

KEELOQ[®] Code Hopping Encoder

FEATURES

Security

- Programmable 28-bit serial number
- Programmable 64-bit encryption key
- Each transmission is unique
- 66-bit transmission code length
- 32-bit hopping code
- 34-bit fixed code (28-bit serial number, 4-bit button code, 2-bit status)
- Encryption keys are read protected

Operating

- 3.5V-13V operation (2.0V min. using the Step up feature)
- Three button inputs
- 7 functions available
- Selectable baud rate
- Automatic code word completion
- Battery low signal transmitted to receiver
- Non-volatile synchronization data

Other

- Simple programming interface
- On-chip EEPROM
- On-chip oscillator and timing components
- Button inputs have internal pull-down resistors
- Minimum component count
- Synchronous Transmission mode
- Built-in step up regulator

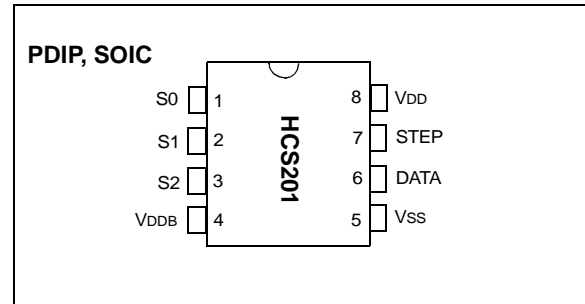
Typical Applications

- The HCS201 is ideal for Remote Keyless Entry (RKE) applications. These applications include:
- Automotive RKE systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Identity tokens
- Burglar alarm systems

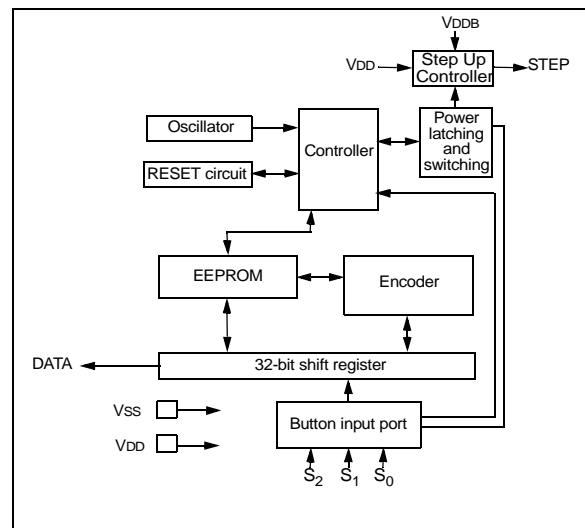
DESCRIPTION

The HCS201 from Microchip Technology Inc. is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS201 utilizes the KEELOQ code hopping technology, incorporating high security, a small package outline and low cost. The HCS201 is a perfect solution for unidirectional remote keyless entry systems and access control systems.

PACKAGE TYPES



HCS201 BLOCK DIAGRAM



The HCS201 combines a 32-bit hopping code, generated by a nonlinear encryption algorithm, with a 28-bit serial number and 6 information bits to create a 66-bit code word. The code word length eliminates the threat of code scanning and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend schemes useless.

The crypt key, serial number and configuration data are stored in an EEPROM array which is not accessible via any external connection. The EEPROM data is programmable but read-protected. The data can be verified only after an automatic erase and programming operation. This protects against attempts to gain access to keys or manipulate synchronization values. The HCS201 provides an easy-to-use serial interface for programming the necessary keys, system parameters and configuration data.

1.0 SYSTEM OVERVIEW

Key Terms

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

- **RKE** - Remote Keyless Entry
- **Button Status** - Indicates what button input(s) activated the transmission. Encompasses the 4 button status bits S3, S2, S1 and S0 (Figure 4-2).
- **Code Hopping** - A method by which a code, viewed externally to the system, appears to change unpredictably each time it is transmitted.
- **Code word** - A block of data that is repeatedly transmitted upon button activation (Figure 4-1).
- **Transmission** - A data stream consisting of repeating code words (Figure 8-1).
- **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.
- **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. 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.

The HCS201 code hopping encoder is designed specifically for keyless entry systems; primarily vehicles and home garage door openers. The encoder portion of a keyless entry system is integrated into a transmitter, carried by the user and operated to gain access to a vehicle or restricted area. The HCS201 is meant to be a cost-effective yet secure solution to such systems, requiring very few external components (Figure 2-1).

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.

The HCS201, on the other hand, employs the KEELOQ code hopping technology coupled with a transmission length of 66 bits to virtually eliminate the use of code 'grabbing' or code 'scanning'. The high security level of the HCS201 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, the next

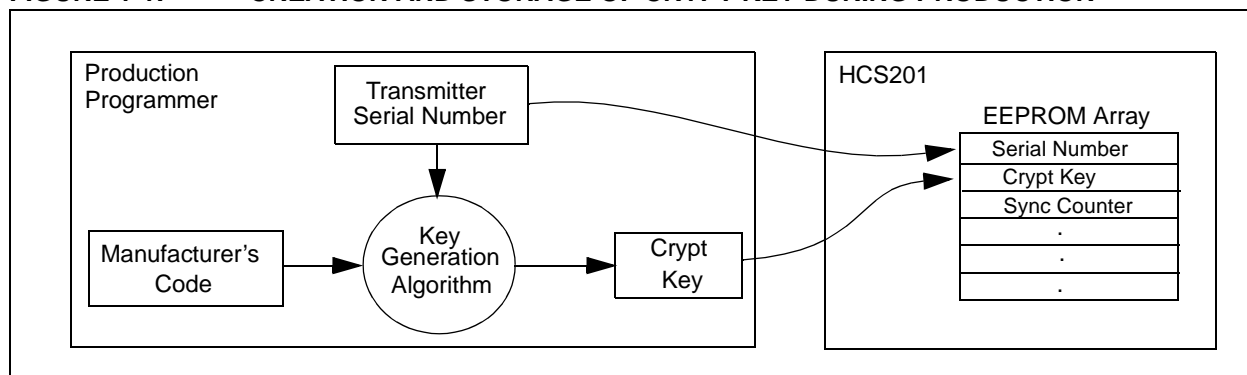
coded transmission will be completely different. Statistically, if only one bit in the 32-bit string of information changes, greater than 50 percent of the coded transmission bits will change.

As indicated in the block diagram on page one, the HCS201 has a small EEPROM array which must be loaded with several parameters before use; most often programmed by the manufacturer at the time of production. The most important of these are:

- A 28-bit serial number, typically unique for every encoder
- A crypt key
- An initial 16-bit synchronization value
- A 16-bit configuration value

The crypt key generation typically inputs the transmitter serial number and 64-bit manufacturer's code into the key generation algorithm (Figure 1-2). The manufacturer's code is chosen by the system manufacturer and must be carefully controlled as it is a pivotal part of the overall system security.

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



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. Due to the code hopping algorithm's complexity, each increment of the synchronization value results in greater than 50% of the bits changing in the transmitted code word.

Figure 1-2 shows how the key values in EEPROM are used in the encoder. Once the encoder 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 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 4.0.

A receiver may use any type of controller as a decoder, but it is typically a microcontroller with compatible firmware that allows the decoder to operate in conjunction with an HCS201 based transmitter. Section 7.0 provides detail on integrating the HCS201 into a system.

A transmitter must first be 'learned' by the receiver before its use is allowed in the system. Learning includes 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.

In normal operation, each received message of valid format is evaluated. The serial number is used to determine if it is from a learned transmitter. If from a learned transmitter, the message is decrypted and the synchronization counter is verified. Finally, the button status is checked to see what operation is requested. Figure 1-3 shows the relationship between some of the values stored by the receiver and the values received from the transmitter.

FIGURE 1-2: BUILDING THE TRANSMITTED CODE WORD (ENCODER)

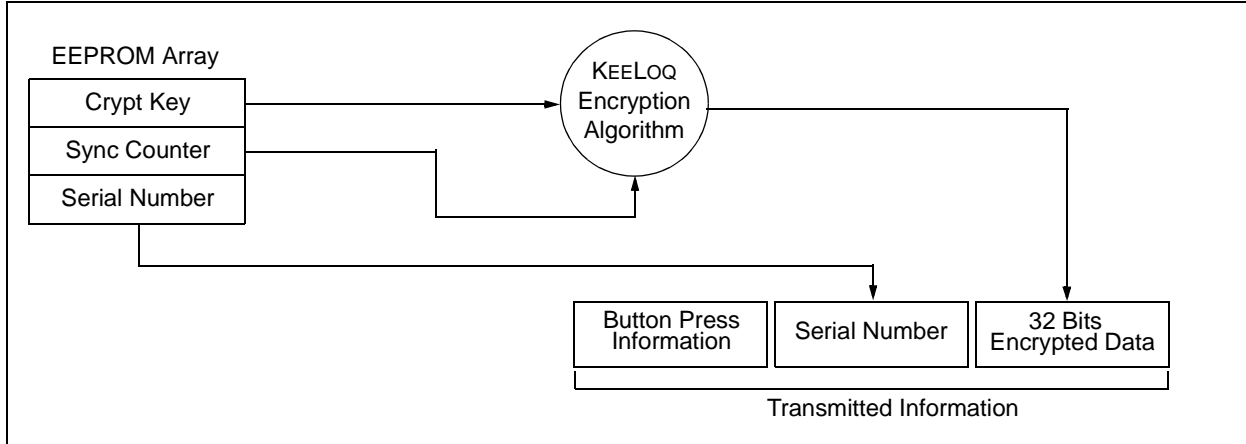
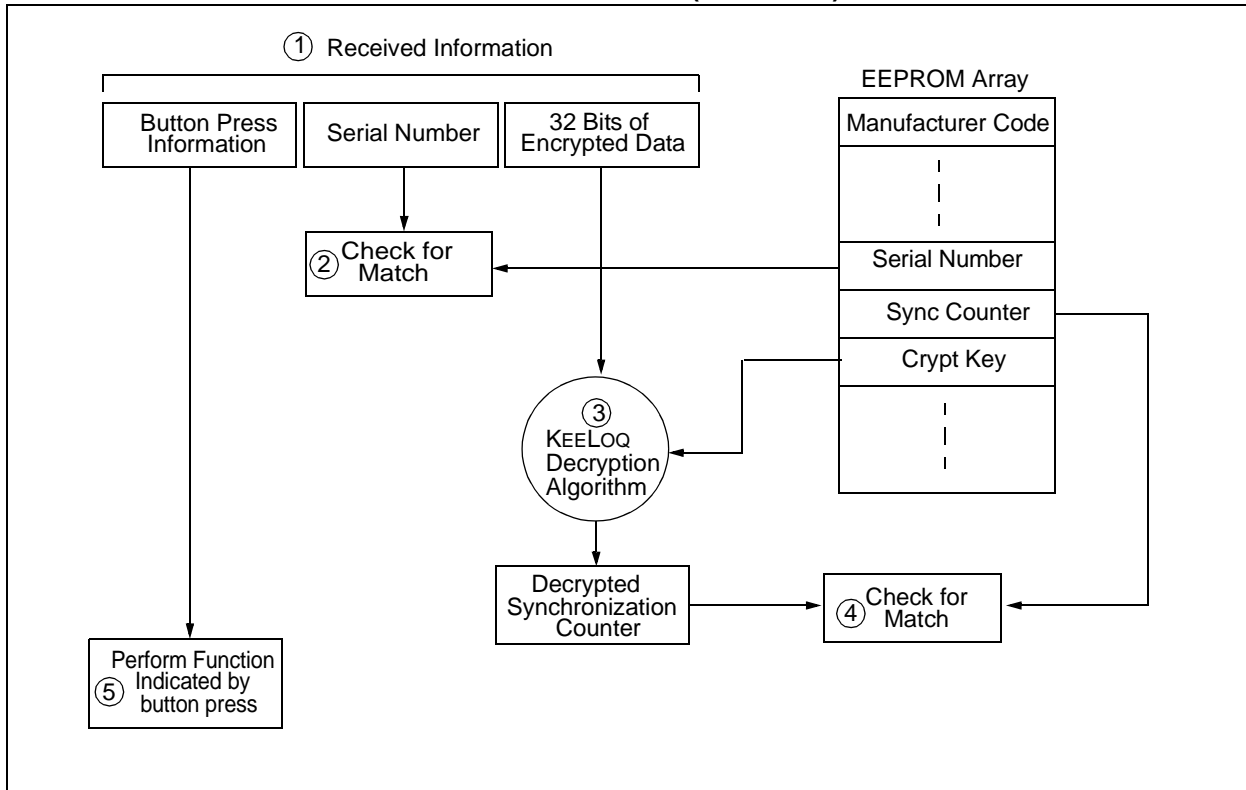


FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



NOTE: Circled numbers indicate the order of execution.

2.0 ENCODER OPERATION

As shown in the typical application circuits (Figure 2-1), the HCS201 is a simple device to use. It requires only the addition of buttons and RF circuitry for use as the transmitter in your security application. A description of each pin is given in Table 2-1.

FIGURE 2-1: TYPICAL CIRCUITS

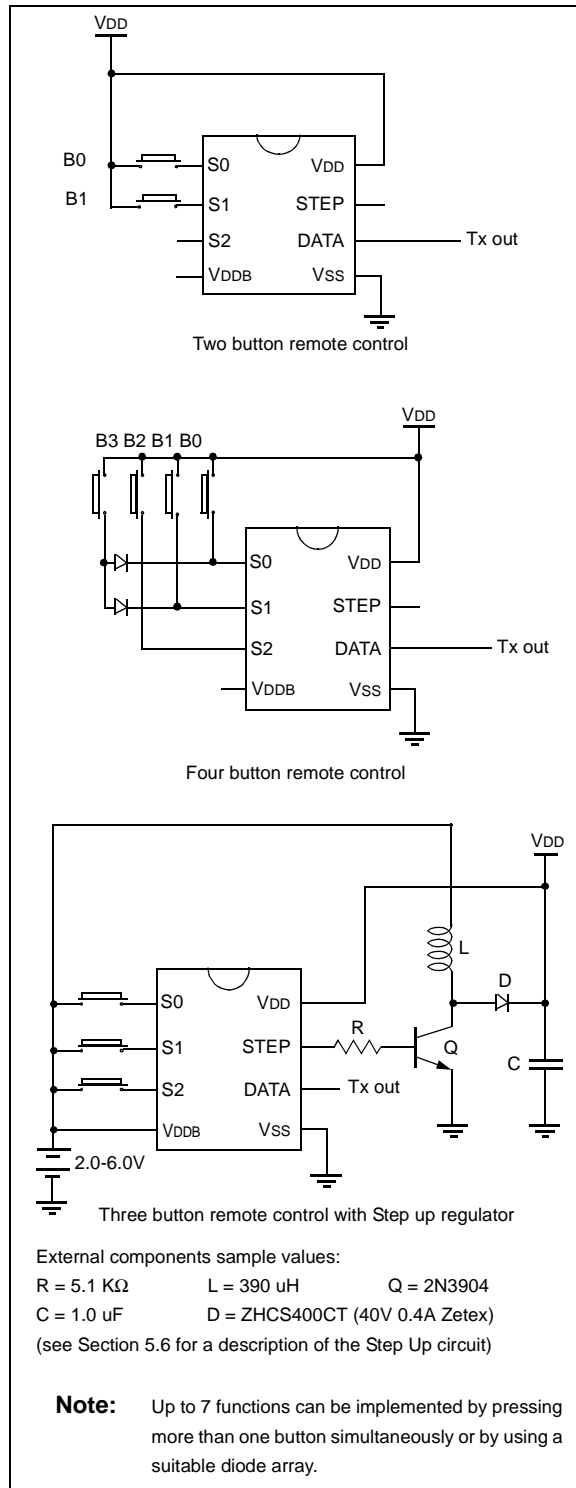


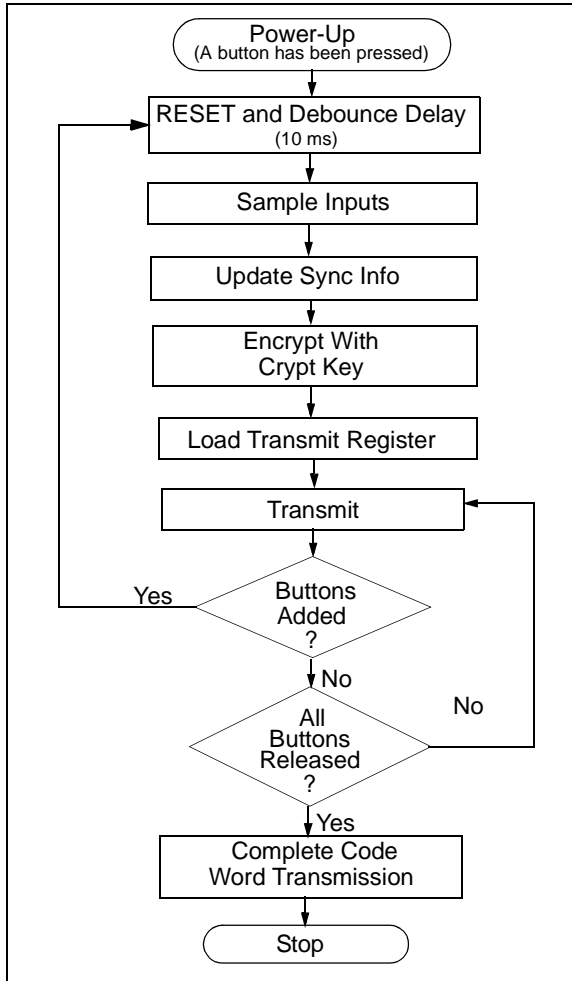
TABLE 2-1: PIN DESCRIPTIONS

Pin Name	Pin Number	Pin Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2 / Clock pin for Programming mode
VDDDB	4	Battery input pin, supplies power to the step up control circuitry
VSS	5	Ground reference connection
DATA	6	Pulse Width Modulation (PWM) output pin / Data pin for Programming mode
STEP	7	Step up regulator switch control
VDD	8	Positive supply voltage

The HCS201 will wake-up upon detecting a button press and delay approximately 10 ms for button debounce (Figure 2-2). The synchronization counter, discrimination value and button information will be encrypted to form the hopping code. The hopping code portion will change every transmission, even if the same button is pushed again. A code word that has been transmitted will not repeat for more than 64K transmissions. This provides more than 18 years of use before a code is repeated; based on 10 operations per day. Overflow information sent from the encoder can be used to extend the number of unique transmissions to more than 192K.

If in the transmit process it is detected that a new button(s) has been pressed, a RESET will immediately occur and the current 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 code word will be completed and the power-down will occur.

FIGURE 2-2: ENCODER OPERATION



3.0 EEPROM MEMORY ORGANIZATION

The HCS201 contains 192 bits (12 x 16-bit words) of EEPROM memory (Table 3-1). This EEPROM array is used to store the encryption key information, synchronization value, etc. Further descriptions of the memory array is given in the following sections.

TABLE 3-1: EEPROM MEMORY MAP

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

3.1 KEY_0 - KEY_3 (64-Bit Crypt Key)

The 64-bit crypt key is used to create the encrypted message transmitted to the receiver. This key is calculated and programmed during production using a key generation algorithm. The key generation algorithm may be different from the KEELOQ algorithm. Inputs to the key generation algorithm are typically the transmitter's serial number and the 64-bit manufacturer's code. While the key generation algorithm supplied from Microchip is the typical method used, a user may elect to create their own method of key generation. This may be done providing that the decoder is programmed with the same means of creating the key for decryption purposes.

3.2 SYNC (Synchronization Counter)

This is the 16-bit synchronization value that is used to create the hopping code for transmission. This value will increment after every transmission.

3.3 Reserved

Must be initialized to 0000H.

3.4 SER_0, SER_1 (Encoder Serial Number)

SER_0 and SER_1 are the lower and upper words of the device serial number, respectively. Although there are 32 bits allocated for the serial number, only the lower order 28 bits are transmitted. The serial number is meant to be unique for every transmitter.

3.5 SEED_0, SEED_1 (Seed Word)

The 2-word (32-bit) seed code will be transmitted when all three buttons are pressed at the same time (see Figure 4-2). 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.

TABLE 3-2: DISCRIMINATION WORD

Bit Number	Bit Description
0	Discrimination Bit 0
1	Discrimination Bit 1
2	Discrimination Bit 2
3	Discrimination Bit 3
4	Discrimination Bit 4
5	Discrimination Bit 5
6	Discrimination Bit 6
7	Discrimination Bit 7
8	Discrimination Bit 8
9	Discrimination Bit 9
10	Discrimination Bit 10
11	Discrimination Bit 11
12	Not Used
13	Not Used
14	Not Used
15	Not Used

3.6 DISC (Discrimination Word)

The discrimination value aids the post-decryption check on the decoder end. It may be any value, but in a typical system it will be programmed as the 12 Least Significant bits of the serial number. Values other than this must be separately stored by the receiver when a transmitter is learned. The discrimination bits are part of the information that form the encrypted portion of the transmission (Figure 4-2). 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 as the 12 LSb's of the

serial number then it may merely be compared to the respective bits of the received serial number; saving EEPROM space.

3.7 CONFIG (Configuration Word)

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

TABLE 3-3: CONFIGURATION WORD

Bit Number	Bit Name
0	OSC0
1	OSC1
2	OSC2
3	OSC3
4	VLOWS
5	BRS
6	MTX4
7	TXEN
8	S3SET
9	XSER
10	Not Used
11	Not Used
12	Not Used
13	Not Used
14	Not Used
15	Not Used

3.7.1 OSCILLATOR TUNING BITS (OSC0 AND OSC3)

These bits are used to tune the frequency of the HCS201 internal clock oscillator to within $\pm 10\%$ of its nominal value over temperature and voltage.

3.7.2 LOW VOLTAGE TRIP POINT SELECT (VLOWS)

The low voltage trip point select bit (VLOWS) and the S3 setting bit (S3SET) are used to determine when to send the VLOW signal to the receiver.

TABLE 3-4: TRIP POINT SELECT

VLOWS	S3SET*	Trip Point
0	0	4.4
0	1	4.4
1	0	9
1	1	6.75

* See also Section 3.7.6

3.7.3 BAUD RATE SELECT BITS (BRS)

BRS selects the speed of transmission and the code word blanking. Table 3-5 shows how the bit is used to select the different baud rates and Section 5.5 provides detailed explanation in code word blanking.

TABLE 3-5: BAUDRATE SELECT

BRS	Basic Pulse Element	Code Words Transmitted
0	400 μ s	All
1	200 μ s	1 out of 2

3.7.4 MINIMUM FOUR TRANSMISSIONS (MTX4)

If this bit is cleared, only one code is completed if the HCS201 is activated. If this bit is set, at least four complete code words are transmitted, even if code word blanking is enabled.

3.7.5 TRANSMIT PULSE ENABLE (TXEN)

If this bit is cleared, no transmission pulse is transmitted before a transmission. If the bit is set, a START pulse (1 TE long) is transmitted after button de-bouncing, before the preamble of the first code word.

3.7.6 S3 SETTING (S3SET)

This bit determines the value of S3 in the function code during a transmission and the high trip point selected by VLOWS in section 3.6.2. If this bit is cleared, S3 mirrors S2 during a transmission. If the S3SET bit is set, S3 in the function code (Button Status) is always set, independent of the value of S2.

3.7.7 EXTENDED SERIAL NUMBER (XSER)

If this bit is set, a long 32-bit Serial Number is transmitted. If this bit is cleared, a standard 28-bit Serial Number is transmitted followed by 4 bits of the function code (Button Status).

4.0 TRANSMITTED WORD

4.1 Code Word Format

The HCS201 code word is made up of several parts (Figure 4-1). Each code word contains a 50% duty cycle preamble, a header, 32 bits of encrypted data and 34 bits of fixed data followed by a guard period before another code word can begin. Refer to Table 8-4 for code word timing.

4.2 Code Word Organization

The HCS201 transmits a 66-bit code word when a button is pressed. The 66-bit word is constructed from a Fixed Code portion and an Encrypted Code portion (Figure 4-2).

The 32 bits of **Encrypted Data** are generated from 4 button bits, 12 discrimination bits and the 16-bit sync value. The encrypted portion alone provides up to four billion changing code combinations.

The 34 bits of **Fixed Code Data** are made up of 2 status bits, 4 button bits and the 28-bit serial number. The fixed and encrypted sections combined increase the number of code combinations to 7.38×10^{19} .

FIGURE 4-1: CODE WORD FORMAT

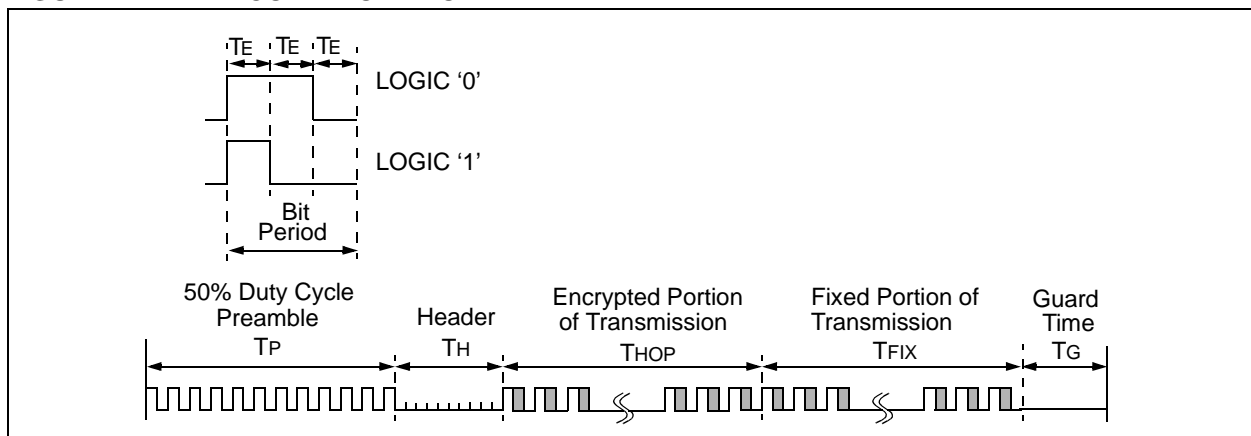
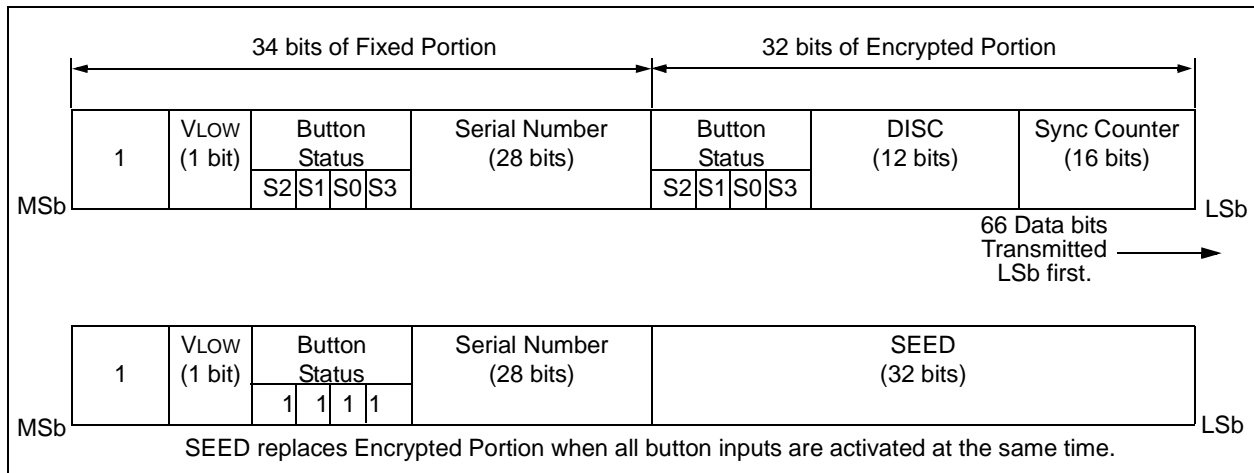


FIGURE 4-2: CODE WORD ORGANIZATION



4.3 Synchronous Transmission Mode

Synchronous Transmission mode can be used to clock the code word out using an external clock.

To enter Synchronous Transmission mode, the Programming mode start-up sequence must be executed as shown in Figure 4-3. If either S1 or S0 is set on the falling edge of S2 (or S3), the device enters Synchronous Transmission mode. In this mode, it functions as a normal transmitter, with the exception that the timing of the PWM data string is controlled externally and 16 extra bits are transmitted at the end with the code word.

The button code will be the S0, S1 value at the falling edge of S2 or S3. The timing of the PWM data string is controlled by supplying a clock on S2 or S3 and should not exceed 20 kHz. The code word is the same as in PWM mode with 16 reserved bits at the end of the word. The reserved bits can be ignored. When in Synchronous Transmission mode S2 or S3 should not be toggled until all internal processing has been completed as shown in Figure 4-4.

FIGURE 4-3: SYNCHRONOUS TRANSMISSION MODE (TXEN=0)

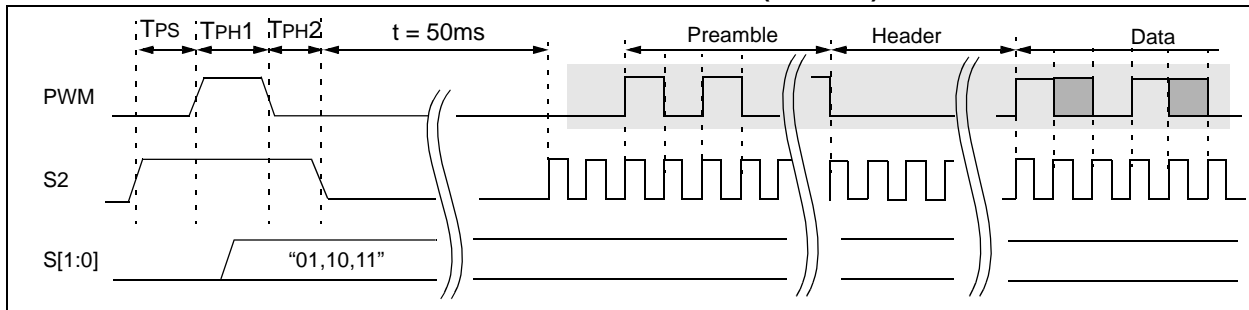
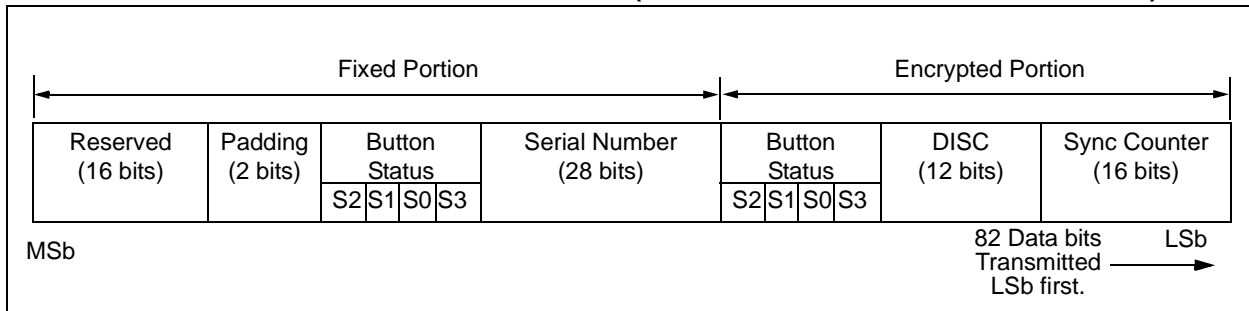


FIGURE 4-4: CODE WORD ORGANIZATION (SYNCHRONOUS TRANSMISSION MODE)



5.0 SPECIAL FEATURES

5.1 Code Word Completion

The code word completion feature ensures that entire code words are transmitted, even if the button is released before the code word is complete. If the button is held down beyond the time for one code word, multiple code words will result. If another button is activated during a transmission, the active transmission will be aborted and a new transmission will begin using the new button information.

5.2 VLOW: Voltage LOW Indicator

The VLOW bit is transmitted with every transmission (Figure 8-4) and will be transmitted as a one if the operating voltage has dropped below the low voltage trip point. The trip point is selectable based on the battery voltage being used. See Section 3.7.2 for a description of how the low voltage select option is set. This VLOW signal is transmitted so the receiver can give an audible signal to the user that the transmitter battery is low.

5.3 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 T_{TO}.

5.4 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 learn function. This can be done by utilizing the seed value stored in EEPROM, transmitted only when all three button inputs are pressed at the same time (Table 5-1). Instead of the normal key generation inputs being used to create the crypt key, this seed value is used.

TABLE 5-1: PIN ACTIVATION TABLE

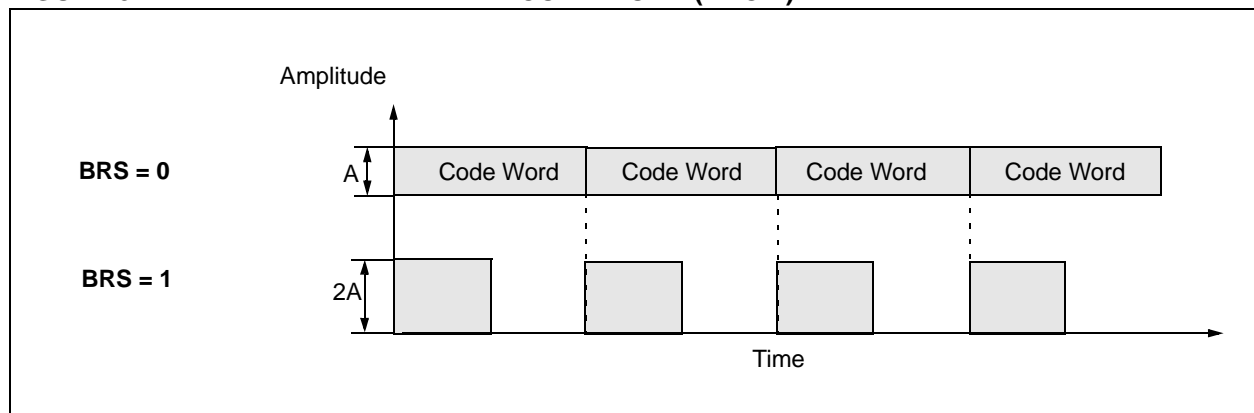
	Function	S2	S1	S0
Standby	0	0	0	0
Hopping Code	1	0	0	1
	2	0	1	0
	-	-	-	-
	5	1	0	1
	6	1	1	0
Seed Code	7	1	1	1

5.5 Blank Alternate Code Word

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 duty cycle of the individual bits as well as by blanking out consecutive code words. Blank Alternate Code Word (BACW) may be used to reduce the average power of a transmission by transmitting only every second code word (Figure 5-1). This is a selectable feature that is determined in conjunction with the baud rate selection bit BSL0.

Enabling the BACW option may likewise allow the user to transmit a higher amplitude transmission as the time averaged power is reduced. BACW 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 5-1: BLANK ALTERNATE CODE WORD (BACW)



HCS201

5.6 Step Up Regulator

The integrated Step Up regulator can be used to ensure the power supply voltage to the encoder and the RF circuit (VDD), is constant independent of what the battery voltage is (VDDb). Input on VDD pin is compared to VSTEP, the internal reference voltage. If VDD falls below this voltage the STEP output is pulsed at fSTEP. This output can be connected to an external circuit as illustrated in Figure 5-2, to provide a step up voltage on the device.

The Step Up regulator is inactive when the device is not transmitting.

Note: Power to the Step up regulator is taken from the VDDb pin. While VDD is limited to a 3.5V minimum, VDDb minimum can be as low as 2.0V for the Step Up circuit to start operating.

FIGURE 5-2: APPLICATION CIRCUIT

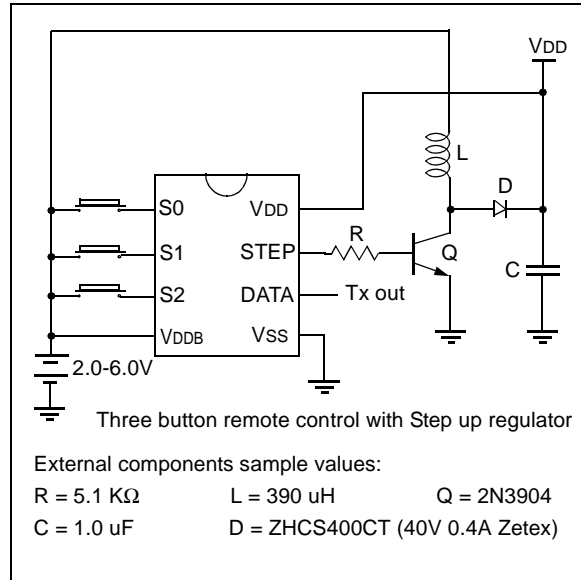
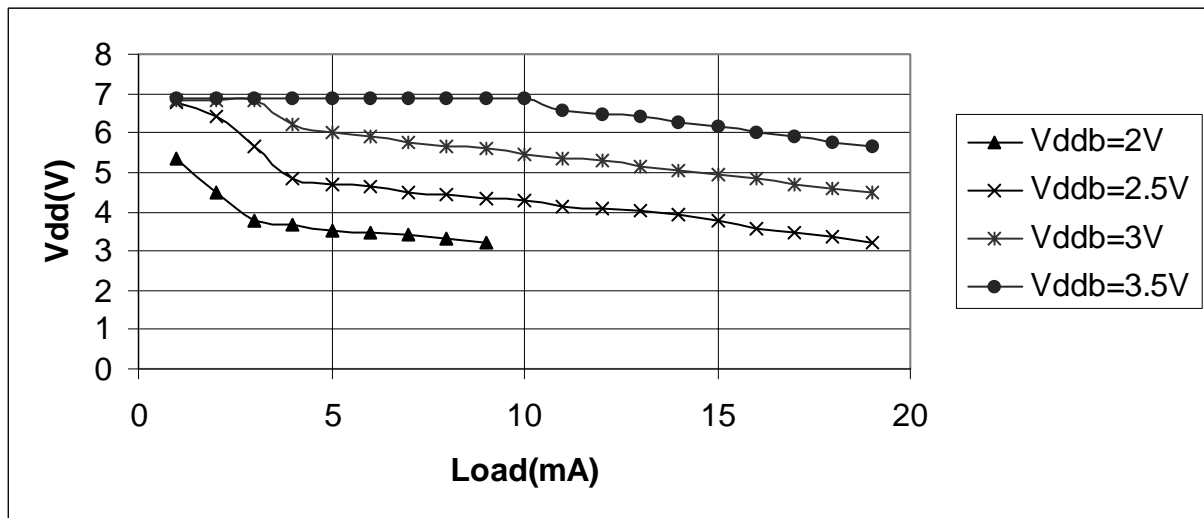


FIGURE 5-3: TYPICAL LOADING CURVES (FIGURE 5-2 CIRCUIT)



Note: These are typical values not tested in production.

TABLE 5-2: STEP UP CIRCUIT CHARACTERISTICS

Symbol	Parameters	Min.	Typ.	Max.	Units	Conditions
fSTEP	Output frequency	125	200	250	kHz	
VSTEP	Reference voltage	5.5	6.5	7.5	V	VDDb = 3V

Note: These parameters are characterized but not tested.

6.0 PROGRAMMING THE HCS201

When using the HCS201 in a system, the user will have to program some parameters into the device including the serial number and the secret key before it can be used. The programming cycle allows the user to input all 192 bits in a serial data stream, which are then stored internally in EEPROM. Programming will be initiated by forcing the DATA line high, after the S2 line has been held high for the appropriate length of time line (Table 6-1 and Figure 6-1). After the Program mode is entered, a delay must be provided to the device for the automatic bulk write cycle to complete. This will write all locations in the EEPROM to an all zeros pattern. The device can then be programmed by clocking in 16 bits at a time, using S2 as the clock line and DATA as the data in line. After each 16-bit word is loaded, a programming delay is required for the internal program cycle to complete. This delay can take up to

Twc. After every 16-bit word is written to the HCS201, the HCS201 will signal that the write is complete by sending out a train of ACK pulses, TACKH high, TACKL low (if the oscillator was perfectly tuned) on DATA. These will continue until S2 is dropped. The first pulse's width should NOT be used for calibration. At the end of the programming cycle, the device can be verified (Figure 6-2) by reading back the EEPROM. Reading is done by clocking the S2 line and reading the data bits on DATA. For security reasons, it is not possible to execute a verify function without first programming the EEPROM. **A Verify operation can only be done once, immediately following the Program cycle.**

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

FIGURE 6-1: PROGRAMMING WAVEFORMS

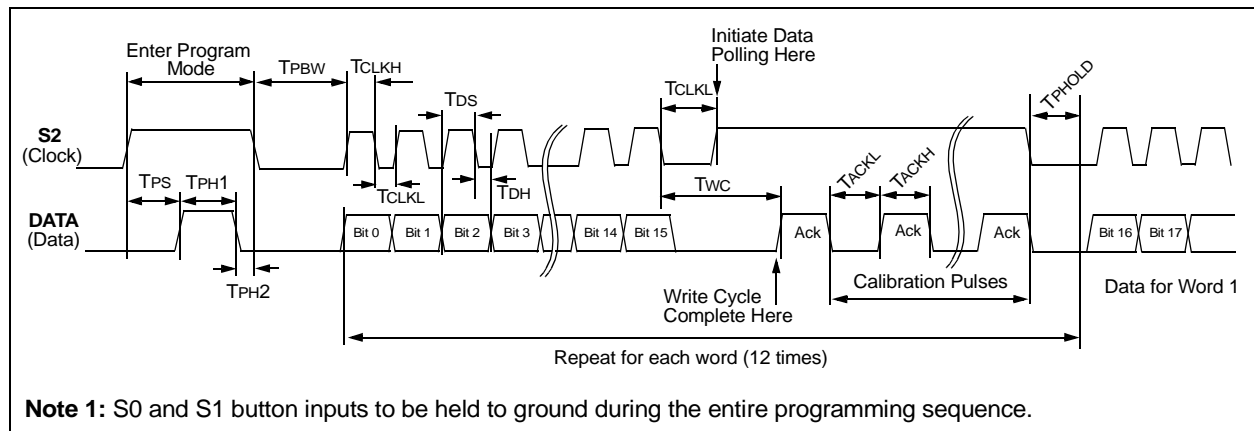
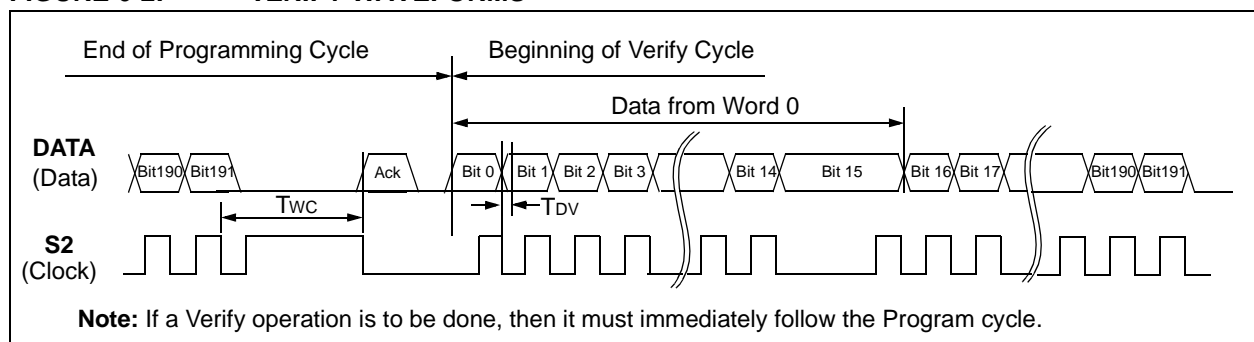


FIGURE 6-2: VERIFY WAVEFORMS



HCS201

TABLE 6-1: PROGRAMMING/VERIFY TIMING REQUIREMENTS

VDD = 5.0V ± 10%, 25° C ± 5 °C				
Parameter	Symbol	Min.	Max.	Units
Program mode setup time	TPS	2	5.0	ms
Hold time 1	TPH1	4.0	—	ms
Hold time 2	TPH2	50	—	μs
Bulk Write time	TPBW	4.0	—	ms
Program delay time	T _{PROG}	4.0	—	ms
Program cycle time	TWC	50	—	ms
Clock low time	TCLKL	50	—	μs
Clock high time	TCLKH	50	—	μs
Data setup time	TDS	0	—	μs
Data hold time	TDH	18	—	μs
Data out valid time	TDV	—	30	μs
Hold time	TPHOLD	100	—	μs
Acknowledge low time	TACKL	800	—	μs
Acknowledge high time	TACKH	800	—	μs

7.0 INTEGRATING THE HCS201 INTO A SYSTEM

Use of the HCS201 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a license agreement) firmware routines that accept transmissions from the HCS201 and decrypt the hopping code portion of the data stream. These routines provide system designers the means to develop their own decoding system.

7.1 Learning a Transmitter to a Receiver

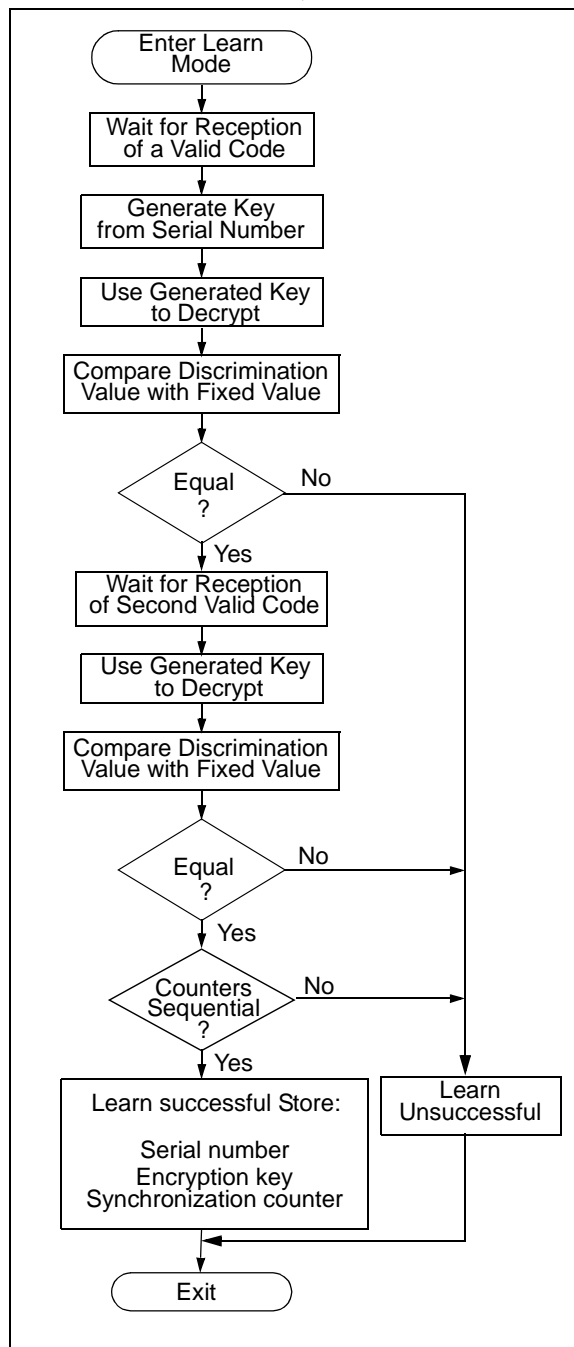
A transmitter must first be 'learned' by a decoder before its use is allowed in the system. Several learning strategies are possible, Figure 7-1 details a typical learn sequence. Core to each, the decoder must minimally store each learned transmitter's serial number and current synchronization counter value in EEPROM. Additionally, the decoder typically stores each transmitter's unique crypt key. The maximum number of learned transmitters will therefore be relative to the available EEPROM.

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

Figure 7-1 summarizes a typical learn sequence. The decoder receives and authenticates a first transmission; first button press. Authentication involves generating the appropriate crypt key, decrypting, validating the correct key usage via the discrimination bits and buffering the counter value. A second transmission is received and authenticated. A final check verifies the counter values were sequential; consecutive button presses. If the learn sequence is successfully complete, the decoder stores the learned transmitter's serial number, current synchronization counter value and appropriate crypt key. From now on the crypt key will be retrieved from EEPROM during normal operation instead of recalculating it for each transmission received.

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

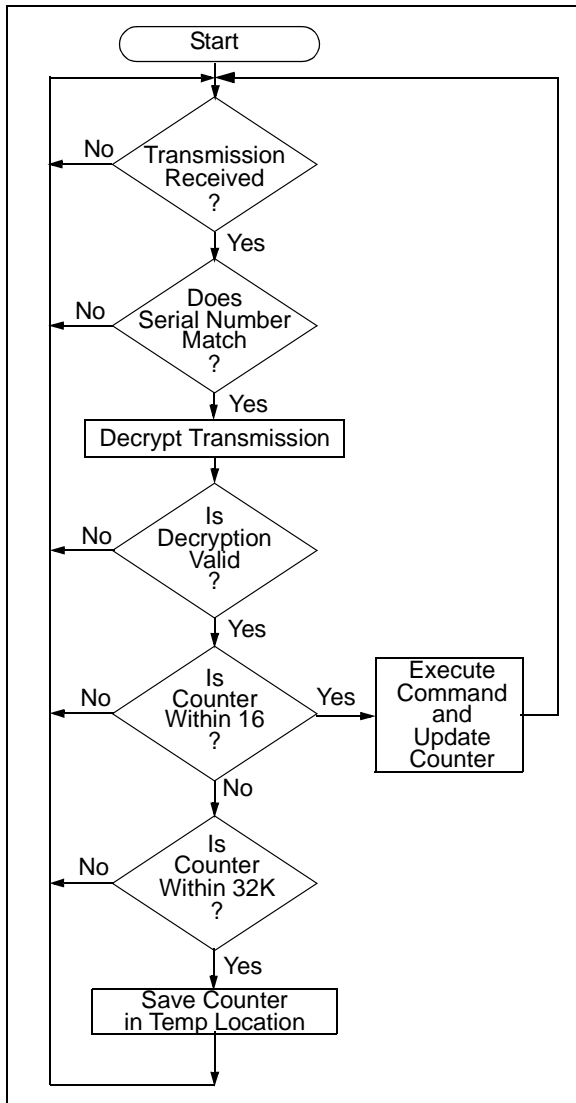
FIGURE 7-1: TYPICAL LEARN SEQUENCE



7.2 Decoder Operation

Figure 7-2 summarizes normal decoder operation. The decoder waits until a transmission is received. The received serial number is compared to the EEPROM table of learned transmitters to first determine if this transmitter's use is allowed in the system. If from a learned transmitter, the transmission is decrypted using the stored crypt key and authenticated via the discrimination bits for appropriate crypt key usage. If the decryption was valid the synchronization value is evaluated.

FIGURE 7-2: TYPICAL DECODER OPERATION



7.3 Synchronization with Decoder (Evaluating the Counter)

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

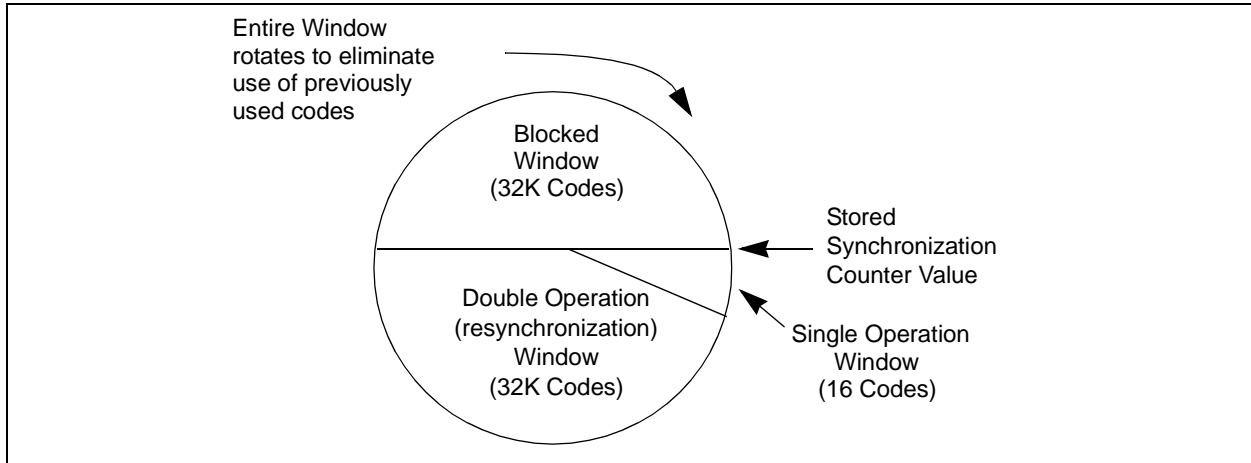
Figure 7-3 shows a 3-partition, rotating synchronization window. The size of each window is optional but the technique is fundamental. Each time a transmission is authenticated, the intended function is executed and the transmission's synchronization counter value is stored in EEPROM. From the currently stored counter value there is an initial "Single Operation" forward window of 16 codes. If the difference between a received synchronization counter and the last stored counter is within 16, the intended function will be executed on the single button press and the new synchronization counter will be stored. Storing the new synchronization counter value effectively rotates the entire synchronization window.

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

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

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

FIGURE 7-3: SYNCHRONIZATION WINDOW



HCS201

8.0 ELECTRICAL CHARACTERISTICS

TABLE 8-1: ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Units
VDD	Supply voltage	-0.3 to 13.5	V
VIN	Input voltage	-0.3 to VDD + 0.3	V
VOUT	Output voltage	-0.3 to VDD + 0.3	V
IOUT	Max output current	50	mA
TSTG	Storage temperature	-55 to +125	C (Note 1)
TLSOL	Lead soldering temp	300	C (Note 1)

Note 1: Stresses above those listed under “ABSOLUTE MAXIMUM RATINGS” may cause permanent damage to the device.

TABLE 8-2: DC CHARACTERISTICS

Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C									
		3.5V < VDD < 5.0V			5.0V < VDD < 13.0V				
Parameter	Sym.	Min.	Typ. ¹	Max.	Min.	Typ. ¹	Max.	Unit	Conditions
Operating Current (avg) ²	ICC	—	0.2	0.5	—	—	—	mA	
						1.5	2	mA	
Standby Current	ICCS	—	0.1	1.0	—	0.1	1.0	μA	
Auto-shutoff Current ^{3,4}	ICCS	—	40	75	—	160	300	μA	
High Level Input Voltage	VIH	0.55VDD	—	VDD+0.3	2.75	—	VDD+0.3	V	
Low level Input Voltage	VIL	-0.3	—	0.15VDD	-0.3	—	0.75	V	
High level Output Voltage	VOH	0.6VDD	—	—	—	—	—	V	IOH = -1.0 mA VDD = 3.5V IOH = -2.0 mA VDD = 12V
					3.3	—	—	V	
Low Level Output Voltage	VOL	—	—	0.08VDD	—	—	—	V	IOL = 1.0 mA VDD = 5V IOL = 2.0 mA VDD = 12V
					—	—	0.4	V	
Pull-down Resistance; S0-S2	RSO-2	40	60	80	40	60	80	kΩ	VDD = 4.0V
Pull-down Resistance; DATA	RDATA	80	120	160	80	120	160	kΩ	VDD = 4.0V

Note 1: Typical values are at 25°C.

2: No load.

3: Auto-shutoff current specification does not include the current through the input pull-down resistors.

4: These values are characterized but not tested.

FIGURE 8-1: POWER-UP AND TRANSMIT TIMING

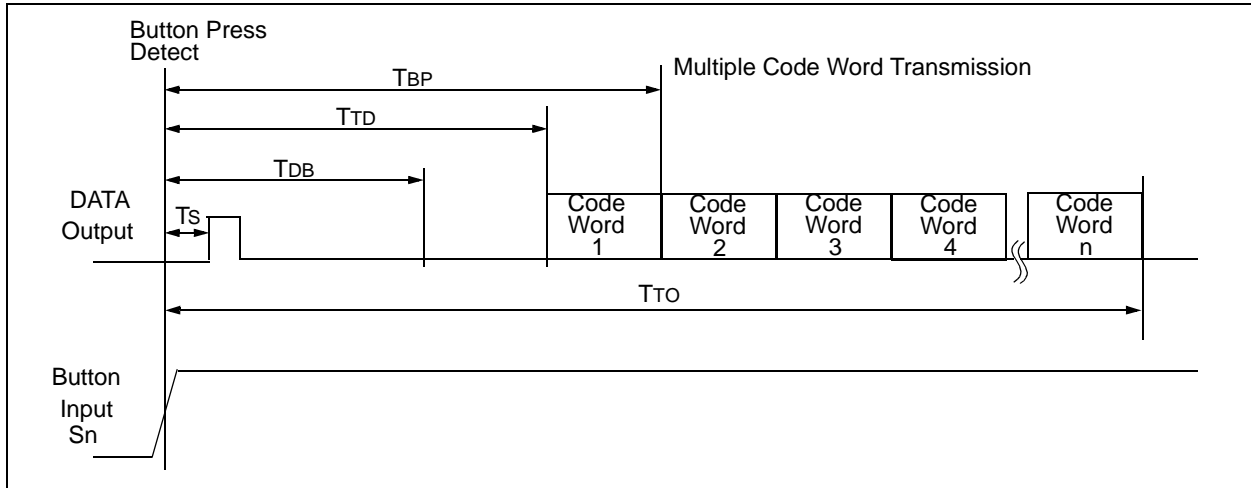


TABLE 8-3: POWER-UP AND TRANSMIT TIMING⁽²⁾

Standard Operating Conditions (unless otherwise specified):
 Commercial(C): Tamb = 0°C to +70°C
 Industrial(I): Tamb = -40°C to +85°C

Symbol	Parameter	Min.	Typ.	Max.	Unit	Conditions
TBP	Time to second button press	10 + Code Word		26 + Code Word	ms	(Note 1)
TTD	Transmit delay from button detect	12		26	ms	
TDB	Debounce Delay	6		20	ms	
TTO	Auto-shutoff time-out period		27		s	
Ts	START Pulse Delay		4.5		ms	

Note 1: TBP is the time in which a second button can be pressed without completion of the first code word (the intention was to press the combination of buttons).

2: Typical values - not tested in production.

FIGURE 8-2: CODE WORD FORMAT

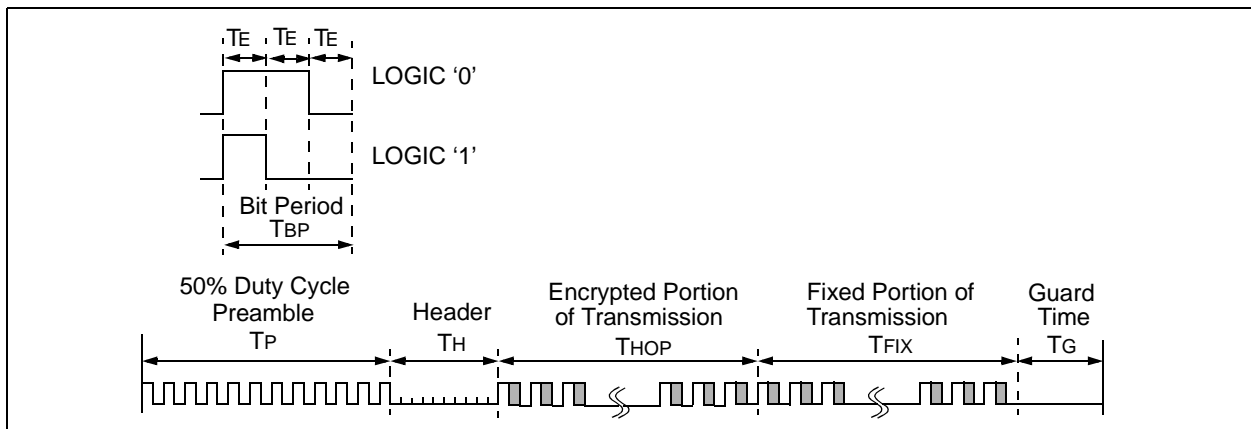


FIGURE 8-3: CODE WORD FORMAT: PREAMBLE/HEADER PORTION

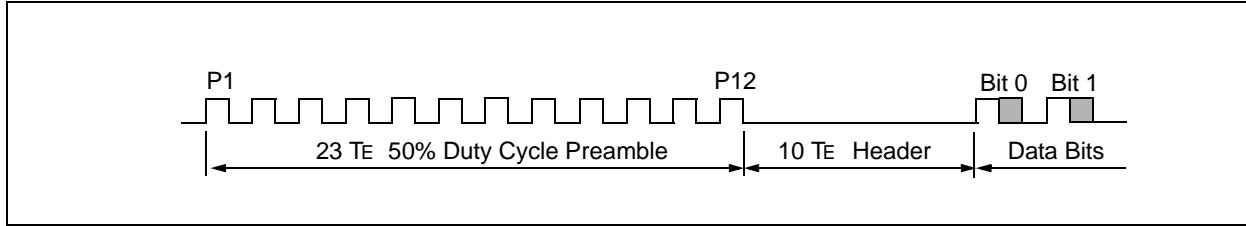


FIGURE 8-4: CODE WORD FORMAT: DATA PORTION (XSER=0)

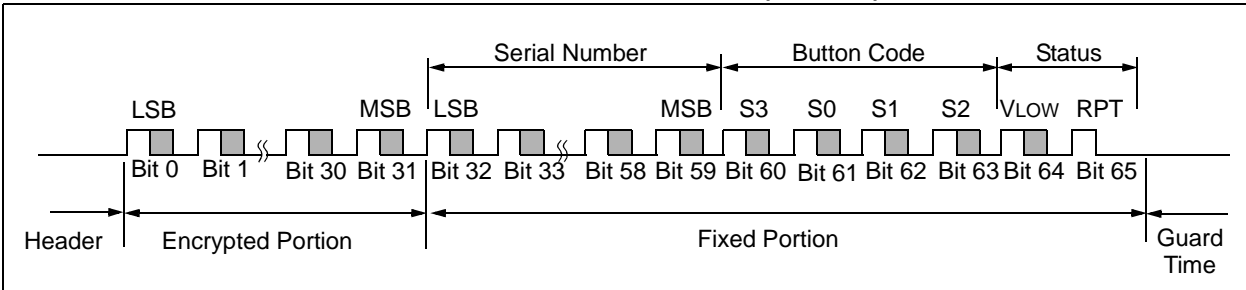


TABLE 8-4: CODE WORD TRANSMISSION TIMING REQUIREMENTS

VDD = +3.5 to 6.0V Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C			Code Words Transmitted						Units
			All			1 out of 2			
Symbol	Characteristic	Number of TE	Min.	Typ.	Max.	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	360	400	440	180	200	220	μs
TBP	PWM bit pulse width	3	1.08	1.2	1.32	0.54	0.6	0.66	ms
TP	Preamble duration	23	8.64	9.2	10.56	4.32	4.6	5.28	ms
TH	Header duration	10	3.6	4.0	4.4	1.8	2.0	2.2	ms
THOP	Hopping code duration	96	34.56	38.4	42.24	17.28	19.2	21.12	ms
TFIX	Fixed code duration	102	36.72	40.8	44.88	18.36	20.4	22.44	ms
TG	Guard Time	39	14.04	15.6	17.16	7.02	7.8	8.58	ms
—	Total Transmit Time	271	97.56	108.4	119.24	48.78	54.2	59.62	ms
—	PWM data rate	—	925	833	757	1851	1667	1515	bps

Note 1: The timing parameters are not tested but derived from the oscillator clock.

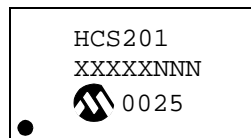
9.0 PACKAGING INFORMATION

9.1 Package Marking Information

8-Lead PDIP (300 mil)



Example



8-Lead SOIC (150 mil)



Example



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

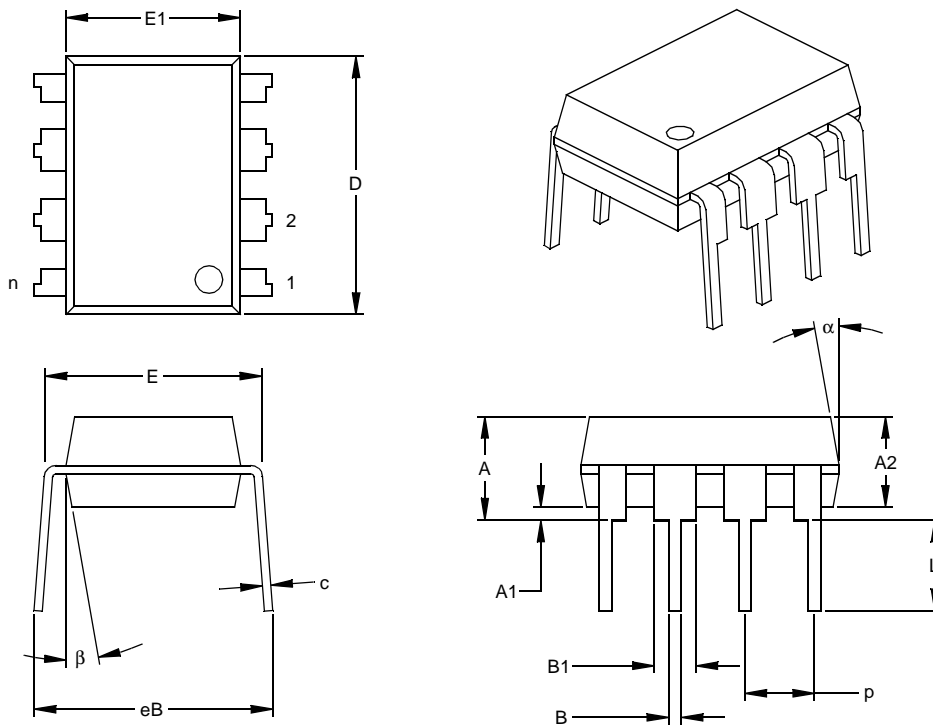
Note:	In the event the full Microchip part number cannot be marked on one line, it will be carried over to the next line thus limiting the number of available characters for customer specific information.
--------------	--

- * Standard OTP marking consists of Microchip part number, year code, week code, facility code, mask rev#, and assembly code. For OTP marking beyond this, certain price adders apply. Please check with your Microchip Sales Office. For QTP devices, any special marking adders are included in QTP price.

HCS201

9.2 Package Details

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



Units		INCHES*			MILLIMETERS		
Dimension	Limits	MIN	NOM	MAX	MIN	NOM	MAX
Number of Pins	n		8			8	
Pitch	p		.100			2.54	
Top to Seating Plane	A	.140	.155	.170	3.56	3.94	4.32
Molded Package Thickness	A2	.115	.130	.145	2.92	3.30	3.68
Base to Seating Plane	A1	.015			0.38		
Shoulder to Shoulder Width	E	.300	.313	.325	7.62	7.94	8.26
Molded Package Width	E1	.240	.250	.260	6.10	6.35	6.60
Overall Length	D	.360	.373	.385	9.14	9.46	9.78
Tip to Seating Plane	L	.125	.130	.135	3.18	3.30	3.43
Lead Thickness	c	.008	.012	.015	0.20	0.29	0.38
Upper Lead Width	B1	.045	.058	.070	1.14	1.46	1.78
Lower Lead Width	B	.014	.018	.022	0.36	0.46	0.56
Overall Row Spacing	§ eB	.310	.370	.430	7.87	9.40	10.92
Mold Draft Angle Top	α	5	10	15	5	10	15
Mold Draft Angle Bottom	β	5	10	15	5	10	15

* Controlling Parameter
 § Significant Characteristic

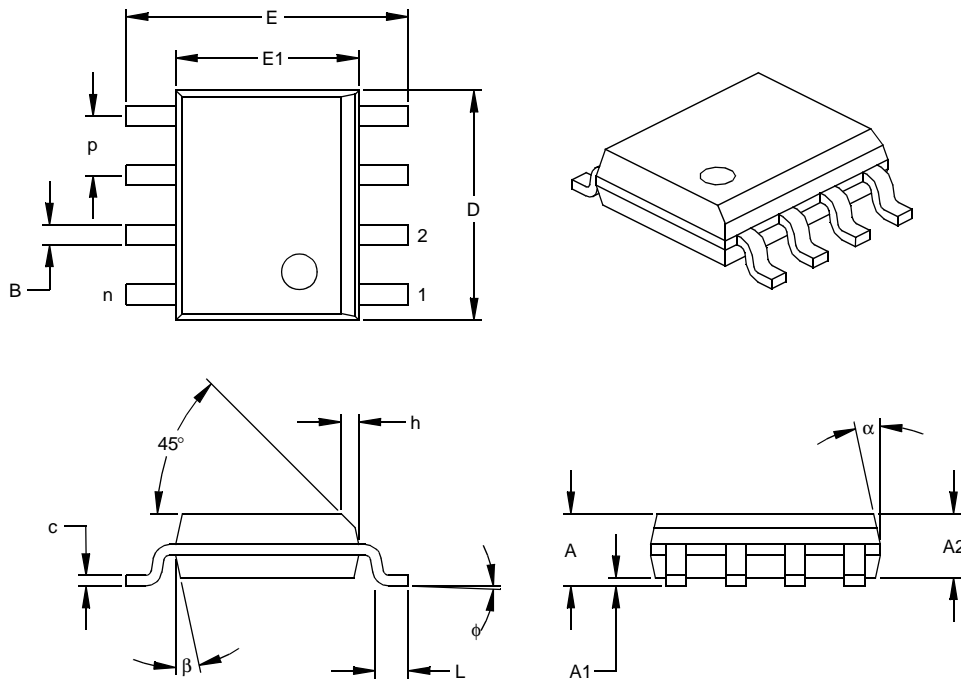
Notes:

Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed .010" (0.254mm) per side.

JEDEC Equivalent: MS-001

Drawing No. C04-018

8-Lead Plastic Small Outline (SN) – Narrow, 150 mil (SOIC)



Units		INCHES*			MILLIMETERS		
Dimension	Limits	MIN	NOM	MAX	MIN	NOM	MAX
Number of Pins	n		8			8	
Pitch	p		.050			1.27	
Overall Height	A	.053	.061	.069	1.35	1.55	1.75
Molded Package Thickness	A2	.052	.056	.061	1.32	1.42	1.55
Standoff §	A1	.004	.007	.010	0.10	0.18	0.25
Overall Width	E	.228	.237	.244	5.79	6.02	6.20
Molded Package Width	E1	.146	.154	.157	3.71	3.91	3.99
Overall Length	D	.189	.193	.197	4.80	4.90	5.00
Chamfer Distance	h	.010	.015	.020	0.25	0.38	0.51
Foot Length	L	.019	.025	.030	0.48	0.62	0.76
Foot Angle	φ	0	4	8	0	4	8
Lead Thickness	c	.008	.009	.010	0.20	0.23	0.25
Lead Width	B	.013	.017	.020	0.33	0.42	0.51
Mold Draft Angle Top	α	0	12	15	0	12	15
Mold Draft Angle Bottom	β	0	12	15	0	12	15

* Controlling Parameter
 § Significant Characteristic

Notes:

Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed

.010" (0.254mm) per side.

JEDEC Equivalent: MS-012

Drawing No. C04-057

ON-LINE SUPPORT

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

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

Connecting to the Microchip Internet Web Site

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

www.microchip.com

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

<ftp://ftp.microchip.com>

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

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

Systems Information and Upgrade Hot Line

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

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

1-480-792-7302 for the rest of the world.

HCS201

NOTES:

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

Information contained in this publication regarding device applications and the like is intended through suggestion only and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. No representation or warranty is given and no liability is assumed by Microchip Technology Incorporated with respect to the accuracy or use of such information, or infringement of patents or other intellectual property rights arising from such use or otherwise. Use of Microchip's products as critical components in life support systems is not authorized except with express written approval by Microchip. No licenses are conveyed, implicitly or otherwise, under any intellectual property rights.

Trademarks


The Microchip name and logo, the Microchip logo, FilterLab, KEELOQ, MPLAB, PIC, PICmicro, PICMASTER, PICSTART, PRO MATE, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

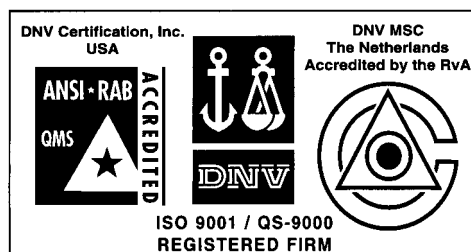
dsPIC, ECONOMONITOR, FanSense, FlexROM, fuzzyLAB, In-Circuit Serial Programming, ICSP, ICEPIC, microID, microPort, Migratable Memory, MPASM, MPLIB, MPLINK, MPSIM, MXDEV, PICC, PICDEM, PICDEM.net, rPIC, Select Mode and Total Endurance are trademarks of Microchip Technology Incorporated in the U.S.A.

Serialized Quick Turn Programming (SQTP) is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

© 2001, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

 Printed on recycled paper.



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.



WORLDWIDE SALES AND SERVICE

AMERICAS

Corporate Office

2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200 Fax: 480-792-7277
Technical Support: 480-792-7627
Web Address: <http://www.microchip.com>

Rocky Mountain

2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-692-7966 Fax: 480-792-7456

Atlanta

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

Boston

2 Lan Drive, Suite 120
Westford, MA 01886
Tel: 978-692-3848 Fax: 978-692-3821

Chicago

333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

Dallas

4570 Westgrove Drive, Suite 160
Addison, TX 75001
Tel: 972-818-7423 Fax: 972-818-2924

Dayton

Two Prestige Place, Suite 130
Miamisburg, OH 45342
Tel: 937-291-1654 Fax: 937-291-9175

Detroit

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

Kokomo

2767 S. Albright Road
Kokomo, Indiana 46902
Tel: 765-864-8360 Fax: 765-864-8387

Los Angeles

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

New York

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

Toronto

6285 Northam Drive, Suite 108
Mississauga, Ontario L4V 1X5, Canada
Tel: 905-673-0699 Fax: 905-673-6509

ASIA/PACIFIC

Australia

Microchip Technology Australia Pty Ltd
Suite 22, 41 Rawson Street
Epping 2121, NSW
Australia
Tel: 61-2-9868-6733 Fax: 61-2-9868-6755

China - Beijing

Microchip Technology Consulting (Shanghai)
Co., Ltd., Beijing Liaison Office
Unit 915
Bei Hai Wan Tai Bldg.
No. 6 Chaoyangmen Beidajie
Beijing, 100027, No. China
Tel: 86-10-85282100 Fax: 86-10-85282104

China - Chengdu

Microchip Technology Consulting (Shanghai)
Co., Ltd., Chengdu Liaison Office
Rm. 2401, 24th Floor,
Ming Xing Financial Tower
No. 88 TIDU Street
Chengdu 610016, China
Tel: 86-28-6766200 Fax: 86-28-6766599

China - Fuzhou

Microchip Technology Consulting (Shanghai)
Co., Ltd., Fuzhou Liaison Office
Rm. 531, North Building
Fujian Foreign Trade Center Hotel
73 Wusi Road
Fuzhou 350001, China
Tel: 86-591-7557563 Fax: 86-591-7557572

China - Shanghai

Microchip Technology Consulting (Shanghai)
Co., Ltd.
Room 701, Bldg. B
Far East International Plaza
No. 317 Xian Xia Road
Shanghai, 200051
Tel: 86-21-6275-5700 Fax: 86-21-6275-5060

China - Shenzhen

Microchip Technology Consulting (Shanghai)
Co., Ltd., Shenzhen Liaison Office
Rm. 1315, 13/F, Shenzhen Kerry Centre,
Renminnan Lu
Shenzhen 518001, China
Tel: 86-755-2350361 Fax: 86-755-2366086

Hong Kong

Microchip Technology Hongkong Ltd.
Unit 901-6, Tower 2, Metroplaza
223 Hing Fong Road
Kwai Fong, N.T., Hong Kong
Tel: 852-2401-1200 Fax: 852-2401-3431

India

Microchip Technology Inc.
India Liaison Office
Divyasree Chambers
1 Floor, Wing A (A3/A4)
No. 11, O'Shaughnessy Road
Bangalore, 560 025, India
Tel: 91-80-2290061 Fax: 91-80-2290062

Japan

Microchip Technology Japan K.K.
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 135-882
Tel: 82-2-554-7200 Fax: 82-2-558-5934

Singapore

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

Taiwan

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

EUROPE

Denmark

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

France

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

Germany

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

Italy

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

United Kingdom

Arizona Microchip Technology Ltd.
505 Eskdale Road
Winnersh Triangle
Wokingham
Berkshire, England RG41 5TU
Tel: 44 118 921 5869 Fax: 44-118 921-5820

10/01/01