HCS320

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 function code, 2-bit status)
- Encryption keys are read protected

Operating

- 3.5V - 13.0V operation
- Shift key and three inputs
  - 16 functions available
- Selectable baud rate
- Automatic code word completion
- Battery low signal transmitted to receiver
- Battery low indication on LED
- Non-volatile synchronization data

Other

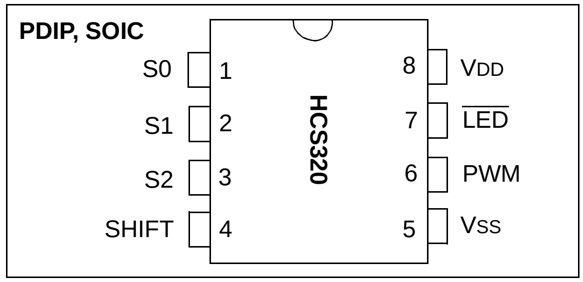
- Easy to use programming interface
- On-chip EEPROM
- On-chip oscillator and timing components
- Button inputs have internal pulldown resistors
- Current limiting on $\overline{\text{LED}}$ output
- Low external component cost

Typical Applications

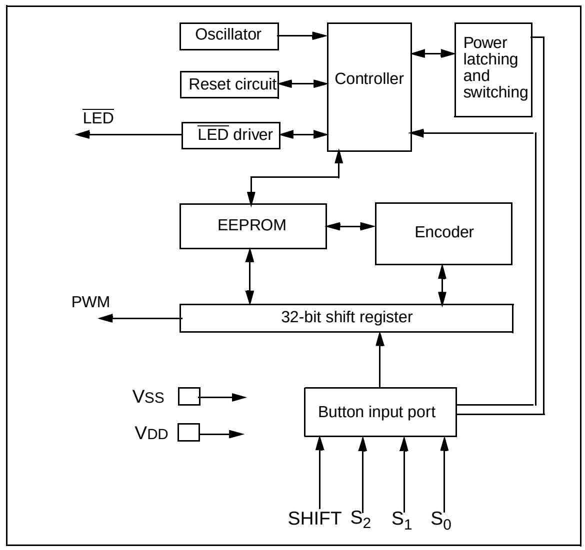
The HCS320 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

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

PACKAGE TYPES



HCS320 BLOCK DIAGRAM



DESCRIPTION

The HCS320, from Microchip Technology Inc., is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS320 utilizes the KEELOQ code hopping technology, which incorporates high security, a small package outline, and low cost, to make this device a perfect solution for unidirectional remote keyless entry systems and access control systems.

The HCS320 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and six status bits to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend (code grabbing) schemes useless.

The encoder key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS320 a very secure unit. The HCS320 provides a serial interface for programming the necessary security keys, system parameters, and configuration data.

The encryption keys and code combinations are programmable but read-protected. The keys can only be verified after an automatic erase and programming operation. This protects against attempts to gain access to keys and manipulate synchronization values.

The HCS320 operates over a voltage range of 3.5 volts to 13.0 volts and has four button inputs in an 8-pin configuration. This allows the system designer the freedom to utilize up to 16 functions. The only components required for device operation are the buttons and RF circuitry, allowing a very low system cost.

1.0 SYSTEM OVERVIEW

1.1 Key Terms

- Manufacturer's Code – a 64-bit word, unique to each manufacturer, used to program a unique encoder key in each transmitter (encoder).
- Encoder Key – a unique 64-bit key generated and programmed into the encoder. The encoder key controls the encryption algorithm and is stored in EEPROM on the encoder device.
- Transmit Button – An transmitter (encoder) button which when pressed, connects one of the switch inputs S0, S1 or S2 to V_{DD}. A transmit button may also simultaneously connect S0 and S1 to V_{DD}, usually via diodes to retain individual use of S0 and S1.
- Shift Button – The encoder button which when pressed, connects the SHIFT switch input to V_{DD}.
- Shift Level – the number of times that the shift button has been pressed before pressing a transmit button.
- Function Code – A four bit word which is derived from the shift level and the transmit button pressed.

1.2 KEELOQ Code Hopping Encoders

The HCS320 is a code hopping encoder device that is designed specifically for 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 low-end keyless entry systems transmit the same code from a transmitter every time a transmit 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 re-transmits it later, or a device that scans all possible combinations until the correct one is found.

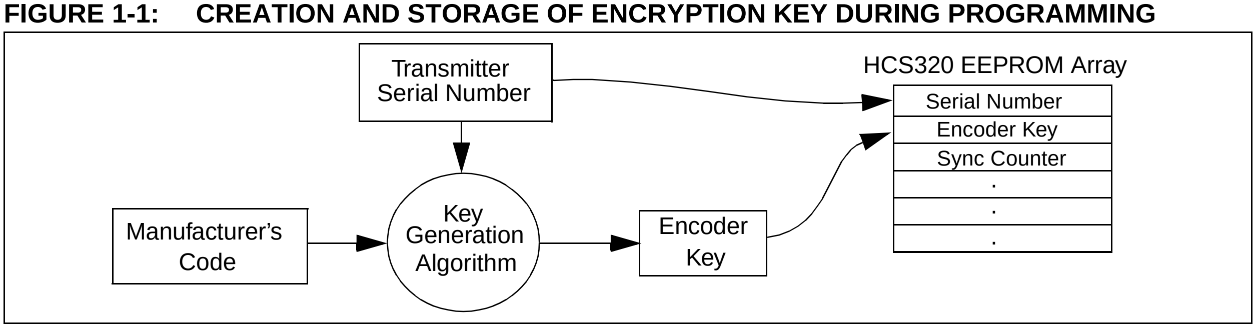
The HCS320 employs the KEELOQ code hopping encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 66 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

As indicated in the block diagram on page one, the HCS320 has a small EEPROM array which must be loaded with several parameters before use. The most important of these values are:

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

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 1-1). Typically, inputs to the key generation algorithm are the serial number of the transmitter 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 1-1: CREATION AND STORAGE OF ENCRYPTION KEY DURING PROGRAMMING



The 16-bit synchronization counter value is the basis for the transmitted code changing for each transmission, and is updated each time a transmit button is pressed. Because of the complexity of the code hopping algorithm, a change in one bit of the synchronization counter value will result in a large change in the actual transmitted code. There is a relationship (Figure 1-2) between the key values in EEPROM and how they are used in the encoder. Once the encoder detects that a transmit button has been pressed, the encoder reads the button and updates the synchronization counter. The synchronization counter value is then combined with the encoder key in the encryption algorithm and the output is 32 bits of encrypted information. This data will change with every transmit button press, hence, it is referred to as the hopping portion of the code word. The 32-bit hopping code is combined with the function code and the serial number to form the code word transmitted to the receiver. The code word format is explained in detail in Section 4.3.

Any type of controller may be used as a receiver, but it is typically a microcontroller with compatible firmware that allows the receiver to operate in conjunction with a transmitter, based on the HCS320. Section 7.0 provides more detail on integrating the HCS320 into a total system.

Before a transmitter can be used with a particular receiver, the transmitter must be 'learned' by the receiver. Upon learning a transmitter, information is stored by the receiver so that it may track the transmitter, including the serial number of the transmitter, the current synchronization value for that transmitter and the same encoder key that is used on the transmitter. If a receiver receives a message of valid format, the serial number is checked and, if it is from a learned transmitter, the message is decrypted and the decrypted synchronization counter is checked against what is stored. If the synchronization value is verified, then the function code is checked to see what operation is needed. 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: BASIC OPERATION OF TRANSMITTER (ENCODER)

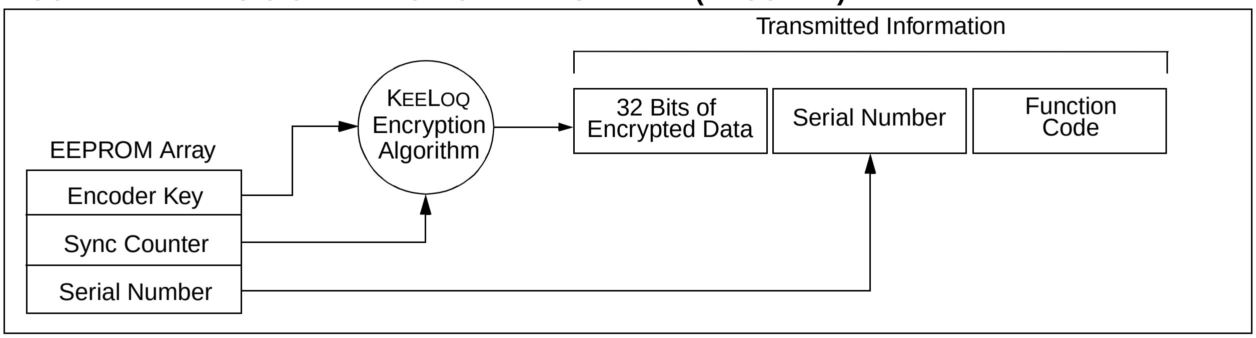
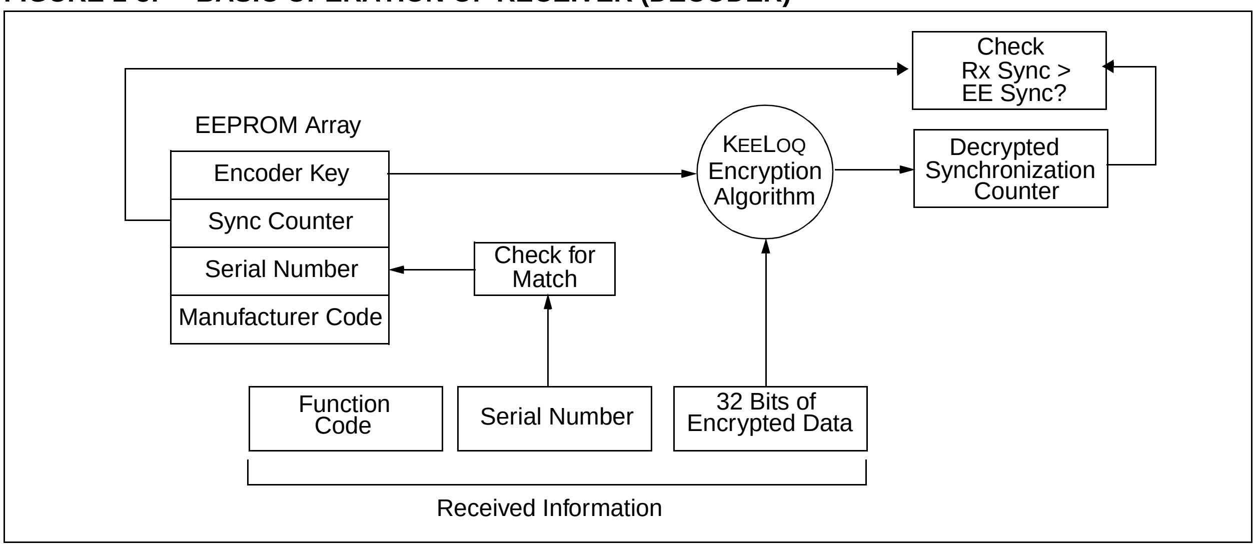


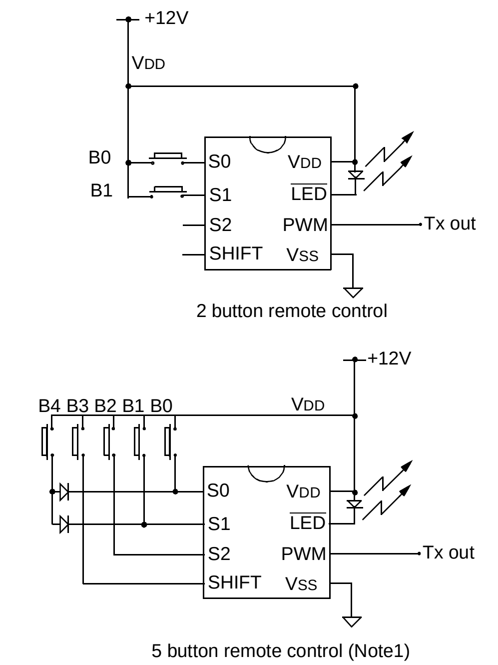
FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



2.0 DEVICE OPERATION

As shown in the typical application circuits (Figure 2-1), the HCS320 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 described in Table 2-1.

FIGURE 2-1: TYPICAL CIRCUITS



Note 1: The full 16 function codes are implemented using the shift button.

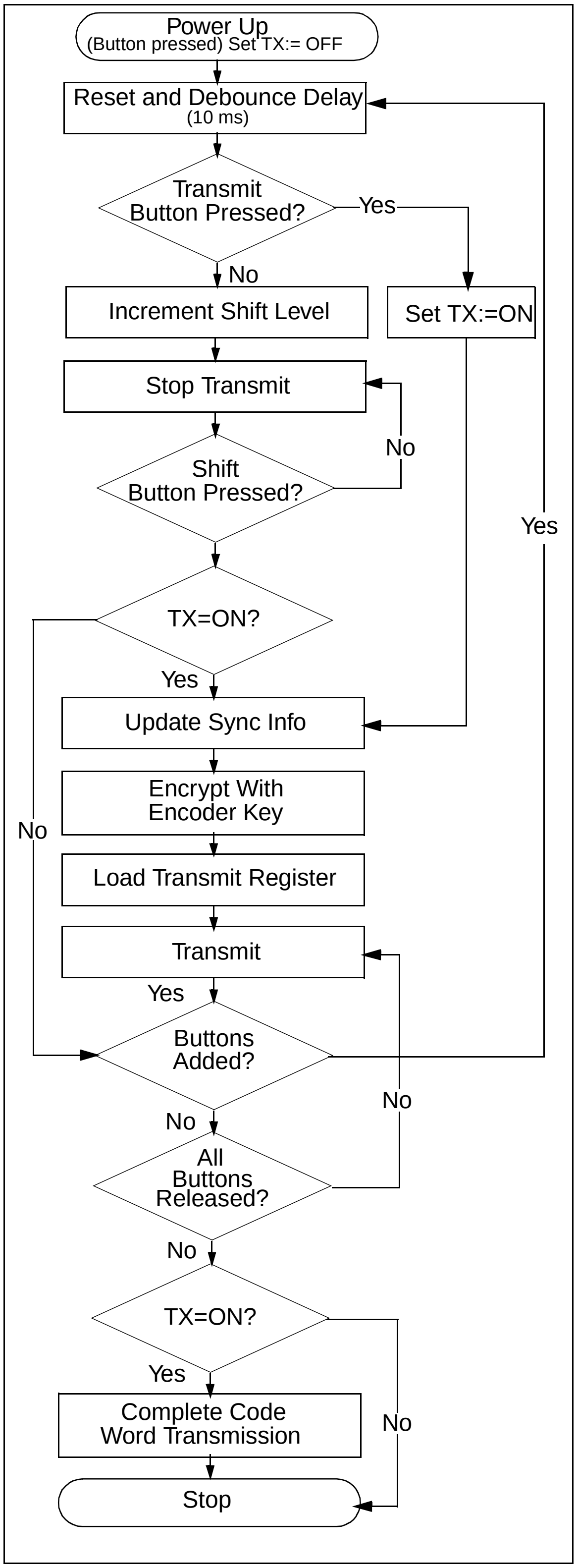
TABLE 2-1: PIN DESCRIPTIONS

Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2/Clock pin when in programming mode
SHIFT	4	Switch input for shift
VSS	5	Ground reference connection
PWM	6	Pulse width modulation (PWM) output pin/Data pin for programming mode
$\overline{\text{LED}}$	7	Cathode connection for directly driving $\overline{\text{LED}}$ during transmission
VDD	8	Positive supply voltage connection

The high security level of the HCS320 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 1 bit from the information in the previous transmission, the next coded transmission will be totally different. Statistically, if only 1 bit in the 32-bit string of information changes, approximately 50 percent of the coded transmission will change. The HCS320 will wake up upon detecting a switch closure and then delay approximately 10 ms for switch debounce (Figure 2-2). The synchronization information, fixed information, and switch information will be encrypted to form the hopping code. The encrypted or hopping code portion of the transmission will change every time, even if the same transmit button is pushed again. A code that has been transmitted will not occur again for more than 64K transmissions. This will provide more than 18 years of typical use before a code is repeated, based on 10 operations per day. Overflow information sent from the encoder can be used by the decoder 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 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 this case, the code word will be completed and the power down will occur.

FIGURE 2-2: ENCODER OPERATION



3.0 EEPROM MEMORY ORGANIZATION

The HCS320 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(Note)	Device Serial Number (word 1)
8	—	Not used
9	—	Not used
10	EN_KEY	16-bit Envelope Key
11	CONFIG	Configuration Word

Note: The MSB of the serial number contains a bit used to select the auto shutoff timer.

3.1 Key_0 - Key_3 (64-Bit Encryption Key)

The 64-bit encryption key is used by the transmitter to create the encrypted message transmitted to the receiver. This key is created and programmed at the time of production using a key generation algorithm. The key generation algorithm is different from the KEELOQ algorithm, although it too is a proprietary encryption method. Inputs to the key generation algorithm are the serial number for the particular transmitter being used 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 be changed after every transmission.

3.3 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. The most significant bit of the serial number (Bit 31) is used to turn the auto shutoff timer on or off.

3.3.1 AUTO-SHUTOFF TIMER SELECT

The most significant bit of the serial number (Bit 31) is used to turn the Auto-shutoff timer on or off. This timer prevents the transmitter from draining the battery should a button get stuck in the on position for a long period of time. The time period is approximately 25 seconds, after which the device will go to the Time-out mode. When in the Time-out mode, the device will stop transmitting, although since some circuits within the device are still active, the current draw within the Shutoff mode will be more than Standby mode. If the most significant bit in the serial number is a one, then the Auto-shutoff timer is enabled, and a zero in the most significant bit will disable the timer. The length of the timer is not selectable.

3.4 EN_Key (Envelope Encryption Key)

Envelope encryption is a selectable option that encrypts the portion of the transmission that contains the transmitter serial number and function code. Selecting this option is done by setting the appropriate bit in the configuration word (Table 3-2). Normally, the serial number and function code are transmitted in the clear (unencrypted), but for an added level of security, the system designer may elect to implement this option. The envelope encryption key is used to encrypt the serial number and function code portion of the transmission, if the envelope encryption option has been selected. The envelope encryption algorithm is a different algorithm than the key generation or transmit encryption algorithm. The EN_key is typically a random number and the same for all transmitters in a system.

3.5 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 3-2: CONFIGURATION 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	Overflow Bit 0 (OVR0)
11	Overflow Bit 1 (OVR1)
12	Low Voltage Trip Point Select
13	Baudrate Select Bit 0 (BSL0)
14	Baudrate Select Bit 1 (BSL1)
15	Envelope Encryption Select (EENC)

3.5.1 DISCRIMINATION VALUE (DISC0 TO DISC9)

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

3.5.2 OVERFLOW BITS (OVR0 AND OVR1)

The overflow bits are used to extend the number of possible synchronization values. The synchronization counter is 16 bits in length, yielding 65,536 values before the cycle repeats. Under typical use of 10 operations a day, this will provide nearly 18 years of use before a repeated value will be used. Should the system designer conclude that is not adequate, then the overflow bits can be utilized to extend the number of unique values. This can be done by programming OVR0 and OVR1 to 1s at the time of production. The encoder will automatically clear OVR0 the first time that the synchronization value wraps from 0xFFFF to 0x0000 and clear OVR1 the second time the counter wraps. Once cleared, OVR0 and OVR1 cannot be set again, thereby creating a permanent record of the counter overflow. This prevents fast cycling of 64K counter. If the decoder system is programmed to track the overflow bits, then the effective number of unique synchronization values can be extended to 196,608.

3.5.3 ENVELOPE ENCRYPTION (EENC)

If the EENC bit is set to a 1, the serial number and function code will also be encrypted so that it will appear to be random. The 16-bit envelope key and envelope algorithm will be used for encryption.

3.5.4 BAUDRATE SELECT BITS (BSL0, BSL1)

BSL0 and BSL1 select the speed of transmission and the code word blanking. Table 3-3 shows how the bits are used to select the different baud rates and Section 5.2 provides detailed explanation in code word blanking.

TABLE 3-3: BAUDRATE SELECT

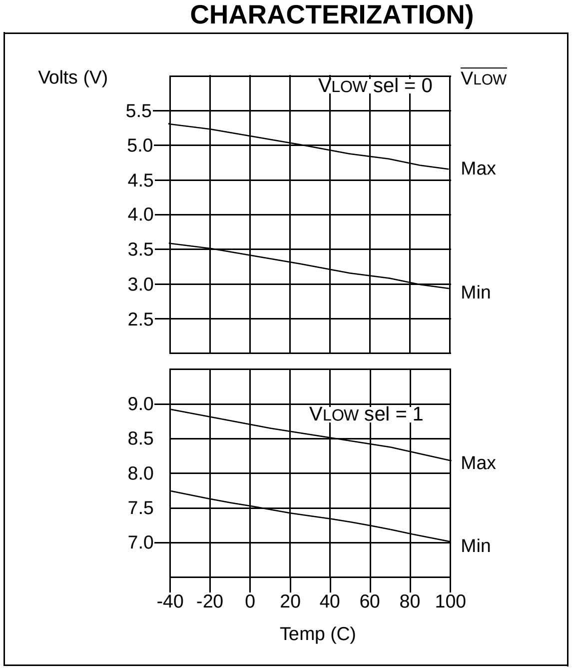
BSL1	BSL0	Basic Pulse Element	Code Words Transmitted
0	0	400µs	All
0	1	200µs	1 out of 2
1	0	100µs	1 out of 2
1	1	100µs	1 out of 4

3.5.5 LOW VOLTAGE TRIP POINT SELECT

The low voltage trip point select bit is used to tell the HCS320 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 to a one, the V_{DD} level is assumed to be operating from a 9.0 volt or 12.0 volt V_{DD} level. If the bit is set low, then the V_{DD} level is assumed to be 6.0 volts. Refer to Figure 3-1 for voltage trip point.

V_{LOW} is tested at 3.5V and 13.0V.

FIGURE 3-1: TYPICAL VOLTAGE TRIP POINTS (BY CHARACTERIZATION)



4.0 TRANSMITTED WORD

4.1 Transmission Format

The HCS320 transmission is made up of several parts (Figure 4-1). Each transmission begins with a preamble and a header, followed by the encrypted data and then the fixed data. The actual data is 66 bits which consists of 32 bits of encrypted data and 34 bits of fixed data. Each transmission is followed by a guard period before another transmission can begin. Refer to Table 8-4 for transmission timing requirements. The encrypted portion provides up to four billion changing code combinations and includes the function code bits (based on which buttons were activated) along with the synchronization counter value and some discrimination bits. The fixed portion is comprised of the status bits, the function bits and the 28-bit serial number. The fixed and encrypted sections combined increase the number of combinations to 7.38×10^{19}.

4.2 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, 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 that 16 extra bits are transmitted at the end after the fixed code word. The function code is derived from the SHIFT level and the S0 and S1 value at the falling edge of S2. The timing of the PWM data string is controlled by supplying a clock on S2 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 should not be toggled until all internal processing has been completed as shown in Figure 4-4.

4.3 Code Word Organization

The HCS320 transmits a 66-bit code word when a transmit button is pressed. The 66-bit word is constructed from a Fixed Code portion and an Encrypted Code portion (Figure 4-2).

The **Encrypted Data** is generated from 4 function code bits, 2 overflow counter bits, 10 discrimination bits and the 16-bit sync value (Figure 8-5).

The **Fixed Code Data** is made up from two status bits, four function code bits and the 28-bit serial number. The four function code bits and the 28-bit serial number may be encrypted with the Envelope Key if the envelope encryption is enabled by the user.

FIGURE 4-1: CODE WORD TRANSMISSION FORMAT

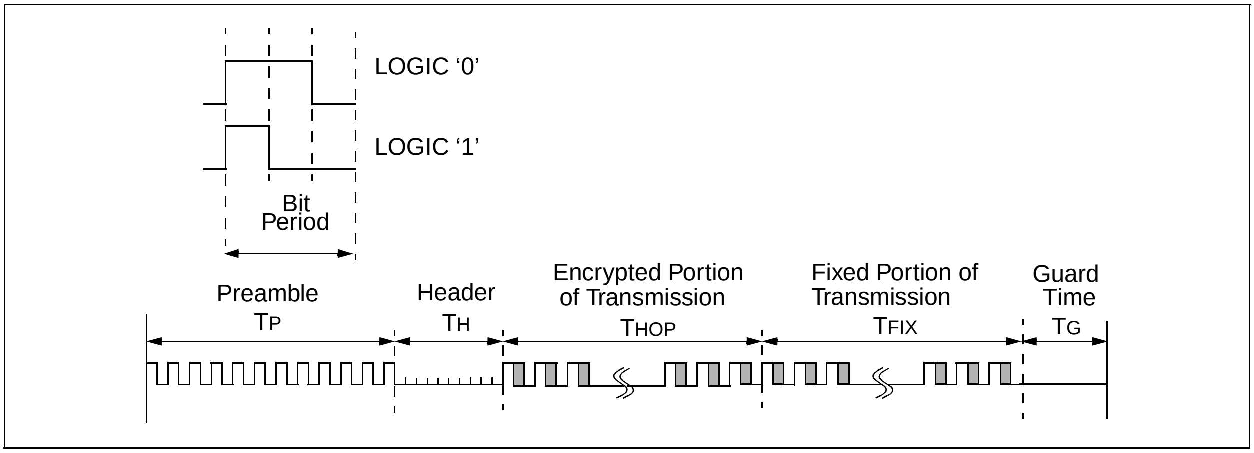


FIGURE 4-2: CODE WORD ORGANIZATION

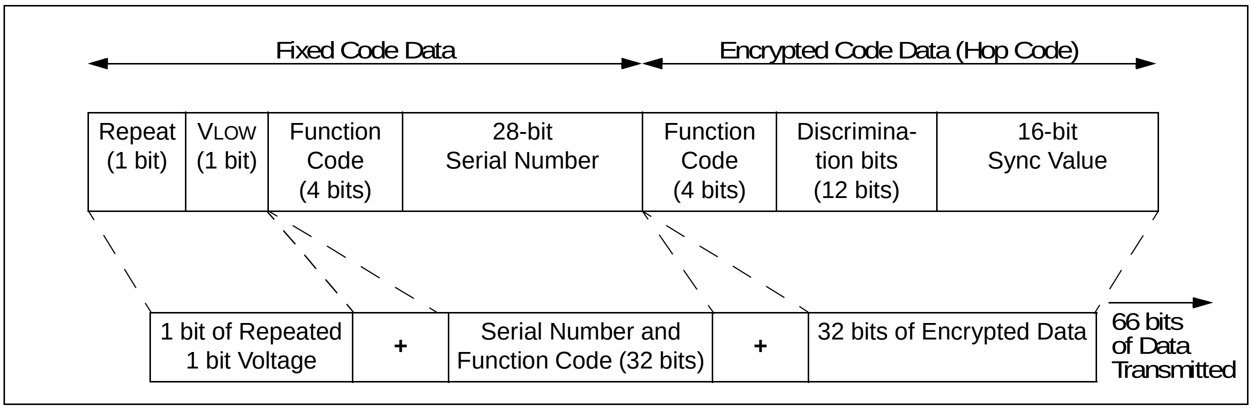


FIGURE 4-3: SYNCHRONOUS TRANSMISSION MODE

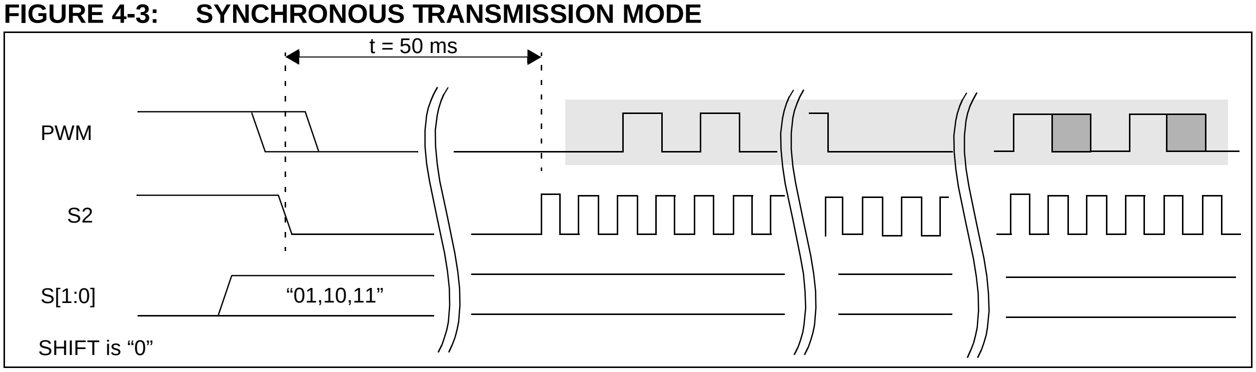
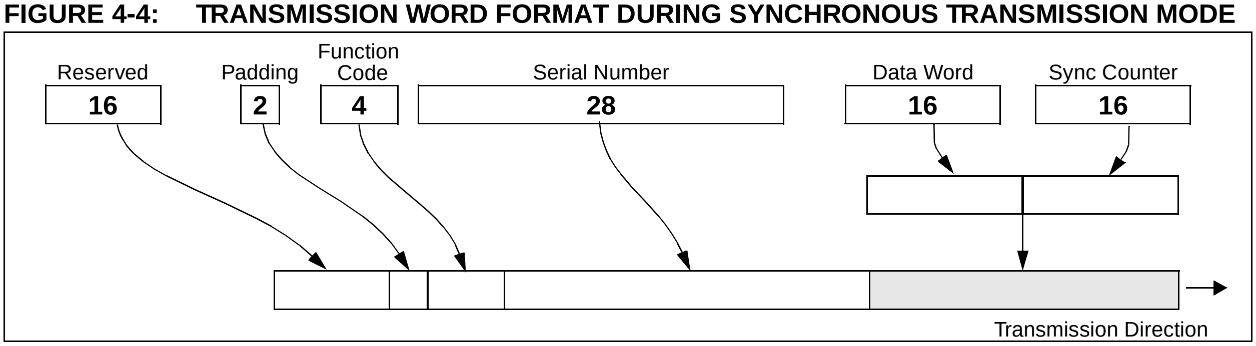


FIGURE 4-4: TRANSMISSION WORD FORMAT DURING SYNCHRONOUS TRANSMISSION MODE



5.0 SPECIAL FEATURES

5.1 Code Word Completion

Code word completion is an automatic feature that makes sure that the entire code word is transmitted, even if the transmit button is released before the transmission is complete. The HCS320 encoder powers itself up when a button is pushed and powers itself down after the command is finished, if the user has already released the button. If the button is held down beyond the time for one transmission, then multiple transmissions will result. If another button is activated during a transmission, the active transmission will be aborted and the function new code will be generated using the new button information.

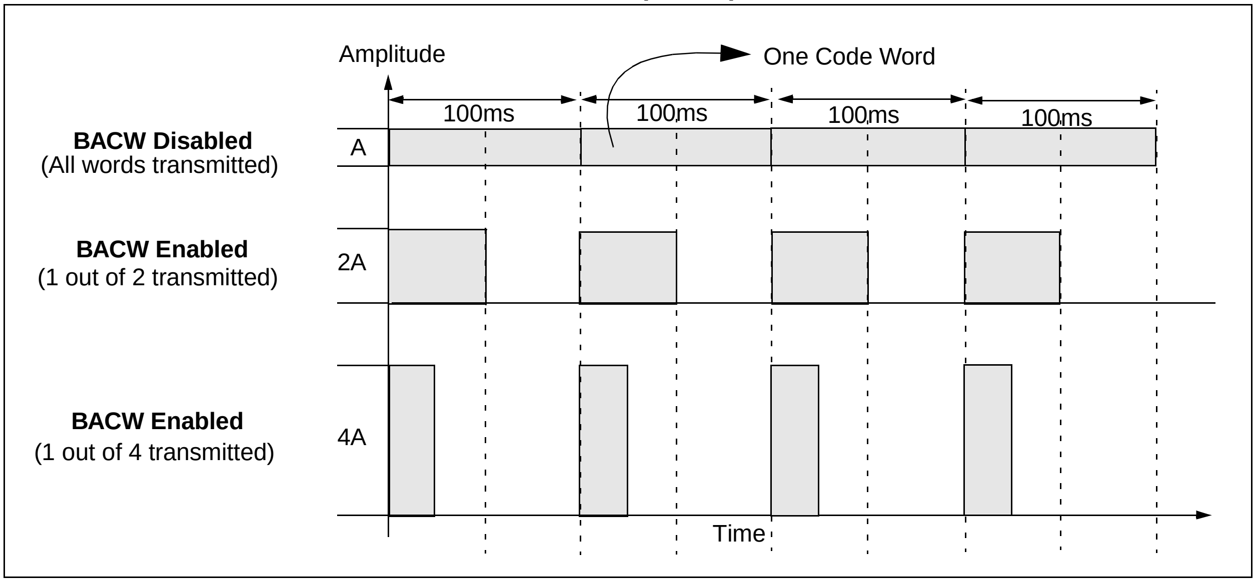
5.2 Blank Alternate Code Word

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. Blank Alternate Code Word (BACW) is used for reducing the average power of a transmission (Figure 5-1). This is a selectable feature that is determined in conjunction with the baudrate selection bits BSL0 and BSL1. Using the BACW 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 BACW effectively prevents continuous transmission by only allowing the transmission of every second or every fourth code word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

5.3 Envelope Encryption Option

Envelope Encryption is a user selectable option which is meant to offer a higher level of security for a code hopping system. During a normal transmission with the envelope encryption turned off, the 28-bit serial number and function code are transmitted in the clear (unencrypted). If envelope encryption is selected, then the serial number and function code are also encrypted before transmission. The encryption for the serial number is done using a different algorithm than the transmission algorithm. The envelope encryption scheme is not nearly as complex as the KEELOQ algorithm and, hence, not as secure. When the envelope encryption is used, the serial number must be decrypted using the envelope key and envelope decryption. After the serial number is obtained, the normal decryption method can be used to decrypt the hopping code.

FIGURE 5-1: BLANK ALTERNATE CODE WORD (BACW)



5.4 SHIFT Key Operation

The HCS320 has four switch inputs usually connected to buttons as shown in Figure 2-1: Typical Circuits.

Any button connected to input S0, S1 or S2 is called a TRANSMIT button as it causes a transmission when pressed.

The SHIFT button is connected to the SHIFT input. Pressing the SHIFT button increments a counter by one count and does not result in a transmission. The counter value is called the shift level. Successive presses of the SHIFT button can increase the shift level up to three before wrapping back to zero. The shift level is available for eight seconds when the SHIFT button is released, after which the shift level is reset to zero.

When a TRANSMIT button is pressed, the function code transmitted for that button depends on the shift level. The transmitted function code corresponding to shift level and S0, S1 and S2 switch activation is shown in Table 5-1 for all legal combinations of shift level and button input. Note that a shift level of zero means that the SHIFT button has not been pressed (or it has been pressed four times). The shift level is reset to zero after a transmission.

The volatile nature of the shift level register requires the HCS320 to be powered continuously for correct operation and not powered via the buttons.

TABLE 5-1: PIN ACTIVATION TABLE

SHIFT LEVEL	S2	S1	S0	FUNCTION CODE
0	0	0	0	No Transmission
0	0	0	1	0h
0	0	1	0	1h
0	0	1	1	2h
0	1	0	0	3h
1	0	0	0	No Transmission
1	0	0	1	4h
1	0	1	0	5h
1	0	1	1	6h
1	1	0	0	7h
2	0	0	0	No Transmission
2	0	0	1	8h
2	0	1	0	9h
2	0	1	1	Ah
2	1	0	0	Bh
3	0	0	0	No Transmission
3	0	0	1	Ch
3	0	1	0	Dh
3	0	1	1	Eh
3	1	0	0	Fh

5.5 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. This function can be enabled or disabled and is selected by setting or clearing the Auto-shutoff bit (Section 3.3.1). Setting this bit high will enable the function (turn Auto-shutoff function on) and setting the bit low will disable the function. Time-out period is dependent on the shift level and is approximately 42 ±10 seconds.

5.6 VLOW: Voltage LOW Indicator

The VLOW bit is transmitted with every transmission (Figure 8-5) and will be transmitted as a one if the operating voltage has dropped below the low voltage trip point. The trip point is selectable between two values, based on the battery voltage being used. See Section 3.5.5 for a description of how the low voltage select option is set. This VLOW signal is transmitted so the receiver can alert the user that the transmitter battery is low.

Note:	Depending on the internal resistance of the VDD source, VDD may normally be above the VLOW trip point except when the LED is turned on. In this case, the VLOW bit will be transmitted as a one when a transmission occurs while the LED is on. The VLOW bit will be transmitted as a zero when a transmission occurs while the LED is off.

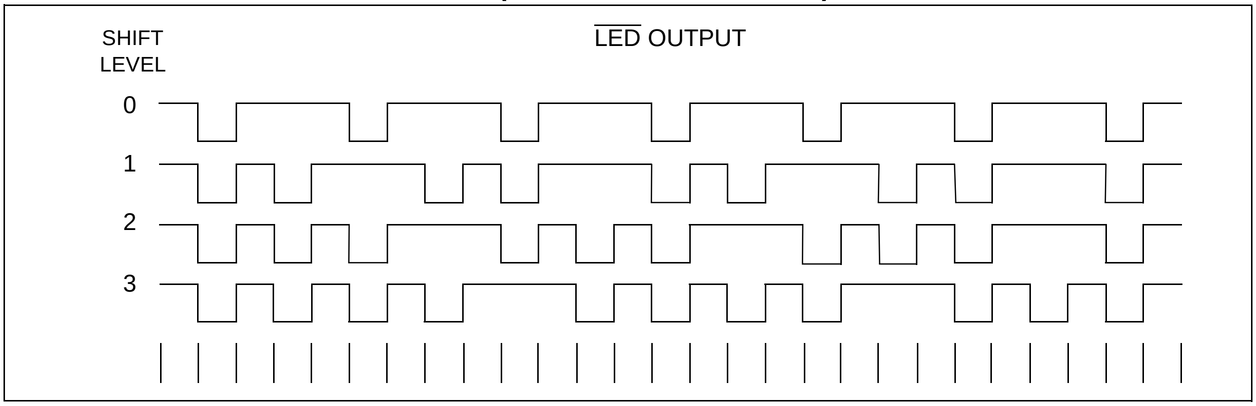
5.7 RPT: Repeat Indicator

This bit will be low for the first transmitted word. If a button is held down for more than one transmitted code word, this bit will be set to indicate a repeated code word and remain set until the button is released.

5.8 $\overline{\text{LED}}$ Output Operation

During normal transmission the $\overline{\text{LED}}$ output (Figure 5-2) indicates the shift level (Section 5.4) by flashing the LED in a pattern corresponding to the shift level. If the supply voltage drops below the low voltage trip point (Section 3.5.5), the $\overline{\text{LED}}$ output will be toggled at approximately 5þHz during the transmission.

FIGURE 5-2: LED FLASH FUNCTION (EACH DIVISION - 180 MS)

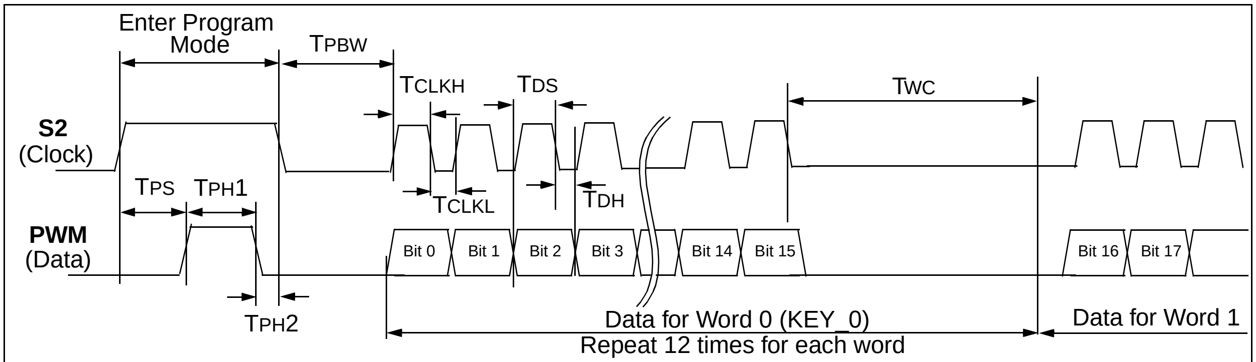


6.0 PROGRAMMING THE HCS320

When using the HCS320 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 PWM line high, after the S2 line has been held high for the appropriate length of time (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 PWM 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. 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 PWM. For security reasons, it is not possible to execute a verify function without first programming the EEPROM. **A verify operation can only be done immediately following the program cycle**.

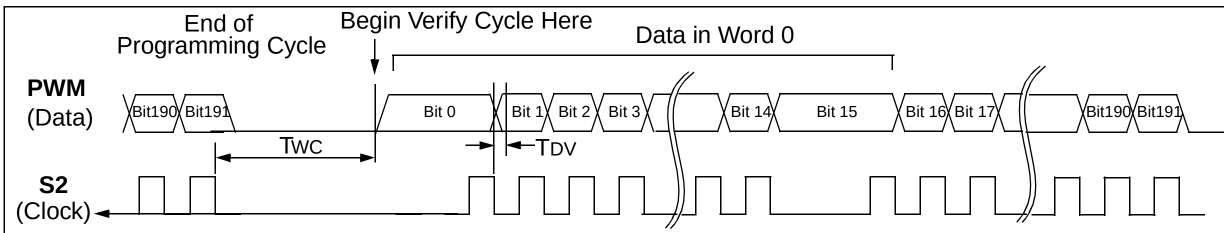
Note:	To ensure that the device does not accidentally enter programming mode (resulting in a bulk erase), PWM should never be pulled high by the circuit connected to it. Special care should be taken when driving PNP RF transistors.

FIGURE 6-1: PROGRAMMING WAVEFORMS



Note 1: Unused button inputs to be held ground during the entire programming sequence.
2: The VDD pin must be taken to ground after a programming/verify cycle.

FIGURE 6-2: VERIFY WAVEFORMS



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

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	3.5	4.5	ms
Hold time 1	TPH1	3.5	—	ms
Hold time 2	TPH2	50	—	µs
Bulk Write time	TPBW	—	2.2	ms
Program delay time	TPROG	—	2.2	ms
Program cycle time	TWC	—	36	ms
Clock low time	TCLKL	25	—	µs
Clock high time	TCLKH	25	—	µs
Data setup time	TDS	0	—	µs
Data hold time	TDH	18	—	µs
Data out valid time	TDV	10	24	µs

 Preliminary

7.0 INTEGRATING THE HCS320 INTO A SYSTEM

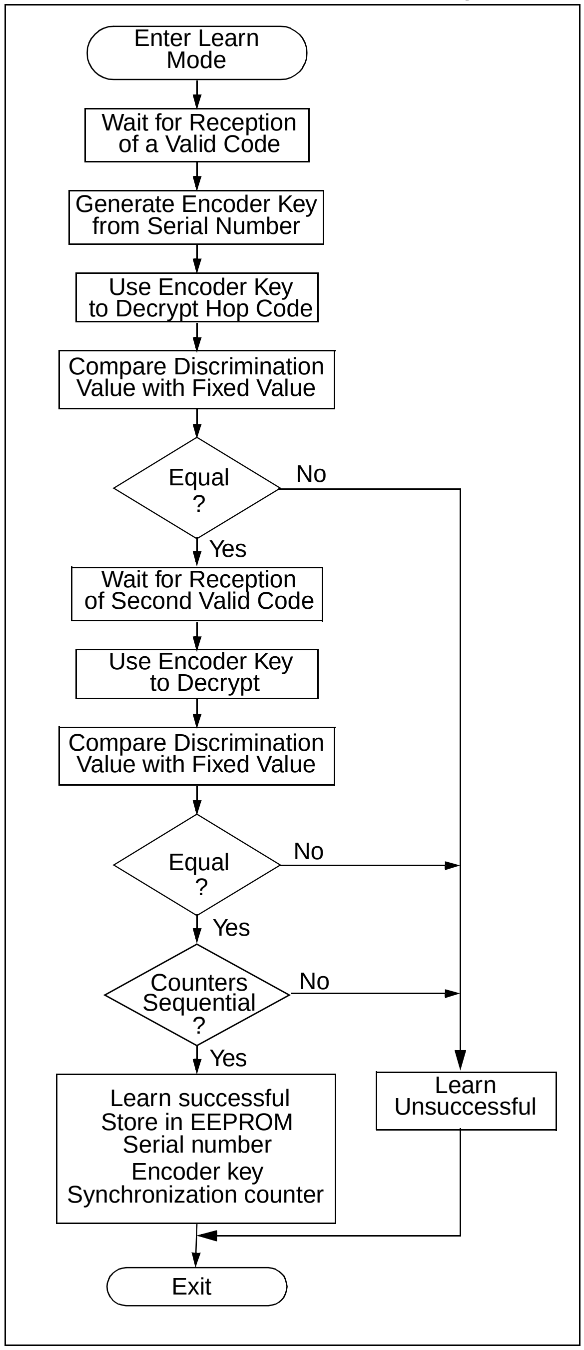
Use of the HCS320 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a license agreement) firmware routines that accept transmissions from the HCS320 and decrypt the hopping code portion of the data stream. These routines provide system designers the means to develop their own decoding system.

7.1 Learning a transmitter to a receiver

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, encoder key and current synchronization counter value in EEPROM. The decoder must keep track of these values for every transmitter that is learned (Figure 7-1). 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 a transmitter, 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.

It must be stated that some learning strategies have been patented and care must be taken not to infringe.

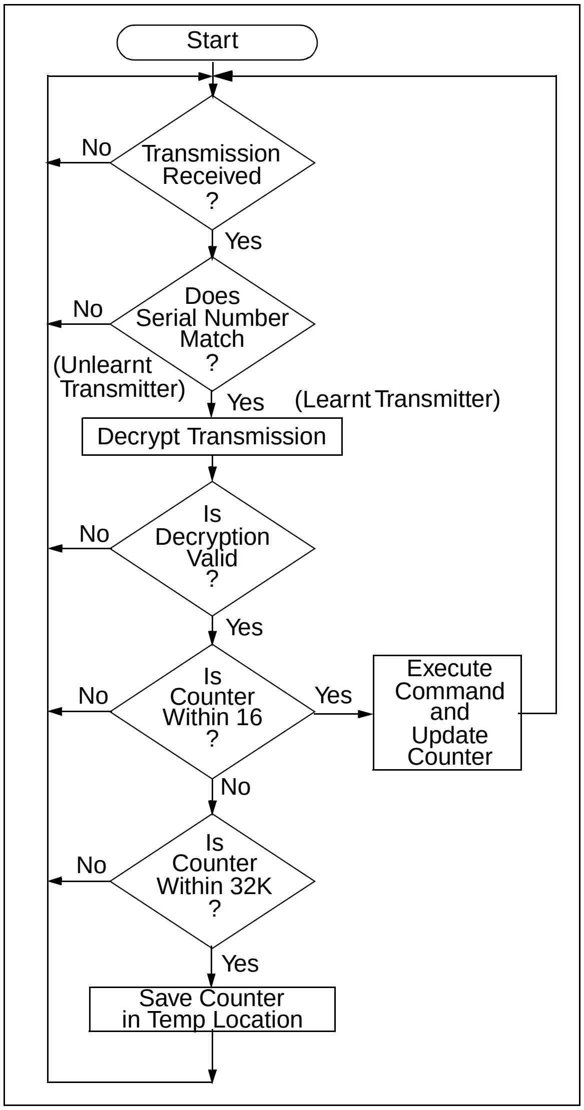
FIGURE 7-1: TYPICAL LEARN SEQUENCE



7.2 Decoder Operation

The decoder (Figure 7-2) waits for a transmission and immediately can check the serial number to determine if it is a learned transmitter. If it is, it takes the encrypted portion of the transmission and decrypts it using the corresponding stored encoder 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 7-2: TYPICAL DECODER OPERATION

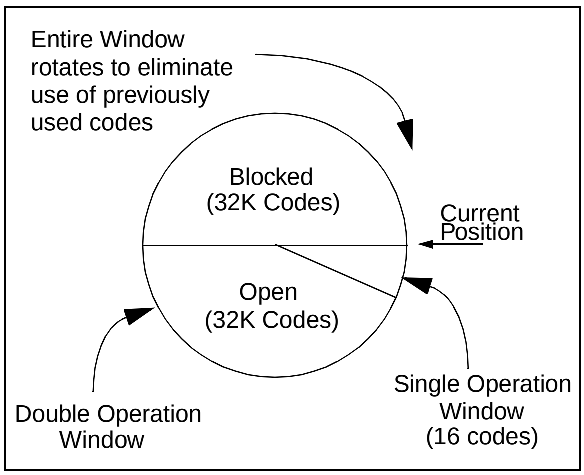


7.3 Synchronization with Decoder

The KEELOQ technology features a sophisticated synchronization technique (Figure 7-3) which does not require the calculation and storage of future codes. If the stored synchronization counter value for that particular transmitter and the synchronization counter value that was just decrypted are within a formatted window of say 16, the synchronization counter is stored and the command is executed. If the synchronization 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 synchronization counter values are sequential, it is assumed that the synchronization 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 re-learned. 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 re-transmitting to gain entry.

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

FIGURE 7-3: SYNCHRONIZATION WINDOW



8.0 ELECTRICAL CHARACTERISTICS

TABLE 8-1: ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Units
V_{DD}	Supply voltage	-0.3 to 13.3	V
V_{IN}	Input voltage	-0.3 to 13.3	V
V_{OUT}	Output voltage	-0.3 to V_{DD} + 0.3	V
I_{OUT}	Max output current	25	mA
T_{STG}	Storage temperature	-55 to +125	°C (Note)
T_{LSOL}	Lead soldering temp	300	°C (Note)
V_{ESD}	ESD rating	4000	V

Note: 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						
		$3.5V < V_{DD} < 13.0V$				
Parameter	**Sym.**	**Min**	**Typ***	**Max**	**Unit**	**Conditions**
Operating current (avg)	I_{CC}		0.6 2.0 10.0	1.0 3.0 15.0	mA	V_{DD} = 3.5V V_{DD} = 6.6V V_{DD} = 13.0V (Figure 8-1)
Standby current	I_{CCS}		1	10	µA	
High level Input voltage	V_{IH}	0.4 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}	0.5V_{DD}			V	I_{OH} = -2 mA
Low level output voltage	V_{OL}			0.11 V_{DD}	V	I_{OL} = 2 mA
$\overline{LED}$ sink current	I_{LED}	5.0 11.0	6.5 14	9.0 20	mA	V_{DD} = 6.6V V_{DD} = 13.0V
Resistance; S0,S1,S2, SHIFT	R_{S0-3}	40	60	80	KΩ	V_{IN} = 4.0V
Resistance; PWM	R_{PWM}	80	120	160	KΩ	V_{IN} = 4.0V

* Typical values are at 25°C.

FIGURE 8-1: TYPICAL ICC CURVE OF HCS320

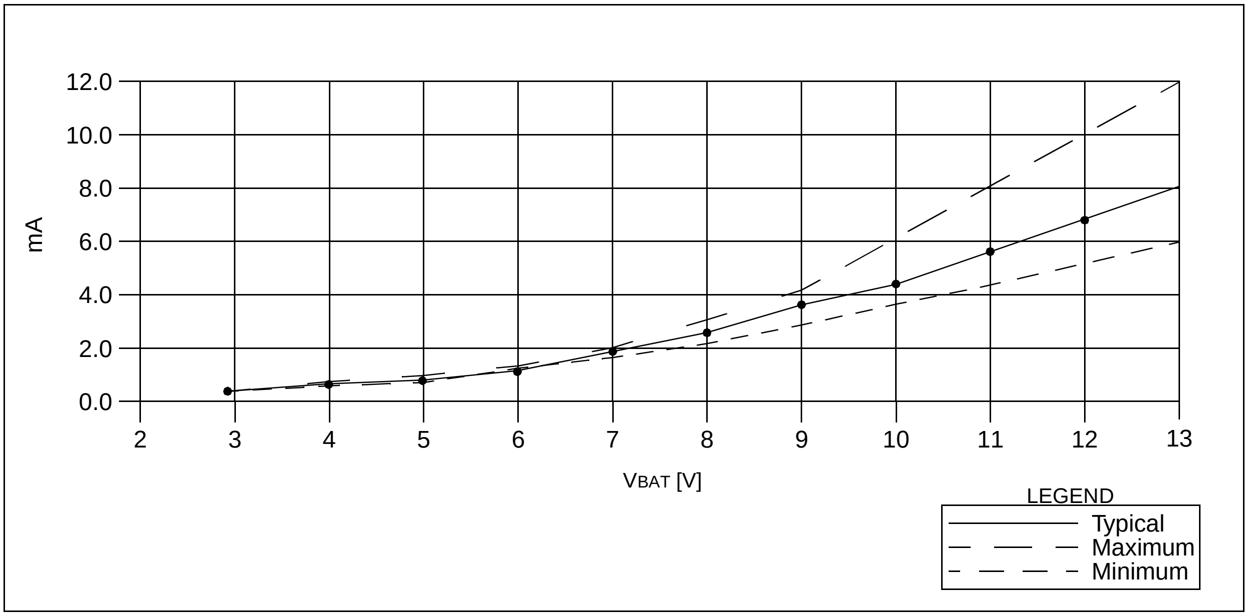


FIGURE 8-2: POWER UP AND TRANSMIT TIMING

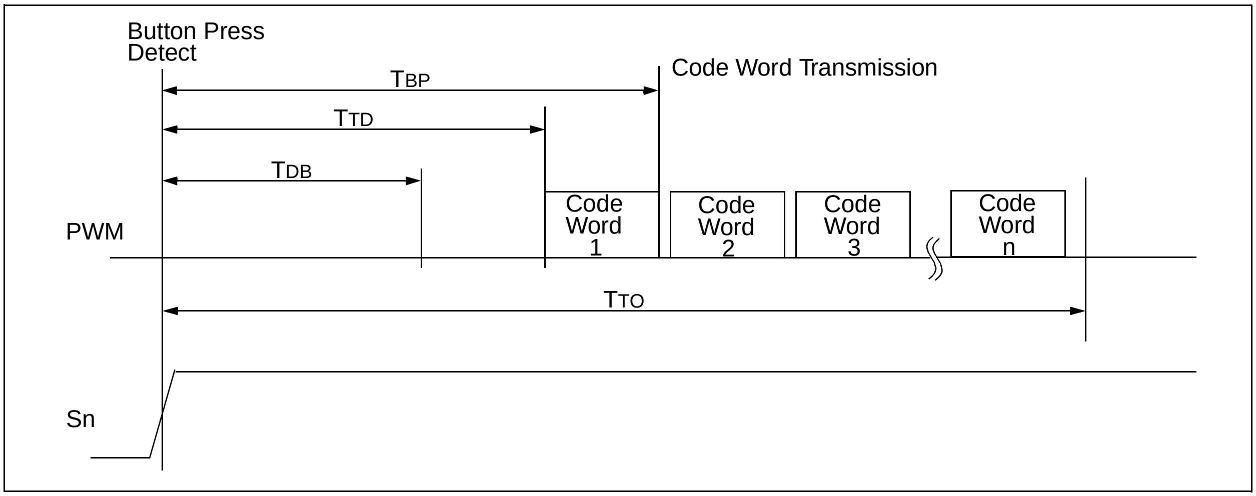


TABLE 8-3: POWER UP AND TRANSMIT TIMING REQUIREMENTS

VDD = +3.5 to13.0V
Commercial (C): Tamb = 0°C to +70°C
Industrial (I): Tamb = -40°C to +85°C

Parameter	Symbol	Min	Max	Unit	Remarks
Time to second button press	TBP	10 + Code Word Time	27 + Code Word Time	ms	(Note 1)
Transmit delay from button detect	TTD	10	27	ms	
Debounce delay	TDB	6	15	ms	
Auto-shutoff time-out period	TTO	22	77	s	(Note 2)

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: The auto shutoff timeout period is not tested.

FIGURE 8-3: PWM FORMAT

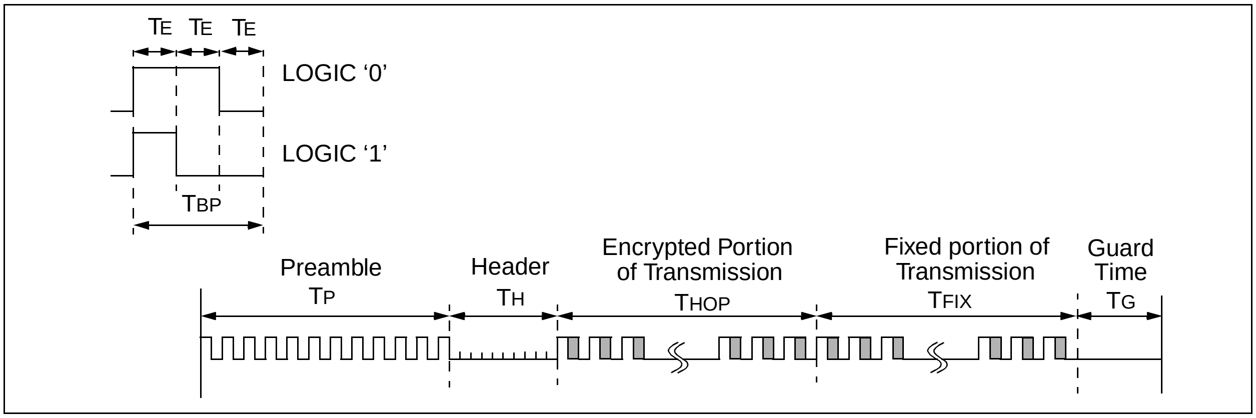


FIGURE 8-4: PREAMBLE/HEADER FORMAT

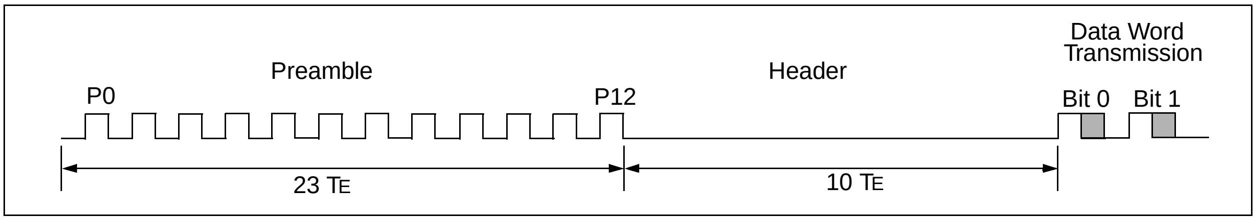


FIGURE 8-5: DATA WORD FORMAT

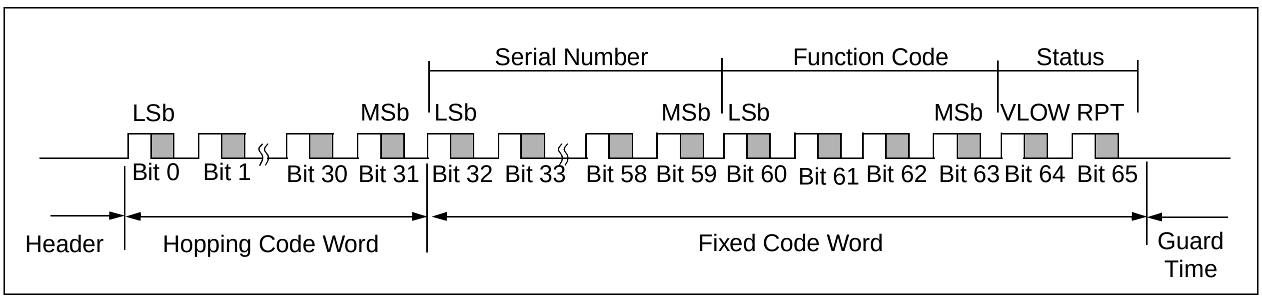
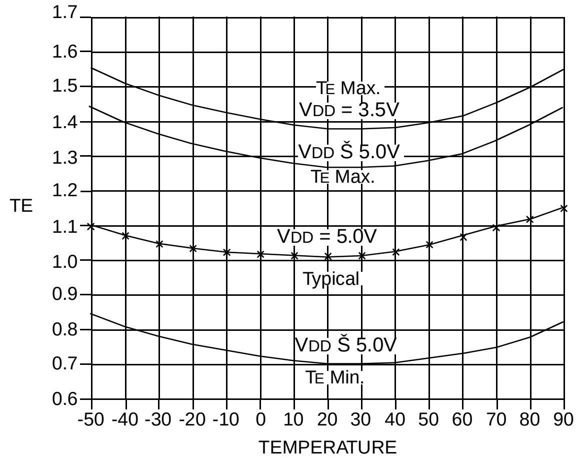


TABLE 8-4: CODE WORD TRANSMISSION TIMING REQUIREMENTS

V_{DD} = +3.5 to 13.0 Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C			Code Words Transmitted									
			All			1 out of 2			1 out of 4			
Symbol	**Characteristic**	**Number of T_E**	**Min.**	**Typ.**	**Max.**	**Min.**	**Typ.**	**Max.**	**Min.**	**Typ.**	**Max.**	**Units**
T_E	Basic pulse element	1	280	400	620	140	200	310	70	100	155	µs
T_{BP}	PWM bit pulse width	3	840	1200	1860	420	600	930	210	300	465	µs
T_P	Preamble duration	23	6.4	9.2	14.3	3.2	4.6	7.1	1.6	2.3	3.6	ms
T_H	Header duration	10	2.8	4.0	6.2	1.4	2.0	3.1	0.7	1.0	1.6	ms
T_{HOP}	Hopping code duration	96	26.9	38.4	59.5	13.4	19.2	29.8	6.7	9.6	14.9	ms
T_{FIX}	Fixed code duration	102	28.6	40.8	63.2	14.3	20.4	31.6	7.1	10.2	15.8	ms
T_G	Guard Time	199	55.6	79.6	123.5	28.1	39.8	61.7	13.8	19.9	30.6	ms
—	Total Transmit Time	430	120.3	172.0	266.7	60.4	86.0	133.3	29.9	43.0	66.5	ms
—	PWM data rate	—	1190	833	538	2381	1667	1075	4762	3333	2151	bps

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

FIGURE 8-6: HCS320 TE VS. TEMP (BY CHARACTERIZATION ONLY)



HCS320 PRODUCT IDENTIFICATION SYSTEM

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

HCS320 — /P

Package:	P =	Plastic DIP (300 mil Body), 8-lead
	SN =	Plastic SOIC (150 mil Body)
Temperature Range:	Blank =	0°C to +70°C
	I =	–40°C to +85°C
Device:	HCS320	Code Hopping Encoder
	HCS320T	Code Hopping Encoder (Tape and Reel)

Sales and Support

Data Sheets

Products supported by a preliminary Data Sheet may have an errata sheet describing minor operational differences and recommended workarounds. To determine if an errata sheet exists for a particular device, please contact one of the following:

1. Your local Microchip sales office
2. The Microchip Corporate Literature Center U.S. FAX: (480) 786-7277
3. The Microchip Worldwide Site (www.microchip.com)

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

New Customer Notification System

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

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

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.