HCS301

Code Hopping Encoder Product Brief*

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, 4-bit function, VLOW, RPT
- Encryption keys are read protected

Operating

- High voltage part
- Four button inputs
  - No additional circuitry required
  - 15 functions available
- Selectable baud rate
- Automatic power down after transmission
- Battery low signal transmitted to receiver
- Nonvolatile synchronization data

Other

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

Typical Applications

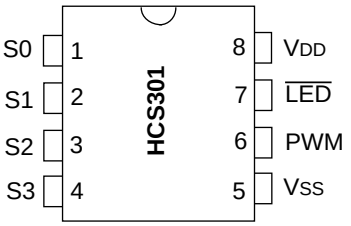
- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Electronic door locks
- Identity tokens
- Burglar alarm systems

GENERAL DESCRIPTION

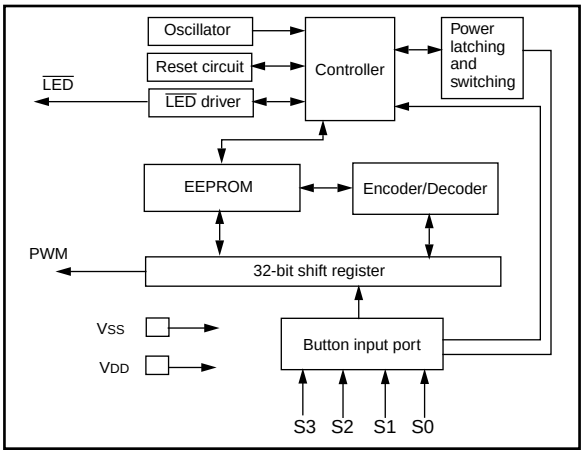
The Microchip Technology Inc. HCS301 is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS301 utilizes the patented KEELOQ® code hopping technology and features high security, a small package outline, high voltage operation, and low cost to make this device a perfect solution for unidirectional RKE and access control systems.

PACKAGE TYPES

PDIP, SOIC



BLOCK DIAGRAM



The HCS301 combines 32-bit code hopping code generated by a non-linear encryption algorithm with a 28-bit serial number and six 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 (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 HCS301 a very secure unit. The HCS301 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.

*Code hopping encoder patents allowed and pending.

KEELOQ is a registered trademark of Microchip Technology Inc.

The HCS301 provides a cost effective solution for systems operating between 6 volts and 12 volts, and has four functional inputs in an 8-pin configuration. This gives the system designer the freedom to have up to 15 functions without adding any additional circuitry.

1.0 DEVICE OPERATION

1.1 Key Terms

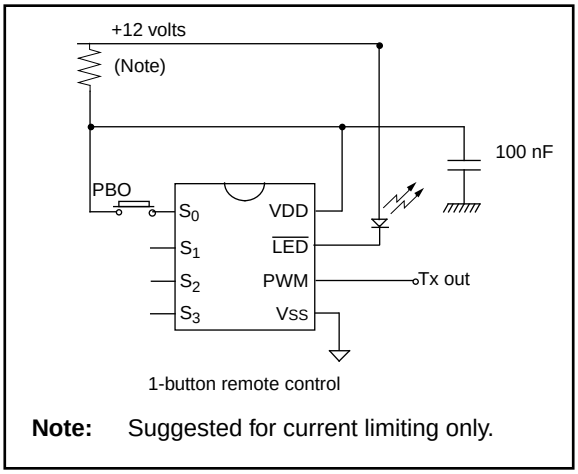
- Manufacturer's key - a 64-bit word unique to each manufacturer used to produce a unique secret key in each encoder.
- Secret Key - a unique 64-bit key generated from the manufacturers key and the encoder serial number and used in the encryption.
- Learn - The ability of the decoder to learn information about an encoder so that future transmissions can be recognized and validated.

As shown in Figure 1-1, the HCS301 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. The high security level of the HCS301 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, at least 50 percent of the coded transmission will change. As indicated in Figure 1-2, the HCS301 will wake up upon detecting a switch closure and then delay 10 ms for switch debounce. The switch information together with the synchronization information will be encrypted using the block cipher to create the variable portion of the transmission. The encrypted or code hopping 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 approximately 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, with the first 128K never repeated.

1.2 Programming the HCS301

The HCS301 must be programmed before use. Programming the device is done using a simple serial interface using two of the pins on the HCS301 for clock and data. When the programming cycle is entered, all EEPROM values are erased and verification of the stored values is not possible until after the programming cycle is complete. These features prevent unauthorized access to the stored values and manipulation of the synchronization counters.

FIGURE 1-1: TYPICAL APPLICATION CIRCUIT



Note: Suggested for current limiting only.

FIGURE 1-2: ENCODER OPERATION

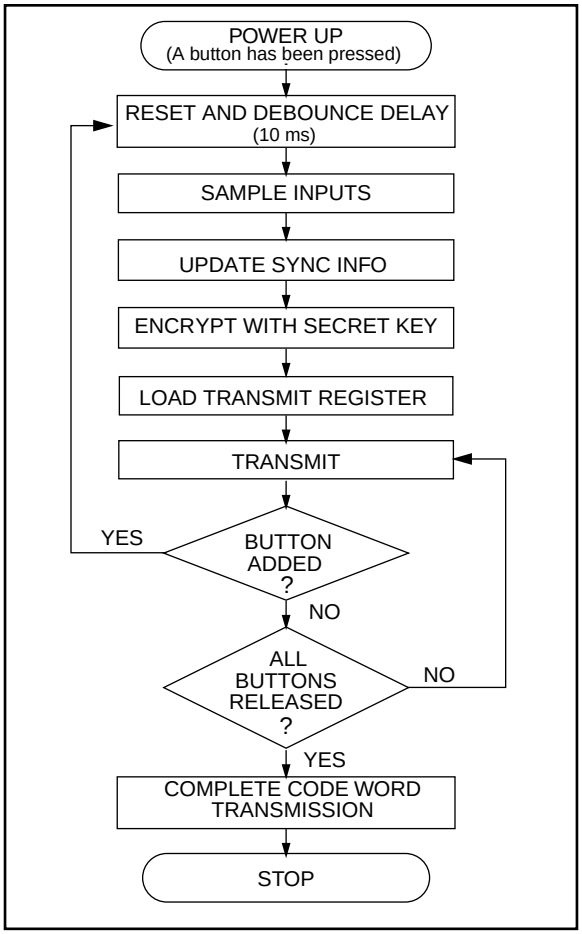
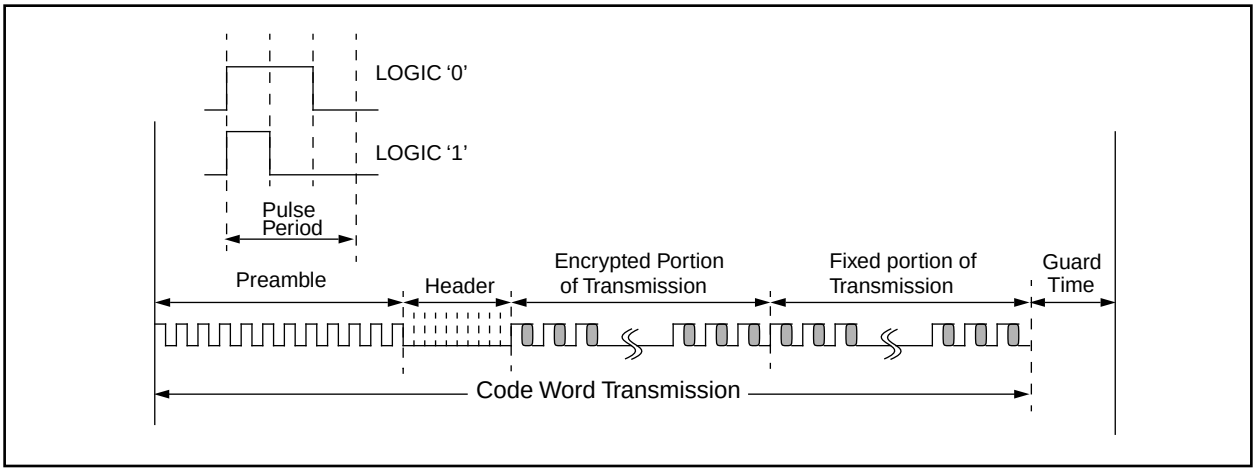


FIGURE 1-3: CODE WORD TRANSMISSION FORMAT



1.3 Transmission Format

As indicated in the diagram above, the 66-bit transmitted word consists of a fixed 34-bit portion and a 32-bit encrypted data portion. The encrypted portion provides up to four billion changing code combinations and includes the function bits along with the synchronization data and discrimination bits. The fixed portion is comprised of a repeat bit (RPT), a battery bit (LOW), the function bits (4) (based on which buttons were activated), and the serial number. The fixed and encrypted sections combined increase the number of combinations to 7.38×10^{19}.

1.4 Decoder Operation*

Use of the HCS301 in a system requires a compatible decoder device on the receiver end of the system. This is typically a microcontroller with compatible firmware which is provided under license agreement from Microchip. Microchip's PIC16/17 microcontroller line provides the user with a large choice of devices that can perform the decoding functions as well as handle the system needs for any customer.

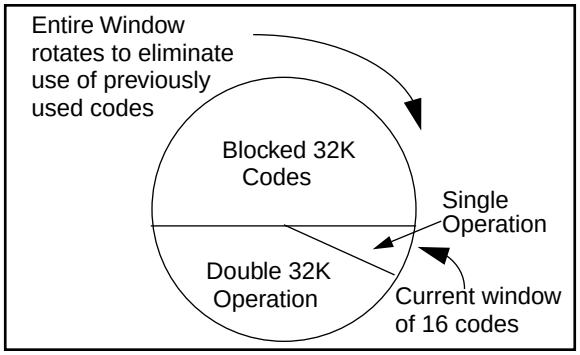
Several learning strategies can be followed in the decoder implementation. Learning can be implemented through a secret manufactuer's function to generate a key from their serial number, using the extra 32-bit fixed code transmission to transmit a seed or even a combination of the two. The following example can be followed.

In order for a transmitter to be used with a decoder, the transmitter must first be 'learned.' When a transmitter is learned to a decoder, it is suggested the decoder stores the serial number, key, and current synchronization value in EEPROM. After learn mode is entered, the decoder must receive two consecutive valid transmissions from the same encoder before the learn values are stored. The decoder must keep track of these values for every transmitter that is learned. The decoder could also store the manufacturer's key in order to learn a transmitter. The secret key is then used to decode the code hopping portion of the transmission.

1.5 Synchronization

The HCS301 facilitates a sophisticated synchronization technique which does not require the recalculation of future codes. The decoder will compare the newly received value against its previously received value and, if the difference is less than a forward window value (i.e., 16), the command will be accepted and the new synchronization value will be stored for future reference. If for some reason a function button is pushed more than the window value while out of the range of the decoder, synchronization can automatically be restored when the decoder receives two successive codes. Figure 1-4 illustrates an example of the synchronization. If the encoder is outside of the 32K window then it would be necessary to relearn the transmitter. Since the entire window rotates after each valid transmission, past codes are invalid which eliminates the possibility of grabbing a previous code and retransmitting to gain entry.

FIGURE 1-4: SYNCHRONIZATION WINDOW



*Encoder and decoder patents are allowed and pending.

WORLDWIDE SALES & SERVICE

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.mchip.com/microchip

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

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

ASIA/PACIFIC

Hong Kong
Microchip Technology
Unit No. 3002-3004, Tower 1
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 851077 Fax: 44 1 628 850259

France
Arizona Microchip Technology SARL
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 Pegaso Ingresso No. 2
Via Paracelso 23, 20041
Agrate Brianza (MI) 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

1/05/96

MICROCHIP