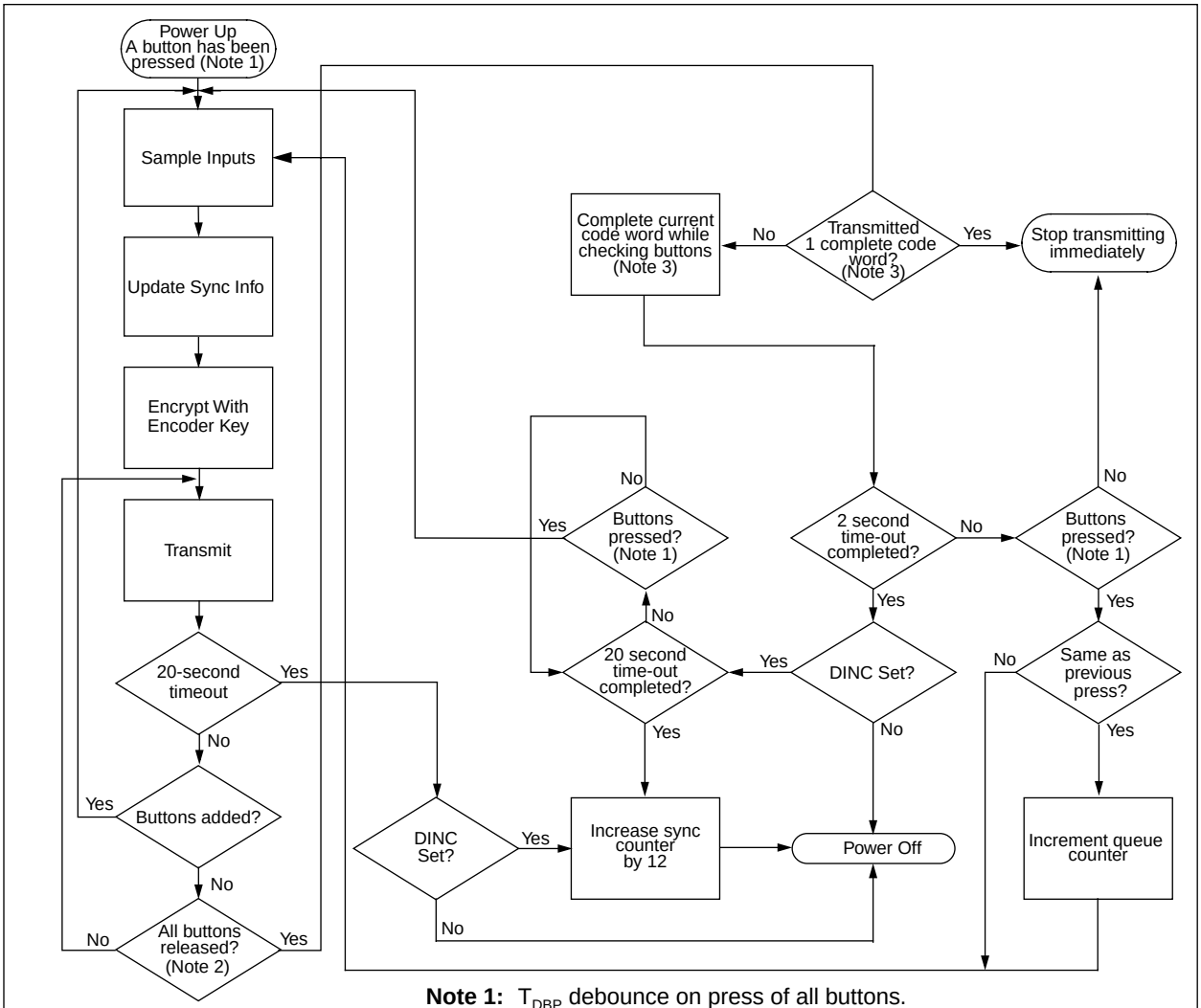
	LC0	S2	S1	S0	Comments
1	0	0	0	1	Normal Code Hopping transmission
2	0	0	1	0	Normal Code Hopping transmission
3	0	0	1	1	Delayed seed transmission after TDSD if allowed by SEED and TMPSD/ Normal Code Hopping transmission
4	0	1	0	0	Normal Code Hopping transmission
5	0	1	0	1	Normal Code Hopping transmission
6	0	1	1	0	Normal Code Hopping transmission
7	0	1	1	1	Immediate seed transmission if allowed by SEED and TMPSD/Normal Code Hopping transmission
8	1	0	0	0	Transponder mode/proximity activated transmission when configured

2.2 Code Hopping Mode (CH Mode)

The HCS412 wakes up upon detecting a switch closure and then delays approximately T_{DBP} for switch debounce (Figure 2-6). The synchronization counter value, fixed information, and switch information are encrypted to form the code hopping portion. The encrypted or code hopping portion of the transmission changes every time a button is pressed, even if the same button is pushed again. Keeping a button pressed for a long time results in the same code word being transmitted until the button is released or time-out occurs. A code that has been transmitted will not occur again for more than 64K transmissions. Overflow information programmed into the encoder can be used by the decoder to extend the number of unique transmissions to more than 192k.

If, during the transmit process, it is detected that a new button(s) has been added, a reset will immediately be forced and the code word will not be completed. Please note that buttons removed will not have any effect on the code word unless no buttons remain pressed in which case the current code word will be completed and the power down will occur. If, after a button combination is pressed, and the same button combination is pressed again within two seconds of the first press, the current transmission will be aborted and a new transmission will start with the queue counter (QUE) incremented.

FIGURE 2-6: CODE HOPPING ENCODER OPERATION



Note 1: T_{DBP} debounce on press of all buttons.

2: T_{DBR} debounce on release of all buttons

3: Completes a minimum of 4 code words if MTX4 is set.

2.2.1 TRANSMISSION DATA FORMAT

The HCS412 transmission (CH Mode) is made up of several parts (Figure 2-9 and Figure 2-10). Each transmission is begun with a preamble and a header, followed by the encrypted and then the fixed data. The actual data is 69 bits which consists of 32 bits of encrypted data and 37 bits of fixed data. Each transmission is followed by a guard period before another transmission can begin. Refer to Table 5-4 and Table 5-5 for transmission timing specifications. The combined encrypted and nonencrypted sections increase the number of combinations to 1.47×10^{20}.

The HCS412 transmits a 69-bit code word when a button is pressed. The 69-bit word is constructed from a Fixed Code portion and Code Hopping portion (Figure 2-7).

The **Encrypted Data** is generated from 4 function bits, 2 overflow bits, and 10 discrimination bits, and the 16-bit synchronization counter value (Figure 2-7).

The **Nonencrypted Code Data** is made up of 2 QUE bits, 2 CRC bits, a VLOW bit, 4 function bits, and the 28-bit serial number. If the extended serial number (32 bits) is selected, the 4 function code bits will not be transmitted (Figure 2-7).

2.2.2 TRANSMISSION DATA MODULE

The Data Modulation Format is selectable between Pulse Width Modulation (PWM) format and Manchester encoding. Both formats are preceded by a preamble and synchronization header, followed by the 69-bits of data. Manchester encoding has a leading and closing '1' for each code word.

The same code word is continuously sent as long as the input pins are kept high with a guard time separating the code words. All of the timing values are in multiples of a Basic Timing Element (RFTE), which can be changed using the baud rate option bits.

2.3 Code Hopping Mode Special Features

2.3.1 CODE WORD COMPLETION

Code word completion is an automatic feature that ensures that the entire code word is transmitted, even if the button is released before the transmission is complete. The HCS412 encoder powers itself up when a button is pushed and powers itself down after the command is finished (Figure 2-6).

If MTX4 is set in the configuration word, a minimum of four transmissions will be transmitted when the HCS412 is activated, even if the buttons are released. After 1 (or 4 if MTX4 is set) complete code words have been transmitted the DATA output will switch off within 1ms when all button inputs are released.

2.3.2 CODE WORD BLANKING ENABLE

Federal Communications Commission (FCC) part 15 rules specify the limits on fundamental power and harmonics that can be transmitted. Power is calculated on the worst case average power transmitted in a 100ms window. It is therefore advantageous to minimize the duty cycle of the transmitted word. This can be achieved by minimizing the duty cycle of the individual bits and by blanking out consecutive words. Code Word Blanking Enable (CWBE) is used for reducing the average power of a transmission (Figure 2-11). Using the CWBE allows the user to transmit a higher amplitude transmission if the transmission length is shorter. The FCC puts constraints on the average power that can be transmitted by a device, and CWBE effectively prevents continuous transmission by only allowing the transmission of every second or fourth word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

The HCS412 will either transmit all code words, 1 in 2 or 1 in 4 code words, depending on the baud rate selected and the code word blanking option. See Section 3.7 for additional details.

2.3.3 CRC (CYCLE REDUNDANCY CHECK) BITS

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

EQUATION 2-1: CRC CALCULATION

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

and

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

with

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

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

FIGURE 2-7: HOP CODE WORD ORGANIZATION (RIGHT-MOST BIT IS CLOCKED OUT FIRST)

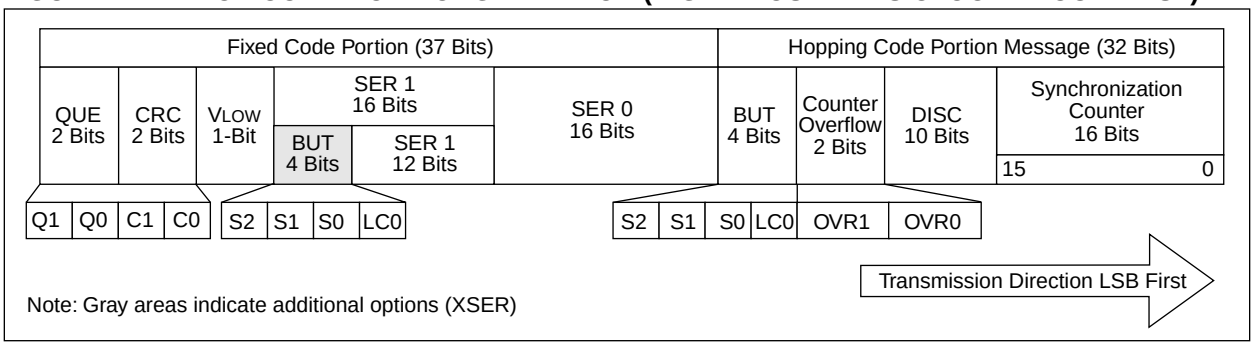


FIGURE 2-8: SEED CODE WORD ORGANIZATION

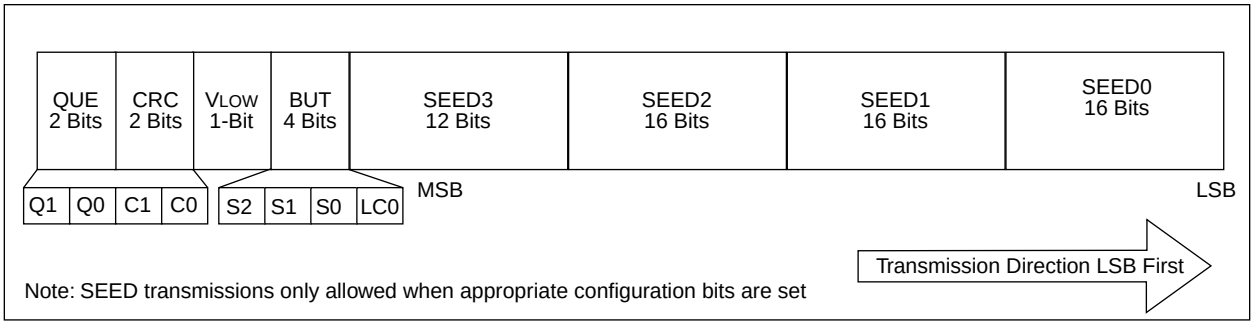


FIGURE 2-9: TRANSMISSION FORMAT—MANCH = 0

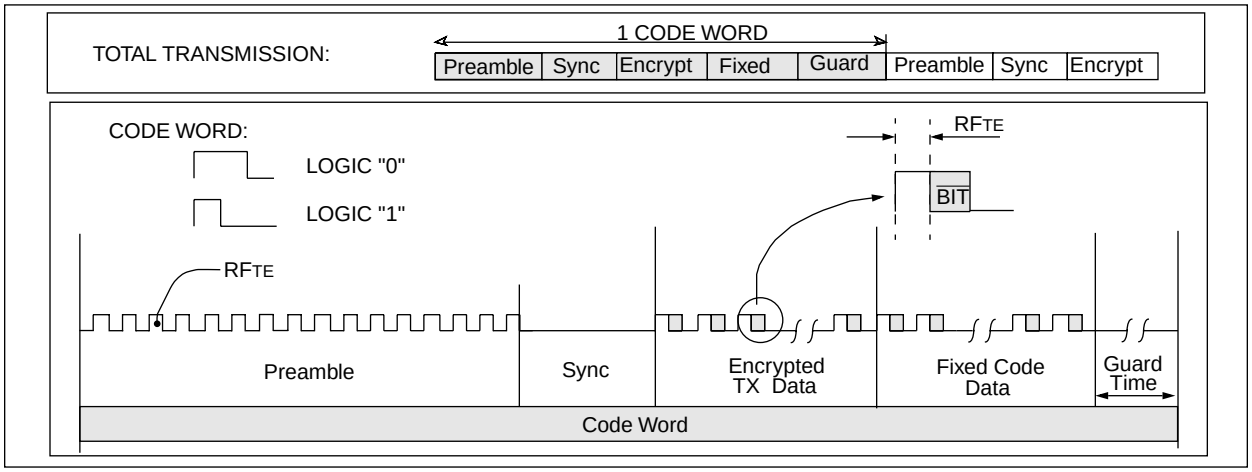


FIGURE 2-10: TRANSMISSION FORMAT—MANCH = 1

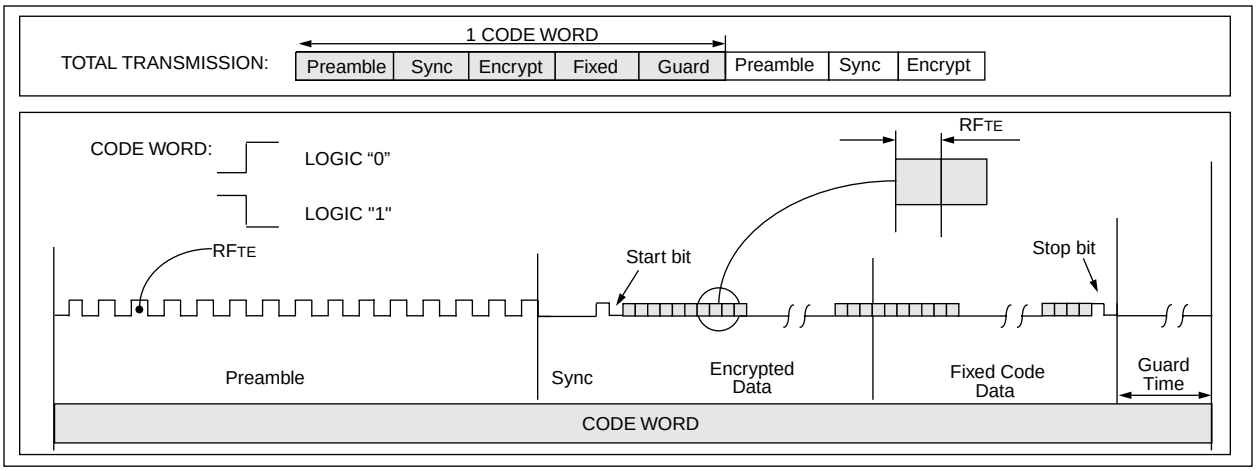
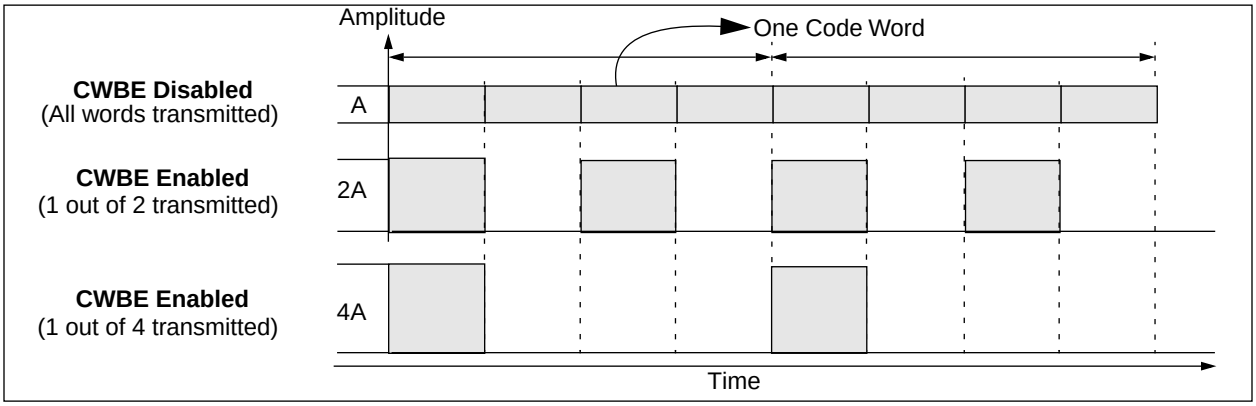


FIGURE 2-11: CODE WORD BLANKING ENABLE



2.3.4 SEED TRANSMISSION

In order to increase the level of security in a system, it is possible for the receiver to implement what is known as a secure learning function. This can be done by utilizing the seed value on the HCS412 which is stored in EEPROM. Instead of the normal key generation method being used to create the encoder key, this seed value is used and there should not be any mathematical relationship between serial numbers and seeds for the best security. See Section 3.7.3 for additional details.

2.3.5 PASSIVE PROXIMITY ACTIVATION

If the HCS412 is brought into a magnetic field it enters IFF mode. In this mode it sends out ACK pulses on the LC lines. If the HCS412 doesn't receive any response to the first set of ack pulses within 50 ms the HCS412 will transmit a normal code hopping transmission for 2 seconds if PXMA is set in the configuration word. The function code during this transmission is S2:S1:S0:LC0 = 0001.

2.3.6 AUTO-SHUTOFF

The Auto-shutoff function automatically stops the device from transmitting if a button inadvertently gets pressed for a long period of time. This will prevent the device from draining the battery if a button gets pressed while the transmitter is in a pocket or purse. Time-out period is approximately TTO seconds.

2.3.7 VLOW: VOLTAGE LOW INDICATOR

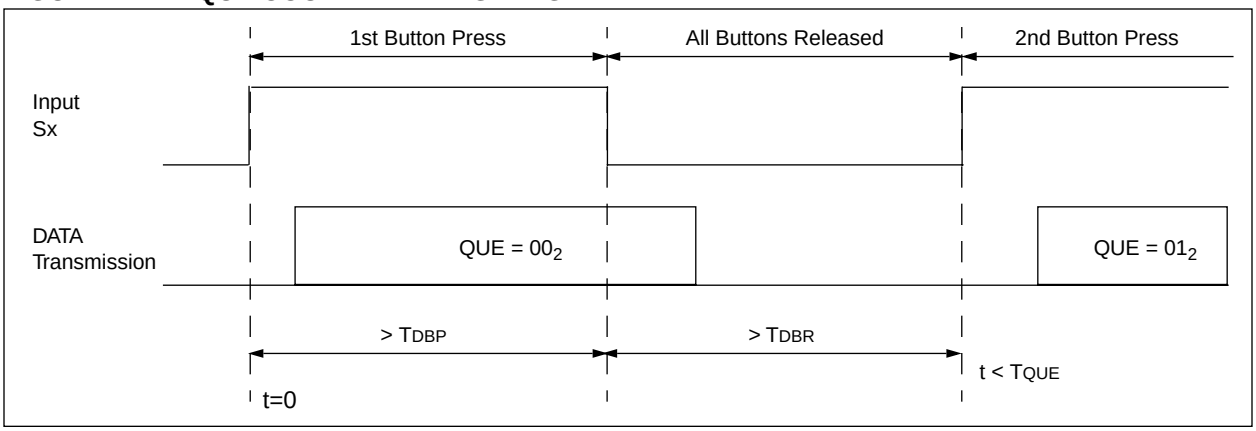
The VLOW bit is transmitted with every transmission (Figure 2-7). VLOW is set when the operating voltage has dropped below the low voltage trip point, approximately 2.2V or 4.4V selectable at 25°C. This VLOW signal is transmitted so the receiver can give an indication to the user that the transmitter battery is low.

2.3.8 QUE0:QUE1: QUEUING INFORMATION

If a button is pressed, released for more than TDBR, and pressed again within TQUE of the first press, the QUE counter is incremented (Figure 2-6). The transmission that the HCS412 is busy with is aborted and a new transmission is begun with the new QUE bits set. These bits can be used by the decoder to perform secondary functions using only a single button without the requirement that the decoder receive more than one completed transmission. For example if none of the QUE bits are set the decoder only unlocks the driver's door, if QUE0 is set (double press on the transmitter) the decoder unlocks all the doors.

Note 1:	The QUE will not overflow.
2:	The button must be pressed for more than TDBP.
3:	The button must be released for more than TDBR between presses.

FIGURE 2-12: QUE COUNTER TIMING DIAGRAM



2.3.9 LED OUTPUT

The LED line can be used to drive a LED when the HCS412 is transmitting. (Figure 2-14 and Figure 2-15)

2.3.10 DELAYED INCREMENT

The HCS412 has a delayed increment feature that increments the counter by 12, 20 seconds after the last button press occurred. The 20-second time-out is reset and the queue counter will increment if another press occurs before the 20 seconds expires. The queue counter is cleared after the buttons have been released for more than 2 seconds. Systems that use this feature will circumvent the latest jamming-code grabbing attackers.

2.3.11 LONG PREAMBLE (LPRE)

The HCS412 has an extended preamble (T_{LPRE} in duration for all selected elemental periods (baud rates)). This preamble only replaces the first preamble of the complete push button requested transmission. The subsequent preambles are T_{PRE} long.

The long preamble is transmitted before the first code word to wake up the receiver. The long preamble will be a square wave at the selected RF_{TE} (elemental period).

2.3.12 RF ENABLE SIGNALS (RFEN)

This option has been implemented on the HCS412 for external PLL interface. If enabled S2/RFEN/LC1 goes high while data is being transmitted. (Figure 2-14)

2.3.13 ASK/FSK OPTION (AFSK)

The ASK / FSK sequence has been implemented to provide the interface to wake up ASK or FSK receivers. Figure 2-14 shows the transmission format over a period of about 1.3 seconds with different combinations of AFSK. As can be seen from this diagram, several data packets are transmitted within the LED Off period. The LED on time is T_{LEDON} and the LED off time is T_{LEDOFF}. Switching of the !LED pin and the RFEN pin occur simultaneously. The RFEN output controls the PLL power up.

FIGURE 2-13: EXTENDED PREAMBLE

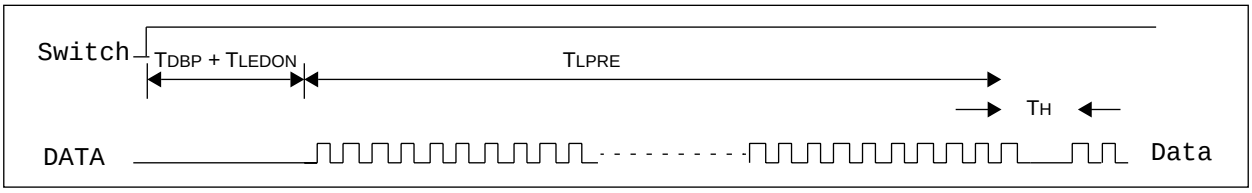
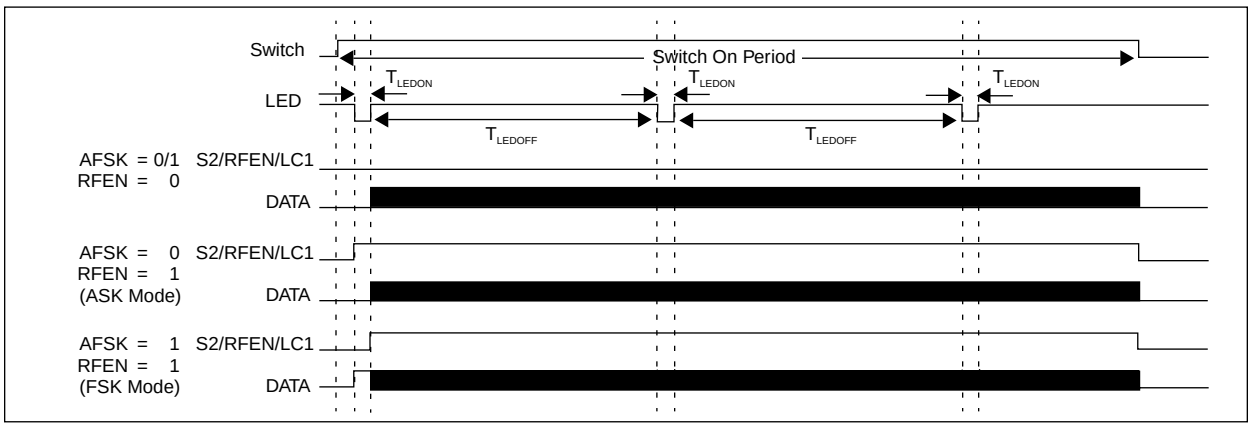


FIGURE 2-14: RF ENABLE/ASK/FSK OPTIONS



2.3.13.1 LOW VOLTAGE CONDITION – LOW BATTERY STATUS

The HCS412 samples the battery voltage at the onset of a transmission and then at the end of each transmission and transmits the bit accordingly. The HCS412 will continue to transmit code words after the LED output has been activated. Refer to Figure 2-15 for LED operation when battery voltage is low.

2.3.14 OTHER CONFIGURABLE OPTIONS

Other configurable code hopping options include an

- Transmission-rate selection
- Extended serial number

These are described in more detail in Section 3.7.

2.4 IFF Mode

IFF mode allows the decoder to perform an IFF validation, to write to the user EEPROM and to read from the user EEPROM. Each operation consists of the decoder sending an opcode, data and the HCS412 giving a response.

There are two IFF modes: IFF1 and IFF2. IFF1 allows only one key IFF, while IFF2 allows two keys to be used.

Note:	When IFF2 is enabled, seed transmissions will not be allowed.

It is possible to use the HCS412 as an IFF token without using a magnetic field for coupling. The HCS412 can be directly connected to the data line of the decoder as shown in Figure 2-3. The HCS412 gets its power from the data line as it would in normal transponder mode. The communication is identical to the communication used in transponder mode.

2.4.1 IFF MODE ACTIVATION

The HCS412 will enter IFF mode if the capacitor/inductor resonant circuit generates a voltage greater than approximately 1.0 volts on LC0. After the verified application of power and elapse of the normal reset period, the device will start responding by pulsing the DATA line (LC0/1) with pulses as shown in Figure 2-18. This action will continue until the pulse train is terminated by receiving a start signal of duration 2LFTE, on the LC inputs before the next expected marker pulse. The device now enters the IFF mode and expects to receive an 'Opcode' and a 0/28/32-bit data stream to react on. The data rate (LFTE) is determined by the LFBSL bit in the configuration word. See Section 3.0 for additional details.

2.4.2 IFF DECODER COMMANDS

As shown in Figure 2-16, a logic 1 and 0 are differentiated by the time between two rising edges. A long pulse indicates a 1; a short pulse, a 0.

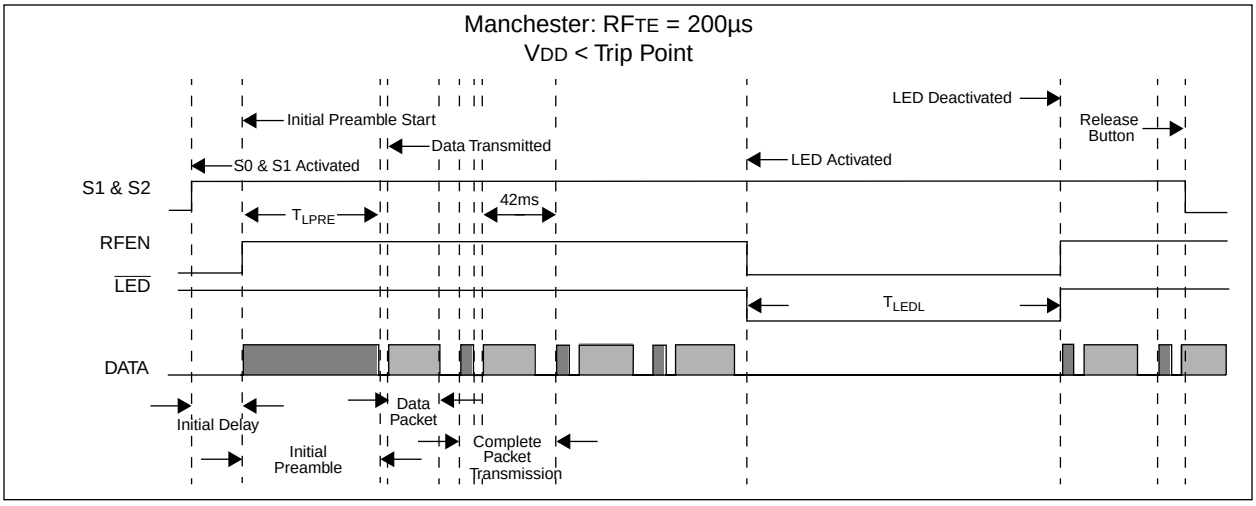
2.4.3 HCS412 RESPONSES

The responses from the HCS412 are in PPM format. See Figure 2-18 for additional information. Every response from the HCS412 is preceded by a "2 bit preamble" of 01_2, and then 16/32 bits of data.

2.4.4 IFF CHALLENGE RESPONSE

The 32-bit response to a 32-bit challenge, is transmitted once, after which the device is ready to accept another command. The opcode written to the device specifies the key and algorithm used. The response always starts with a leading preamble of 01_2 followed by the 32 bits of data.

FIGURE 2-15: LED WITH LOW VOLTAGE



2.4.5 IFF WRITE

The decoder can write to USER[0:3], SER[0:1], and the configuration word in the EEPROM.

After the HCS412 has written the word into the EEPROM, it will give four acknowledge pulses (LFTE wide and LFTE apart) on the LC pins.

When writing to the serial number or configuration word, the user must send the transport code before the write will begin (Section 3.4).

Note:	If the configuration word is written, the device must be reset to allow the new configuration settings to come into effect.

2.4.6 IFF READ

The decoder can read USER[0:3], SER[0:1], and the configuration word in the EEPROM. After the data has been read, the device is ready to receive a command again.

Each read command is followed by a 16-bit data response. The response always starts with a leading preamble of 01_2 and then the 16-bits of data.

2.4.7 IFF PROGRAMMING

Upon receiving a programming opcode and the transport code, the EEPROM is erased (Section 3.4). Thereafter, the first 16 bits of data can be written. After indicating that a write command has been successfully completed the device is ready to receive the next 16 bits. After a complete memory map was received, it will be transmitted in PPM format on the LC pins as 16-bit words. This enables wireless programming of the device.

After the EEPROM is erased, the configuration word is reloaded. This results in oscillator tuning bits of 0000 being used during programming. When using IFF programming, the user should read the configuration word and store the oscillator bits in the memory map to be programmed. A program command should be sent and the next set of ACK pulses transmitted by the HCS412 should be used to determine the LFTE. A second program command can then be sent, and the device programmed using the LFTE just calibrated.

2.4.8 IFF HOP CODE

After receiving this command the HCS412 will increment the counter and build a normal code hopping word, encrypting it using the KeeLoq code hopping algorithm. This is then transmitted on the LC lines as normal.

2.4.9 DISABLE ANTI-COLLISION OPTION

In this mode the anti-collision/ proximity activation and IFF baud rate options are all set to 0 for the rest of the communication. This means that the transponder has anti-collision disabled, RF echo disabled and the transponder is working at the slow IFF baud rate.

FIGURE 2-16: MODULATION FOR IFF COMMUNICATION

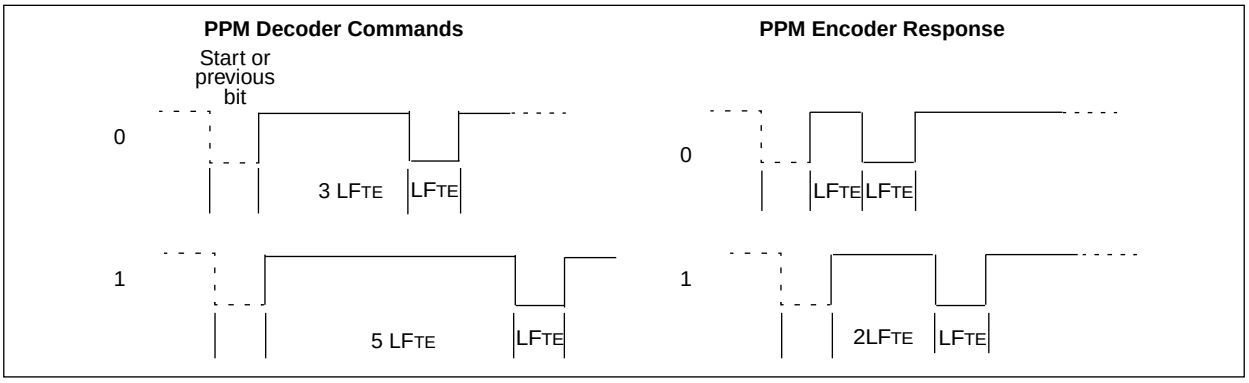


FIGURE 2-17: OVERVIEW OF IFF OPERATION

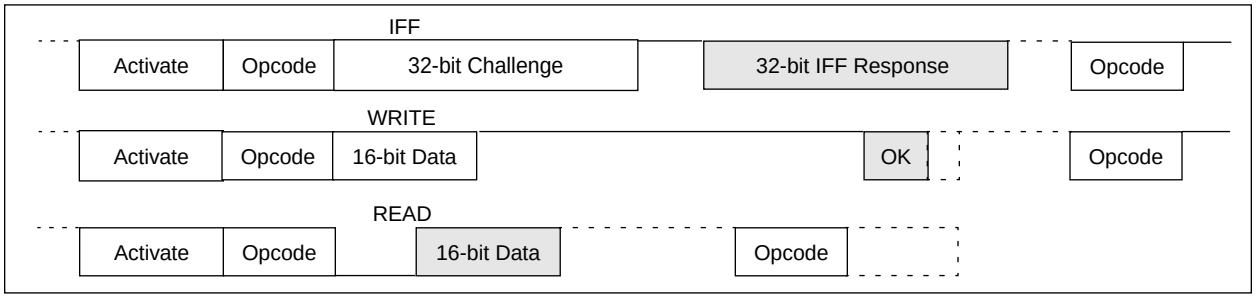


FIGURE 2-18: DECODER IFF COMMANDS AND WAVEFORMS

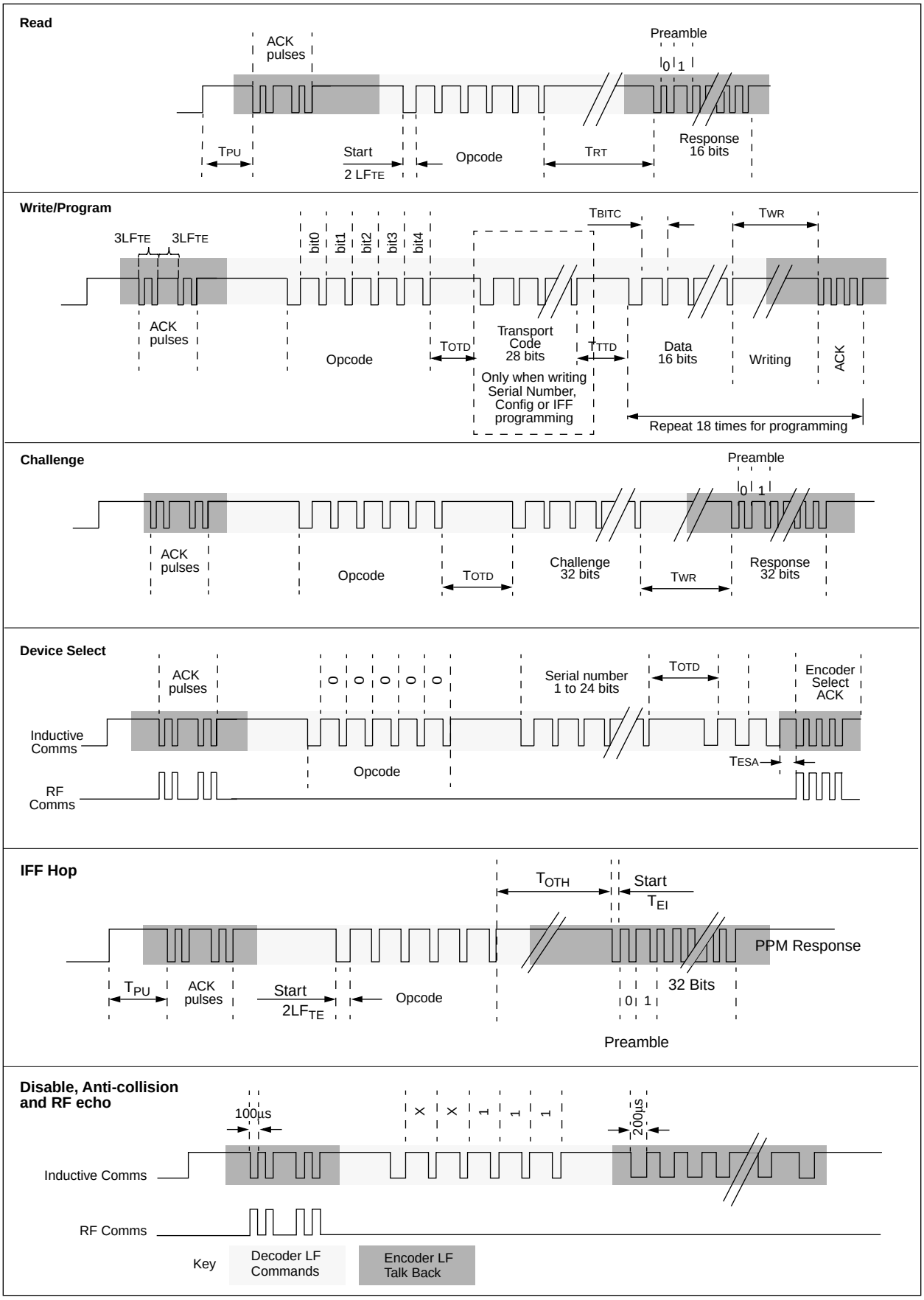


TABLE 2-3: IFF TIMING PARAMETERS

Parameter	Symbol	Minimum	Typical	Maximum	Units
Time Element LFBSL = 0 LFBSL = 1	LF_{TE}	— —	200 100	— —	µs
PPM Command Bit Time Data = 1 Data = 0	T_{BITC}	3.5 5.5	4 6	— —	LF_{TE}
PPM Response Bit Time Data = 1 Data = 0	T_{BITR}	— —	2 3	— —	LF_{TE}
PPM Command Minimum High Time	T_{PMH}	1.5	—	—	LF_{TE}
Response Time (Minimum for Read)	T_{RT}	6.5	—	—	ms
Opcode to Data Input Time	T_{OTD}	1.8	—	—	ms
Transport Code to Data Input Time	T_{TTD}	6.8	—	—	ms
IFF EEPROM Write Time (16 bits)	T_{WR}	—	—	30	ms
Power Up Time	T_{PU}	—	6	—	ms
Op Code to Hop Code Response Time	T_{OTH}	—	114	—	ms

2.5 IFF Opcodes

TABLE 2-4: LIST OF IFF COMMANDS

Command	Description	Expected data In	Response
00000	Select HCS412, used if Anticollision enabled	1 to 24 bits of the serial number (SER)	Encoder select acknowledge if serial number match
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 area 0	None	16 Bits of User EEPROM USR0
00101	Read user area 1	None	16 Bits of User EEPROM USR1
00110	Read user area 2	None	16 Bits of User EEPROM USR2
00111	Read user area 3	None	16 Bits of User EEPROM USR3
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
01001	Write configuration word	Transport code (28 bits); 16 Bit configuration word	Write acknowledge pulse
01010	Write low serial number	Transport code (28 bits); Lower 16 bits of serial number (SER0)	Write acknowledge pulse
01011	Write high serial number	Transport code (28 bits); Higher 16 bits of serial number (SER1)	Write acknowledge pulse
01100	Write user area 0	16 Bits of User EEPROM USR0	Write acknowledge pulse
01101	Write user area 1	16 Bits of User EEPROM USR1	Write acknowledge pulse
01110	Write user area 2	16 Bits of User EEPROM USR2	Write acknowledge pulse
01111	Write user area 3	16 Bits of User EEPROM USR3	Write acknowledge pulse
10000	IFF1 using key-1 and IFF algorithm	32-Bit Challenge	32-Bit Response
10001	IFF1 using key-1 and HOP algorithm	32-Bit Challenge	32-Bit Response
10100	IFF2 32-bit using key-2 and IFF algorithm	32-Bit Challenge	32-Bit Response
10101	IFF2 32-bit using key-2 and HOP algorithm	32-Bit Challenge	32-Bit Response
11000	Increments the counter and generates a hopping code portion for a transmission	None	32-Bit Hopping Code
11100-11111	Disable anticollision, RF echo and sets to slow IFF baud rate	None	Data in the user EEPROM given by the 2 LS bits of the op code

2.6 IFF Special Features

2.6.1 ANTI-COLLISION (ACOLI)

The anti-collision works as follows:

When the HCS412 enters a magnetic field the HCS412 starts sending ACK pulses to the decoder. The ACK pulses stop as soon as the HCS412 detects an opcode from the decoder. The HCS412 will not transmit ANY data (ACKS included) once it has received a select encoder opcode from the decoder.

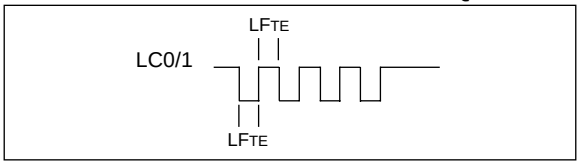
The decoder needs to send a 'select encoder' op code (00000) to the HCS412 followed by 1 to 24 bits of the HCS412's serial number starting with the 4th bit of the serial number. After TOTD the base station can start sending out a string of 1's (increment serial number). These 'increment' bits are used to patch in the 3 LSB's of the serial number. The first '1' sent sets the 3 LSB's of the serial number sent by the base station 000, the second to 001 and so on. If the resultant serial number transmitted matches the HCS412's serial number the HCS412 will respond with an encoder select ack pulse on both the inductive and RF (if enabled) outputs.

This allows the base station to send the minimum number of bits before starting the IFF process. Typically the base station needs only clock as many bits as needed to differentiate between encoders learned onto the system. Typically if the serial numbers of the learned encoders are 1 and 2 the base station will only need to send 1 bit and a single 'increment' opcode. If the two HCS412 serial numbers differ only in their MSB, the base station will have to clock out all 24 bits. A second advantage of this scheme is that it will be possible to inductively program an HCS412 that is in anti-collision mode even if the serial number is not known. The base station can select the transponder with a single bit (either a 1 or a 0) and checking for an acknowledge pulse from the HCS412 indicating that the bit matched the LSB of the serial number.

The HCS412 responds to all opcodes from the decoder once it has been selected. If the serial number's don't match the HCS412 monitors the opcodes from the decoder till it receives a new 'select encoder' opcode after which the serial number received in the data is checked against it's serial number.

Note:	It will not be possible to differentiate between two transponders if their serial numbers only differ in the most significant nibble.

FIGURE 2-19: SERIAL NUMBER CORRECT ACKNOWLEDGE SEQUENCE



2.6.2 TRANSPONDER IN/RF OUT

When in transponder mode with ACOLI and PXMA set, the outputs of the HCS412's LC0:LC1 pins are echoed on the DATA output line. After transmitting the data on the DATA line, the data is then transmitted on the LC pins. The transmission format mirrors a code hopping transmission. The response replaces the 32-bit code hopping portion of the transmission. If the output is a 16-bit output (read), the 16 bits are duplicated to make up the 32-bit code hopping portion. The preamble, serial number, CRC, and queuing bits are all transmitted as normal (Figure 2-21).

This feature will be used in applications which use RF for long distance uni-directional, bi-directional and authentication and short distance IFF.

2.6.3 INTELLIGENT DAMPING

If the LC circuit on the transponder has a high Q-factor, the circuit will keep on resonating for a long time after the field has been shut down by the reader. This makes fast communication from the reader to the HCS412 difficult. If the IDAMP bit is set to 0, the HCS412 will clamp the LC pins for 5 µs every 1/4 LFTE, whenever the HCS412 is expecting data from the decoder. The intelligent damping pulses start 12.5 LFTE after the acknowledge pulses have been sent and continue for 12.5 LFTE. If the HCS412 detects data from the base station while sending out damping pulses, the damping pulses will continue to be sent. This option can be set in the configuration word.

2.6.4 RF ECHO OPTION (PXMA, ACOL)

If both ACOL and PXMA are set to 1 the HCS412 response is echoed on the LC lines being sent out on the DATA output. The 16/32 bit data (either a response to a challenge or a word read from the EEPROM) replaces the encrypted data in the normal Code Hopping Code Word.

FIGURE 2-20: INTELLIGENT DAMPING OPTION

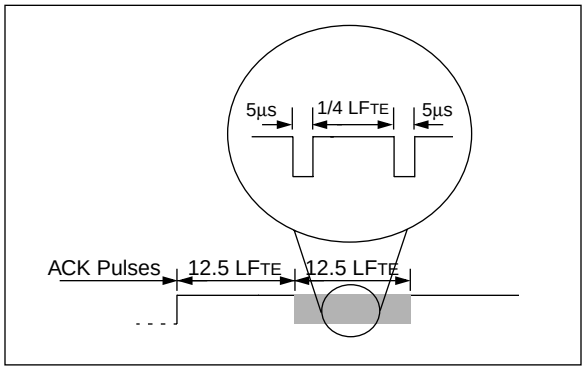
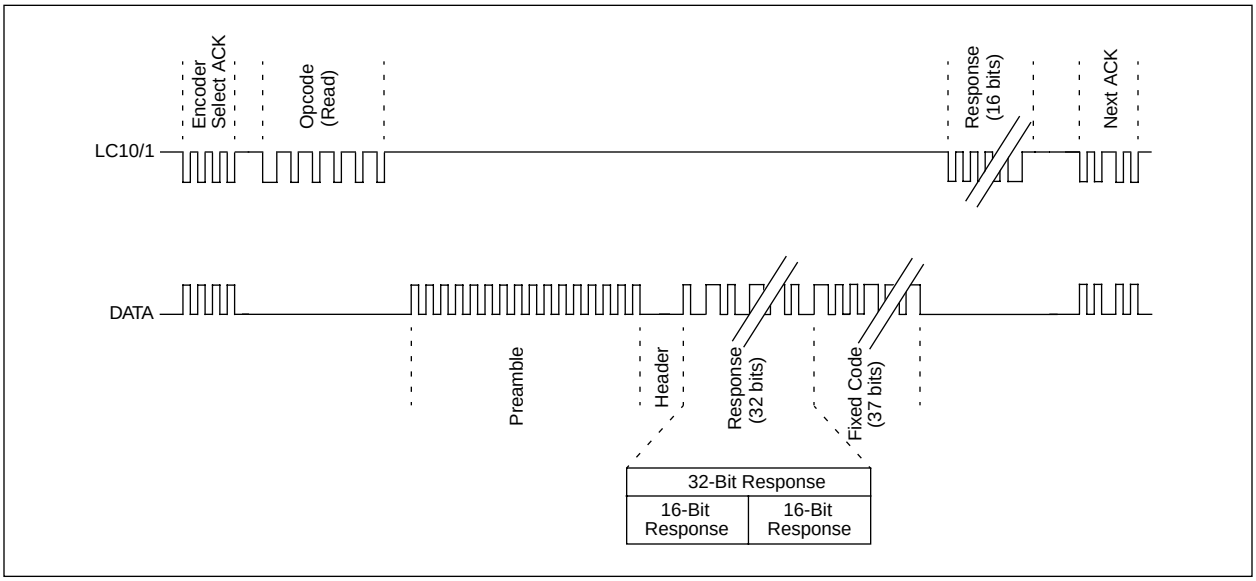


FIGURE 2-21: RE ECHO WAVEFORM AND CODE WORD FORMAT



*Patents have been applied for.

3.0 EEPROM ORGANIZATION AND CONFIGURATION

The HCS412 has nonvolatile EEPROM memory which is used to store user programmable options. This information includes encoder keys, serial number, and up to 64-bits of user information.

The HCS412 has two modes in which it operates as specified by the configuration word. In the first mode the HCS412 has a single encoder key which is used for encrypting the code hopping portion of a CH Mode transmission and generating a response during IFF validation. Seed transmissions are allowed in this mode. In the second mode the HCS412 is a transponder device with two encoder keys.

The two different operating modes of the HCS412 lead to different EEPROM memory maps.

In IFF1 mode, the HCS412 can act as a code hopping encoder with seed transmission, and as an IFF token with one key.

IFF1 Mode
64-bit Encoder Key 1
60-bit Seed/Transport Code (SEED0, SEED1, SEED2, SEED3)
32-bit Serial Number (SER0, SER1)
64-bit User Area (USR0, USR1, USER2, USR3)
10-bit Discrimination Value and 2 Overflow Bits.
16-bit Synchronization Counter
Configuration Data

In IFF2 mode, the HCS412 is able to act as a code hopping transmitter and an IFF token with two transponder keys.

IFF2 Mode
64-bit Encoder Key 1
60-bit Encoder Key 2/Transport Code
32-bit Serial Number (SER0, SER1)
64-bit User EEPROM (USR0, USR1, USER2, USR3)
10-bit Discrimination Value and 2 Overflow Bits.
16-bit Synchronization Counter
Configuration Data

3.1 Encoder Key 1 and 2

The 64-bit encoder key1 is used by the transmitter to create the encrypted message transmitted to the receiver in Code Hopping Mode. An IFF operation, can use encoder key 1 or key 2 to generate the response to a challenge received. The key(s) is created and programmed at the time of production using a key generation algorithm. Inputs to the key generation algorithm are the serial number or seed for the particular transmitter being used and a secret manufacturer's code. While a number of key generation algorithms are supplied by Microchip, a user may elect to create their own method of key generation. This may be done providing that the decoder is programmed with the same means of creating the key for decryption purposes. If a seed is used (CH Mode), the seed will also form part of the input to the key generation algorithm.

Key 2 is only 60 bits long, the most significant 4 bits being part of the configuration word. When key 2 is used for an IFF operator, the configuration bits are used as the 4 most significant bits at the key.

3.2 Discrimination Value and Overflow

The discrimination value forms part of the code hopping portion of a code hopping transmission. The least significant 10 bits of the discrimination value are typically set to the least significant bits of the serial number. The next 2 bits of the code hopping portion are the overflow bits (OVR1: OVR0). These are used to extend the range of the synchronization counter. When the synchronization counter wraps from $FFFF_{16}$ to 0000_{16} OVR0 is cleared and the second time a wrap occurs OVR1 is cleared.

Once cleared, the overflow bits cannot be set again, thereby creating a permanent record of the counter overflow.

3.3 16-Bit Synchronization Counter

This is the 16-bit synchronization counter value that is used to create the code hopping portion for transmission. This value will be changed after every transmission. The synchronization counter is not used in IFF mode except when the IFF hop command is given.

*Patents have been applied for.

3.4 60-bit Seed Word/Transport Code

This is the 60-bit seed code that is transmitted when seed transmission is selected. This allows the system designer to implement the secure learn feature or use this fixed code word as part of a different key generation/tracking process or purely as a fixed code transmission. The seed is not available in IFF2-mode. A Seed transmission can be initiated in two ways, depending on the button inputs (Figure 3-1).

Seed transmission is available for function codes (Table 2-2) S[2:0] = 111 and S[2:0] = 011 (delayed). The delayed seed transmission starts with a normal code hopping transmission being transmitted for TDSD, before switching to a seed transmission. The two seed transmissions are shown in Figure 3-1.

The least significant 28-bits of the seed are used as the transport code. The transport code is used to write-protect the serial number, configuration word, as well as preventing accidental programming of the HCS412 when in IFF mode.

Note:	If both SEED and TMPSD are set, IFF2 mode is enabled.

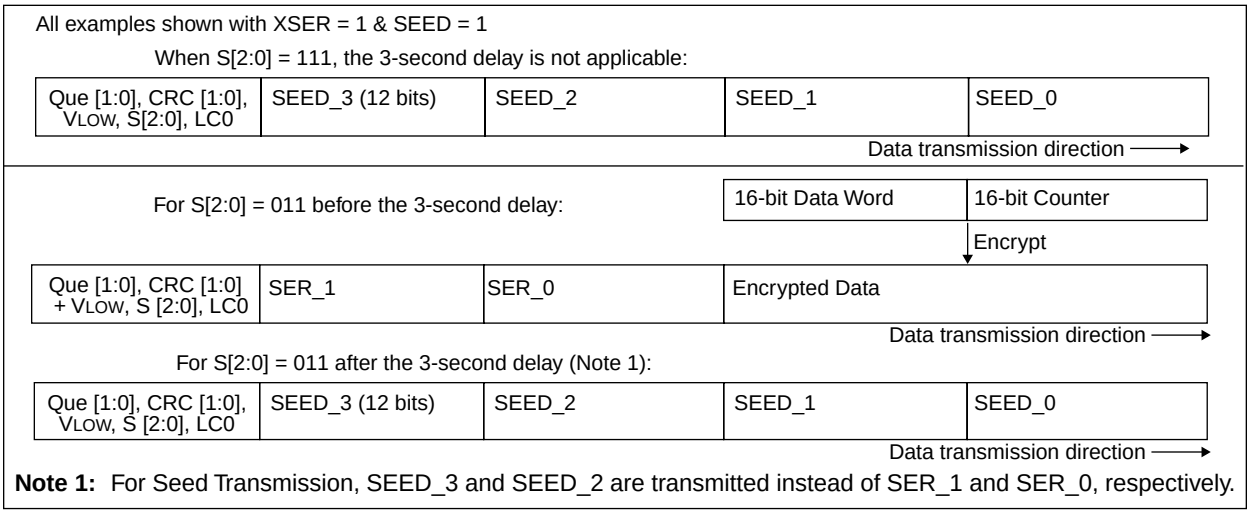
3.5 Encoder Serial Number

There are 32 bits allocated for the serial number and a selectable configuration bit (XSER) determines whether 32 or 28 bits will be transmitted. The serial number is meant to be unique for every transmitter.

3.6 User Data

The 64-bit user EEPROM can be reprogrammed and read at any time using the IFF interface.

FIGURE 3-1: SEED TRANSMISSION



Note 1: For Seed Transmission, SEED_3 and SEED_2 are transmitted instead of SER_1 and SER_0, respectively.

3.7 Configuration Data

The configuration data is used to select various encoder options. Further explanations of each of the bits are described in the following sections.

TABLE 3-1: CONFIGURATION OPTIONS

	Symbol	Description
1	CWBE	Code Word Blanking Enable
2	IDAMP	Intelligent Damping Option
3	SEED	Enable Seed Transmissions
4	TMPSD	Temporary Seed Transmissions
5	OSC0	Onboard Oscillator Tuning Bits
6	OSC1	
7	OSC2	
8	OSC3	
9	MTX4	Minimum 4 Code Word Option
10	AFSK	ASK/FSK - Signal Control Options
11	RFEN	RF Enable Output
12	LPA	Long Preamble
13	VLOW	Low Voltage Trip Point Selection
14	LFBSL	IFF Communication Baud Rate
15	RFBSL0	Transmission Baud Rate Selection Bits
16	RFBSL1	
17	S2LC	Selects S2 Usage
18	OVR0	Synchronization Counter Overflow Bits
19	OVR1	
20	MANCH	Manchester Modulation Mode
21	ACOL	Anti Collision Option
22	PXMA	Proximity Activation
23	DINC	Delayed Increment Option
24	DISC[0:9]	10-Bit Discrimination Value
25	XSER	Extended Serial Number

3.7.1 **CWBE:** CODE WORD BLANKING ENABLE

Selecting this option allows code blanking as shown in Table 3-3. If this option is not selected, all code words are transmitted.

3.7.2 **IDAMP:** INTELLIGENT DAMPING

If IDAMP is set to '1' intelligent damping is disabled.

3.7.3 **SEED, TMPSD:** SEED TRANSMISSION

SEED	TMPSD	Description
0	0	No Seed/1 IFF Key
0	1	Seed Limited*
1	0	Always Enabled
1	1	IFF2/No Seed/2 IFF Keys

* Seed transmissions are allowed till the synchronization counter crosses a $XX7F_{16}$ boundary. e.g. If the counter is initialized to 0000_{16} when the device is programmed, seed transmissions will be allowed until the counter wraps from $007F_{16}$ to 0080_{16} giving the user 128 transmissions before seed transmissions are disabled.

3.7.4 **OSC:** OSCILLATOR TUNING BITS

These bits allow the onboard oscillator to be tuned to within 10% of the nominal oscillator speed over both temperature and voltage.

TABLE 3-2: OSCILLATOR TUNING

OSC	Description
1000	Fastest
1001 1010 • • • 1111	Faster
0000	Nominal
0001 0010 • • • 0110	Slower
0111	Slowest

TABLE 3-3: BAUD RATE SELECTION

		Code Hopping Transmissions (RFTE)			Transponder Communication (LFTE)	
RFBSL 1	RFBSL 0	DATA	Manchester	Codes Word Transmitted*	LFBSL	PPM
0	0	400 µs	800 µs	All	0	200 µs
0	1	200 µs	400 µs	1 of 2	—	—
1	0	100 µs	200 µs	1 of 2	—	—
1	1	100 µs	200 µs	1 of 4	1	100 µs

*If code word blanking is enabled.

3.7.5 **MTX4:** MINIMUM CODE WORDS COMPLETED

If this bit is set, the HCS412 will transmit a minimum of 4 words before it powers itself down. If this bit is cleared, the HCS412 will only complete the current transmission. This feature will only work if V_{DD} is connected directly to the battery as shown in Figure 2-1.

3.7.6 **AFSK:** ASK/FSK - SIGNAL CONTROL OPTIONS

The ASK/FSK sequence has been implemented to wake up ASK or FSK receivers. Refer to Section 2.3.13 for more details.

3.7.7 **RFEN:** RF ENABLE OUTPUT

Allows RF Enable signals on the RFEN/S2/LC1 line. Refer to Section 2.3.12 for more details

3.7.8 **LPA:** LONG PREAMBLE

Allows a long preamble on the first code word. Refer to Section 2.3.11 for more details

3.7.9 **V_{LOW}:** LOW VOLTAGE TRIP POINT

The low voltage trip point select bit is used to tell the HCS412 what V_{DD} level is being used. This information will be used by the device to determine when to send the voltage low signal to the receiver. When this bit is set, the V_{DD} level is assumed to be operating from a 5 volt or 6 volt supply. If the bit is cleared, then the Vdd level is assumed to be 3.0 volts. Refer to Figure 5-3 for voltage trip point. When the battery reaches the Vlow point, the LED will flash once for T_{LEDL} on during a code hopping transmission.

3.7.10 **LFBSL:** TRANSPONDER COMMUNICATION BAUD RATE

If the bit is cleared, the LF_{TE} is 200µs. When this bit is set to 1 the LF_{TE} for IFF communication is 100µs. All the timing parameters decrement to half the default value.

3.7.11 **RFBSL[0:1]:** RF TRANSMISSION BAUD RATE

These bits set the communication rate (RF_{TE}) for RF transmission. Refer to Table 3-3 for more details.

3.7.12 **S2LC:** SELECTS S2 USAGE

This option is used to select whether the S2/RFEN/LC1 pin is used as S2/RFEN or as a transponder pin (LC1). The first time the device is powered up the debounce time (T_{DB}) be a little longer to allow the HCS412 to read the configuration word and set the port accordingly.

3.7.13 **OVR[0:1]:** SYNCHRONIZATION COUNTER OVERFLOW BITS

These bits can be used to extend the counter range and prevent fast cycling at the counter. Refer to Section 3.4 for more details.

3.7.14 **MANCH:** MANCHESTER CODE ENCODING

MANCH selects between Manchester code modulation and PWM modulation in code hopping mode. If MANCH = 1, Manchester code modulation is selected. If MANCH is cleared, PWM modulation is selected.

3.7.15 **ACOLI:** ANTI-COLLISION COMMUNICATION AND **PXMA**: TRANSPONDER ECHOING ON DATA OUTPUT)

ACOLI = 1, PXMA = 0

If ACOLI is set the anti-collision operation during bi-directional transponder mode (IFF) is enabled. This feature is useful in situations where multiple transponders enter the magnetic field simultaneously.

ACOLI = 0, PXMA = 1

If PXMA is set, and ACOLI is cleared, proximity activation is enabled. the HCS412 starts sending out ACK pulses when it detects a magnetic field. If the HCS412 doesn't receive a start bit from the decoder within 50 ms of sending the first set of ACK pulses, the HCS412 will transmit a code hopping transmission DATA pin for two seconds.

ACOLI = 1, PXMA = 1

If both the ACOLI and PXMA are set, all of the HCS412 transponder responses are echoed on the DATA output, as described in Section 2.6.2.

3.7.16 **DINC:** DELAYED INCREMENT

If DINC is set to '1', the delayed increment feature is enabled. If DINC is cleared, the counter only increments once each time the button is pressed.

3.7.17 **DISC[0:9]:** DISCRIMINATION VALUE

The discriminator is only used in HOP code transmissions. The 10-bit discriminator forms part of the encrypted message and can be used by the decoder to verify a decryption if known data is used.

3.7.18 **XSER:** EXTENDED SERIAL NUMBER

If XSER is set, bits 60 to 63 of the transmission are the most significant bits of the serial number. If XSER bit is cleared, bits 60 to 63 of the transmission are set to the function code used to activate the device (S2:S1:S0:LC0). This option doesn't affect SEED transmissions.

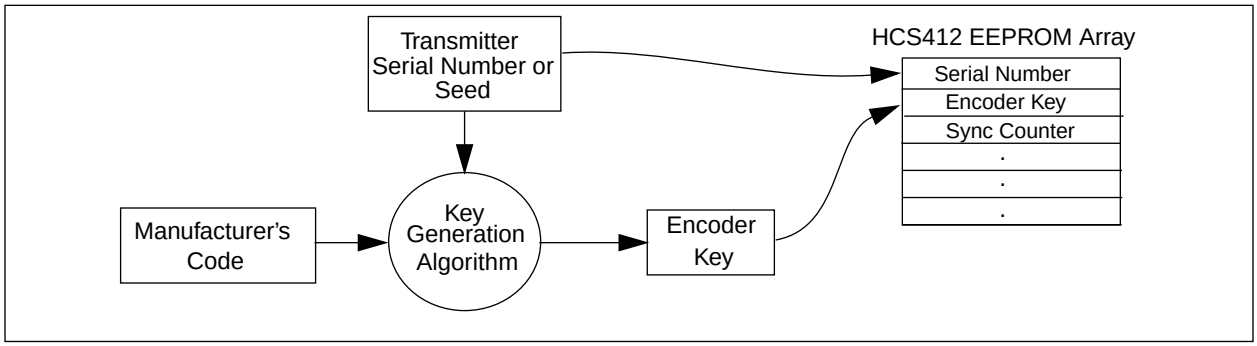
4.0 INTEGRATING THE HCS412 INTO A SYSTEM

Use of the HCS412 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Firmware routines that accept transmissions from the HCS412, decrypt the code hopping portion of the data stream and perform IFF functions are available. These routines provide system designers the means to develop their own decoding system.

4.1 Key Generation

The serial number for each transmitter is programmed by the manufacturer at the time of production. The generation of the encoder key is done using a key generation algorithm (Figure 4-1). Typically, inputs to the key generation algorithm are the serial number of the transmitter or seed value, and a 64-bit manufacturer's code. The manufacturer's code is chosen by the system manufacturer and must be carefully controlled. The manufacturer's code is a pivotal part of the overall system security.

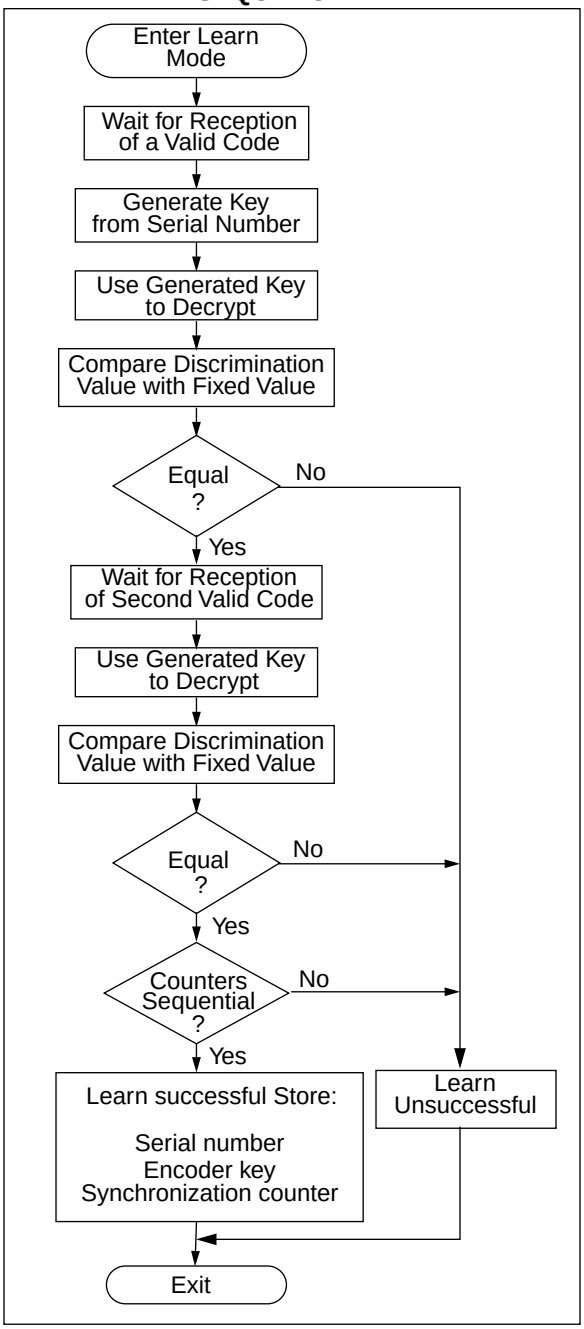
FIGURE 4-1: CREATION AND STORAGE OF ENCODER KEY DURING PRODUCTION



4.2 Learning an HCS412 to a Receiver

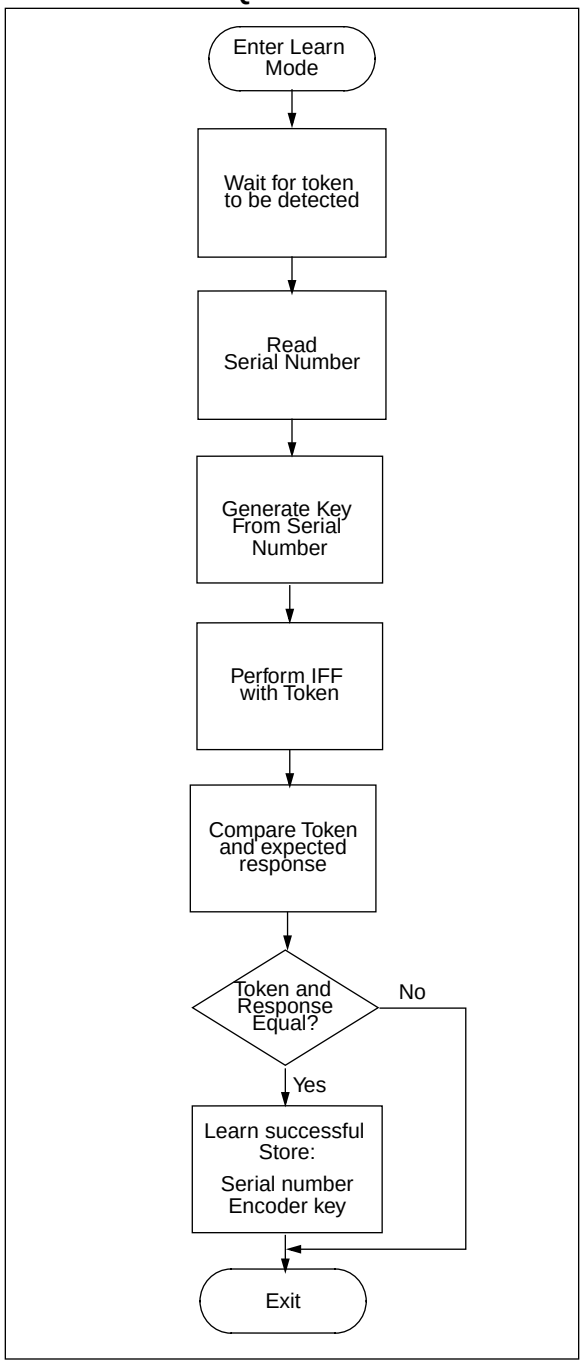
In order for a transmitter to be used with a decoder, the transmitter must first be 'learned'. Several learning strategies can be followed in the decoder implementation. When a transmitter is learned to a decoder, it is suggested that the decoder stores the serial number and current synchronization counter value (synchronization counter stored in CH Mode only) in EEPROM. The decoder must keep track of these values for every transmitter that is learned (Figure 4-2 and Figure 4-3).

FIGURE 4-2: TYPICAL CH MODE LEARN SEQUENCE



The maximum number of transmitters that can be learned is only a function of how much EEPROM memory storage is available. The decoder must also store the manufacturer's code in order to learn an HCS412, although this value will not change in a typical system so it is usually stored as part of the microcontroller ROM code. Storing the manufacturer's code as part of the ROM code is also better for security reasons.

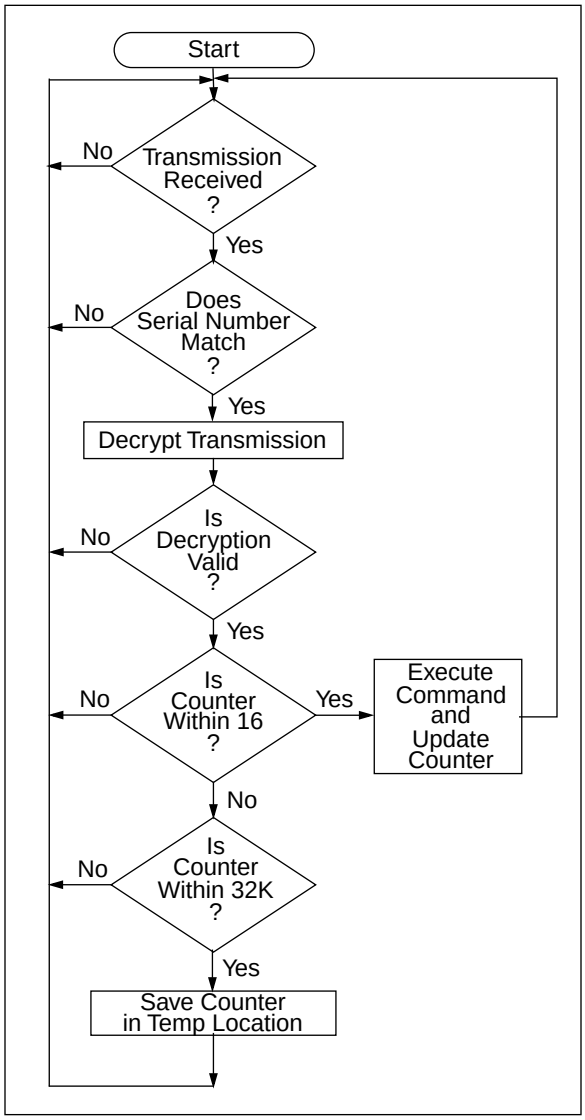
FIGURE 4-3: TYPICAL IFF LEARN SEQUENCE



4.3 CH Mode Decoder Operation

In a typical decoder operation (Figure 4-4), the key generation on the decoder side is done by taking the serial number from a transmission and combining that with the manufacturer's code to create the same encoder key that is stored in the HCS412. Once the encoder key is obtained, the rest of the transmission can be decrypted. The decoder waits for a transmission and immediately checks the serial number to determine if it is a learned transmitter. If it is, the code hopping portion of the transmission is decrypted using the stored key. It uses the discrimination bits to determine if the decryption was valid. If everything up to this point is valid, the synchronization counter value is evaluated.

FIGURE 4-4: TYPICAL CH MODE DECODER OPERATION



4.3.1 SYNCHRONIZATION WITH DECODER

The KEELOQ technology features a sophisticated synchronization technique (Figure 4-5) which does not require the calculation and storage of future codes. If the stored counter value for that particular transmitter and the counter value that was just decrypted are within a window of say 16, the counter is stored and the command is executed. If the counter value was not within the single operation window, but is within the double operation window of say 32K window, the transmitted synchronization counter value is stored in temporary location and it goes back to waiting for another transmission. When the next valid transmission is received, it will compare the new value with the one in temporary storage. If the two values are sequential, it is assumed that the counter had just gotten out of the single operation 'window', but is now back in sync, so the new synchronization counter value is stored and the command executed. If a transmitter has somehow gotten out of the double operation window, the transmitter will not work and must be relearned. Since the entire window rotates after each valid transmission, codes that have been used are part of the 'blocked' (32K) codes and are no longer valid. This eliminates the possibility of grabbing a previous code and retransmitting to gain entry.

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

FIGURE 4-5: SYNCHRONIZATION WINDOW

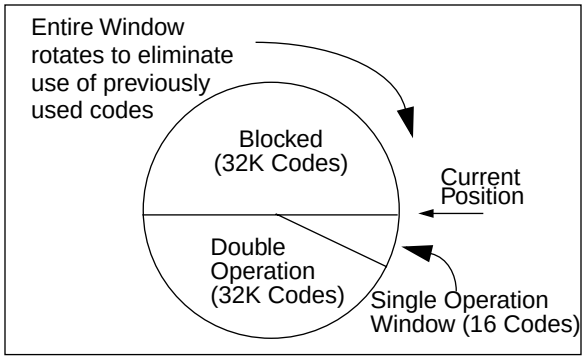
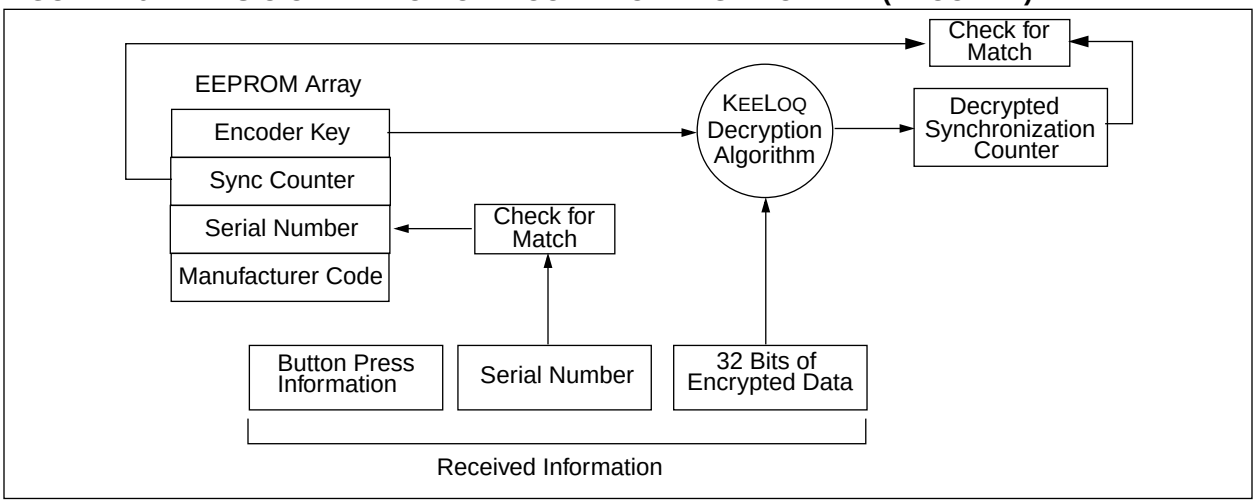


FIGURE 4-6: BASIC OPERATION OF A CODE HOPPING RECEIVER (DECODER)



4.4 IFF Decoder Operation

In a typical IFF decoder, the key generation on the decoder side is done by reading the serial number from a token and combining that with the manufacturer's code to recreate the encoder key that is stored on the token. The decoder polls for the presence of a token. Once detected the decoder reads the serial number. If the token has been learned, the decoder sends a challenge and reads the token's response. The decoder uses the encoder key stored in EEPROM and decrypt response. The decrypt response is compared to the challenge. If they match the appropriate output is activated.

FIGURE 4-7: TYPICAL IFF DECODER OPERATION

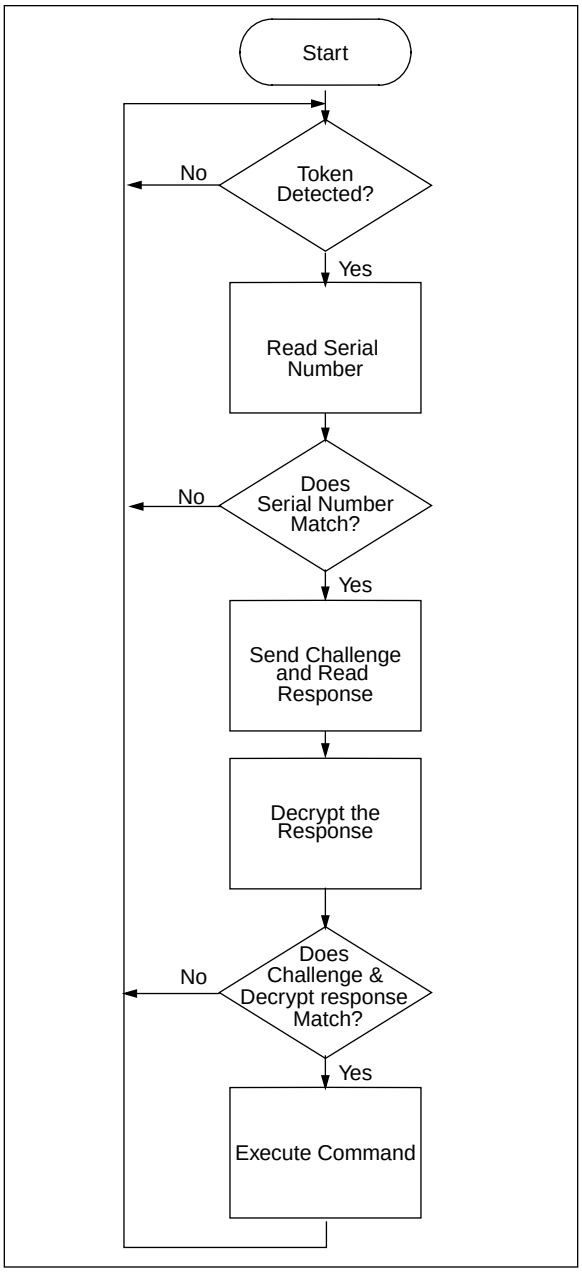
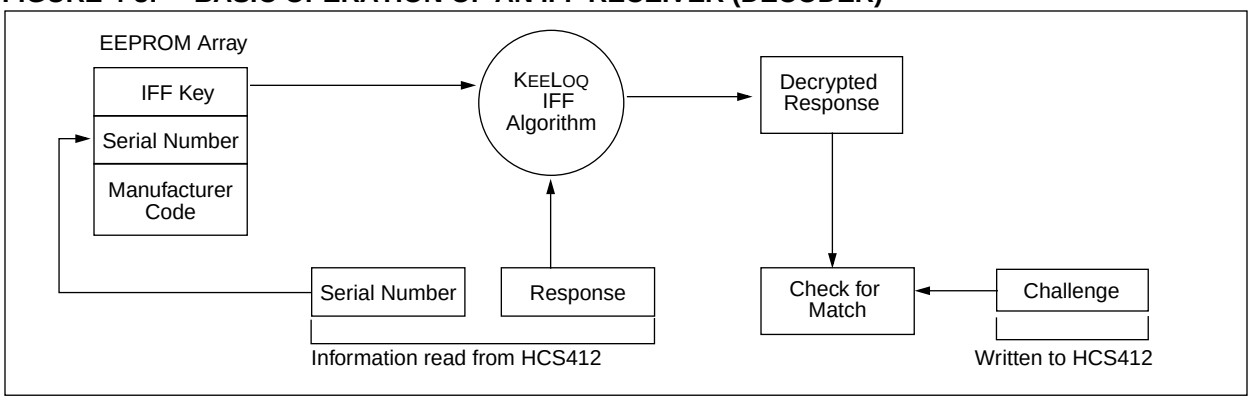


FIGURE 4-8: BASIC OPERATION OF AN IFF RECEIVER (DECODER)



5.0 ELECTRICAL CHARACTERISTICS

TABLE 5-1: ABSOLUTE MAXIMUM RATING

Symbol	Item	Rating	Units
V_{DD}	Supply voltage	-0.3 to 6.9	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 5-2: 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} < 6.6V			Unit	Conditions
		Min	Typ[1]	Max		
Average operating current[2]	I_{DD} (avg)	—	50 200	100 300	µA	V_{DD} = 3.0V V_{DD} = 6.6V
Programming current	I_{DDP}	—	1.0 2.3	2.0 4.0	mA	V_{DD} = 3.0V V_{DD} = 6.6V
Standby current	I_{DDS}	—	0.1	100	nA	LC = off else < 5µA
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} = 6.6V, 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} = 6.6V,I_{OH} = 5mA
LED output current	I_{LED}	3.0	4.0	7.0	mA	V_{DD} = 3.0V, V_{LED} = 1.5V
Switch input resistor	RS	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	*f*c	—	0.125	13.6	MHz	
External LC Inductor value	L	—	900	—	µH	
External LC Capacitor value	C	—	1.8	—	nF	

Note 1: Typical values at 25°C.
2: No load connected.
3: LC inputs are clamped at 10 volts.

FIGURE 5-1: POWER UP AND TRANSMIT TIMING

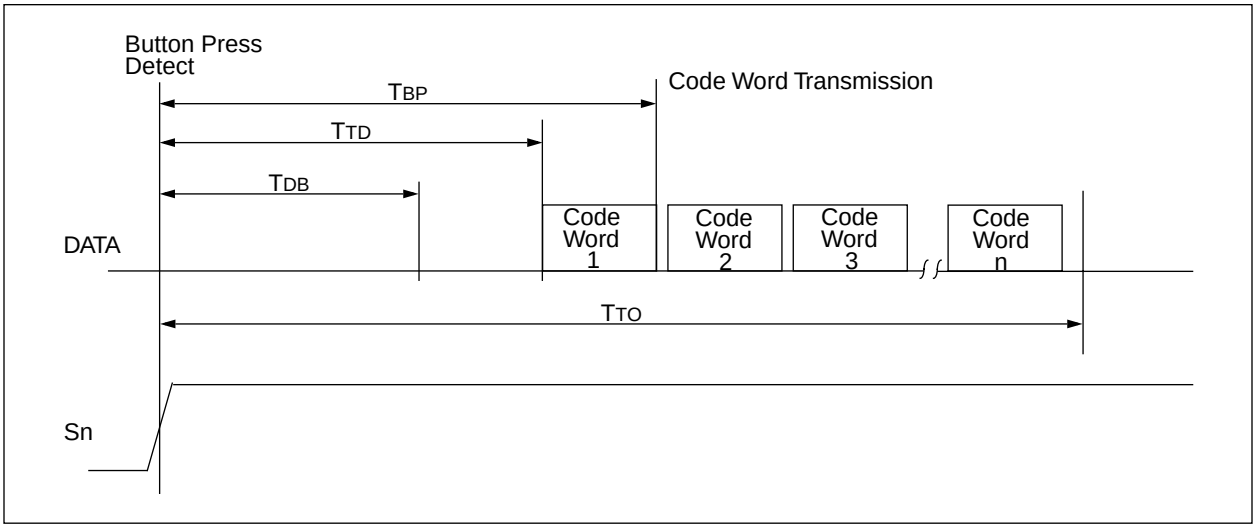


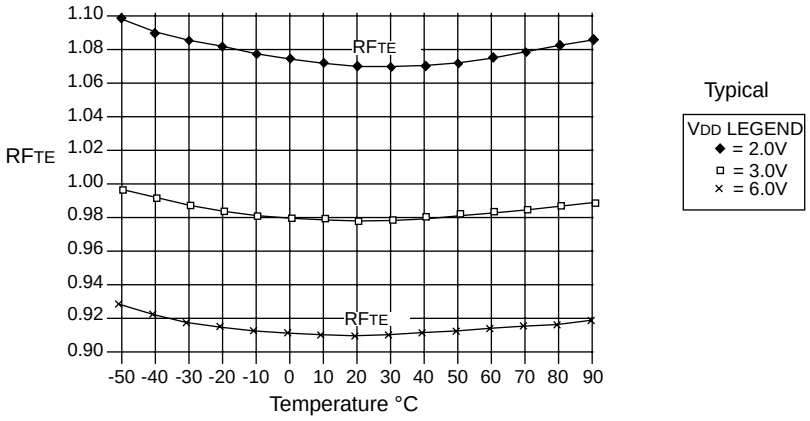
TABLE 5-3: POWER UP AND TRANSMIT TIMING REQUIREMENTS

VDD = +2.0 to 6.6V
Commercial (C): TAMB = 0°C to +70°C
Industrial (I): TAMB = -40°C to +85°C

Parameter	Symbol	Min	Typ.	Max	Unit	Remarks
Time to second button press	TBP	44 + Code Word Time	58 + Code Word Time	63 + Code Word Time	ms	(Note 1)
Transmit delay from button detect	TTD	39	44	48	ms	(Note 2)
Debounce delay on button press	TDBP	31	35	39	ms	
Debounce delay on button release	TDBR		30		ms	
Auto-shutoff time-out period	TTO	18	20	22	s	(Note 3)
Long preamble	TLPRE		64.4		ms	
LED on time	TLEDON		32		ms	(Note 4)
LED off time	TLEDOFF		480		ms	(Note 4)
LED on time	TLEDL		200		ms	(Note 5)
Time to delayed SEED transmission	TDSD		3		s	

Note 1: TBP is the time in which a second button can be pressed without completion of the first code word and the intention was to press the combination of buttons.
2: Transmit delay maximum value if the previous transmission was successfully transmitted.
3: The auto-shutoff timeout period is not tested.
4: The LED times specified for VDD > VTRIP specified by VLOW in the configuration word.
5: LED on time if VDD < VTRIP specified by VLOW in the configuration word.

FIGURE 5-2: HCS412 NORMALIZED RFTE VS. TEMP



Note: Values are for calibrated oscillator.

TABLE 5-4: CODE WORD TRANSMISSION TIMING PARAMETERS—PWM MODE

VDD = +2.0V to 6.6V Commercial (C): TAMB = 0°C to +70°C Industrial (I): TAMB = -40°C to +85°C			**Code Words Transmitted**							
			RFBSL1 = 1, RFBSL0 = 0				**RFBSL1 = 0, RFBSL0 = 1**			
Symbol	**Characteristic**	**Number of RFTE**	**Min.**	**Typ.**	**Max.**	**Number of RFTE**	**Min.**	**Typ.**	**Max.**	**Units**
RFTE	Basic pulse element	1	360	400	440	1	180.0	200.0	220.0	µs
TBP	DATA bit pulse width	3	1080	1200	1320	3	540.0	600.0	660.0	µs
TP	Preamble duration	32	12	12.8	14	32	5.76	6.0	7.04	ms
TH	Header duration	10	3.6	4.0	4.4	10	1.80	2.0	2.20	ms
THOP	Code hopping duration	96	35	38.4	42	96	17.28	19.20	21.12	ms
TFIX	Fixed code duration	111	39.96	44.4	48.84	111	19.98	22.20	24.42	ms
TG	Guard time	46	16.6	18.4	20.2	46	8.3	9.6	10.1	ms
—	Total transmit time	295	106.2	118.0	129.8	295	53.1	59.0	64.9	ms

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

VDD = +2.0V to 6.6V Commercial (C): TAMB = 0°C to +70°C Industrial (I): TAMB = -40°C to +85°C			**Code Words Transmitted**							
			RFBSL1 = 1, RFBSL0 = 0				**RFBSL1 = 0, RFBSL0 = 1**			
Symbol	**Characteristic**	**Number of RFTE**	**Min.**	**Typ.**	**Max.**	**Number of RFTE**	**Min.**	**Typ.**	**Max.**	**Units**
RFTE	Basic pulse element	1	180.0	200.0	220.0	1	90.0	100.0	110.0	µs
TBP	DATA bit pulse width	3	540.0	600.0	660.0	3	270.0	300.0	330.0	µs
TP	Preamble duration	32	5.76	6.0	7.04	32	2.88	3.0	3.52	ms
TH	Header duration	10	1.80	2.0	2.20	10	0.90	1.0	1.10	ms
THOP	Code hopping duration	96	17.28	19.20	21.12	96	8.64	9.60	10.56	ms
TFIX	Fixed code duration	111	19.98	22.2	24.42	111	9.99	11.1	12.21	ms
TG	Guard time	46	8.3	9.6	10.1	46	41	4.6	5.1	ms
—	Total transmit time	295	53.1	59.0	64.9	295	26.6	29.5	32.5	ms

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

TABLE 5-5: CODE WORD TRANSMISSION TIMING PARAMETERS—MANCHESTER MODE

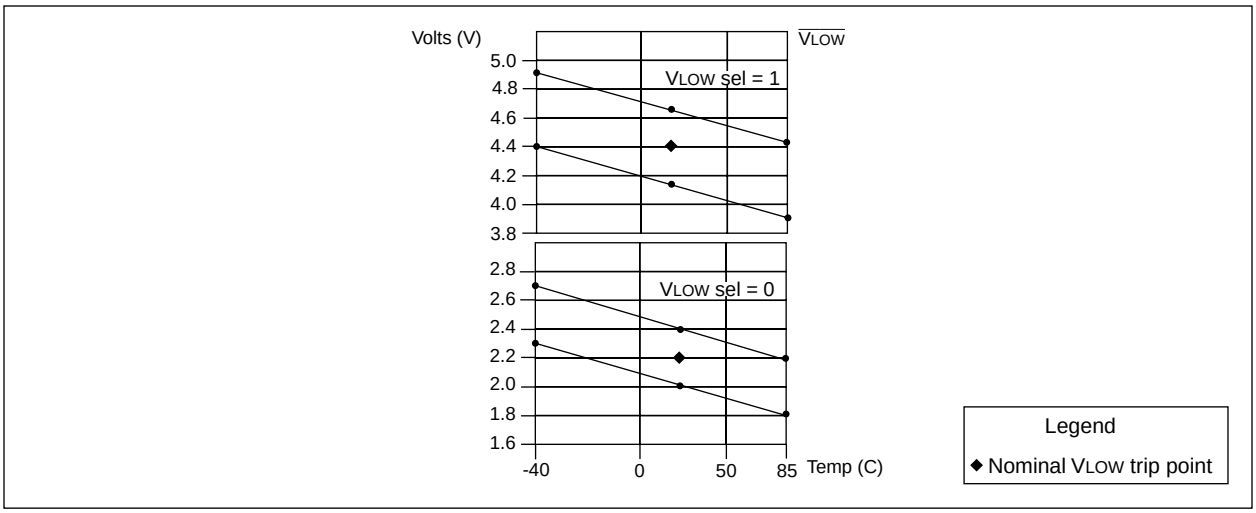
V_{DD} = +2.0V to 6.6V Commercial (C): T_{AMB} = 0°C to +70°C Industrial (I): T_{AMB} = -40°C to +85°C			Code Words Transmitted							
			RFBSL1 = 0, RFBSL0 = 0				RFBSL1 = 0, RFBSL0 = 1			
Symbol	**Characteristic**	**Number of RF_{TE}**	**Min.**	**Typ.**	**Max.**	**Number of RF_{TE}**	**Min.**	**Typ.**	**Max.**	**Units**
RF_{TE}	Basic pulse element	1	720.0	800.0	880.0	1	360.0	400.0	440.0	µs
T_P	Preamble duration	32	23.04	25.60	28.16	32	11.52	12.80	14.08	ms
T_H	Header duration	4	2.88	3.20	3.52	4	1.44	1.60	1.76	ms
T_{START}	Start bit	2	1.44	1.60	1.76	2	0.72	0.80	0.88	ms
T_{HOP}	Code hopping duration	64	46.08	51.20	56.32	64	23.04	25.60	28.16	ms
T_{FIX}	Fixed code duration	74	53.28	59.20	65.12	74	26.64	29.60	32.56	ms
T_{STOP}	Stop bit	2	1.44	1.60	1.76	2	0.72	0.80	0.88	ms
T_G	Guard time	31	23.0	25.6	28.2	31	11.5	12.8	14.1	ms
—	Total transmit time	209	151.2	168	184.8	209	75.6	84.0	92.4	ms

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

V_{DD} = +2.0V to 6.6V Commercial (C): T_{AMB} = 0°C to +70°C Industrial (I): T_{AMB} = -40°C to +85°C			Code Words Transmitted							
			RFBSL1 = 1, RFBSL0 = 0				RFBSL1 = 1, RFBSL0 = 1			
Symbol	**Characteristic**	**Number of RF_{TE}**	**Min.**	**Typ.**	**Max.**	**Number of RF_{TE}**	**Min.**	**Typ.**	**Max.**	**Units**
RF_{TE}	Basic pulse element	1	360.0	400.0	440.0	1	180.0	200.0	220.0	µs
T_P	Preamble duration	32	11.52	12.80	14.08	32	5.76	6.40	7.04	ms
T_H	Header duration	4	1.44	1.60	1.76	4	0.72	0.80	0.88	ms
T_{START}	Start bit	2	0.72	0.80	0.88	2	0.36	0.40	0.44	ms
T_{HOP}	Code hopping duration	64	23.04	25.60	28.16	64	11.52	12.80	14.08	ms
T_{FIX}	Fixed code duration	74	26.64	29.60	32.56	74	13.32	14.8	16.28	ms
T_{STOP}	Stop bit	2	0.72	0.80	0.88	2	0.36	0.40	0.44	ms
T_G	Guard time	31	11.5	12.8	14.1	31	5.75	6.4	7.05	ms
—	Total transmit time	209	75.6	84.0	92.4	209	37.8	42.0	46.2	ms

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

FIGURE 5-3: TYPICAL VOLTAGE TRIP POINTS



NOTES:

WORLDWIDE SALES AND SERVICE

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-786-7200 Fax: 480-786-7277
Technical Support: 480-786-7627
Web Address: http://www.microchip.com

Atlanta
Microchip Technology Inc.
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770-640-0034 Fax: 770-640-0307

Boston
Microchip Technology Inc.
5 Mount Royal Avenue
Marlborough, MA 01752
Tel: 508-480-9990 Fax: 508-480-8575

Chicago
Microchip Technology Inc.
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

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

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

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

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

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

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

AMERICAS (continued)

Toronto
Microchip Technology Inc.
5925 Airport Road, Suite 200
Mississauga, Ontario L4V 1W1, Canada
Tel: 905-405-6279 Fax: 905-405-6253

ASIA/PACIFIC

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

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

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

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

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

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

ASIA/PACIFIC (continued)

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

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

EUROPE

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

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

France
Arizona Microchip Technology SARL
Parc d'Activite du Moulin de Massy
43 Rue du Saule Trapu
Batiment A - ler Etage
91300 Massy, France
Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany
Arizona Microchip Technology GmbH
Gustav-Heinemann-Ring 125
D-81739 München, Germany
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

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

11/15/99

DNV Certification, Inc. USA — ANSI-RAB QMS ACCREDITED — DNV — DNV MSC The Netherlands Accredited by the RvA
ISO 9001 / QS-9000 REGISTERED FIRM

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