HCS201

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

- 3.5 -13V operation
- Three button inputs
  - No additional circuitry required
  - 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 pulldown 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

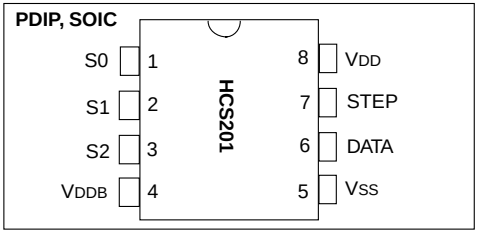
DESCRIPTION

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, 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.

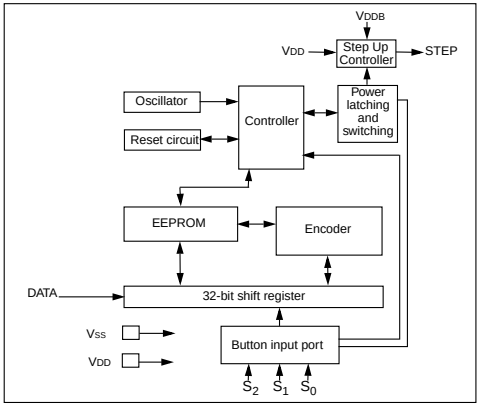
The HCS201 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and six status bits to create a 66-bit transmission steam.

PACKAGE TYPES

PDIP, SOIC



HCS201 BLOCK DIAGRAM



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 encryption key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS201 a very secure unit. The HCS201 provides an easy to use serial interface for programming the necessary security keys, system parameters, and configuration data.

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

The HCS201 operates over a wide voltage range of 3.5V to 13V and has three button inputs in an 8-pin configuration, which allows the system designer the freedom to utilize up to 7 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 KEELOQ product family facilitates several learn strategies to be implemented on the decoder. The following are examples of what can be done.*

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 random seed value 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 HCS201 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 held by the user and operated to gain access to a vehicle or restricted area. The HCS201 requires very few external components (Figure 2-1).

Most keyless entry systems transmit the same code from a transmitter every time a button is pushed. The number of code combinations in a low end security system is also small. 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.

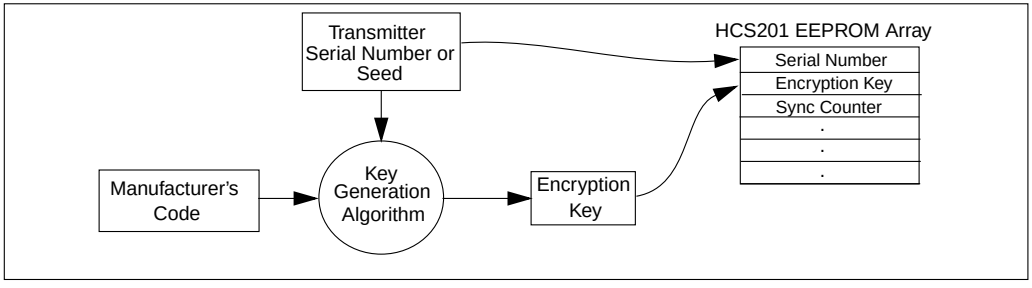
The HCS201 employs the KEELOQ code hopping technology and an encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 66 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

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. The most important of these values are:

- A 28-bit serial number which is meant to be unique for every encoder
- 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



* Third party patents on learning strategy and implementation may apply.

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 encryption 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 4.2.

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 HCS201. Section 7.0 provides more detail on integrating the HCS201 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)

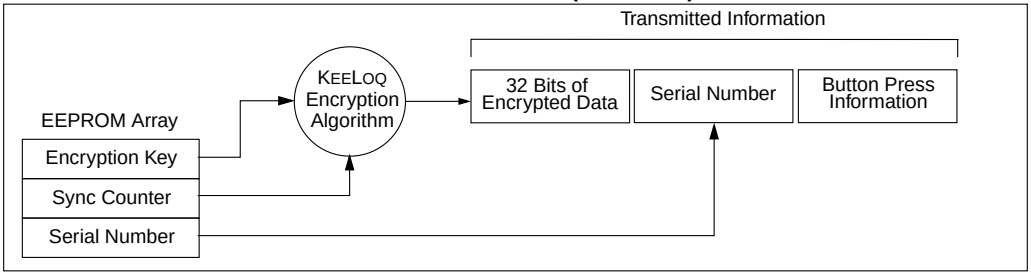
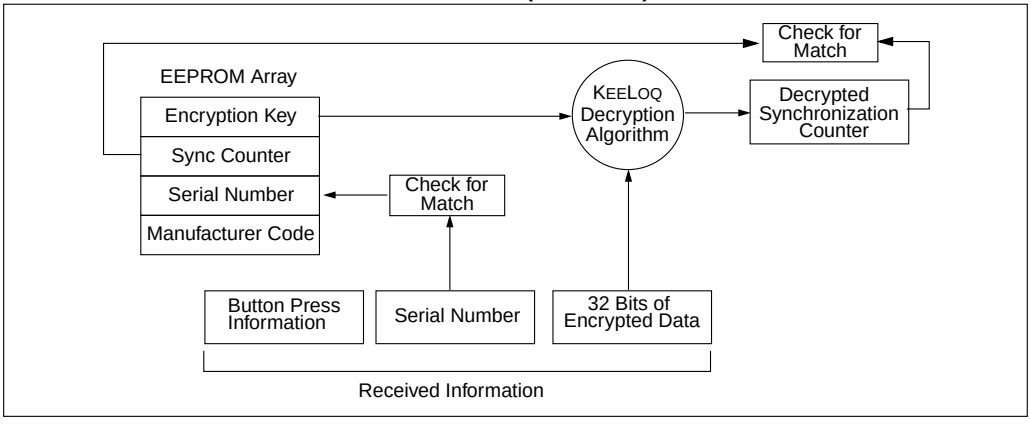


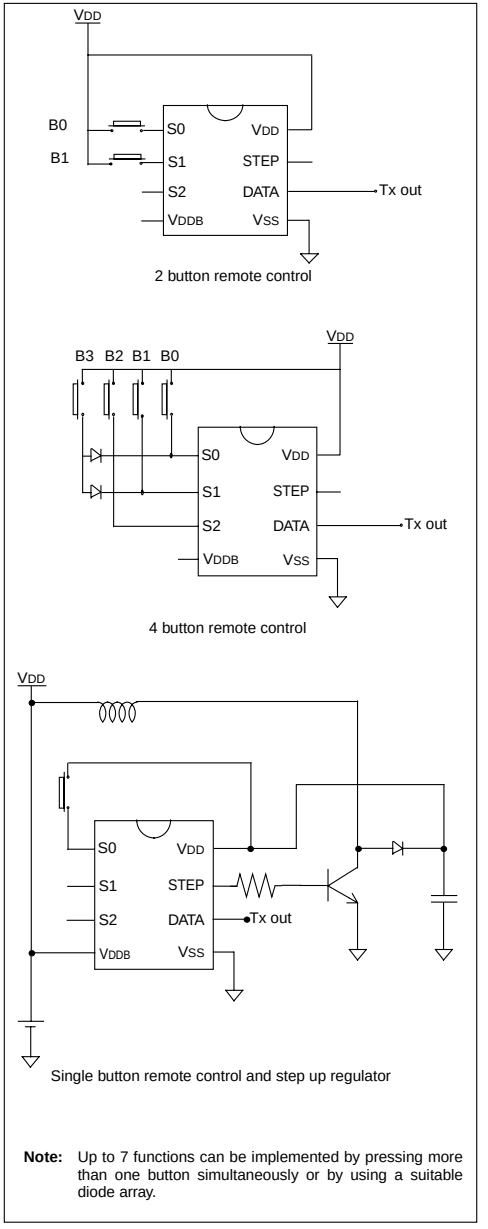
FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



2.0 DEVICE OPERATION

As shown in 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



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

TABLE 2-1: PIN DESCRIPTIONS

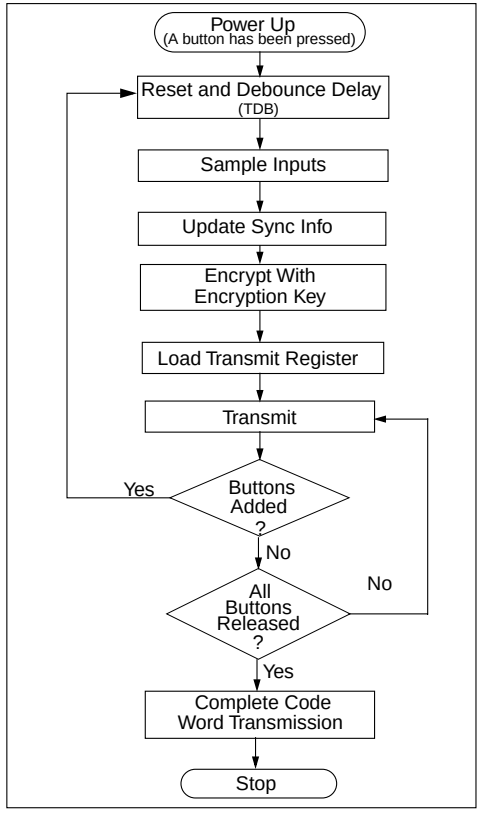
Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2/Clock pin for programming mode
VDDB	4	Battery input pin, supplies power to the step up control circuitry
VSS	5	Ground reference connection
DATA	6	Pulse width modulation (PWM) output pin/Data pin for programming mode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

The security of the HCS201 is based on the patented KEELOQ technology. A block cipher encryption algorithm based on a block length of 32 bits and a key length of 64 bits is used. The algorithm obscures the information in such a way that even if the 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 bits in the coded transmission will change.

The HCS201 will wake up upon detecting a switch closure and then delay approximately 4.5 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 a button is pressed, even if the same button is pushed again. Keeping a button pressed for a long time will result in the same code word being transmitted until the button is released or timeout occurs. A code that has been transmitted will not occur again for more than 64K transmissions. This will provide more than 17 years of typical use before a code is repeated based on 10 operations per day.

If additional buttons are pressed during a transmission, the current transmission is abruptly terminated. The HCS201 restarts, and the new transmission contains the latest button information. When all buttons are released, the device completes the current transmission and then powers down. Released buttons do not terminate and/or restart transmissions.

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 Value
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. Inputs to the key generation algorithm are the serial number for the particular transmitter being used and a secret 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. If a seed is used, the seed will also form part of the input to the key generation algorithm.

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. There are 32 bits allocated for the serial number, only the lower order 28 bits are transmitted if XSER in the config word is cleared. The top four bits are replaced by the function code. The serial number is meant to be unique for every transmitter.

3.4 SEED_0, SEED_1 (Seed Word)

This is the two word (32 bits) 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 or purely as a fixed code transmission.

3.5 Discrimination Value (DISC0 to DISC11)

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, 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.

3.6 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: 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

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

3.6.1 OSCILLATOR TUNING BITS (OSC0 AND OSC3)

These bits are used to tune the nominal frequency of the HCS201 to within ±10% of its nominal value over temperature and voltage.

3.6.2 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 3.6.6

3.6.3 BAUDRATE 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 5.2 provides detailed explanation in code word blanking.

TABLE 3-5: BAUDRATE SELECT

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

3.6.4 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.

3.6.5 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 before the preamble of the first code word.

3.6.6 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 is always set, independent of the value of S2.

3.6.7 EXTENDED SERIAL NUMBER (XSER)

If this bit is cleared the most significant four bits of the HCS201's serial number are replaced with the function code. If this bit is set, the full serial number is transmitted.

4.0 TRANSMITTED WORD

4.1 Transmission Format (PWM Mode)

The HCS201 transmission is made up of several parts (Figure 4-1). Each transmission is begun 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 4-4.

4.3 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 **Encrypted Data** is generated from four function bits, 12 discrimination bits, and the 16-bit synchronization value (Figure 8-4).

The **Fixed Code Data** is made up from two status bits, four function bits, and the 28/32-bit serial number depending on XSER in the configuration word.

FIGURE 4-1: CODE WORD TRANSMISSION FORMAT

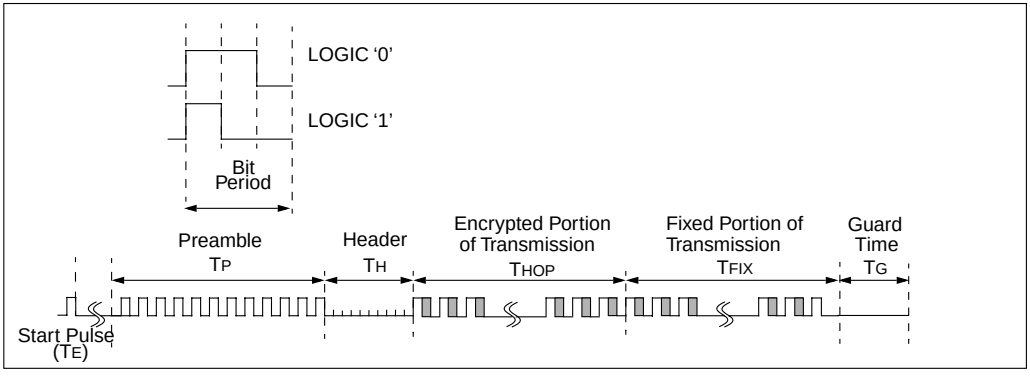


FIGURE 4-2: CODE WORD ORGANIZATION

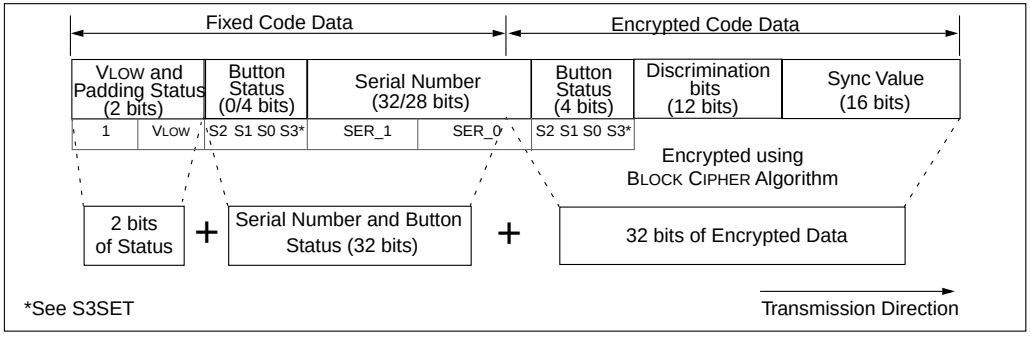


FIGURE 4-3: SYNCHRONOUS TRANSMISSION MODE

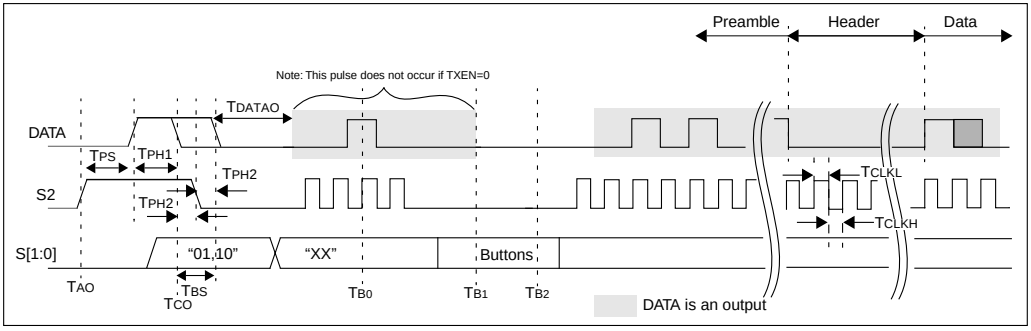
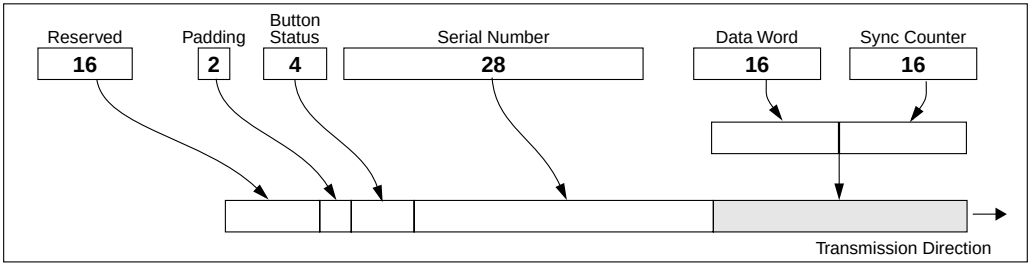


TABLE 4-1: SYNCHRONOUS TRANSMISSION TIMING

Description	Symbol	Time	Units
TX buttons stable (TXEN = 0) (TXEN = 1)	T_{B1}	450 450	µs (relative to T_{C0}) µs (relative to T_{B0})
TX buttons sample (TXEN = 0) (TXEN = 1)	T_{B2}	1.9 1.36	µs (relative to T_{C0}) µs (relative to T_{B0})
Synchronous transmission mode test	T_{BS}	25	µs
Time till DATA is an output	T_{DATAO}	90	µs

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 ensures that the entire code word is transmitted, even if the button is released before the transmission is complete. The HCS201 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 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. The transmission duty cycle can be lowered by setting BSL. Using the BSL bit allows the user to transmit a higher amplitude transmission, if the transmission length is shorter. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

5.3 Secure Learn

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 HCS201 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 and there need not be any mathematical relationship between serial numbers and seeds.

5.4 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 TTO.

TABLE 5-1: PIN ACTIVATION TABLE

	S2	S1	S0	Notes
1	0	0	1	1
2	0	1	0	1
3	0	1	1	1
4	1	0	0	1
5	1	0	1	1
6	1	1	0	1
7	1	1	1	1
8	0	0	0	1
9	0	0	1	1
10	0	1	0	1
11	0	1	1	1
12	1	0	0	1
13	1	0	1	1
14	1	1	0	1
15	1	1	1	2

Note 1: Transmit generated 32-bit code hopping word.

Note 2: Seed transmission.

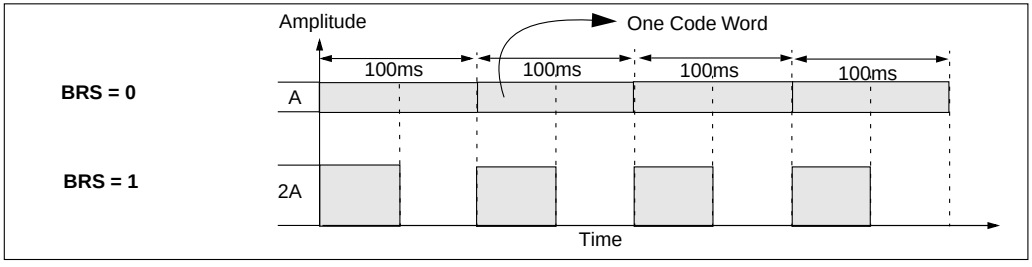
5.5 Step Up Regulator

The onboard step up regulator can be used to ensure the voltage in the RF circuit is constant, independent of what the battery voltage is. VDD is compared to VSTEP, the reference voltage. If VDD falls below this voltage the STEP output is pulsed at fSTEP. This can be connected to a transistor, inductor and capacitor to provide a step up voltage on the device. This is inactive when the device is not transmitting. The power to the step up regulator is taken from the VDDB pin.

5.6 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 3.6.2 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.

FIGURE 5-1: CODE WORD TRANSMISSIONS

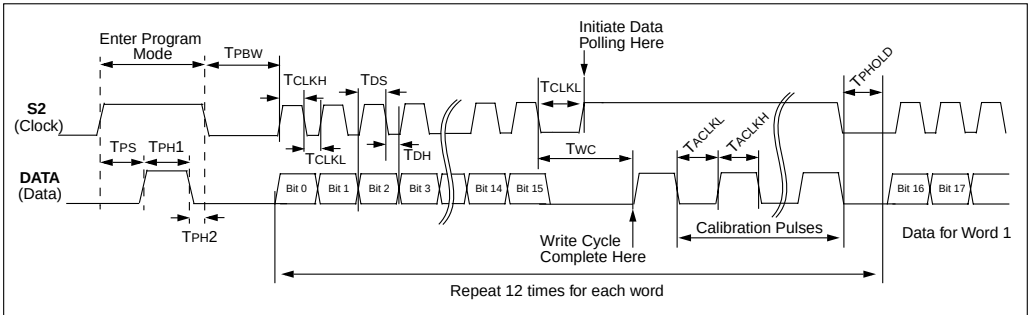


6.0 PROGRAMMING THE HCS201

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**.

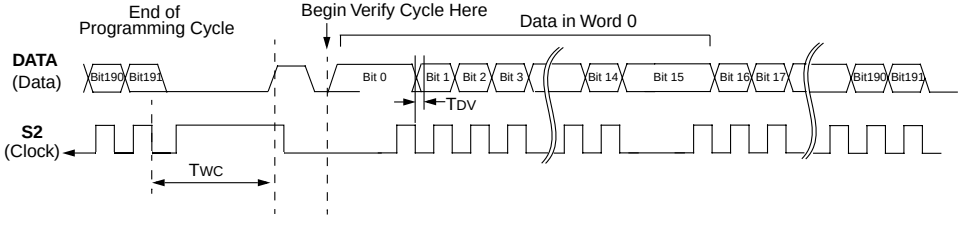
Note:	To ensure that the device does not accidentally enter programming mode, DATA should never be pulled high by the circuit connected to it. Special care should be taken when driving PNP RF transistors.

FIGURE 6-1: PROGRAMMING WAVEFORMS



Note 1: S0 and S1 button inputs to be held to ground during the entire programming sequence.

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

V_{DD} = 5.0V ± 10% 25° C ± 5 °C				
Parameter	**Symbol**	**Min.**	**Max.**	**Units**
Program mode setup time	T_{PS}	2	—	ms
Hold time 1	T_{PH1}	4.0	—	ms
Hold time 2	T_{PH2}	50	—	µs
Bulk Write time	T_{PBW}	—	2.2	ms
Program delay time	T_{PROG}	—	2.2	ms
Program cycle time	T_{WC}	—	36	ms
Clock low time	T_{CLKL}	25	—	µs
Clock high time	T_{CLKH}	25	—	µs
Data setup time	T_{DS}	0	—	µs
Data hold time	T_{DH}	18	—	µs
Data out valid time	T_{DV}	10	24	µs
Hold time	T_{PHOLD}	100	—	µs
Acknowledge low time	T_{ACKL}	800	—	µs
Acknowledge high time	T_{ACKH}	800	—	µs

7.0 INTEGRATING THE HCS201 INTO A SYSTEM

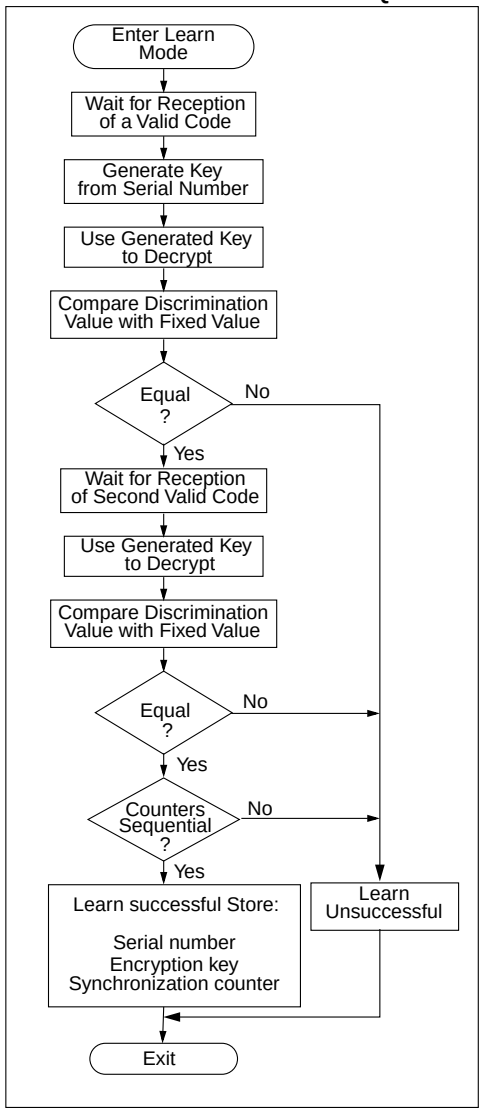
Use of the HCS201 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip provides (via a license agreement) firmware routines and pre-programmed decoders that accept transmissions from the HCS201 and decrypt the hopping code portion of the data stream. These routines and devices 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.

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

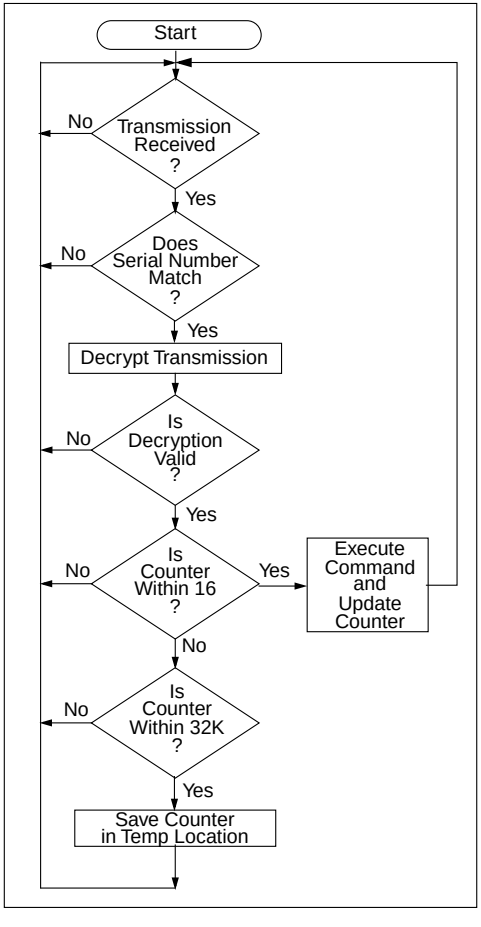
FIGURE 7-1: TYPICAL LEARN SEQUENCE



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

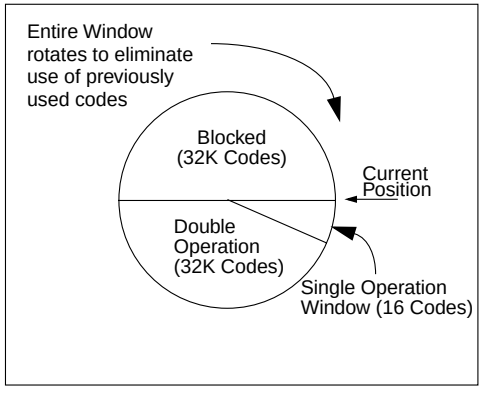


7.3 Synchronization with Decoder

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 13.5	V
V_{IN}	Input voltage	-0.3 to V_{DD} + 0.3	V
V_{OUT}	Output voltage	-0.3 to V_{DD} + 0.3	V
I_{OUT}	Max output current	50	mA
T_{STG}	Storage temperature	-55 to +125	C (Note)
T_{LSOL}	Lead soldering temp	300	C (Note)
V_{ESD}	ESD rating	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} < 5.0V			5.0V < V_{DD} < 13.3V				
Parameter	**Sym.**	**Min**	**Typ[1]**	**Max**	**Min**	**Typ[1]**	**Max**	**Unit**	**Conditions**
Operating current (avg)[2]	I_{CC}		0.2	0.5		1.5	2	mA mA	
Standby current	I_{CCS}		0.1	1.0		0.1	1.0	µA	
Auto-shutoff current[3,4]	I_{CCS}		40	75		160	300	µA	
High level Input voltage	V_{IH}	0.55V_{DD}		V_{DD}+0.3	2.75		V_{DD}+0.3	V	
Low level input voltage	V_{IL}	-0.3		0.15V_{DD}	-0.3		0.75	V	
High level output voltage	V_{OH}	0.6V_{DD}			3.3			V V	I_{OH} = -1.0 mA V_{DD} = 3.5V I_{OH} = -2.0 mA V_{DD} = 12V
Low level output voltage	V_{OL}			0.08V_{DD}			0.4	V V	I_{OL} = 1.0 mA V_{DD} = 5V I_{OL} = 2.0 mA V_{DD} = 12V
Resistance; S0-S2	R_{SO-2}	40	60	80	40	60	80	kΩ	V_{DD} = 4.0V
Resistance; DATA	R_{DATA}	80	120	160	80	120	160	kΩ	V_{DD} = 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 pulldown resistors.
4: Auto-shutoff current is periodically sampled and not 100% tested.

TABLE 8-3: AC CHARACTERISTICS

		Standard Operating Conditions (unless otherwise specified): Commercial (C): 0°C ≤ TA ≤ +70°C Industrial (I): -40°C ≤ TA ≤ +85°C				
Symbol	**Parameters**	**Min**	**Typ**	**Max**	**Units**	**Conditions**
TBP	Time to second button press	10 + Code Word Time	—	26 + Code Word Time	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	(Note 2)
TS	Start pulse delay	—	4.5	—	ms	
fSTEP	Stepper output frequency	125	200	250	kHz	
VSTEP	Stepper reference voltage	6.0	6.5	7	V	

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.
3: These parameters are characterized but not tested.

FIGURE 8-1: POWER UP AND TRANSMIT TIMING

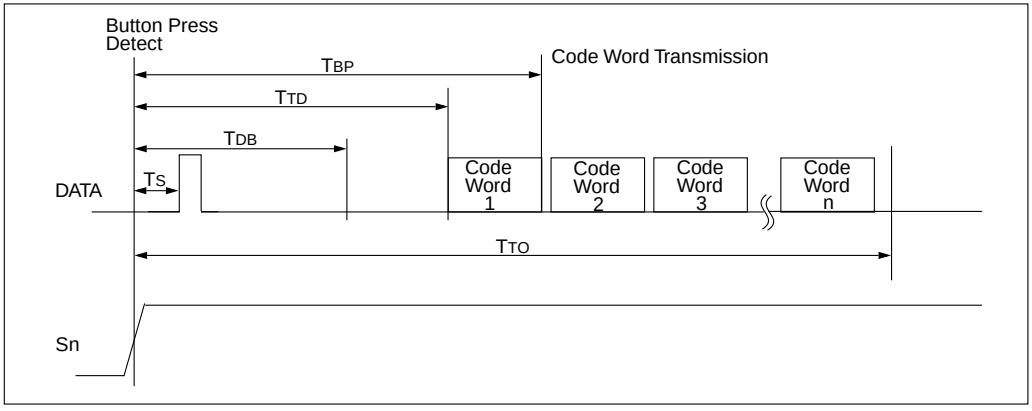


FIGURE 8-2: PWM FORMAT

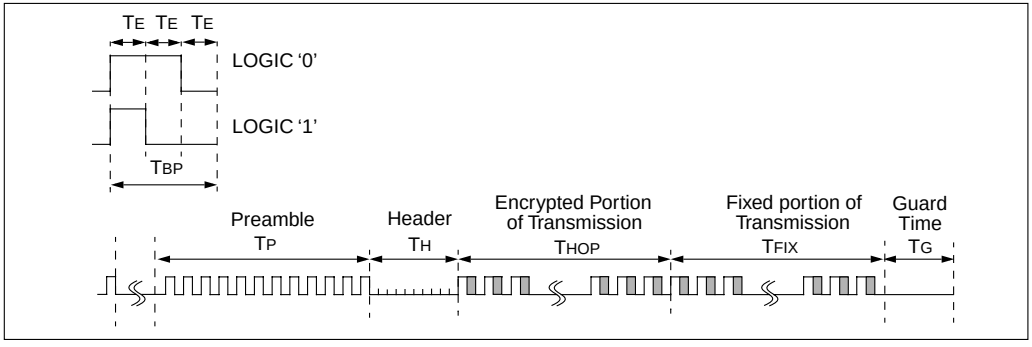


FIGURE 8-3: PREAMBLE/HEADER FORMAT (XSER = 0)

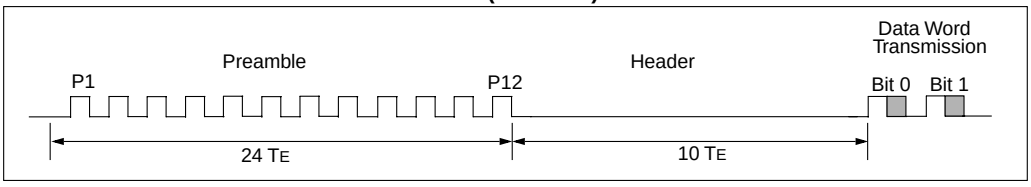


FIGURE 8-4: DATA WORD FORMAT (XSER = 0)

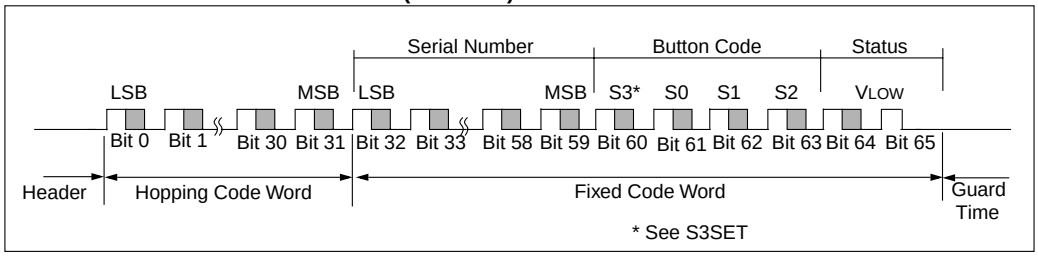


TABLE 8-4: CODE WORD TRANSMISSION TIMING REQUIREMENTS

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						
			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	24	8.64	9.6	10.56	4.32	4.8	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: The timing parameters are not tested but derived from the oscillator clock.

NOTES:

HCS201 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.

HCS201 - /P

Package:	P	=	Plastic DIP (300 mil Body), 8-lead
	SN	=	Plasitic SOIC (150 mil body), 8-lead
Temperature Range:	Blank	=	0˚C to +70˚C
	I	=	–40˚C to +85˚C
Device:	HCS201		Code Hopping Encoder
	HCS201T		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: (602) 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 — ANSI-RAB QMS ACCREDITED — DNV — DNV MSC The Netherlands Accredited by the RvA
ISO 9001 / QS-9000 REGISTERED FIRM

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