HCS200

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
- 28-bit serial number, 4-bit function code, VLOW indicator transmitted
- Encryption keys are read protected

Operating

- 3.5–13.0V operation
- Three button inputs
  - seven functions available
- Selectable baud rate
- Automatic code word completion
- Battery low signal transmitted to receiver
- 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
- Low external component cost

Typical Applications

The HCS200 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

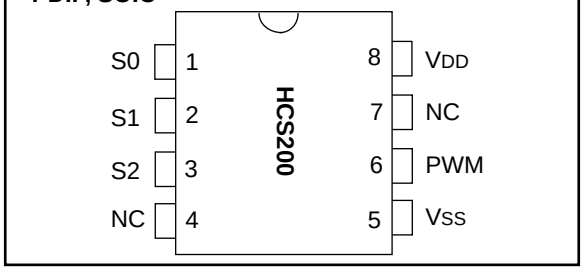
- Fixed code replacement
- Automotive RKE systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Identity tokens
- Burglar alarm systems

DESCRIPTION

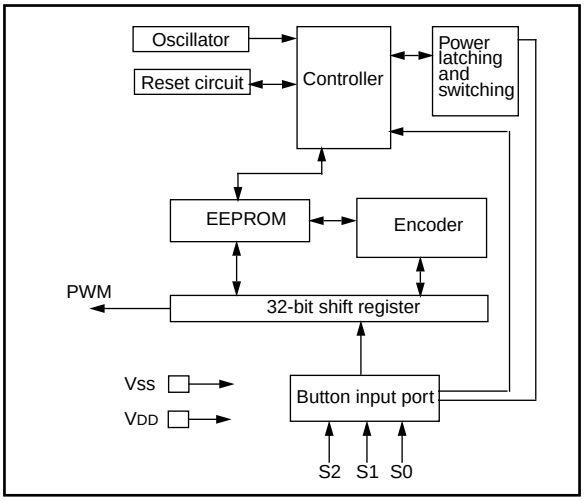
The HCS200, from Microchip Technology Inc., is a code hopping encoder designed for Remote Keyless Entry (RKE) systems. The HCS200 utilizes the Keeloq® code hopping technology, which incorporates high security, a small package outline and low cost, to make this device a perfect solution for replacement of fixed code devices in unidirectional remote keyless entry systems and access control systems.

PACKAGE TYPES

PDIP, SOIC



BLOCK DIAGRAM



The HCS200 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and 6 information 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 schemes useless.

The encryption key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS200 a very secure unit. The HCS200 provides an easy to use serial interface for programming the necessary security keys, system parameters, and configuration data.

All 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.

KeeLoq is a trademark of Microchip Technology Inc.
*Code hopping encoder patents issued in Europe, U. S. A., and R. S. A.

The HCS200 operates over a wide voltage range of 3.5 volts to 13.0 volts and has three button inputs in an 8-pin configuration. This allows the system designer the freedom to utilize up to seven functions. The only components required for device operation are the buttons and RF circuitry, allowing a very low system cost.

1.0 SYSTEM OVERVIEW

Key Terms

- Manufacturer's code — a 64-bit word, unique to each manufacturer, used to produce a unique encryption key in each transmitter (encoder).
- Encryption Key — a unique 64-bit key generated and programmed into the encoder during the manufacturing process. The encryption key controls the encryption algorithm and is stored in EEPROM on the encoder device.

1.1 Learn

The HCS product family facilitates several learn strategies to be implemented on the decoder. The following are examples of what can be done. It must be pointed out that their exists some third-party patents on learning strategies and implementation.

1.1.1 NORMAL LEARN

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

1.1.2 SECURE LEARN*

The transmitter is activated through a special button combination to transmit a stored 48-bit value (random seed) that can be used for key generation or be part of the key. Transmission of the random seed can be disabled after learning is completed.

The HCS200 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. The HCS200 requires very few external components (Figure 2-1).

Most low-end keyless entry systems transmit the same code from a transmitter every time a button is pushed. The number of possible 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.

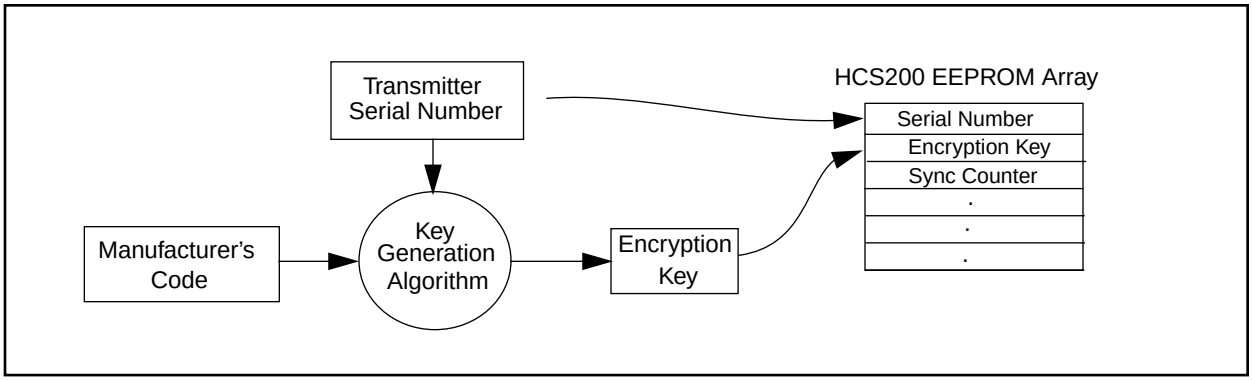
The HCS200 employs the KEELOQ code hopping encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 66 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

As indicated in the block diagram on page one, the HCS200 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 16-bit configuration value
- An encryption key that is generated at the time of production
- A 16-bit synchronization value

The serial number for each transmitter is programmed by the manufacturer at the time of production. The generation of the encryption 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 PRODUCTION



* Code Hopping learn patents pending.

The 16-bit synchronization value is the basis for the transmitted code changing for each transmission, and is updated each time a button is pressed. Because of the complexity of the code hopping algorithm, a change in one bit of the synchronization 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 button has been pressed, the encoder reads the button and updates the synchronization counter. The synchronization value is then combined with the encryption key in the encryption algorithm and the output is 32 bits of encrypted information. This data will change with every button press, 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 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 HCS200. Section 7.0 provides more detail on integrating the HCS200 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 encryption 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 button status 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)

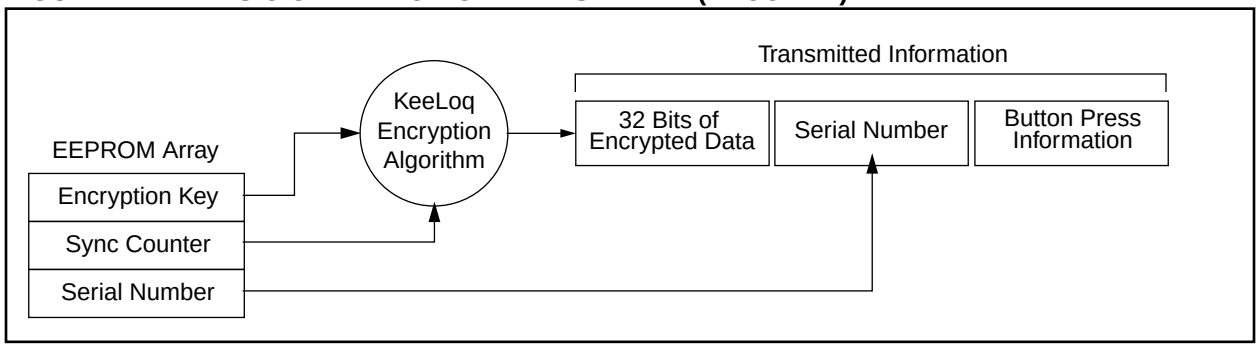
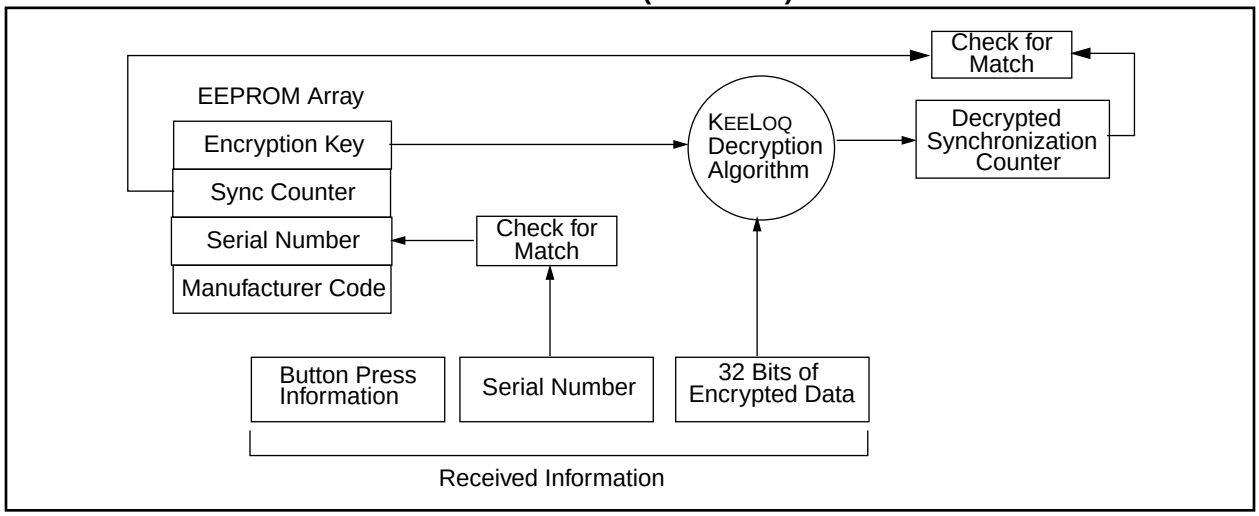


FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)

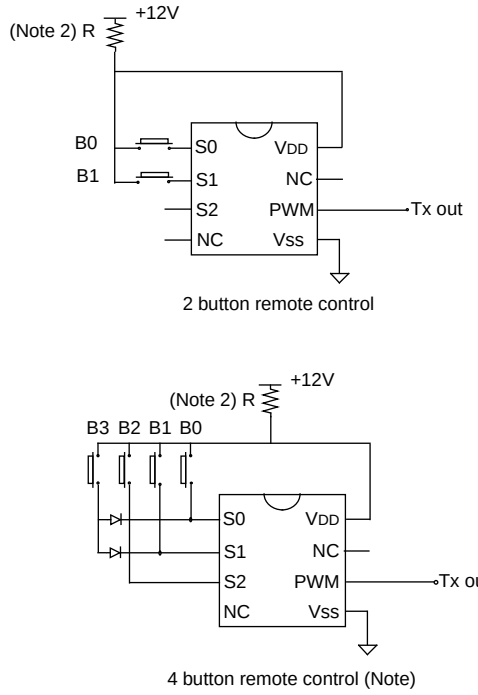


2.0 DEVICE OPERATION

As shown in Figure 2-1, the HCS200 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.

Note:	When V_{DD} > 9.0V and driving low capacitive loads, a resistor with a minimum value of 50Ω should be used in line with V_{DD}. This prevents clamping of PWM at 9.0V in the event of PWM overshoot.

FIGURE 2-1: TYPICAL CIRCUITS



Note 1: Up to 7 functions can be implemented by pressing more than one button simultaneously or by using a suitable diode array.

2: Resistor (R) is recommended for current limiting.

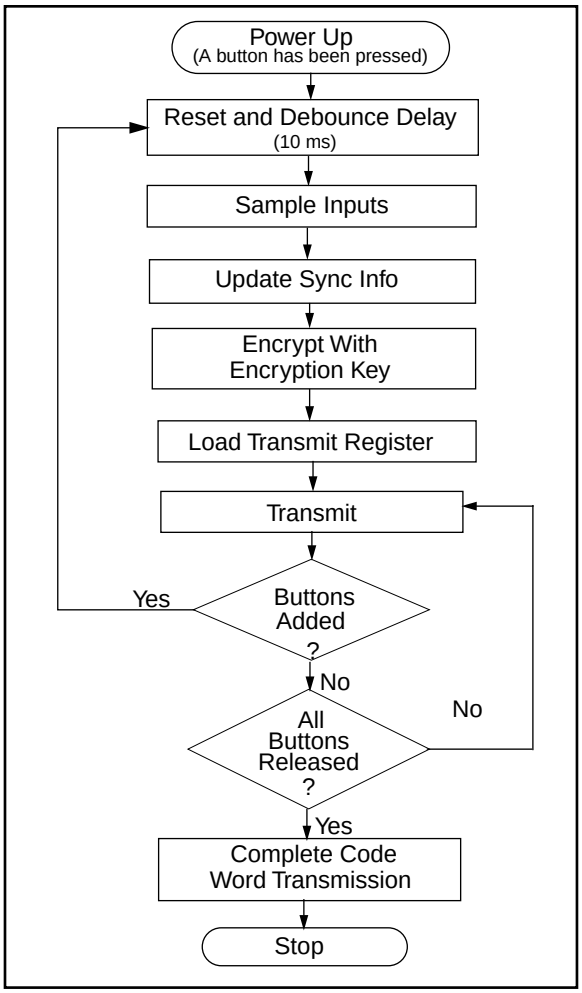
TABLE 2-1: PIN DESCRIPTIONS

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
V_{SS}	5	Ground reference connection
PWM	6	Pulse width modulation (PWM) output pin/Data pin for programming mode
V_{DD}	8	Positive supply voltage connection

The high security level of the HCS200 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 the information in the previous transmission, the next coded transmission will be totally different. Statistically, if only one bit in the 32-bit string of information changes, approximately 50 percent of the coded transmission will change. The HCS200 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 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 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 HCS200 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	Reserved	Set to 0000H
11	CONFIG	Config Word

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 may be different from the KEELOQ algorithm. 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 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)

This is the 2-word (32-bit) seed code that will be transmitted when all three buttons are pressed at the same time. 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.

3.6 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	Discrimination Bit 10
11	Discrimination Bit 11
12	Voltage Trip Point Select (VLOW SEL)
13	Baudrate Select Bit 0 (BSL0)
14	Reserved
15	Reserved

3.6.1 DISCRIMINATION VALUE (DISC0 TO DISC11)

Bits 14 and 15 should be set to zero. 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 12 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 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.

3.6.2 BAUD RATE SELECT BITS (BSL0)

BSL0 selects 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: BAUD RATE SELECT

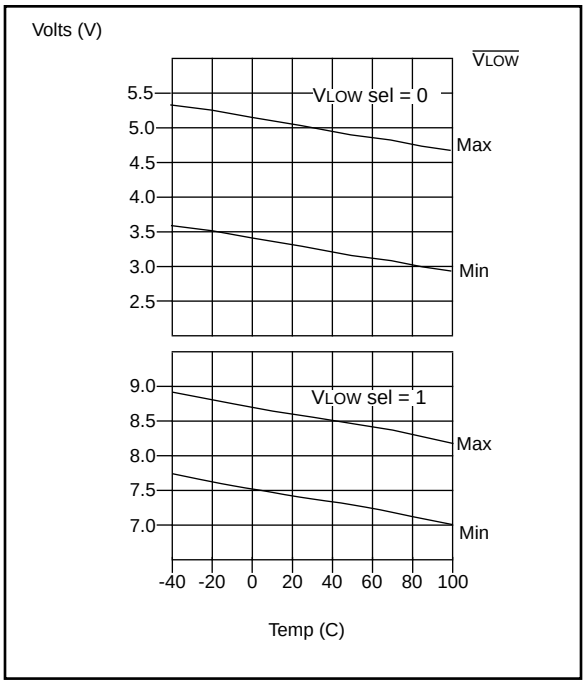
BSL0	Basic Pulse Element	Code Words Transmitted
0	400 µs	All
1	200 µs	1 out of 2

3.6.3 LOW VOLTAGE TRIP POINT SELECT

The low voltage trip point select bit is used to tell the HCS200 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: VOLTAGE TRIP POINTS BY CHARACTERIZATION



4.0 TRANSMITTED WORD

4.1 Transmission Format

The HCS200 transmission is made up of several parts (Figure 4-1). Each transmission begins with a preamble and a header, followed by the encrypted 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 button status 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 with he code word. The button code will be the S0, S1 value at the falling edge 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 4-3.

4.3 Code Word Organization

The HCS200 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 **Encrypted Data** is generated from 3 button bits, 12 discrimination bits, and the 16-bit sync value (Figure 4-2).

The **Fixed Code Data** is made up from 1 status bit, 1 fixed bit, 4 button bits, and the 28-bit serial number.

FIGURE 4-1: CODE WORD TRANSMISSION FORMAT

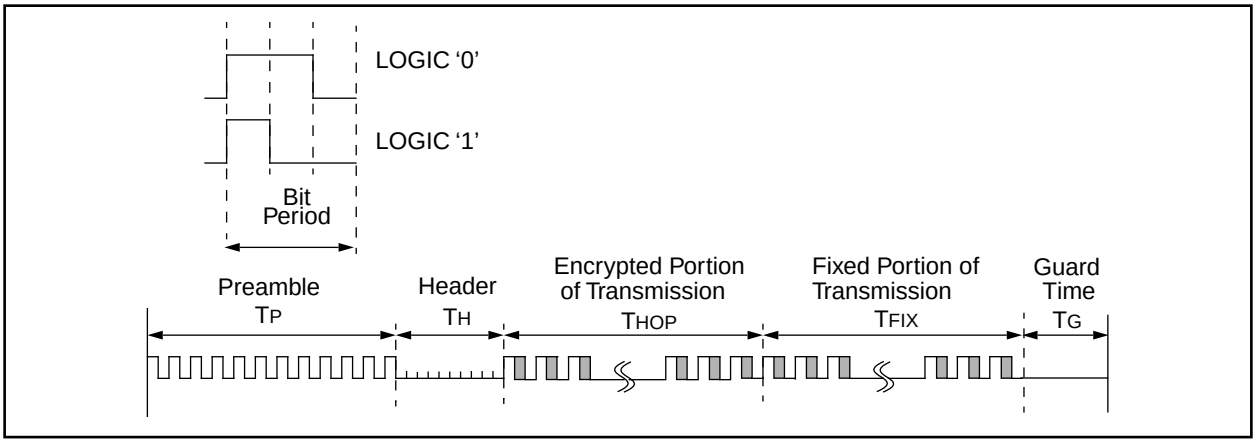


FIGURE 4-2: CODE WORD ORGANIZATION

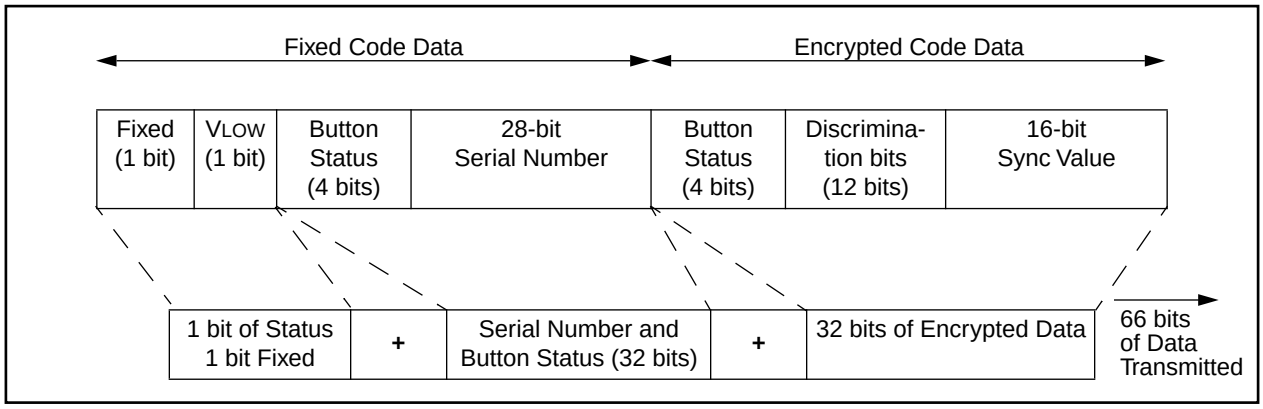


FIGURE 4-3: SYNCHRONOUS TRANSMISSION MODE

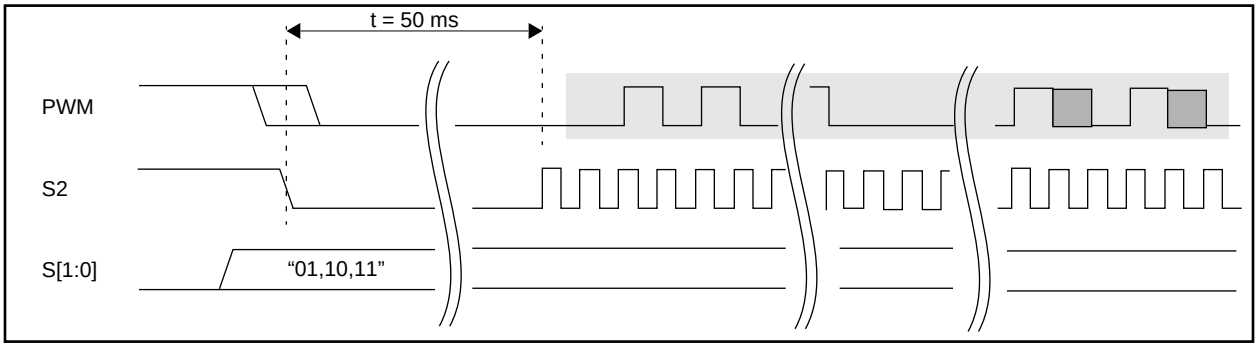
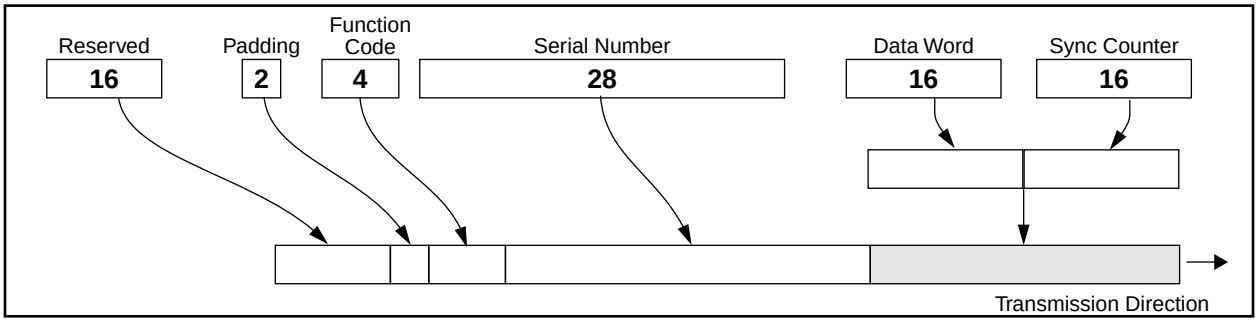


FIGURE 4-4: TRANSMISSION WORD FORMAT DURING SYNCHRONOUS TRANSMISSION MODE



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 button is released before the transmission is complete. The HCS200 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 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 100 ms 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 baud rate selection bit BSL0. 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 word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

5.3 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 on the HCS200 which is stored in EEPROM and can only be transmitted when all three button inputs are pressed at the same time (Table 5-1). Instead of the normal key generation method being used to create the encryption key, this seed value is used.

5.4 VLOW: Voltage LOW indicator

The VLOW bit is transmitted with every transmission (Figure 4-2 and Figure 8-5) and will be transmitted as a zero if the operating voltage is above the voltage trip point. The VLOW signal is transmitted so the receiver can give an indication to the user that the transmitter battery is low.

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

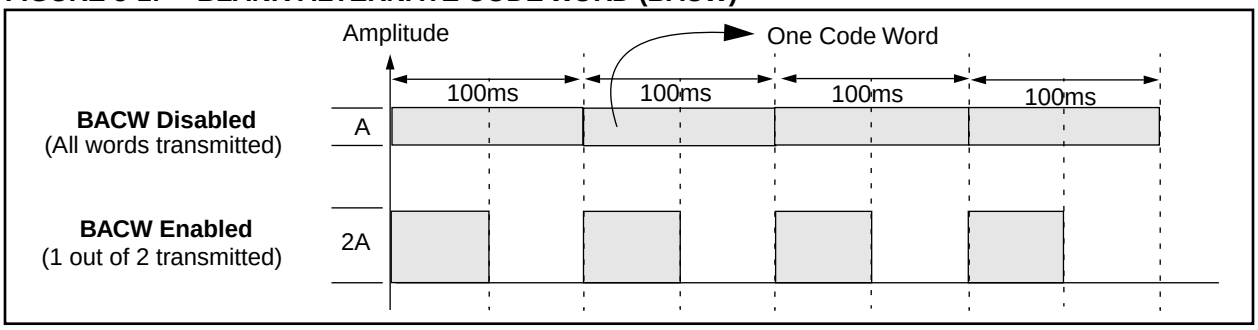


TABLE 5-1: PIN ACTIVATION TABLE

	External			Internal			
	S2	**S1**	**S0**	**S3**	**S2**	**S1**	**S0**
Standby after CC	0	0	0	0	0	0	0
Hop	0	0	1	0	0	0	1
	0	1	0	0	0	1	0
	0	1	1	0	0	1	1
	1	0	0	1	1	0	0
	1	0	1	1	1	1	0
	1	1	0	1	1	1	0
Fixed	1	1	1	1	1	1	1

6.0 PROGRAMMING THE HCS200

When using the HCS200 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 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 PWM as the data in line. Data clocked in on falling edge of S2.

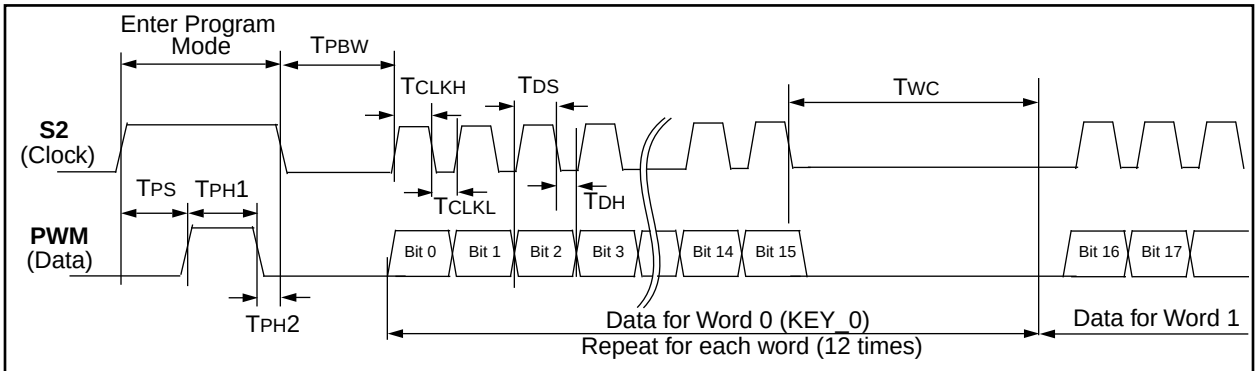
After each 16-bit word is loaded, a programming delay of TWC is required for the internal program cycle to complete. At the end of the programming cycle, the device can be verified (Figure 6-2) by reading back the EEPROM. Reading is done by clocking the S2 line and reading the data bits on PWM. Falling edge of S2 initiated reading. 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.

TABLE 6-1: PROGRAMMING/VERIFY TIMING REQUIREMENTS

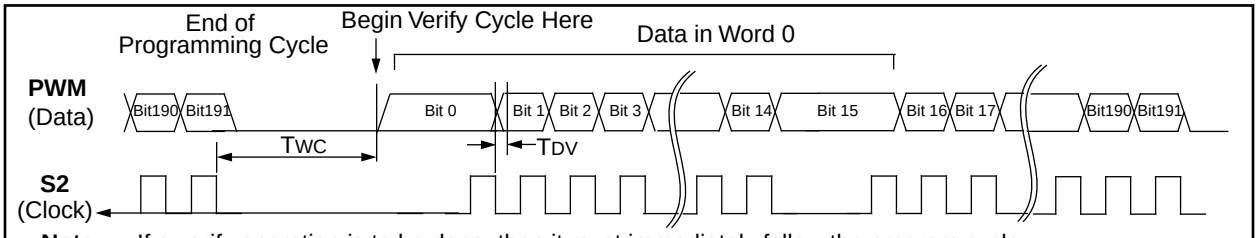
VDD = 5.0V ± 10%, 25°C ± 5 °C				
Parameter	**Symbol**	**Min.**	**Max.**	**Units**
Program mode setup time	TPS	3.5	4.5	ms
Hold time 1	TPH1	3.5	—	ms
Hold time 2	TPH2	50	—	µs
Bulk Write time	TPBW	—	3.5	ms
Program delay time	TPROG	—	3.5	ms
Program cycle time	TWC	—	36	ms
Clock low time	TCLKL	25	—	µs
Clock 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

FIGURE 6-1: PROGRAMMING WAVEFORMS



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

FIGURE 6-2: VERIFY WAVEFORMS



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

7.0 INTEGRATING THE HCS200 INTO A SYSTEM

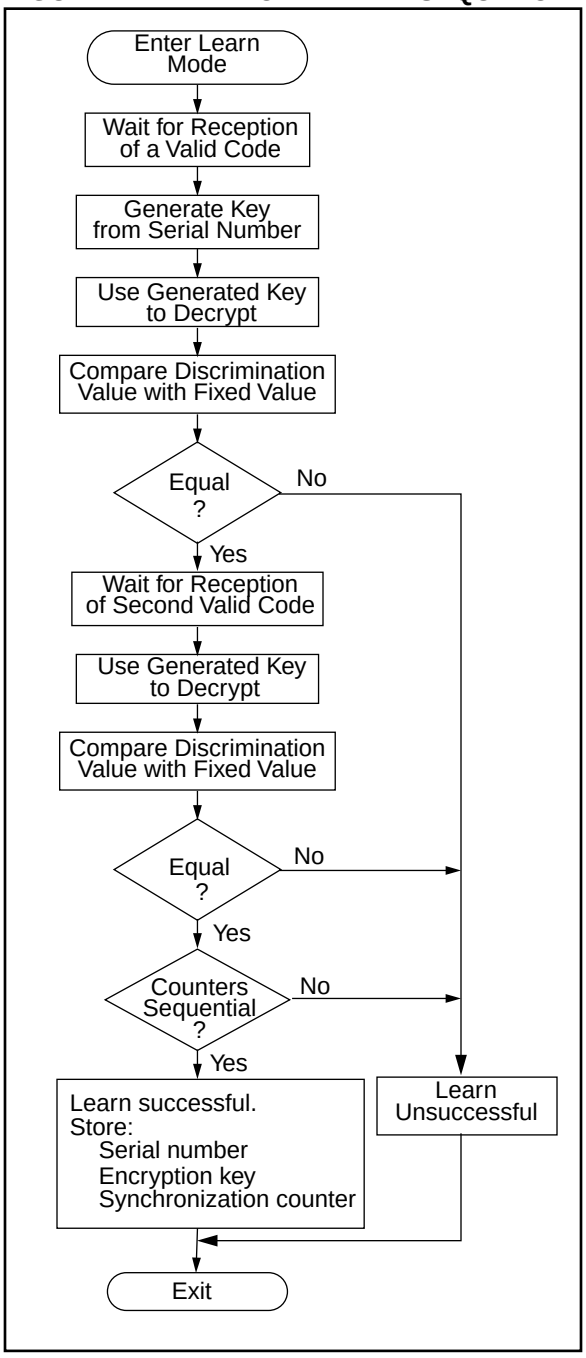
Use of the HCS200 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a license agreement) firmware routines that accept transmissions from the HCS200 and decrypt the hopping code portion of the data stream. These 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 and current synchronization 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 transmission 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.

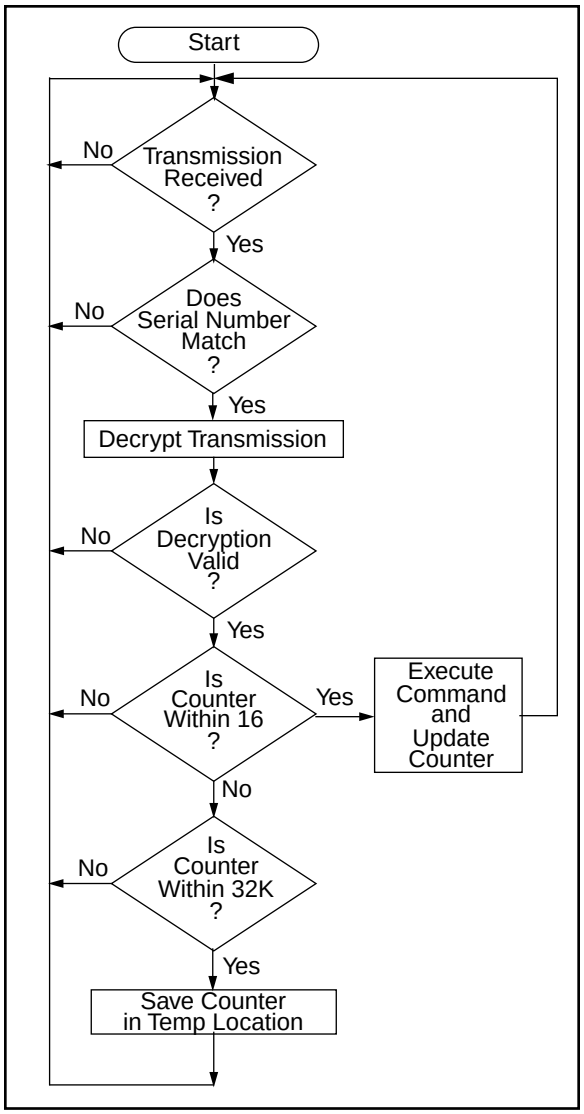
FIGURE 7-1: TYPICAL LEARN SEQUENCE



7.2 Decoder operation

In a typical decoder operation (Figure 7-2), the key generation on the decoder side is done by taking the serial number from a transmission and combining that with the manufacturer's code to create the same secret key that was used by the transmitter. Once the secret key is obtained, the rest of the transmission can be decrypted. The decoder 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 stored key It uses the discrimination bits to determine if the decryption was valid. If everything up to this point is valid, the synchronization value is evaluated.

FIGURE 7-2: TYPICAL DECODER OPERATION

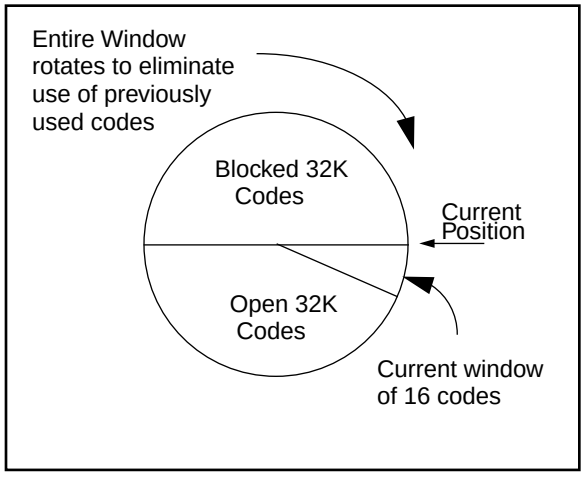


7.3 Synchronization with Decoder

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 counter value for that particular transmitter and the counter value that was just decrypted are within a formatted window of say 16, the counter is stored and the command is executed. If the counter value was not within the single operation window, but is within the double operation window of say 32K window, the transmitted synchronization value is stored in temporary location and it goes back to waiting for another transmission. When the next valid transmission is received, it will check the new value with the one in temporary storage. If the two values are sequential, it is assumed that the counter had just gotten out of the single operation 'window', but is now back in sync, so the new synchronization 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 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



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 1.5 8.0	1.0 3.0 12.0	mA	V_{DD} = 3.5V V_{DD} = 6.6V V_{DD} = 13.0V
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} = -2.0mA
Low level output voltage	V_{OL}			0.08 V_{DD}	V	I_{OL} = 2.0mA
Resistance; S0-S2	R_{S0-2}	40	60	80	KΩ	V_{IN} = 4.0V
Resistance; PWM	R_{PWM}	80	120	160	KΩ	V_{IN} = 4.0V

Note: Typical values are at 25°C.

FIGURE 8-1: TYPICAL ICC CURVE OF HCS200 WITH EXTERNAL RESISTORS

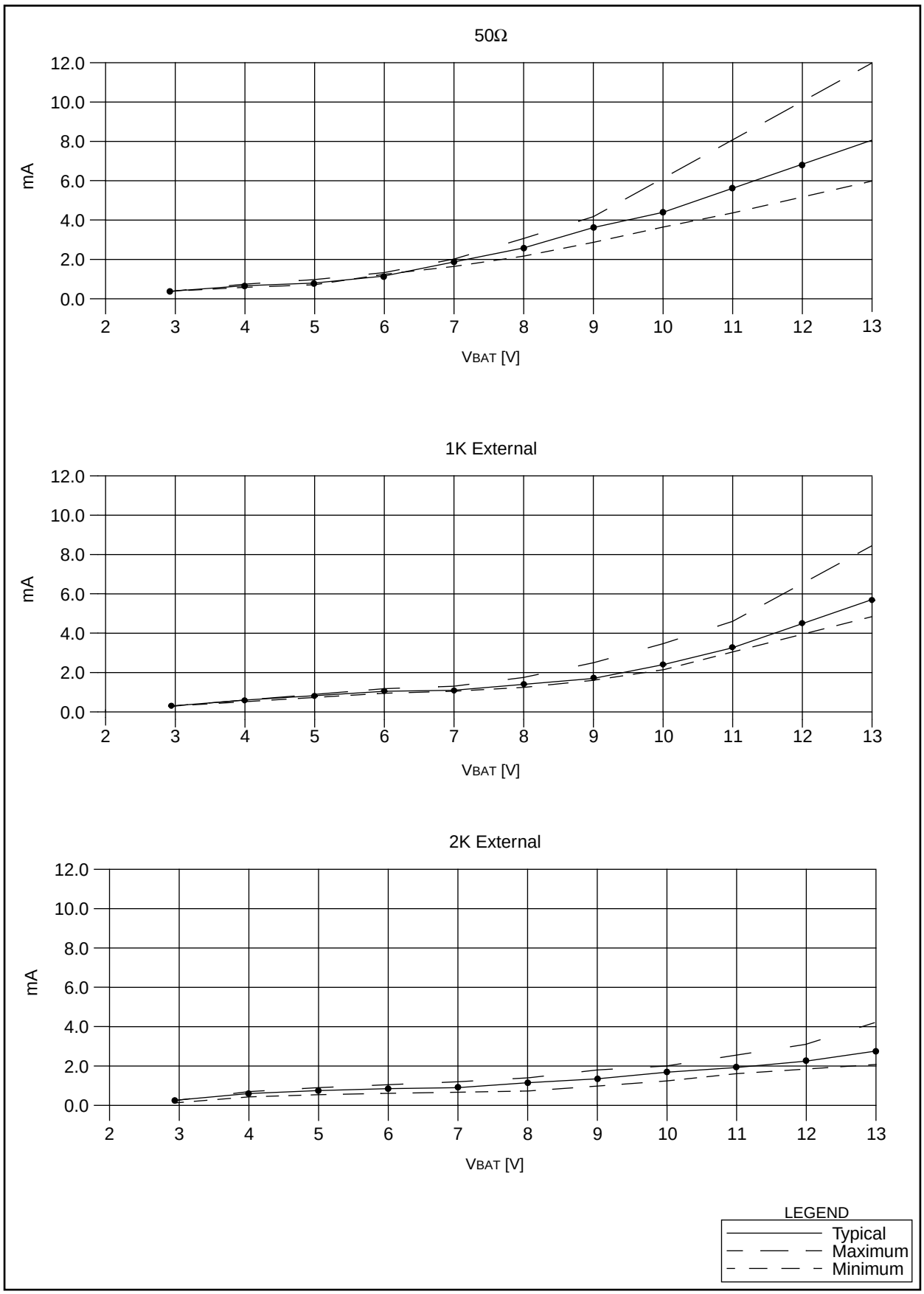


FIGURE 8-2: POWER UP AND TRANSMIT TIMING

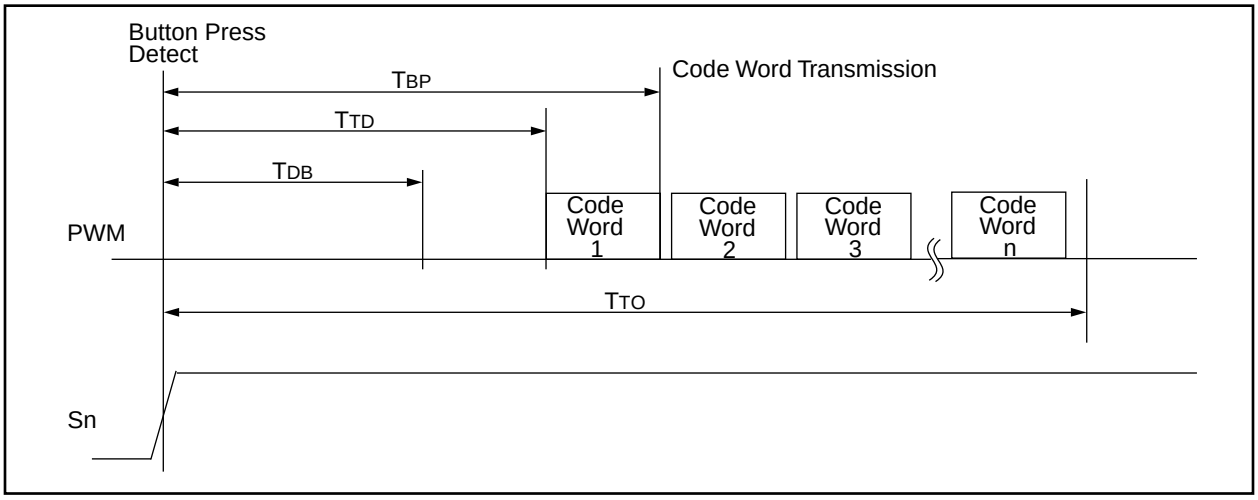


TABLE 8-3: POWER UP AND TRANSMIT TIMING REQUIREMENTS

V_{DD} = +3.5 to 13.0V 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	T_{BP}	10 + Code Word	26 + Code Word	ms	(Note 1)
Transmit delay from button detect	T_{TD}	10	26	ms	
Debounce Delay	T_{DB}	6	15	ms	
Auto-shutoff time-out period	T_{TO}	20	120	s	(Note 2)

Note 1: T_{BP} 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 time-out period is not tested.

FIGURE 8-3: PWM FORMAT

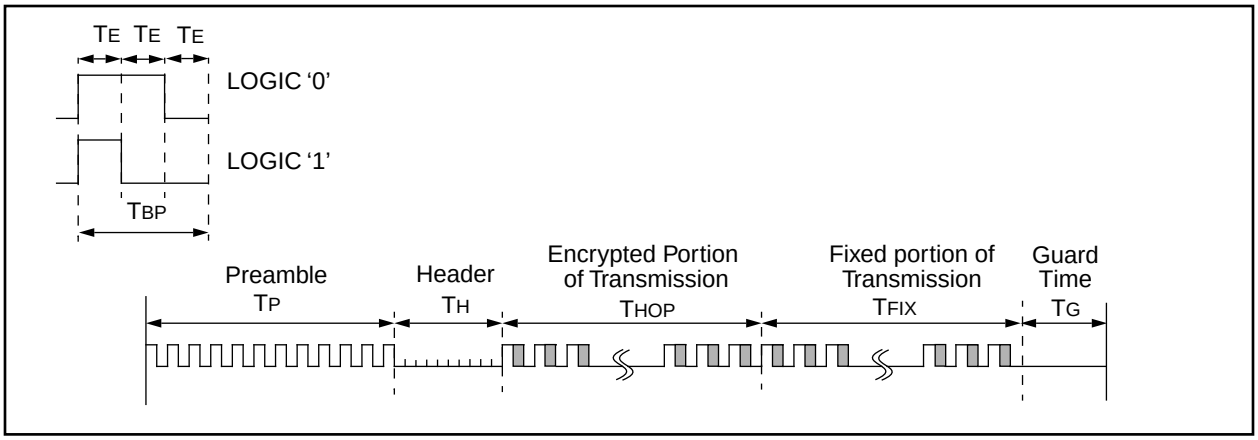


FIGURE 8-4: PREAMBLE/HEADER FORMAT

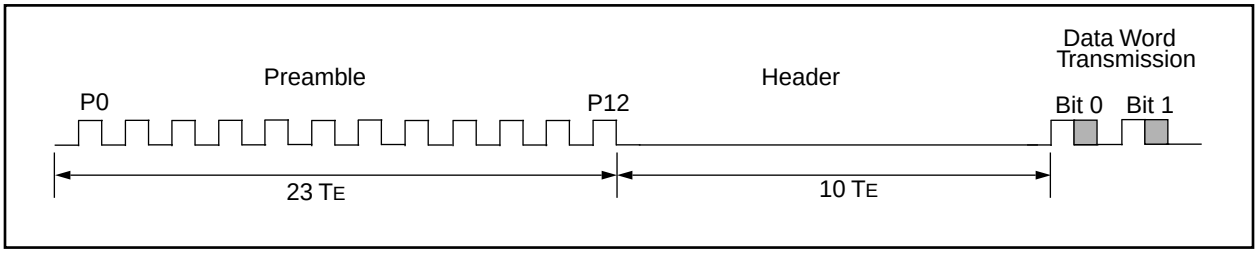


FIGURE 8-5: DATA WORD FORMAT

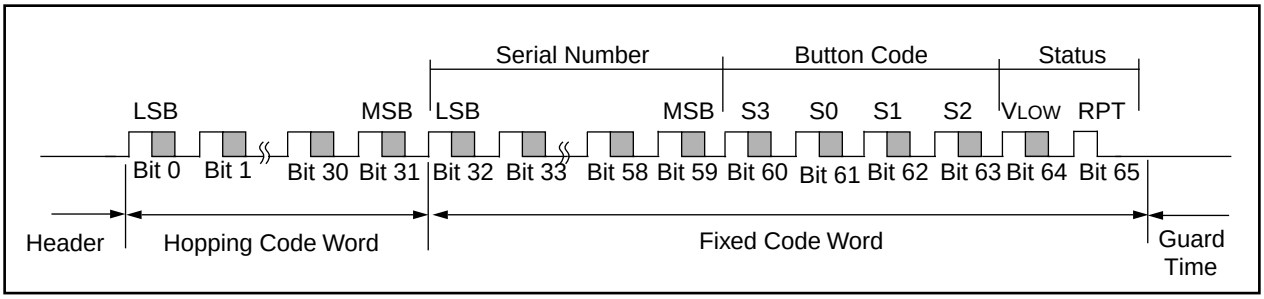
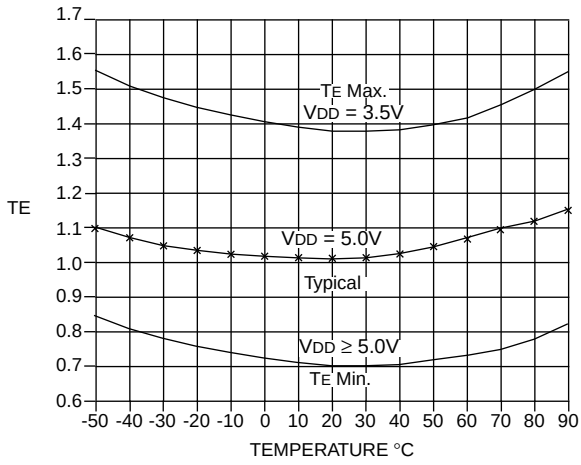


TABLE 8-4: CODE WORD TRANSMISSION TIMING REQUIREMENTS

VDD = +3.5 to 13.0V Commercial (C): Tamb = 0°C to +70°C Industrial (I): Tamb = -40°C to +85°C			Code Words Transmitted						
			All			1 out of 2			
Symbol	**Characteristic**	**Number of TE**	**Min.**	**Typ.**	**Max.**	**Min.**	**Typ.**	**Max.**	**Units**
TE	Basic pulse element	1	280	400	620	140	200	310	µs
TBP	PWM bit pulse width	3	840	1200	1860	420	600	930	µs
TP	Preamble duration	23	6.4	9.2	14.3	3.2	4.6	7.1	ms
TH	Header duration	10	2.8	4.0	6.2	1.4	2.0	3.1	ms
THOP	Hopping code duration	96	26.9	38.4	59.5	13.4	19.2	29.8	ms
TFIX	Fixed code duration	102	28.6	40.8	63.2	14.3	20.4	31.6	ms
TG	Guard Time	39	10.9	15.6	24.2	5.5	7.8	12.1	ms
—	Total Transmit Time	270	75.6	108.0	167.4	37.8	54.0	83.7	ms
—	PWM data rate	—	1190	833	538	2381	1667	1075	bps

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

FIGURE 8-6: HCS200 TE VS. TEMP (BY CHARACTERIZATION)



HCS200 Product Identification System

To order or to obtain information (e.g., on pricing or delivery), please use the listed part numbers, and refer to the factory or the listed sales offices.

HCS200 - /P

Package:	P	=	Plastic DIP (300 mil Body), 8-lead
	SN	=	Plastic SOIC (150 mil Body), 8-lead
Temperature Range:	Blank	=	0°C to +70°C
	I	=	-40°C to +85°C
Device:	HCS200		Code Hopping Encoder
	HCS200T		Code Hopping Encoder (Tape and Reel)

AMERICAS

Corporate Office
Microchip Technology Inc.
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 602 786-7200 Fax: 602 786-7277
Technical Support: 602 786-7627
Web: 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: 708 285-0071 Fax: 708 285-0075

Dallas
Microchip Technology Inc.
14651 Dallas Parkway, Suite 816
Dallas, TX 75240-8809
Tel: 214 991-7177 Fax: 214 991-8588

Dayton
Microchip Technology Inc.
Suite 150
Two Prestige Place
Miamisburg, OH 45342
Tel: 513 291-1654 Fax: 513 291-9175

Los Angeles
Microchip Technology Inc.
18201 Von Karman, Suite 1090
Irvine, CA 92715
Tel: 714 263-1888 Fax: 714 263-1338

New York
Microchip Technology Inc.
150 Motor Parkway, Suite 416
Hauppauge, NY 11788
Tel: 516 273-5305 Fax: 516 273-5335

AMERICAS *(continued)*

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

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

ASIA/PACIFIC

Hong Kong
Microchip Technology
Rm 3801B, Tower Two
Metroplaza,
223 Hing Fong Road,
Kwai Fong, N.T., Hong Kong
Tel: 852 2 401 1200 Fax: 852 2 401 3431

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

Singapore
Microchip Technology
200 Middle Road
#10-03 Prime Centre
Singapore 188980
Tel: 65 334 8870 Fax: 65 334 8850

Taiwan
Microchip Technology
10F-1C 207
Tung Hua North Road
Taipei, Taiwan, ROC
Tel: 886 2 717 7175 Fax: 886 2 545 0139

EUROPE

United Kingdom
Arizona Microchip Technology Ltd.
Unit 6, The Courtyard
Meadow Bank, Furlong Road
Bourne End, Buckinghamshire SL8 5AJ
Tel: 44 1 628 850303 Fax: 44 1 628 850178

France
Arizona Microchip Technology SARL
Zone Industrielle de la Bonde
2 Rue du Buisson aux Fraises
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 Muenchen, 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 39 689 9939 Fax: 39 39 689 9883

JAPAN

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

6/14/96

MICROCHIP