REMOTE KEYLESS ENTRY SYSTEM FOR CARS

PROJECT REPORT

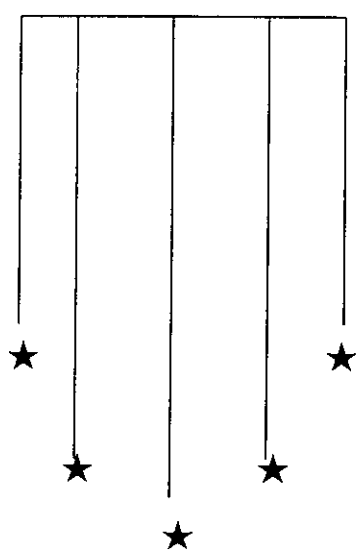
Submitted By

N.SUBRAMANI

S.RAJIV

R.BHARATHIRAJA

R.MANIKANDAN



1999 - 2000

Guided By

Miss. M.DENNIS CYNTHIA, B.E.,

Lecturer, Dept of EEE

Submitted in partial fulfilment of the requirements for the award of the degree of BACHELOR OF ENGINEERING in ELECTRICAL AND ELECTRONICS ENGINEERING of the Bharathiar University, Coimbatore.

Department Of Electrical and Electronics Engineering

KUMARAGURU COLLEGE OF TECHNOLOGY

COIMBATORE

CERTIFICATE

KUMARAGURU COLLEGE OF TECHNOLOGY

Coimbatore - 641 006

Department of Electrical and Electronics Engineering

Certificate

This is to Certify that the Project report entitled

"REMOTE KEYLESS ENTRY SYSTEM FOR CARS"

has been submitted by

Mr. N. SUBRAMANI, S. RAJIV
R. BARATHIRAJA, R. MANIKANDAN

in partial fulfillment for the award of the Degree of Bachelor of Engineering in the Electrical and Electronics Engineering Branch of the Bharathiar University, Coimbatore - 641 046 during the academic year 1999 - 2000.

Dr. K. A. PALANISWAMY, B.E.,M.Sc.(Engg).,Ph.D
M.ISTE,C.Engg.(I).,F.I.E
Professor and Head
Department of Electrical and Electronics Engineering
Head of the Department

Guide

Date

Certified that the candidate with the University Registration No.…… was examined in the project viva-voce held on ……

Internal Examiner

External Examiner

EMIER INSTRUMENTS & CONTROLS LIMITED

✦pricol✦

P.B. NO. 4209, PERIANAICKENPALAYAM
COIMBATORE - 641 020. INDIA
PHONE : 0422 - 892901 TO 10
FAX : 0422 - 892028
TELEX : 0855 - 834 PIL IN
CABLE : DASHBOARD

HRD/PROJ-TRG/2000
11-Mar-2000

PROJECT CERTIFICATE

This is to certify that the following final year BE (EEE) students of Kumaraguru College of Technology, Coimbatore have undergone a project in our organization:-

1. **Mr N Subramani**
2. **Mr S Rajiv**
3. **Mr R Bharathiraja**
4. **Mr R Manikandan**

Title of the Project : *"Remote Keyless Entry System for Cars"*

Period of Project : *July 1999 to February 2000*

Department : *Product Engineering (Electroniocs)*

During this period their attendance and conduct were found to be ***good.***

We wish them the very best in their future endeavours.

ANTHONY THIAGARAJAN
DY. MANAGER – HRD

DEDICATED TO

OUR BELOVED PARENTS

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

We feel highly elated in manifesting our deep sense of thankfulness to our project guide **Miss. M. Dennis Cynthia,** B.E.,Lecturer, Electrical and Electronics for her keen interest, valuable guidance, useful suggestion and constant help during the course of this project.

We are highly grateful to our beloved Professor and Head of the Department **Dr.K.A.Palaniswamy,**B.E., M.Sc. (Engg) ,Ph.D., C.Eng(I), M.I.S.T.E., F.I.E., for his encouragement which has been instrumental for the success of this project.

We wish to express our heartfelt regards and sincere thanks to our Principal **Dr.K.K.Padmanabhan.,** B.Sc.(Engg), M.Tech., Ph.D., for his patronge.

We take great pleasure in expressing our sincere thanks to **Mr. Vijay Mohan** Vice chairman and Managing director ,the Management of Premier Instruments and controls Limited, Coimbatore and **Mr. R. Krishnamurthy,** Deputy General Manager,

Production Engineering (electronics) Department for permitting us to undertake this project.

We acknowledge with thanks the very useful suggestions and valuable guidance given by **Mr. Uma Mahesh Babu,** Asst. Manager. Production Engineering (Electronics)., Pricol.

We also express our sincere gratitude to our teaching and non-teaching staff for their kind co-operation during the course of this project.

Last but not the least, we thank our beloved parents and friends for their consistent and unlimited support.

SYNOPSIS

SYNOPSIS

With the liberalization of Indian economy automobile industries are striving to retain their competitive edge, which is quite clear from the urgency shown towards meeting the consumers need. A consumer gives prime importance to safe guard his car against theft & unnecessary intervention. Hence it becomes the utmost objective of all automobile industries to incorporate a safety scheme in product to cater to the needs of his customer.

This project titled "Remote keyless Entry system" helps to solve the above problem. This system is capable of performing 15 different functions like windows, door, bonnet & fuel tank lid opening, Ignition control, wiper operation & burglar alarm, all performed with the touch of press button switch.

The circuits are designed and a PCB is fabricated comprising of regulated power supply, code hopping encoder, code hopping decoder, transmitter & receiver. These various modules are properly integrated to produce the desired result.

This project employs a technique called Keeloq technique to generate multiple codes at random which are transmitted. The advancements in Electronics has helped a great deal in making this project efficient.

This system has a number of advantages over the existing method. This method proves to be economical and reliable compared to the existing system to safe guard automobiles from theft. The shortcomings of the existing method like code scanning and code grabbing are overcome by employing Keeloq Technique.

CONTENTS

CONTENTS

CHAPTER 1

INTRODUCTION

CHAPTER - 1

INTRODUCTION

' PREVENTION IS BETTER THAN CURE '

As per the saying our project entitled " Remote Keyless Entry systems for cars" aims at saving cars from thefts which often happen in our country.

This model comprises of two main parts

1. Transmitting unit
2. Receiving unit

Further the transmitting unit shown in figure 1.1 can be subdivided into four modules.

a. Power supply unit

b. Input unit

c. Code hopping encoder

d. Transmitter

The first module comprises of a filtering capacitor & a regulator IC to give a constant DC power supply to the encoder & transmitter.

The second module - the input unit is a combination of four switches which are used to give different binary input to the encoder to perform different functions as per the given input code.

Code hopping encoder (HCS 300) constitutes the third module which produces codes corresponding to the binary output signals. These codes produced by the encoder changes randomly with every operation.

The transmitter forms the fourth module which receives the PWM signals from encoder & transmits it in the form of RF signals at a frequency of 433 MHZ.

The signals transmitted by the transmitter units are received by receiver & these signals are decoded to retrieve the original signals.

The receiving unit is shown in Fig. 1.2 made up of four modules.

a. Power supply unit
b. Receiver
c. Code hopping decoder
d. Relay and output unit

The first module is the power supply unit which is same as that of power supply used in encoding unit. It gives a constant dc power supply to the receiver and code hopping decoder.

The receiver constitutes the second module. It receives the RF signals which are transmitted at an frequency of 433 MHZ by the transmitter and produces equivalent PWM signals.

The code hopping decoder forms the third module which decodes the PWM signals and extract the original binary input signals.

The fourth module is the relay unit. It actuates the output unit via motor to open the door and windows etc depending on the signals it receives from the previous unit.

BASIC BLOCK DIAGRAM OF A REMOTE KEYLESS ENTRY SYSTEM

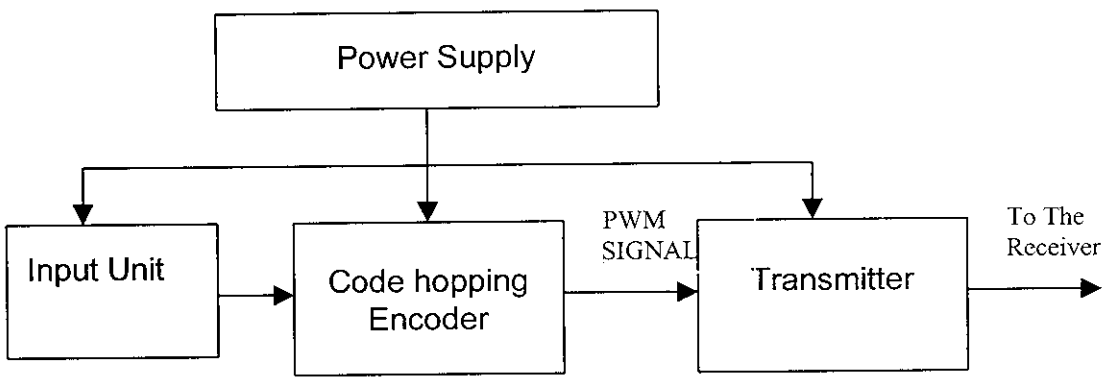


Fig 1.1 Transmitting Unit

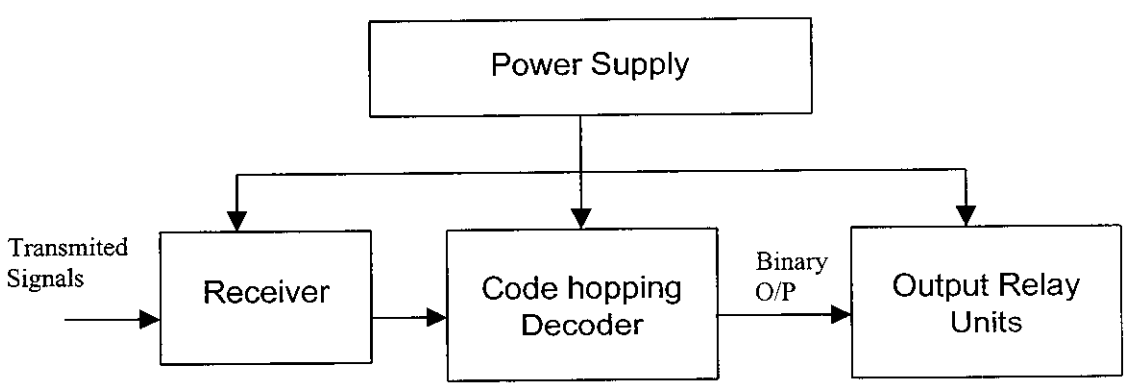


Fig 1.2 Receiving Unit

CHAPTER 2

EXISTING SECURITY SYSTEM

CHAPTER - 2

EXISTING SECURITY SYSTEM

Remote control via RF or IR is popular for many applications, including vehicle alarms and automatic garage doors. Conventional remote control systems are based on unidirectional transmission and have limited security. More sophisticated devices based on bi-directional transmission are also available but, because of their high cost and practical disadvantage, they are not widely used in commercial remote control devices.

The popular unidirectional transmission system currently used have two very important security short comings called code scanning & code grabbing. The codes they transmit are usually fixed and the number of possible code combination is relatively small. Either of these short comings can lead to unauthorised access.

2.1 CODE SCANNING :

The limited number of possible combinations available in most remote control systems makes it possible to transmit all possible

combinations in a relatively short time. A hand held micro processor based system for this purpose (called a code scanner) can easily be constructed.

In system using eight Dip switches this scanning process can typically be accomplished in less than 32 seconds (when trying 8 combination per second). Even in system with 16 bit keys (yielding roughly 65,000 combinations) only 2.25 hours would be required to try all possible combinations. It should also be noted that the scanner may gain access in for less than this maximum time.

2.2 CODE GRABBING

A far easier way of gaining unauthorized access to a security system is freely available. Such a unit is being advertised as a tool for the legal repossession of vehicles. To understand its operation, it is useful to know something about remote controls.

A remote control transmitter of the type normally used in vehicle security systems is nothing but a small radio transmitter that transmits

a code number on a certain frequency. This code number is normally generated by an integrated circuit encoder The transmit frequency is normally fixed by legislation within a particular country, enabling anybody to build a simple receiver that can receive signals from all such transmitters.

It is a simple matter to build a circuit to record such transmissions captured by the receiver, such a device is known as a code or key grabber. A would be vehicle thief would typically lurk in a parking lot, waiting until a vehicle owner arms his alarm with a remote control. The key grabber would capture the transmitted code, enabling the theif to retransmit this code as soon as the owner leaves the parking lot. Typically this would leave the alarm and immobilizer disabled & even the central locking unlocked.

CHAPTER 3

KEELOQ TECHNIQUE

CHAPTER - 3

KEELOQ TECHNIQUE

The shortcomings of the existing method viz code scanning & code grabbing is overcome by employing a technique called Keeloq techniques. Keeloq is an patented product of microchip which is an rock solid security system. The Keeloq technique works on code hopping technique. The Keeloq system uses a seperate 66 bit key for each transmitter. Such a key is simply a very large random number unique to that transmitter. Effectively, this arrangement provides a unique encoding and decoding algorithm for each transmitter. An outsider who does not know the key, cannot decode the variable code portion of a transmission and consequently cannot determine the identity parameters of the originating transmitter.

This uniqueness of each transmitters encoding algorithm complicates learning. The key cannot be determined from variable code transmission and no information can be derived from the transmission without the key.

Keeloq is a proprietary block cipher based on a block length of 32 bits and a key length of 64 bits. The algorithm is characterized by a very economical hardware implementation, while retaining a level of security comparable to Data Encryption Standards (DES). This level of security makes it eminently suitable for code communication application such as code hopping antitheft or access control devices.

The Keeloq algorithm is designed to make it impossible for a potential assailant to predict the next code that will be transmitted by a valid transmitter. Even if the assailant makes a reasonable guess regarding the way in which transmitted information changes with each transmission, the algorthim obscures this information sufficiently that the next code can not be anticipated. In particular even if the transmitted information (before encoding) differs only in one bit from the information in the previous transmission, the next transmission will be totally different.

3.1 CODE HOPPING TECHNIQUE:

In this code hopping technique, a 66 bit random code is produced and transmitted. There are nearly 7.3×10^9 combinations produced using this 66 bits. The speciality of this technique is that the consecutive codes differ by above 50% and they are transmitted in a random manner.

There are two methods by which the 50% change occurs. They are

3.1.1 Avalanche Effect (AE):

A block cipher satisfies the AE if changing one bit of the information causes, on average half of the bits in the transmission to change. In the KEELOQ algorithm this implies that changing one bit in the function and / or synchronization information will cause an average of 16 of the 32 bits in the transmitted code to change.

3.1.2 STRICT AVALANCHE CRITERION (SAC)

The SAC requires that if one bit of the encoded information is changed, each bit in the output must have a chance of 0.5 of changing as well. Consequently, the probability of guessing any one bit correctly is 0.5 and the probability of guessing an entire 32 bit string correctly is in about 4,300,000,000.

The tests involved using a random 64 bit key and a array counter (starting at zero) as input to the algorithm. In each case the output was compared with a reference (SAC) or with the previous code (AE). In both cases, the results were as expected: For the AE, the average number of bits changed was 16 (50%), with a standard deviation of 2.83 (8.8%). For the SAC, each individual bit changed an average of 50% of the time, with a standard deviation of 8.8%.

3.2 CODE HOPPING ENCODER AND DECODER:

The code hopping encoder and decoder are designed for secure remote keyless entry systems. This encoder and decoder

utilises the patented KEELOQ code hopping system and high security learning mechanism. These device makes a perfect solution for unidirectional remote key less entry system and access control systems.

The code hopping encodes encrypts a 66 bit code from 4 bit input. Similarly, the code hopping decodes decrypts the 66 bit code to 4 bit output.

The encryption Keys, Decryption 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 value.

CHAPTER 4

HARDWARE DESCRIPTION

CHAPTER 4

HARDWARE DESCRIPTION

4.1 REGULATED POWER SUPPLY UNIT

The power supply unit consists of filtering capacitors and regulator IC 7805 to give the regulated power Supply. The input to the Regulator is given by a 12v dc battery.

The regulator produces a constant 5v dc. The Capacitors C_i & C_o are connected to cancel the inductive effects due to long distribution leads. The output capacitor is used to improve the transient response. The diode is used to prevent the back flow current.

The power supply unit is same for both encoding and decoding unit and is depictedin fig 4.1 and fig 4.2.

4.2 CODE HOPPING ENCODER (HCS 300)

It is an eight pin IC (fig 4.1) which is used to encode the given inputs. The first four pins of this chip used as input pins. These input bits are encrypted using encryption algorithim which is already stored in EEPROM. The encrypted code of 66 bits will be in the sixth pin as Pulse Width Modulated signal (PWM). Then these encrypted bits are transmitted through the transmitter.

The HCS 300, from Microchip Technology Inc., is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS 300 utilizes the KEELOQ code hopping technology, which incorporates high security, a small package outline and low cost, to make this device a perfect solution of undirectional remote keyless entry systems and access control systems.

4.3 TRANSMITTER (FT - COM - TX2)

The transmitter (fig 4.1) is used to transmit the output of encoder. The FT-COM - TX2 is a miniature transmitter module that generates on-off keyed modulation from an external digital encoder.

The carrier frequency is quartz, Surface - Acoustic - Wave (SAW) stabilized, output harmonics are suppressed by a SAW filter. The result is excellent performance in a simple - to - use, surface mount device with a low external component count. The PWM output from HC 300 is transmitted in the form of RF signals at frequency of 433 MHZ by this transmitter.

4.4 RECEIVER (FT-COM-RX2)

The Receiver (fig 4.2) is used to receive the transmitted data from the transmitter at frequency of 433 MHZ.

It is a complete radio frequency receiver module which facilitate the designers to implement them on Electronic circuit directly. It is easy to integrate this module with micro controllers, encoders and decoders. The circuit of this module is designed with latest technology using SMD components and its size is small and compact to fit in many applications.

This receiver module is super-regenerative version with TSV DC power. It's senstivity is - 103 dbm. Power consumption is 2.7 mA. Frequency is 433.92 MHZ / LRC and Band width is 4 MHZ. This module is very useful in wireless applications required data rate of less than 4800 BPS.

The received data is then given to the decoder in the form of a PWM signal.

4.5 DECODER (HCS512)

The transmitted data is received by the decoder (fig 4.2) and the matching process takes place. The decoder checks whether the received data is a valid one. If it is valid, the code is decrypted by the decrypting algorithm which is already stored in its EEPROM. The outputs from the four input pins are given to the relay units.

The HCS 512 utilizes the patented KEELOQ code hopping system and high security learning mechanisms to make this a canned solution when used with the HCS encoders to implement a

unidirectional remote keyless entry system. The decoder employs automatic band rate detection which allows it to compensate for wide variations in transmitter data rate. The decoder contains sophisticated error checking algorithms to ensure only valid codes are accepted.

4.6 RELAY UNIT

A static relay is used in this circuit to activate the relevant motors to perform the desired application. According to the 'American standards Association' a stable relay is defined as one in which there is no armature or moving elements. Most of the relays used are electro magnetic relays.

The output of the decoder is used to energise the exciting will of the relay. This is turn activates the corresponding circuits to perform the desired functions.

4.6.1 ADVANTAGES OF STATIC RELAYS

i) The moving parts and the contacts are highly reduced

ii) Occupy less space

iii) Robust and quite reliable

iv) High speed of operation

4.6.2 PARTS OF A RELAY

The relays consist of the following parts.

i) Pole

ii) Normally Opened pin (NO)

iii) Normally Closed pin (NC)

4.6.3. Representation of a Relay

The details of various IC's are furnished in the appendix

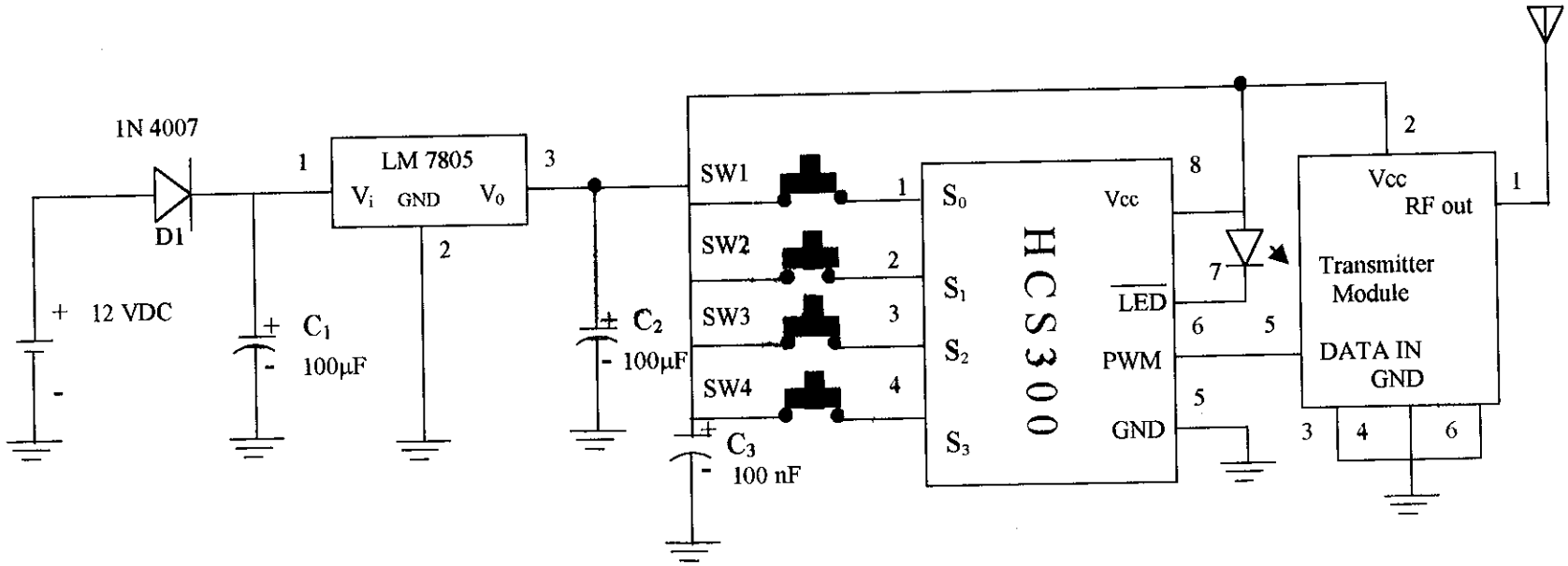


Fig 4.1 TRANSMITTING UNIT

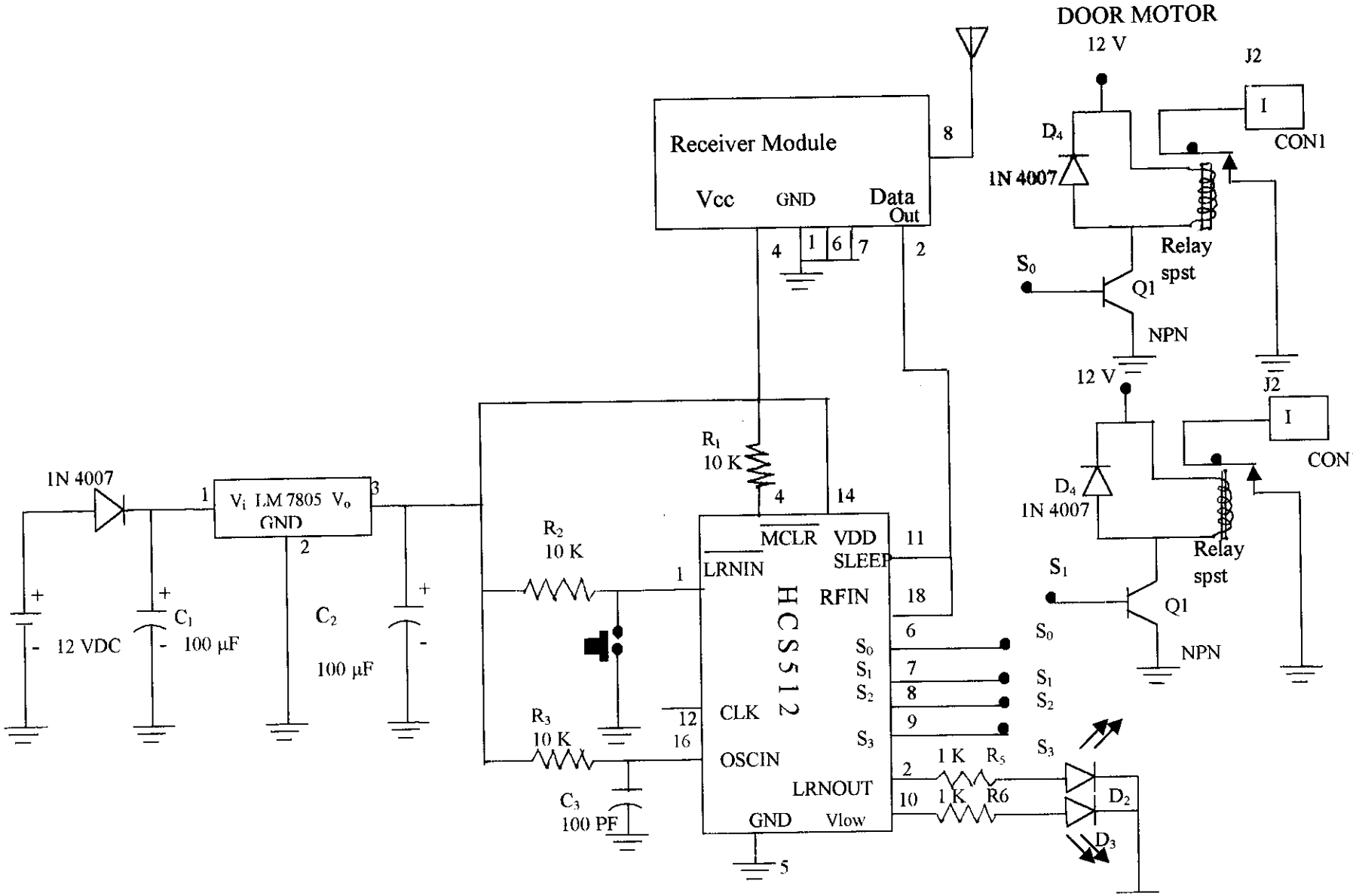


Fig 4.2 Receiving Unit

CHAPTER 5

CODE HOPPING ENCODER & DECODER

CHAPTER 5

CODE HOPPING ENCODER & DECODER

The heart of this project is the Keeloq Code Hopping Encoder & Decoder. Hence these two chips are dealt in detail in this chapter.

5.1 CODE HOPPING ENCODER:

The internal block diagram of the code hopping encoder (HCS 300) is as shown in fig. 5.1. The various parts of encoder are.

- EEPROM
- 32 bit shift register
- Encryptor.
- Oscillator
- Input port
- Controller
- Reset Circuit
- LED Driver
- Power Latching and Switching

➢ EEPROM

The Code hopping encoder contains 192 bits (12 x 16 bit words) of EEPROM. This EEPROM array is used to store encryption key information, synchronisation value etc. Further description of the memory array is given in the following sections.

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 0)
8	Seed – 0	Seed Value (word 0)
9	Seed – 1	Seed Value (word 1)
10	EN – Key	16 – bit Envelope Key
11	Config	Config word

- **Key- O – 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 by the programme at the time of production using a key generation algorithm, using are the serial number and manufacture code.

- **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.

- **SER 0, SER 1(Encoded serial number)**

SER 0, SER 1 are the lower and upper words of the device serial number respectively. Although there are 32 bits allocated for Serial number only the lower order 28 bits are transmitted. It is unique for every transmitter.

- **SEED 0, SEED 1 (Seed word)**

This is the two word seed code that will be transmitted when all four 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.

- **EN_KEY (Envelope Encryption Key)**

Envelope encryption is a selectable option that encrypts the portion of the Transmission that contains the transmitter serial number. Selecting this option is done by setting the appropriate bit in the configuration word.

- **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

- **32 bit Shift Register:**

The 32 bit shift register stores the 32 bit of encrypted data consisting of 4 bit of button status, 2 overflow bits, 10 discrimination bits and 16 bits of Synchronization value.

- **Encrypter:**

The function of this encrypter block in the block diagram is production of 32 bit encrypted data from 4 button input bits.

- **Oscillator :**

It consists of an internally built oscillator (RC or LC network) which is used to provide clock pulses.

- **Input port:**

Input port consists of input lines S_0, S_1,S2 & S3. Through this port the function to the performed is given in the form of binary input.

It is connected to the controller & power latching & switching block of encoder.

- **Controller, Reset, LED driver, Power Latching**

It Controls the activities of every other blocks.

The LED driver block helps to indicate whether the transmission process is taking place.

A reset circuit is provided to reset the encoder after every function is performed.

Power Latching & Switching Circuit serves as an interface between input signal to the controller.

5.1.1 Code word Organisation of the Transmitted Data :

The HCS 300 transmits a 66 – bit code when a button is pressed. The 66-bit word is constructed from a fixed code portion and encrypted Code portion.

The encryption data is generated from four button bits, two over flow counter bits the discrimination bits and the 16 bit Synchronization Value.

The fixed code data is made up from two status bits, four button bits, and the 28 bit serial number. The four button bits and the 28 bit serial number may be encrypted with the Envelope key if the envelope encryption is enabled by the user. The code word organisation is depicted in Fig 5.3.

5.1.2 PROGRAMMING OF CODE HOPPING ENCODER (HCS 300)

When using the code hopping encoder, 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 serial data stream, which are then stored internally in EEPROM. Programming will be initiated by forcing the PWM line high, after S_3 line has been held high for the appropriate length of time. After the program mode is entered, a delay must be provided to the a device for the automatic bulk write cycle to complete. The device can then be programmed by clocking in 16 bits at a time, using S_3 as the clock – line and PWM as data line. After each 16 bit word is loaded a programming delay is required for the internal program cycle to complete. This delay can take upto Two. At the end of programming cycle, the device can be verified by

reading back the EEPROM. Reading is done by clocking the S_3 line and reading the data bits on PWM.

The serial number for each transmitter is programmed by the manufacturer at the time of production. The generation of encryption is done by the key generation algorithm as shown in fig.5.2. Typically inputs to the key generation algorithm are the serial number of the transmitter & a 64 bit manufacturer code. The manufacturer code is choosen by the manufacturer & must be carefully controlled. The 16 bit synchronisation value is the basis for the transmitted code changing for each transmission & is updated each time a button is pressed. Because of the complexity of the code hopping encryption algorithm, a change in one bit of Synchronization value will result in a large change in a actual transmitted code.

Once the encoder detects that the button has been pressed, the encoder reads the button & then updates the synchronisation counter. The synchronisation value is then combined with the encryption key in the encryption algorithm & the o/p is 32 bits of encrypted information. These data will change with every button

pressed, hence, it is referred to a hopping portion of code word. The 32 bit code word is combined with the button information & the serial number to form the code word transmitted.

5.2 CODE HOPPING DECODER (HCS 512)

The internal block diagram of the code hopping decoder is shown in fig: 5.4.

The block diagram consist of :

- EEPROM
- 67 – bit Reception Register
- Decrypter
- Oscillator
- Output Port
- Controller
- Control Signals Port

- **EEPROM**

Same as encoder.

➢ 67- BIT RECEPTION REGISTER

The received RF signal is given to this Reception register. The output of this Register is given to the controller.

➢ CONTROLLER:

From the controller the signal is given to Decrypter & to the control signal port. After decryption, decrypted data is given to controller. The Controller also Connected to the EEPROM. The matching (checking) of synchroniztion counter, serial number & manufacturer's code takes place in the controller.

➢ DECRYPTER:

The encrypted data which is received as RF signal is given to the decrypter via Controller. In decrypter, the encrypted data is decoded. From that the serial number, Synchronization counter of the manufacturer's code are obtained. These values are given to the controller for checking (validation). The validation is done by comparing the values which is decoded with the values which is stored in EEPROM.

- **OSCILLATOR**

It consists of an internally built oscillator which is used to provide clock pulse.

- **OUTPUT PORT**

It consists of four output lines, through which the output signals are sent.'

- **CONTROL SIGNALS PORT**

The signals associated with this port are DATA, CLK, $\overline{\text{LRNIN}}$, SEL, $\overline{\text{MCLR}}$, SLEEP. The DATA & CLK Pins are used during the programming of manufacturer's code. LRNIN signal is used to initiate the learning process. The signal is activate by pressing$\overline{\text{IN}}$ button. The SLEEP mode is activated by setting the SLEEP bit in Configuration byte. When sleep mode is enabled the clock stops and thereby the current consumption is reduced. $\overline{\text{MCLR}}$ is the master clear input.

5.2.1 PROGRAMMING OF CODE HOPPING DECODER (HCS 512)

The manufacturer's code must be programmed into EEPROM memory through the synchronous programming interface using the DATA & CLK lines. Provision must be made for connections to these plus if the decoder is going to be programmed in circuit.

Programming mode is activated if the CLK is low for at least 1ms & then goes high within 64 ms after power up stays high for longer then 8 ms but not longer than 128ms. After entering programming mode, the 64 bit manufacturer's code 8- bit configuration byte & 8- bit configuration byte, & 8 bit check sum is sent to the device using the synchronous interface. After receiving the 80 – bit message the checksum is verified and the information is written to EEPROM. If the programming operation was successful, the HCS512 will respond with an acknowledge pulse.

After programming the manufacturers Code, the HCS512 decoder will automatically activate an Erase all function, removing all transmitters from the system.

The operation of the decoder is depicted in Fig 5.5.

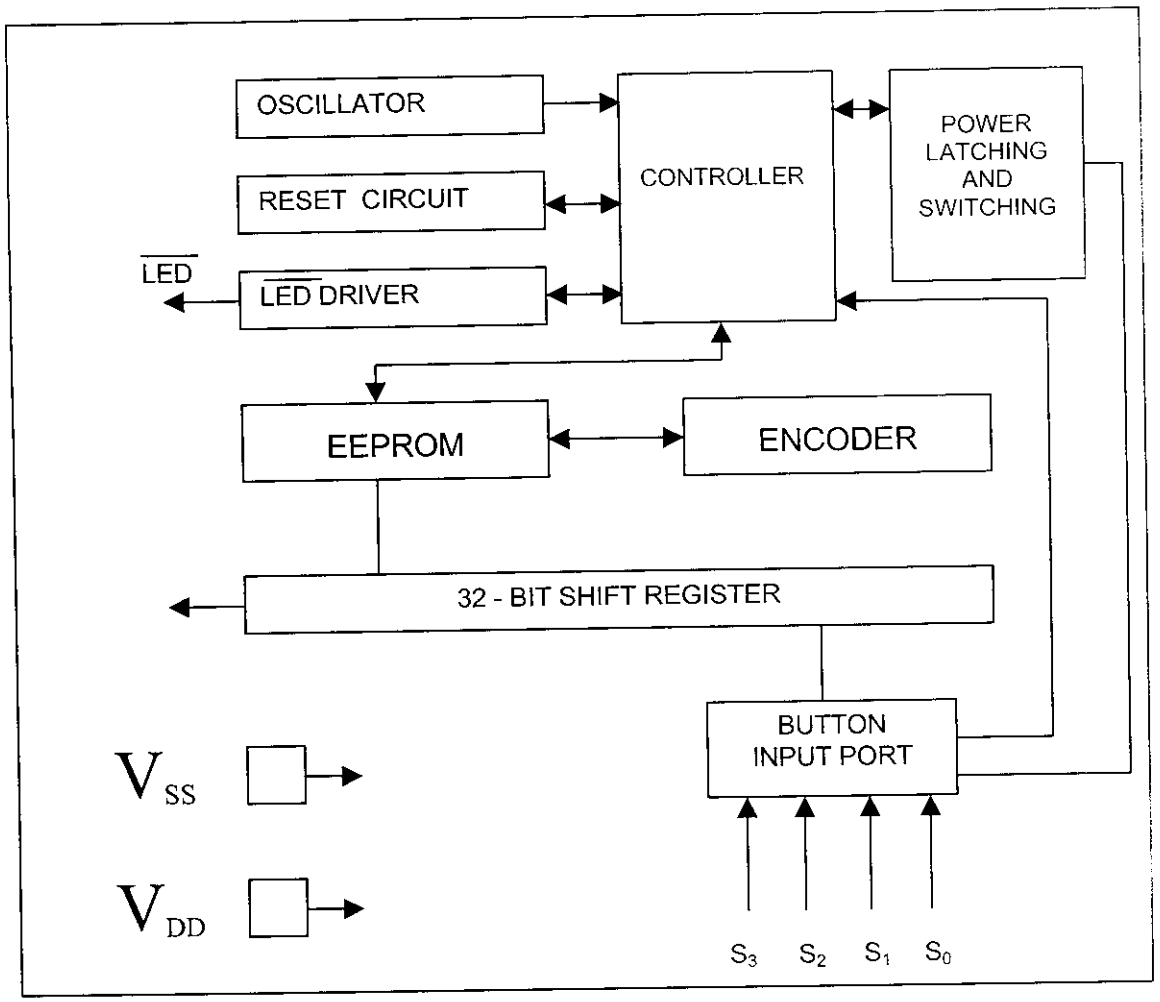


Fig 5.1 Internal block diagram of code Hopping Encoder (HCS 300)

CREATIION AND STORAGE OF ENCODER KEY DURING PRODUCTION

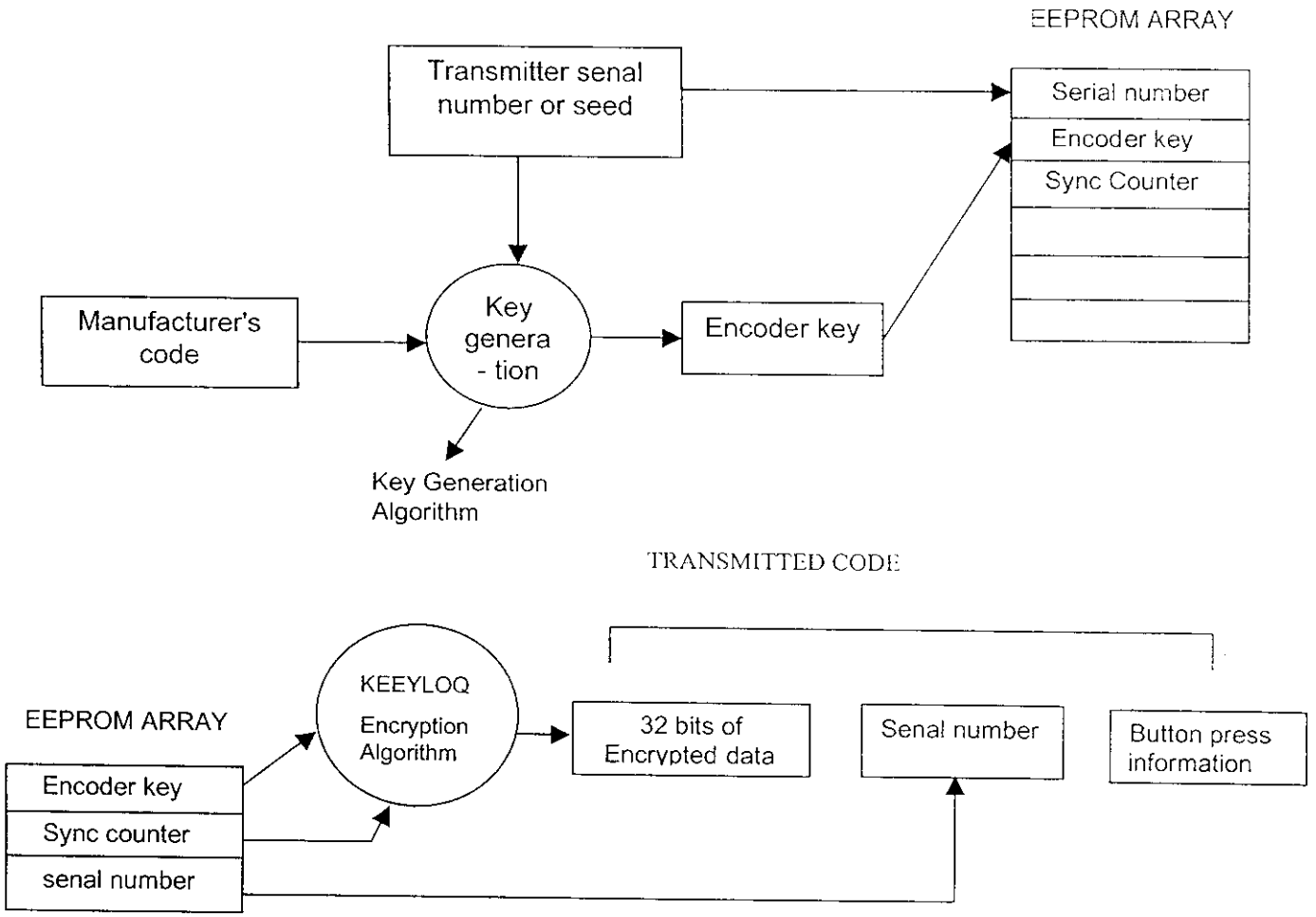


FIG 5.2 BASIC OPERATION OF TRANSMITTER

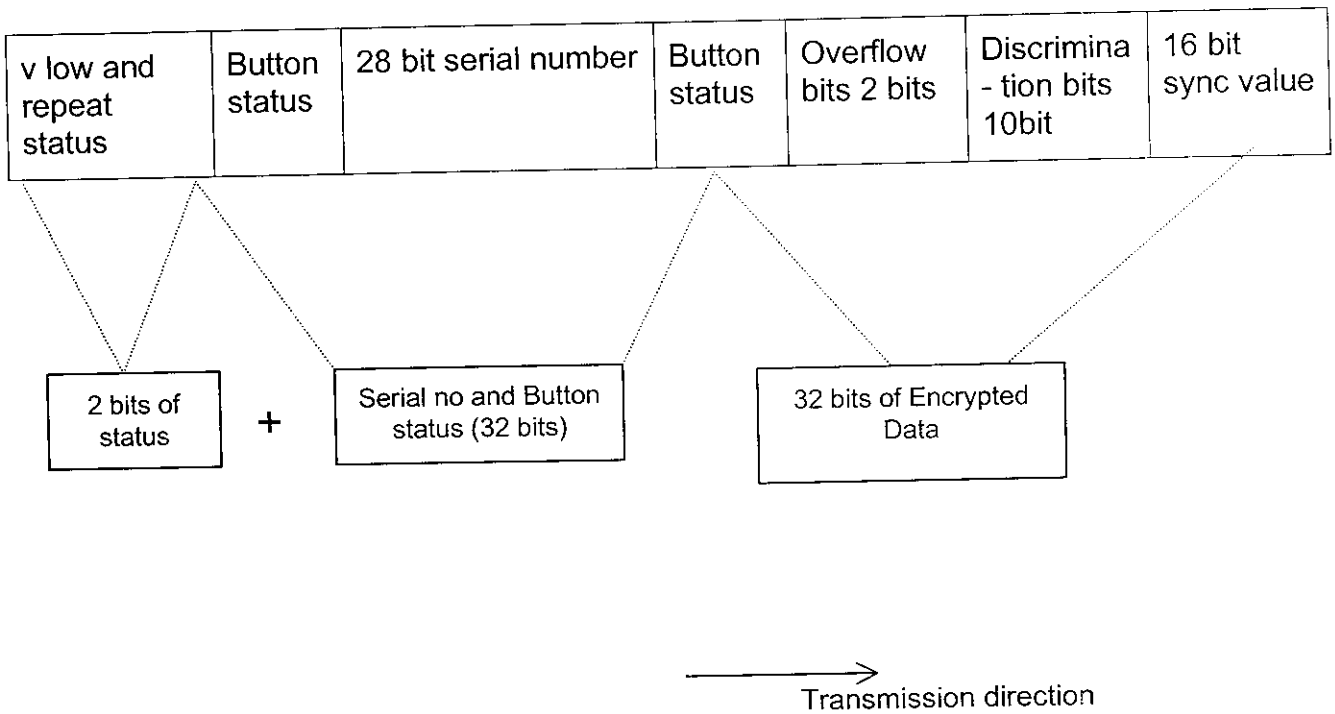


Fig 5.3 Code word Organisation

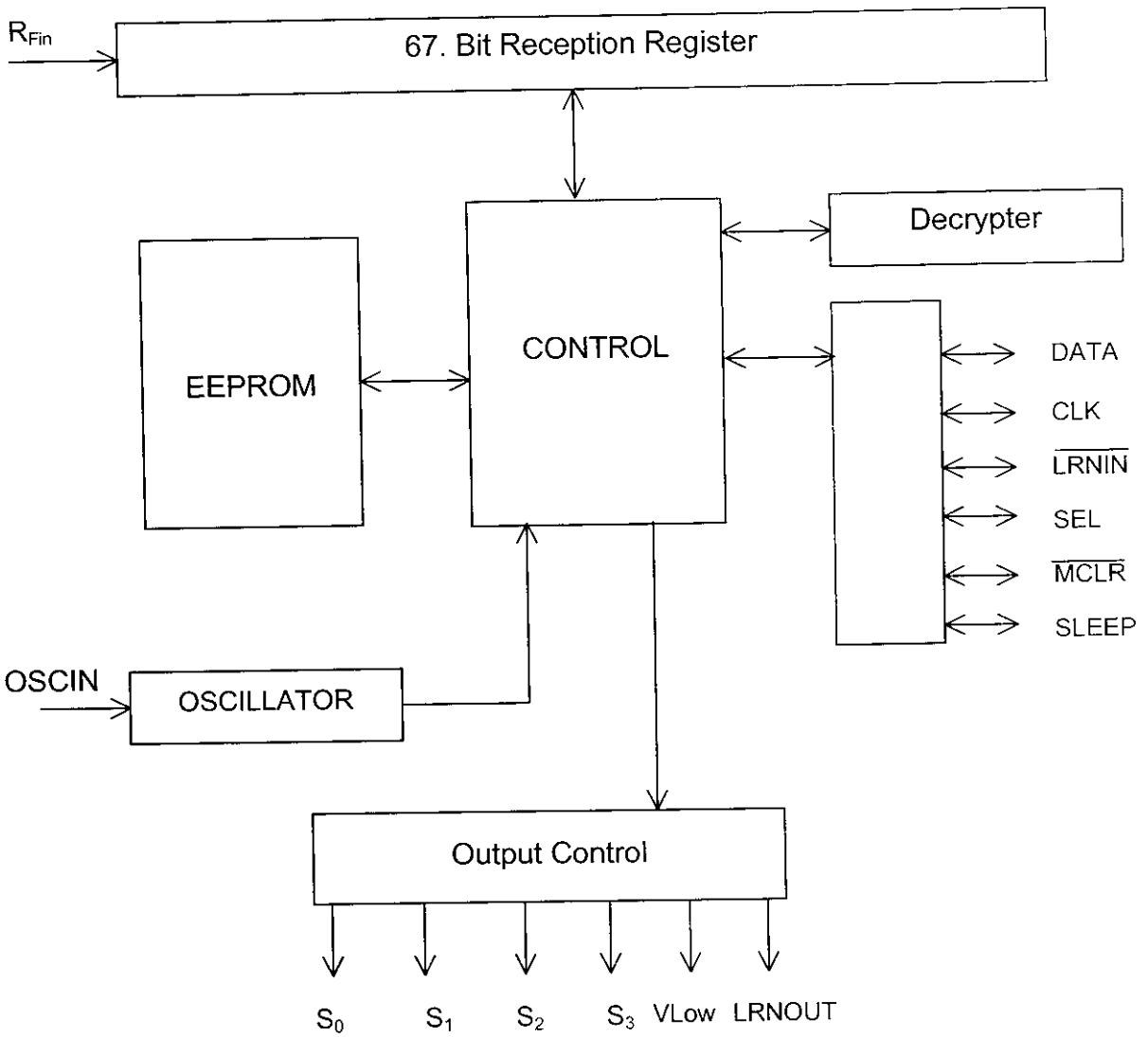


Fig 5.4 INTERNAL BLOCK DIAGRAM OF CODE HOPPING DECODER HCS 512

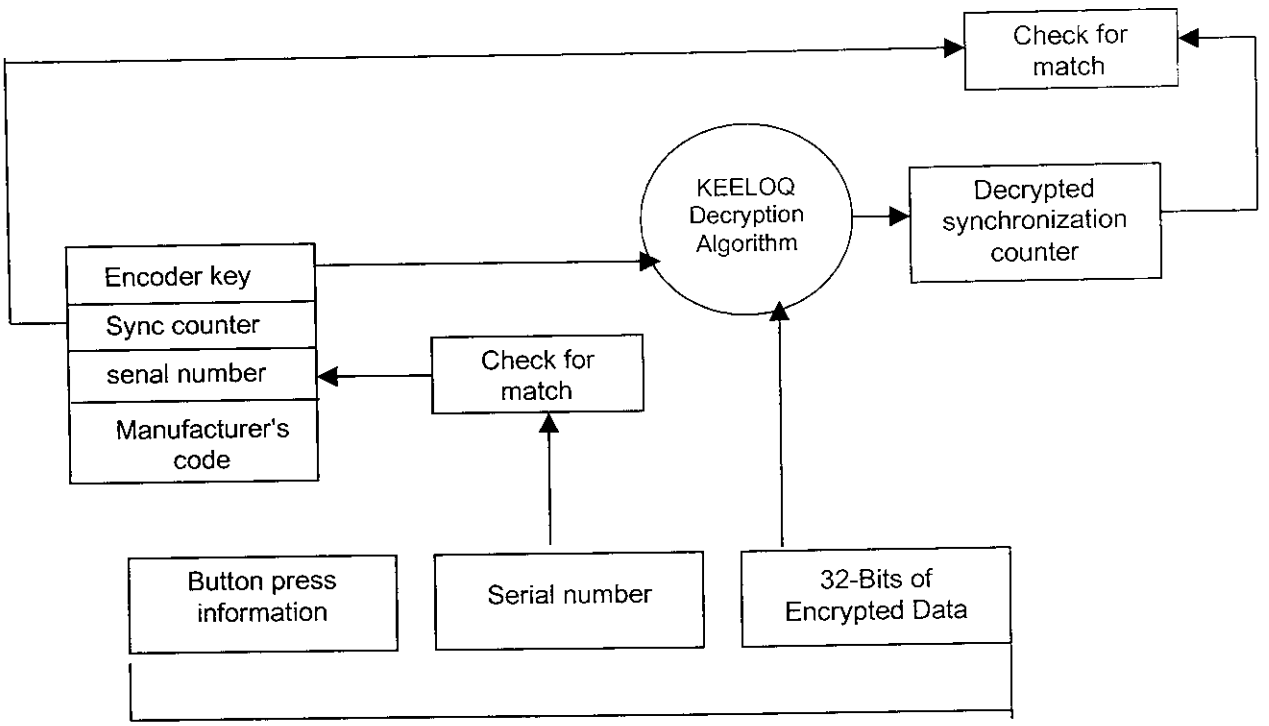


Fig 5.5 Basic Operation of Decoder

CHAPTER 6

TESTING PROCEDURE

CHAPTER - 6

TESTING PROCEDURE

It is important to test the components before they are assembled in the circuit for their satisfactory operation.

6.1 TESTING OF TRANSMITTER AND RECEIVER

A series of pulses at a particular frequency generated by a function generator is given as input to the fifth pin of FT-COM-TX2. This signal is being transmitted by connecting a wire as antenna to the first pin. These transmitted signals are received by the receiver (FTCOM-RX2). A digital storage oscilloscope is connected to the second pin of (FTCOM-RX2) and the output waveforms are noted. These output waveforms are compared with the input waveforms.

6.2 TESTING OF ENCODER AND DECODER

The LRNIN switch is first pressed and the LRNOUT LED glows. Anyone of the switches (S_0 to S_3) is pressed and the LRNOUT LED is

turned off, indicating the reception of a valid code. The same switch (S_0 to S_3) is activated a second time until the LRNOUT LED toggles for 4 seconds. The corresponding to the switch pressed LED will glow at the output side of the decoder. The transmitter is now learned into the decoder.

CONCLUSION

CHAPTER 7

CONCLUSION

A "REMOTE KEYLESS ENTRY SYSTEM" has been designed and fabricated. The discrete model of this system was tested in laboratory environment and their performance was observed.

This project is advantageous compared to the existing method. The foremost advantage is the use of KEELOQ code hopping technique.

FURTHER DEVELOPMENT:

The number of functions that this system can perform can be increased by incorporating a microprocessor or a micro-controller. Depending on the willingness of the user the number of functions like opening of the fuel tank lid, ignition control, bonnet opening, etc. are included.

A password can also be set by programming the micro-controller so that unauthorised persons cannot use the remote.

REFERENCE

REFERENCES

1. Kobus Marneweck, Chris R. Burger, "MICROCHIP HAND BOOK", Microchip Technology Inc., 1997.

2. Earl E. Clark, "RF SOLUTIONS FOR COMMUNICATION AND COMPUTING", RF Monolithics Inc., Texas, 1997.

3. Dennis Reddy, John Coolen, "ELECTRONIC COMMUNICATION", Prentice Hall of India, New Delhi, 1995.

4. D. Roy Choudry, Shail Jain, "LINEAR INTEGRATED CIRCUITS", New Age International (p) Limited, New Delhi,1996.

5. M. Morris Mano, "DIGITAL DESIGN", Prentice Hall of India (P) Limited, New Delhi, 1997.

6. Robert L. Shrader, "ELECTRONIC COMMUNICATION", Mc Graw Hill International, New Delhi, 1988.

7. C.A. Brant, "ELECTRONICS FOR COMMUNICATION", Science Research Associates, Inc., Chicago, 1983.

PHOTOGRAPHS

APPENDIX

NOTES:

MICROCHIP

HCS512

KEELOQ® Code Hopping Decoder

FEATURES

Security

- Secure storage of Manufacturer's Code
- Secure storage of transmitter's keys
- Up to four transmitters can be learned
- KEELOQ code hopping technology
- Normal and secure learning mechanisms

Operating

- 3.0V - 6.0V operation
- 4 MHz RC oscillator
- Learning indication on LRNOUT
- Auto baud rate detection
- Power saving sleep mode

Other

- Stand alone decoder
- On-chip EEPROM for transmitter storage
- Four binary function outputs--15 functions
- 18-pin DIP/SOIC package

Typical Applications

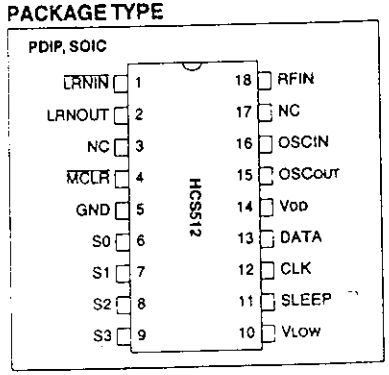
- Automotive remote entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks
- Identity tokens
- Burglar alarm systems

Compatible Encoders

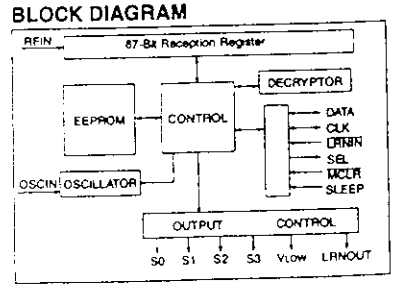
- HCS200, HCS300, HCS301, HCS360, HCS361
- NTQ106

PACKAGE TYPE

PDIP, SOIC



BLOCK DIAGRAM



DESCRIPTION

The Microchip Technology Inc. HCS512 is a code hopping decoder designed for secure Remote Keyless Entry (RKE) systems. The HCS512 utilizes the patented KEELOQ code hopping system and high security learning mechanisms to make this a canned solution when used with the HCS encoders to implement a unidirectional remote keyless entry system.

The Manufacturer's Code, transmitter keys, and synchronization information are stored in protected on-chip EEPROM. The HCS512 uses the DATA and CLK inputs to load the Manufacturer's Code which cannot be read out of the device.

The HCS512 operates over a wide voltage range of 3.0 volts to 6.0 volts. The decoder employs automatic baud rate detection which allows it to compensate for wide variations in transmitter data rate. The decoder contains sophisticated error checking algorithms to ensure only valid codes are accepted.

KEELOQ is a registered trademark of Microchip Technology Inc.
*Code hopping patents issued in Europe, U.S.A. and R.S.—US:5,517,187, Europe: 0459781

1.0 KEELOQ SYSTEM OVERVIEW

1.1 Key Terms

- Manufacturer's Code – a 64-bit word, unique to each manufacturer, used to produce a unique encoder key in each transmitter (encoder).
- Encoder Key – a 64-bit key, unique for each transmitter. The encoder key controls the decryption algorithm and is stored in EEPROM on the decoder device.
- Learn – The receiver uses information that is transmitted to derive the transmitter's secret key, decrypt the discrimination value and the synchronization counter in learning mode. The encoder key is a function of the Manufacturer's Code and the device serial number and/or seed value.

The HCS encoders and decoders employ 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'.

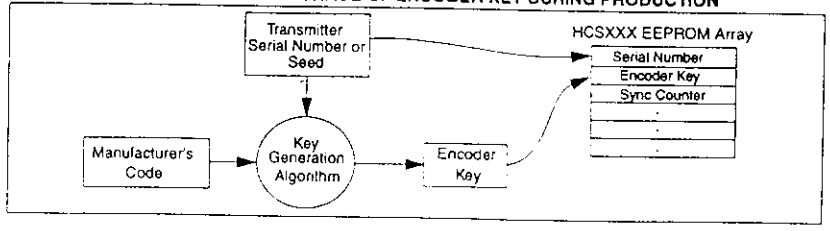
1.2 HCS Encoder Overview

The HCS encoders have 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 encoder key that is generated at the time of production
- A 16-bit synchronization value

The serial number for each encoder is programmed by the manufacturer at the time of production. The generation of the encoder key is done using a key generation algorithm (Figure 1-1). Typically, inputs to the key generation algorithm are the serial number of the encoder 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 ENCODER KEY DURING PRODUCTION



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 1-3) 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 encoder 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.

1.3 HCS Decoder Overview

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

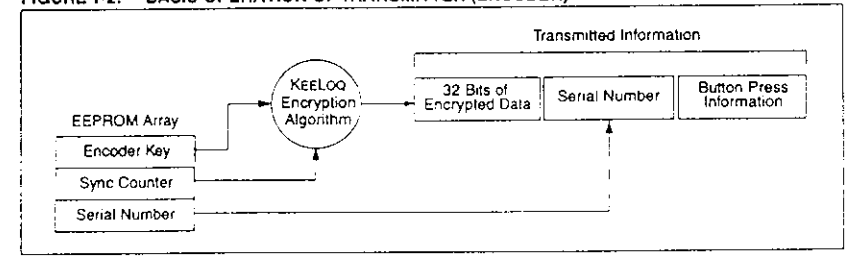
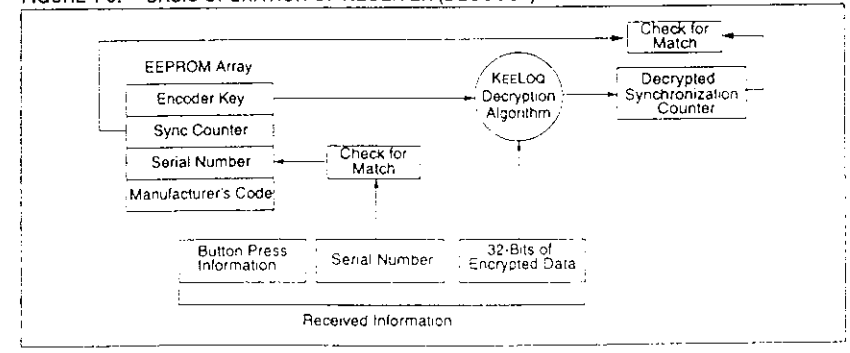


FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



2.0 PIN ASSIGNMENT

PIN	Decoder Function	I/O (1)	Buffer Type(1)	Description
1	LRNIN	I	TTL	Learn input - initiates learning, 10K pull-up required on input
2	LRNOUT	O	TTL	Learn output - indicates learning
3	NC	—	TTL	Do not connect
4	MCLR	I	ST	Master clear input
5	Ground	P	—	Ground connection
6	S0	O	TTL	Switch 0
7	S1	O	TTL	Switch 1
8	S2	O	TTL	Switch 2
9	S3	O	TTL	Switch 3
10	VLOW	O	TTL	Battery low indication output
11	SLEEP	I	TTL	Connect to RFIN to allow wake-up from sleep
12	CLK	I/O	TTL/ST (2)	Clock in programming mode and synchronous mode
13	DATA	I/O	TTL/ST(2)	Data in programming mode and synchronous mode
14	VDD	P	—	Power connection
15	OSCOUT	—	—	Oscillator out – no connection
16	OSCIN (4 MHz)	I	ST	Oscillator in – recommended values 10 kΩ and 10pF
17	NC	—	—	
18	RFIN	I	TTL	RF input from receiver

Note 1: P = power, I = in, O = out, and ST = Schmitt Trigger input.

2: Pin 12 and Pin 13 have a dual purpose. After reset, these pins are used to determine if programming mode is selected in which case they are the clock and data lines. In normal operation, they are the clock and data lines of the synchronous data output stream.

3.0 DESCRIPTION OF FUNCTIONS

3.1 Parallel Interface

The HCS512 activates the S3, S2, S1 & S0 outputs according to Table 3-1 when a new valid code is received. The outputs will be activated for approximately 500 ms. If a repeated code is received during this time, the output extends for approximately 500 ms.

TABLE 3-1: FUNCTION OUTPUT TABLE

Function Code	S3	S2	S1	S0
0001	0	0	0	1
0010	0	0	1	0
0011	0	0	1	1
0100	0	1	0	0
0101	0	1	0	1
0110	0	1	1	0
0111	0	1	1	1
1000	1	0	0	0
1001	1	0	0	1
1010	1	0	1	0
1011	1	0	1	1
1100	1	1	0	0
1101	1	1	0	1
1110	1	1	1	0
1111	1	1	1	1

3.2 Serial Interface

The decoder has a PWM/Synchronous interface connection to microcontrollers with limited I/O. An output data stream is generated when a valid transmission is received. The data stream consists of one start bit, four function bits, one bit for battery status, one bit to indicate a repeated transmission, two status bits, and one stop bit. (Table 3-1). The DATA and CLK lines are used to send a synchronous event message.

A special status message is transmitted on the second pass of learn. This allows the controlling microcontroller to determine if the learn was successful (Result = 1) and if a previous transmitter was overwritten (Overwrite = 1). The status message is shown in Figure 3-2.

Table 3-2 show the values for TX1:0 and the number of transmitters learned.

TABLE 3-2: STATUS BITS

TX1	TX0	Number of Transmitters
0	0	One
0	1	Two
1	0	Three
1	1	Four

FIGURE 3-1: DATA OUTPUT FORMAT

START	S3	S2	S1	S0	VLOW	REPEAT	TX1	TX0	STOP

FIGURE 3-2: STATUS MESSAGE FORMAT

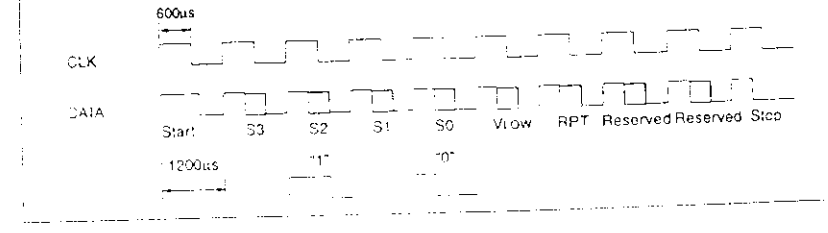
START	0	0	0	0	RESULT	OVRWR	TX1	TX0	STOP

A 1-wire PWM or 2-wire synchronous interface can be used.

In 1-wire mode, the data is transmitted as a PWM signal with a basic pulse width of 400 µs.

In 2-wire mode, synchronous mode PWM bits start on the rising edge of the clock, and the bits must be sampled on the falling edge. The start and stop bits are '1'.

FIGURE 3-3: PWM TRANSMISSION FORMAT



4.0 DECODER OPERATION

4.1 Learning a Transmitter to a Receiver

Either the serial number-based learning method or the seed-based learning method can be selected. The learning method is selected in the configuration byte. 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, the decoder stores the encoder key, a check value of the serial number and current synchronization value in EEPROM. The decoder must keep track of these values for every transmitter that is learned. The maximum number of transmitters that can be learned is four. The decoder must also contain the Manufacturer's Code in order to learn a transmitter. The Manufacturer's Code will typically be the same for all decoders in a system.

The HCS512 has four memory slots. After an "erase all" procedure, all the memory slots will be cleared. Erase all is activated by taking $\overline{\text{LRNIN}}$ low for approximately 10 seconds. When a new transmitter is learned, the decoder searches for an empty memory slot and stores the transmitter's information in that memory slot. When all memory slots are full, the decoder randomly overwrites existing transmitters.

4.1.1 LEARNING PROCEDURE

Learning is activated by taking the $\overline{\text{LRNIN}}$ input low for longer than 64 ms. This input requires an external pull-up resistor.

To learn a new transmitter to the HCS512 decoder, the following sequence is required:

1. Enter learning mode by pulling $\overline{\text{LRNIN}}$ low for longer than 64 ms. The LRNOUT output will go high.
2. Activate the transmitter until the LRNOUT output goes low indicating reception of a valid code (hopping message).
3. Activate the transmitter a second time until the LRNOUT toggles for 4 seconds (in secure learning mode, the seed transmission must be transmitted during the second stage of learn by activating the appropriate buttons on the transmitter).

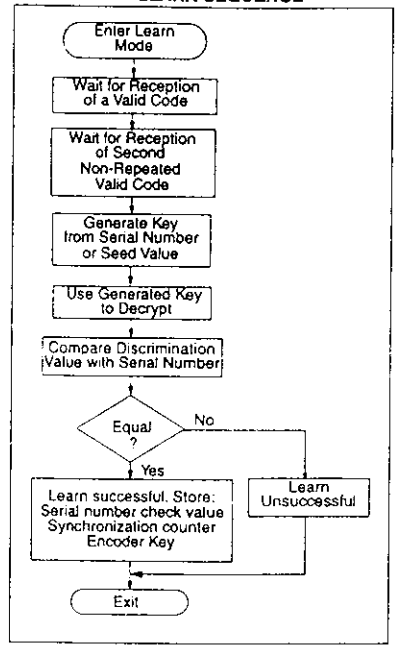
   If $\overline{\text{LRNIN}}$ is taken low momentarily during the learn status indication, the indication will be terminated. Once a successful learning sequence is detected, the indication can be terminated allowing quick learning in a manufacturing setup.
4. The transmitter is now learned into the decoder.
5. Repeat steps 1-4 to learn up to four transmitters.
6. Learning will be terminated if two non-sequential codes were received or if two acceptable codes were not decoded within 30 seconds.

The following checks are performed on the decoder to determine if the transmission is valid during learn:

- The first code word is checked for bit integrity.
- The second code word is checked for bit integrity.
- The hopping code is decrypted.
- If all the checks pass, the serial number and synchronization counters are stored in EEPROM memory.

Figure 4-1 shows a flow chart of the learn sequence.

FIGURE 4-1: LEARN SEQUENCE



4.2 Validation of Codes

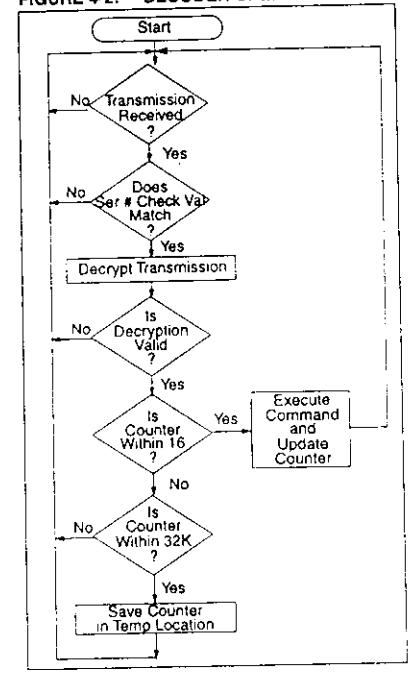
The decoder waits for a transmission and checks the serial number to determine if the transmitter has been learned. If learned, the decoder decrypts the encrypted portion of the transmission using the encoder key. It uses the discrimination bits to determine if the decryption was valid. If everything up to this point is valid, the synchronization value is evaluated.

4.3 Validation Steps

Validation consists of the following steps:

- Search EEPROM to find the Serial Number Check Value Match
- Decrypt the Hopping Code
- Compare the 10 bits of discrimination value with the lower 10 bits of serial number
- Check if the synchronization counter falls within the first synchronization window.
- Check if the synchronization counter falls within the second synchronization window.
- If a valid transmission is found, update the synchronization counter, else use the next transmitter block and repeat the tests.

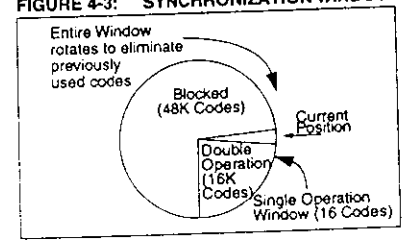
FIGURE 4-2: DECODER OPERATION



4.4 Synchronization with Decoder

The KEELOQ technology features a sophisticated synchronization technique (Figure 4-3) 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 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 16K, the transmitted synchronization value is stored in a 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 was outside 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 relearned. Since the entire window rotates after each valid transmission, codes that have been used become part of the 'blocked' (48K) codes and are no longer valid. This eliminates the possibility of grabbing a previous code and retransmitting it to gain entry.

FIGURE 4-3: SYNCHRONIZATION WINDOW



4.5 Sleep Mode

The sleep mode of the HCS512 is used to reduce current consumption when no RF input signal is present. Sleep mode will only be effective in systems where the RF receiver is relatively quiet when no signal is present. During sleep, the clock stops, thereby significantly reducing the operating current. Sleep mode is enabled by the SLEEP bit in the configuration byte.

The HCS512 will enter sleep mode when:
- The RF line is low
- After a function output is switched off
- Learn mode is terminated (time-out reached)

The device will not enter sleep mode when:
- A function output is active
- Learn sequence active
- Device is in programming mode

The device will wake up from sleep when:
- The SLEEP input pin changes state
- The CLOCK line changes state

Note: During sleep mode the CLK line will change from an output line to an input line that can be used to wake up the device. Connect CLK to $\overline{\text{LRNIN}}$ via a 100K resistor to reliably enter the learn mode whenever sleep mode is active.

5.0 INTEGRATING THE HCS512 INTO A SYSTEM

The HCS512 can act as a stand alone decoder or be interfaced to a microcontroller. Typical stand alone applications include garage door openers and electronic door locks. In stand alone applications, the HCS512 will handle learning, reception, decryption, and validation of the received code; and generate the appropriate output. For a garage door opener, the HCS512 input will be connected to an RF receiver, and the output, to a relay driver to connect a motor controller.

Typical systems where the HCS512 will be connected to a microcontroller include vehicle and home security systems. The HCS512 input will be connected to an RF receiver and the function outputs to the microcontroller. The HCS512 will handle all the decoding functions and the microcontroller, all the system functions. The serial output mode with a 1- or 2-wire interface can be used if the microcontroller is I/O limited.

6.0 DECODER PROGRAMMING

The PG306001 production programmer will allow easy setup and programming of the configuration byte and the manufacturer's code.

6.1 Configuration Byte

The configuration byte is used to set system configuration for the decoder. The LRN bits determine which algorithm (Decrypt or XOR) is used for the key generation. SC_LRN determines whether normal learn (key derived from serial number) or secure learn (key derived from seed value) is used.

TABLE 6-1: CONFIGURATION BYTE

Bit	Name	Description
0	LRN0	Learn algorithm select
1	LRN1	Not used
2	SC_LRN	Secure Learn enable (1 = enabled)
3	SLEEP	Sleep enable (1 = enabled)
4	RES1	Not used
5	RES2	Not used
6	RES3	Not used
7	RES4	Not used

TABLE 6-2: LEARN METHOD LRN0, LRN1 DEFINITIONS

LRN0	Description
0	Decrypt algorithm
1	XOR algorithm

6.2 Programming the Manufacturer's Code

The manufacturer's code must be programmed into EEPROM memory through the synchronous programming interface using the DATA and CLK lines. Provision must be made for connections to these pins if the decoder is going to be programmed in circuit.

Programming mode is activated if the CLK is low for at least 1ms and then goes high within 64 ms after power-up, stays high for longer than 8ms but not longer than 128 ms. After entering programming mode the 64-bit manufacturer's code, 8-bit configuration byte, and 8-bit checksum is sent to the device using the synchronous interface. After receiving the 80-bit message the checksum is verified and the information is written to EEPROM. If the programming operation was successful, the HCS512 will respond with an acknowledge pulse.

After programming the manufacturer's code, the HCS512 decoder will automatically activate an Erase All function, removing all transmitters from the system.

6.3 Download Format

The manufacturer's code and configuration byte must be downloaded least significant byte, least significant bit first as shown in Table 6-3.

6.4 Checksum

The checksum is used by the HCS512 to check that the data downloaded was correctly received before programming the data. The checksum is calculated so that the 10 bytes added together (discarding the overflow bits) is zero. The checksum can be calculated by adding the first 9 bytes of data together and subtracting the result from zero. Throughout the calculation the overflow is discarded.

Given a manufacturer's code of 01234567-89ABCDEF$_{16}$ and a configuration word of 1$_{16}$, the checksum is calculated as shown in Figure 6-1. The checksum is 3F$_{16}$.

6.5 Test Transmitter

The HCS512 decoder will automatically add a test transmitter each time an Erase All Function is done. A test transmitter is defined as a transmitter with a serial number of zero. After an Erase All, the test transmitter will always work without learning and will not check the synchronization counter of the transmitter. Learning of any new transmitters will erase the test transmitter.

Note 1: A transmitter with a serial number of zero cannot be learned. Learning [illegible] first transmission [illegible] **2:** Always learn at least one transmitter after an Erase All sequence. This ensures that the test transmitter is erased.

TABLE 6-3: DOWNLOAD DATA

Byte 9	Byte 8	Byte 7	Byte 6	Byte 5	Byte 4	Byte 3	Byte 2	Byte 1	Byte 0
Check-sum	Config	Man Key_7	Man Key_6	Man Key_5	Man Key_4	Man Key_3	Man Key_2	Man Key_1	Man Key_0

Byte 0, right-most bit downloaded first.

FIGURE 6-1: CHECKSUM CALCULATION

$01_{16} + 23_{16} = 24_{16}$
$24_{16} + 45_{16} = 69_{16}$
$69_{16} + 67_{16} = D0_{16}$
$D0_{16} + 89_{16} = 159_{16}$
$59_{16} + AB_{16} = 104_{16}$ (Carry is discarded)
$04_{16} + CD_{16} = D1_{16}$ (Carry is discarded)
$D1_{16} + EF_{16} = 1C0_{16}$
$C0_{16} + 1_{16} = C1_{16}$ (Carry is discarded)
$(FF_{16} - C1_{16}) + 1_{16} = 3F_{16}$

FIGURE 6-2: PROGRAMMING WAVEFORMS

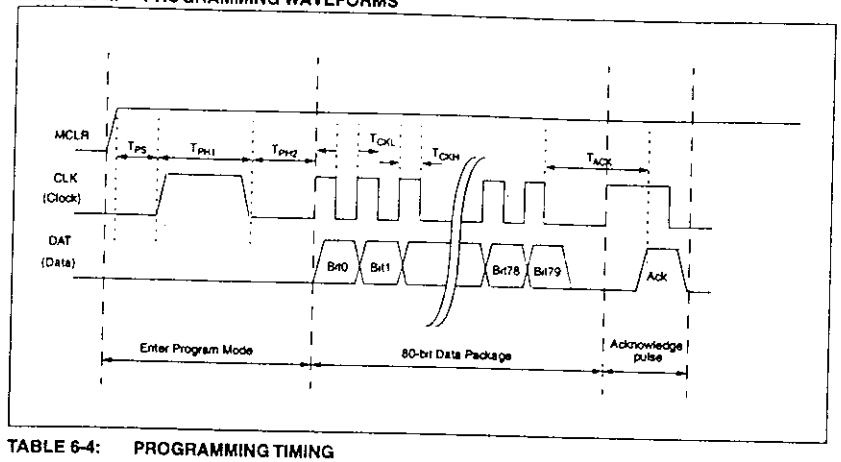


TABLE 6-4: PROGRAMMING TIMING REQUIREMENTS

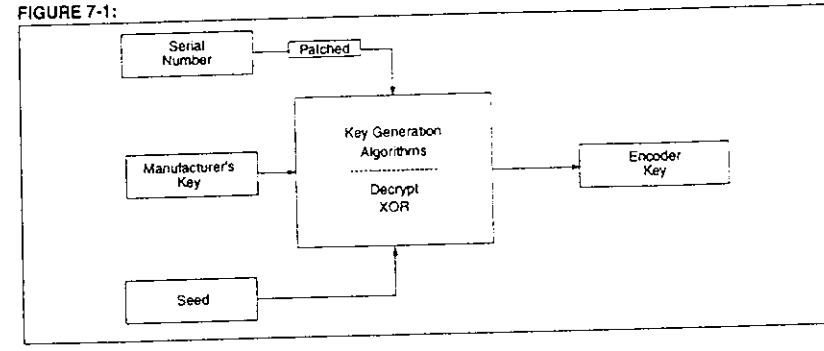
Parameter	Symbol	Min.	Max.	Units
Program mode setup time	TPS	1	64	ms
Hold time 1	TPH1	8	128	ms
Hold time 2	TPH2	0.05	320	ms
Clock High Time	TCKH	0.05	320	ms
Clock Low Time	TCKL	0.050	320	ms
Acknowledge Time	TACK	—	80	ms

Note: Fosc equals 4 MHz.

7.0 KEY GENERATION SCHEMES

The HCS512 decoder has two key generation schemes. Normal learning uses the transmitter's serial number to derive two input seeds which are used as inputs to the key generation algorithm. Secure learning uses the seed transmission to derive the two input seeds. Two key generation algorithms are available to convert the inputs seeds to secret keys. The appropriate scheme is selected in the configuration word.

FIGURE 7-1:



7.1 Normal Learning (Serial Number Derived)

The two input seeds are composed from the serial number in two ways, depending on the encoder type. The encoder type is determined from the number of bits in the incoming transmission. SourceH is used to calculate the upper 32 bits of the encoder key, and SourceL, for the lower 32 bits.

For 24-bit serial number encoders (56-bit transmissions):

SourceH = 65H + 24 bit Serial Number
SourceL = 2BH + 24 bit Serial Number

For 28-bit serial number encoders (66 / 67-bit transmissions):

SourceH = 6H + 28 bit Serial Number
SourceL = 2H + 28 bit Serial Number

7.2 Secure Learning (Seed Derived)

The two input seeds are composed from the seed value that is transmitted during secure learning. The lower 32 bits of the seed transmission is used to compose the lower seed, and the upper 32 bits, for the upper seed. The upper 4 bits (function code) are set to zero.

For 32-bit seed encoders:

SourceH = Serial Number $_{\text{Lower 28 bits}}$ with upper 4 bits always zero
SourceL = Seed $_{\text{32 bits}}$

For 48-bit seed encoders:

SourceH = Seed $_{\text{Upper 16 bits}}$ + Serial Number $_{\text{Upper 16 bits}}$ with upper 4 bits always zero
SourceL = Seed $_{\text{Lower 32 bits}}$

For 64-bit seed encoders:

Note: 64-bit seeds are handled as 48-bit seeds

SourceH = Seed $_{\text{Upper 16 bits}}$ + Serial Number $_{\text{Upper 16 bits}}$ with upper 4 bits always zero
SourceL = Seed $_{\text{Lower 32 bits}}$

7.3 Key Generation Algorithms

There are two key generation algorithms implemented in the HCS512 decoder. The KEELOQ decryption algorithm provides a higher level of security than the XOR algorithm. Section 6.1 describes the selection of the algorithms in the configuration byte.

7.3.1 KEELOQ DECRYPT ALGORITHM

This algorithm uses the KEELOQ decryption algorithm and the manufacturer's code to derive the encoder key as follows:

$Key_{Upper\ 32\ bits} = F_{KEELOQ\ Decrypt}(SourceH) \mid_{64\ Bit\ Manufacturers\ Code}$

$Key_{Lower\ 32\ bits} = F_{KEELOQ\ Decrypt}(SourceL) \mid_{64\ Bit\ Manufacturers\ Code}$

7.3.2 XOR WITH THE MANUFACTURER'S CODE

The two 32-bits seeds are XOR with the manufacturer's code to form the 64 bit encoder key.

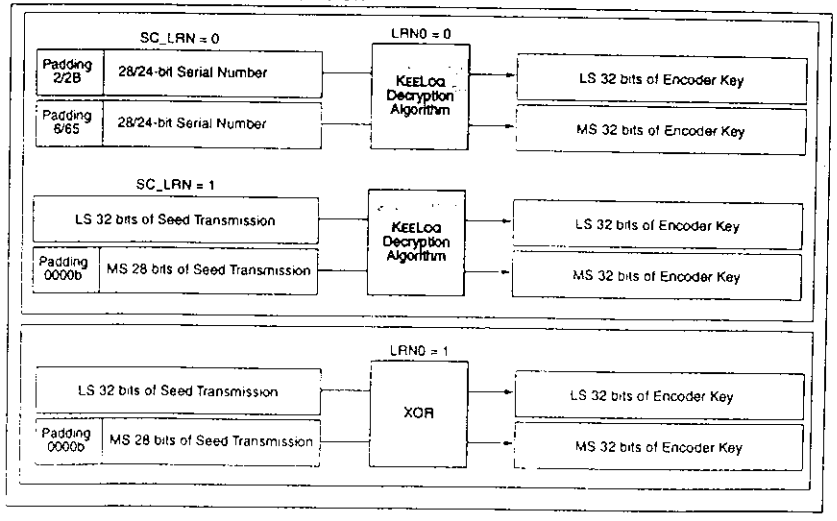
$Key_{Upper\ 32\ bits} = SourceH \otimes Manufacturers\ Code \mid_{Upper\ 32\ bits}$

$Key_{Lower\ 32\ bits} = SourceL \otimes Manufacturers\ Code \mid_{Lower\ 32\ bits}$

After programming the manufacturer's code, the HCS512 decoder will automatically activate an Erase All function, removing all transmitters from the system.

If $\overline{LRNIN}$ is taken low momentarily during the learn status indication, the indication will be terminated. Once a successful learning sequence is detected, the indication can be terminated, allowing quick learning in a manufacturing set up.

FIGURE 7-2: HCS512 KEY GENERATION



8.0 KEELOQ ENCODERS

8.1 Transmission Format (PWM)

The KEELOQ encoder transmission is made up of several parts (Figure 8-1). Each transmission begins with a preamble and a header, followed by the encrypted and then the fixed data. The actual data is 56/66/67 bits which consists of 32 bits of encrypted data and 24/34/35 bits of non-encrypted data. Each transmission is followed by a guard period before another transmission can begin. 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 non-encrypted portion is comprised of the status bits, the function bits, and the 24/28-bit serial number. The encrypted and non-encrypted combined sections increase the number of combinations to 7.38×10^{19}.

8.2 Code Word Organization

The HCSXXX encoder transmits a 66/67-bit code word when a button is pressed. The 66/67-bit word is constructed from an encryption portion and a non-encrypted code portion (Figure 8-2).

The **Encrypted Data** is generated from four button bits, two overflow counter bits, ten discrimination bits, and the 16-bit synchronization value.

The **Non-encrypted Data** is made up from 2 status bits, 4 function bits, and the 28/32-bit serial number.

FIGURE 8-1: CODE WORD TRANSMISSION FORMAT

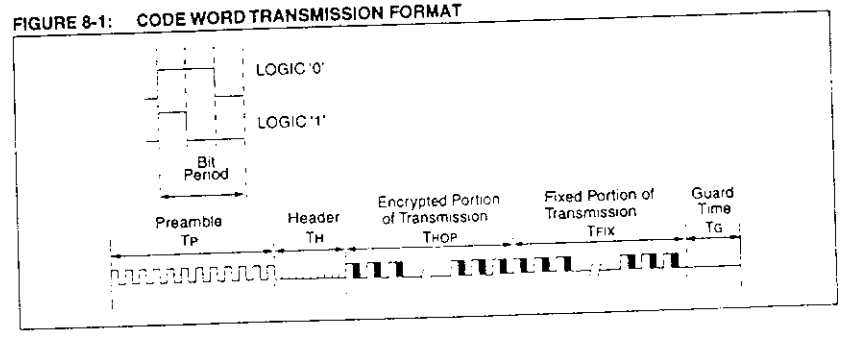
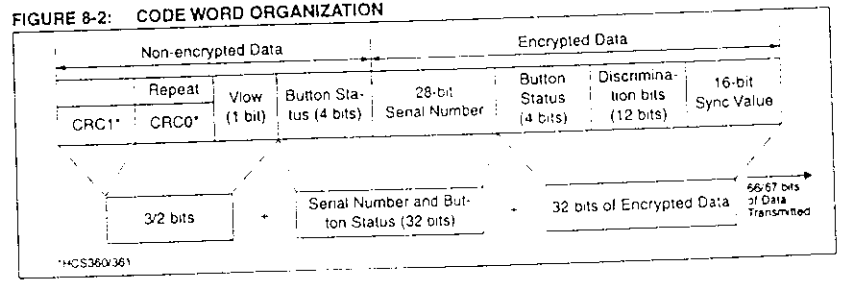


FIGURE 8-2: CODE WORD ORGANIZATION



9.0 ELECTRICAL CHARACTERISTICS FOR HCS512

Absolute Maximum Ratings †

Ambient temperature under bias ..... -55°C to +125°C
Storage temperature ..... -65°C to +150°C
Voltage on any pin with respect to Vss (except VDD) ..... -0.6V to VDD +0.6V
Voltage on VDD with respect to Vss ..... 0 to +7.5V
Total power dissipation (Note 1) ..... 800 mW
Maximum current out of Vss pin ..... 150 mA
Maximum current into VDD pin ..... 100 mA
Input clamp current, IIK (VI < 0 or VI > VDD) ..... ± 20 mA
Output clamp current, IOK (VO < 0 or VO >VDD) ..... ± 20 mA
Maximum output current sunk by any I/O pin ..... 25 mA
Maximum output current sourced by any I/O pin ..... 20 mA

Note: Power dissipation is calculated as follows: Pdis = VDD x {IDD - Σ IOH} + Σ {(VDD–VOH) x IOH} + Σ(VOL x IOL)

† NOTICE: Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at those or any other conditions above those indicated in the operation listings of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

TABLE 9-1: DC CHARACTERISTICS

		Standard Operating Conditions (unless otherwise stated) Operating temperature Commercial (C): 0°C ≤ TA ≤ +70°C Industrial (I): -40°C ≤ TA ≤ +85°C				
Symbol	**Characteristic**	**Min**	**Typ(†)**	**Max**	**Units**	**Conditions**
VDD	Supply Voltage	3.0	—	6.0	V	
VPOR	VDD start voltage to ensure Reset	—	VSS	—	V	
SVDD	VDD rise rate to ensure Reset	0.05*	—	—	V/ms	
IDD	Supply Current	— —	1.8 7.3 15	4.5 10 32	mA mA µA	FOSC = 4 MHz, VDD = 5.5V (During EEPROM programming) In SLEEP mode
VIL	Input Low Voltage	VSS	—	0.16 VDD	V	except $\overline{MCLR}$ = 0.2 VDD
VIH	Input High Voltage	0.48 VDD	—	VDD	V	except $\overline{MCLR}$ = 0.85 VDD
VOL	Output Low Voltage	—	—	0.6	V	IOL = 8.5 mA, VDD = 4.5V
VOH	Output High Voltage	VDD-0.7	—	—	V	IOH = -3.0 mA, VDD = 4.5V

† Data in "Typ" column is at 5.0V, 25°C unless otherwise stated. These parameters are for design guidance only and are not tested.
* These parameters are characterized but not tested.
Note: Negative current is defined as coming out of the pin.

TABLE 9-2: AC CHARACTERISTICS

Symbol	**Characteristic**	**Min**	**Typ**	**Max**	**Units**	**Conditions**
FOSC	Oscillator frequency	2.7	4	6.21	MHz	Rext = 10K, Cext = 10pF
TE	PWM elemental pulse width	65	—	1080	µs	4.5V < VDD < 5.5V Oscillator components tolerance < 6%.
		130	—	1080	µs	3V < VDD < 6V Oscillator components tolerance <10%
TOD	Output delay	70	90	115	ms	
TA	Output activation time	322	500	740	ms	
TRPT	REPEAT activation time	32	50	74	ms	
TLRN	LRNIN activation time	21	32	—	ms	
TMCLR	MCLR low time	150	—	—	ns	
TOV	Time output valid	—	150	222	ms	

FIGURE 9-1: RESET WATCHDOG TIMER, OSCILLATOR START-UP TIMER AND POWER-UP TIMER TIMING

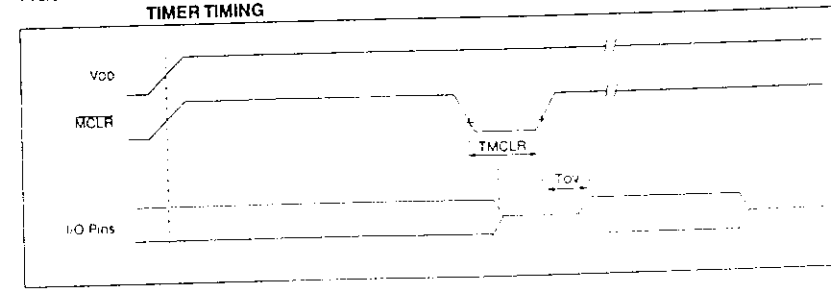
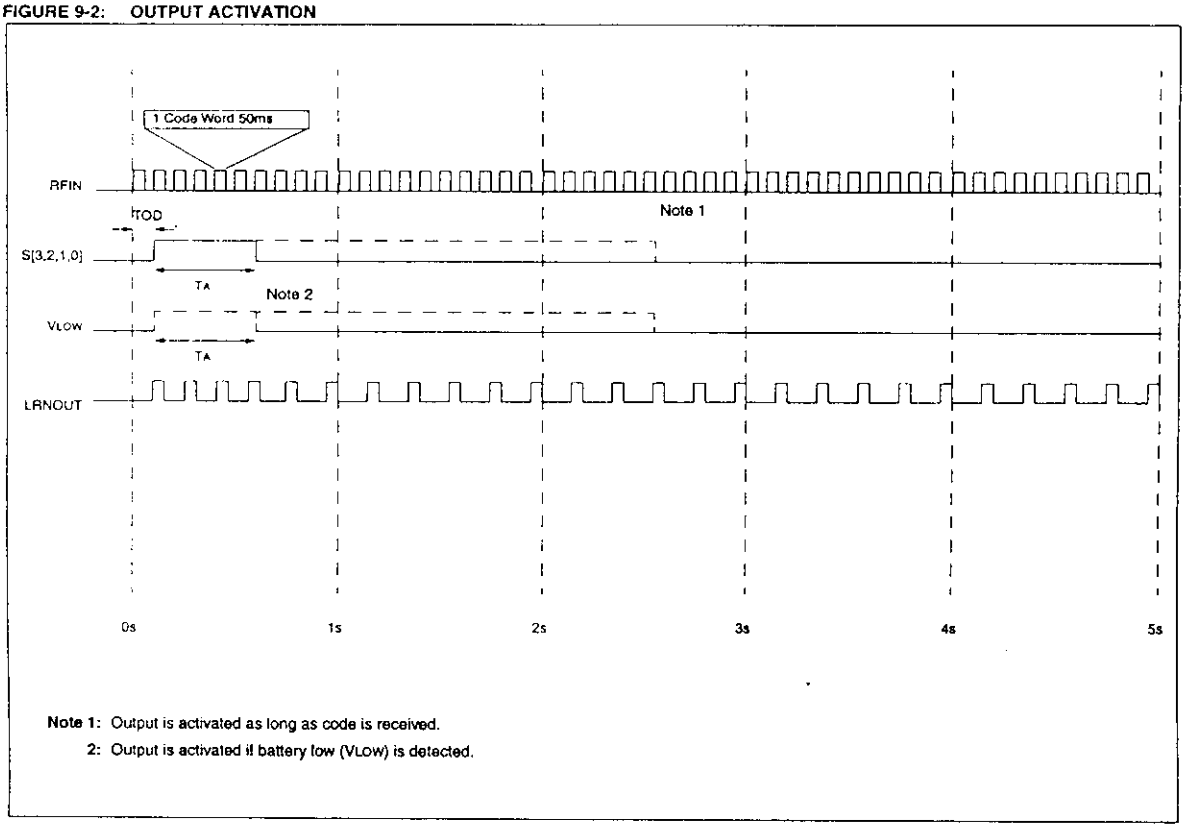
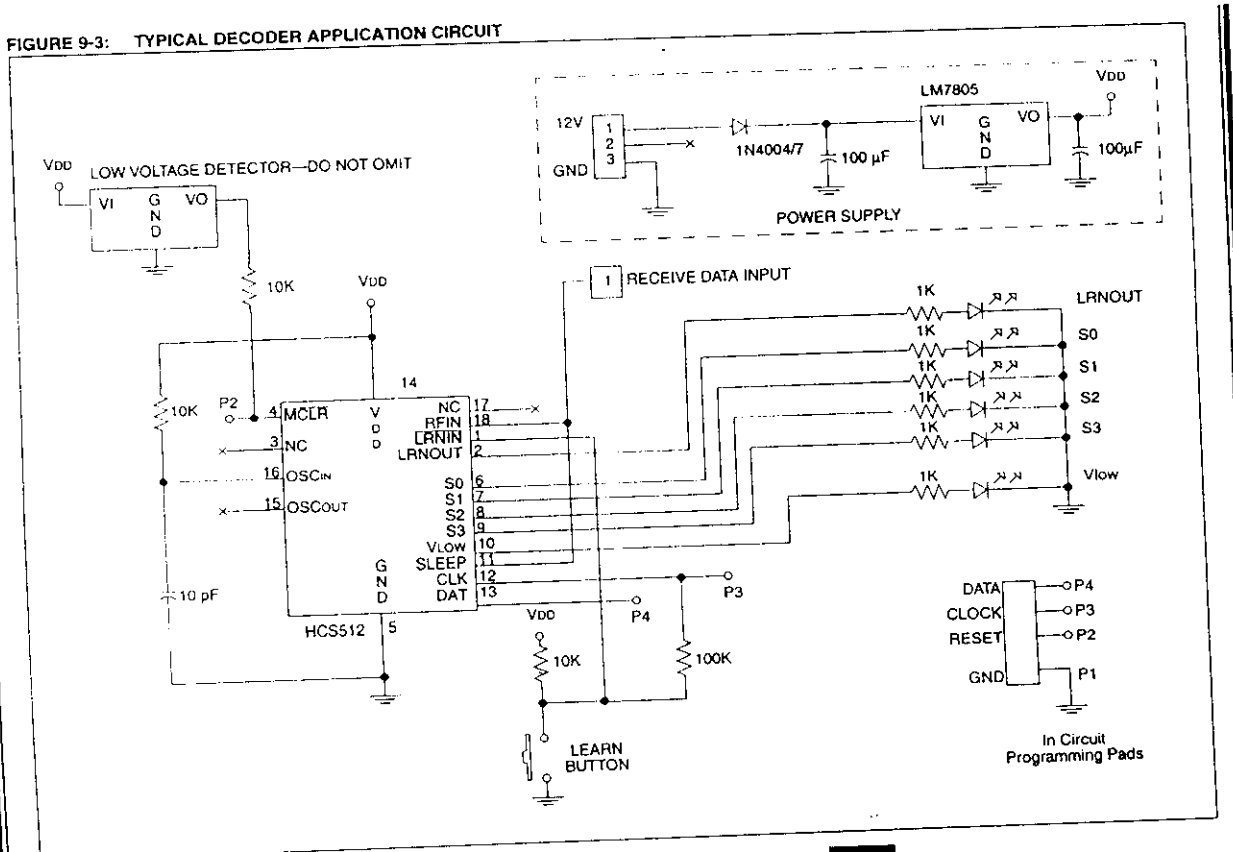


FIGURE 9-2: OUTPUT ACTIVATION



Note 1: Output is activated as long as code is received.
2: Output is activated if battery low (VLOW) is detected.

FIGURE 9-3: TYPICAL DECODER APPLICATION CIRCUIT



HCS512 PRODUCT IDENTIFICATION SYSTEM

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

HCS512 — /P		
Package:	P =	Plastic DIP (300 mil Body), 8-lead
	SN =	Plastic SOIC (300 mil Body), 18-lead
Temperature Range:	Blank =	0°C to +70°C
	I =	-40°C to +85°C
Device:	HCS512	Code Hopping Decoder
	HCS512T	Code Hopping Decoder (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's Bulletin Board, via your local CompuServe number (CompuServe membership NOT required).

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

MICROCHIP

SECTION 3
CODE HOPPING ENCODERS

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)

MICROCHIP

HCS300

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

- 2.0—6.3V operation
- Four button inputs
  - No additional circuitry required
  - 15 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
- Current limiting on LED output
- Minimum component count
- Synchronous transmission mode

Typical Applications

The HCS300 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

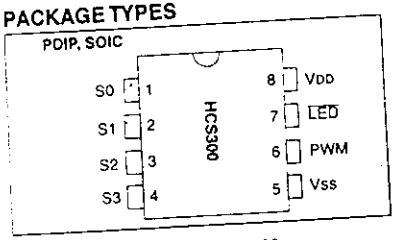
- Automotive RKE systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Identity tokens
- Burglar alarm systems

DESCRIPTION

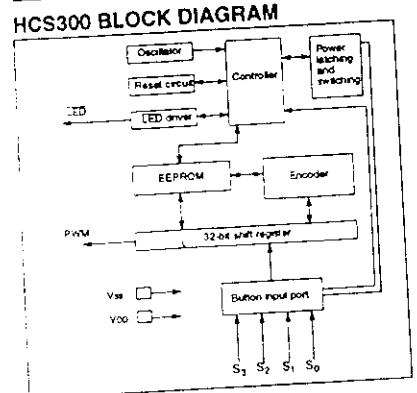
The HCS300, from Microchip Technology Inc., is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS300 utilizes the KEELOQ code hopping technology, which incorporates high security, a small package outline and low cost, to make this device a perfect solution for unidirectional remote keyless entry systems and access control systems.

PACKAGE TYPES

PDIP, SOIC



HCS300 BLOCK DIAGRAM



The HCS300 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and six status bits to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend (code grabbing) schemes useless.

The encryption key, serial number, and configuration data are stored in EEPROM which is not accessible via any external connection. This makes the HCS300 a very secure unit. The HCS300 provides an easy to use serial interface for programming the necessary security keys, system parameters, and configuration data.

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

KEELOQ is a registered trademark of Microchip Technology Inc.
*Code hopping encoder patents allowed and pending.

The HCS300 operates over a wide voltage range of 2.0V to 6.3V and has four button inputs in an 8-pin configuration. This allows the system designer the freedom to utilize up to 15 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 HCS300 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 HCS300 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 relative number of code combinations for a low end system is also a relatively small number. These shortcomings provide the means for a sophisticated thief to create a device that 'grabs' a transmission and re-transmits it later or a device that scans all possible combinations until the correct one is found.

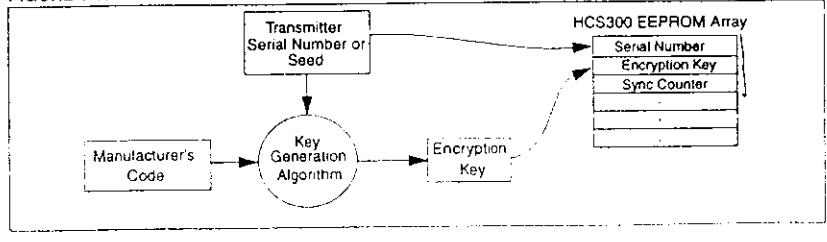
The HCS300 employs the KEELOQ code hopping technology and an encryption algorithm to achieve a high level of security. Code hopping is a method by which the code transmitted from the transmitter to the receiver is different every time a button is pushed. This method, coupled with a transmission length of 66 bits, virtually eliminates the use of code 'grabbing' or code 'scanning'.

As indicated in the block diagram on page one, the HCS300 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



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 HCS300. Section 7.0 provides more detail on integrating the HCS300 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)

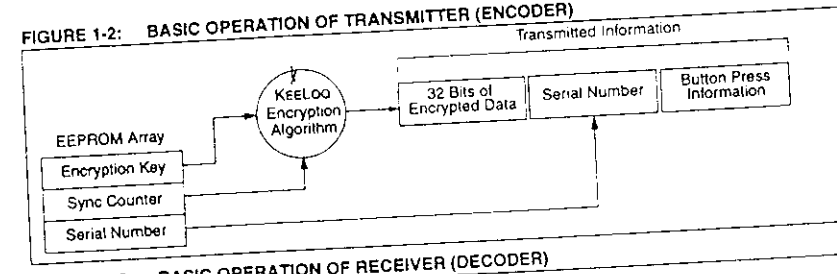
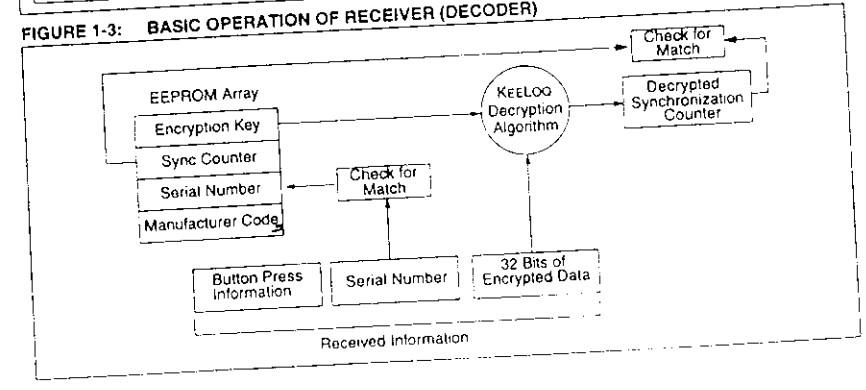


FIGURE 1-3: BASIC OPERATION OF RECEIVER (DECODER)



2.0 DEVICE OPERATION

As shown in the typical application circuits (Figure 2-1), the HCS300 is a simple device to use. It requires only the addition of buttons and RF circuitry for use as the transmitter in your security application. A description of each pin is described in Table 2-1.

FIGURE 2-1: TYPICAL CIRCUITS

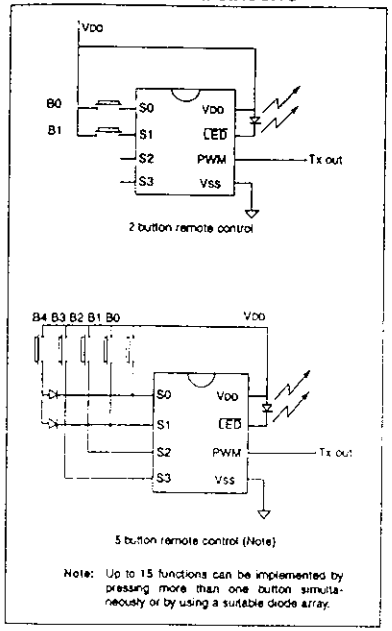


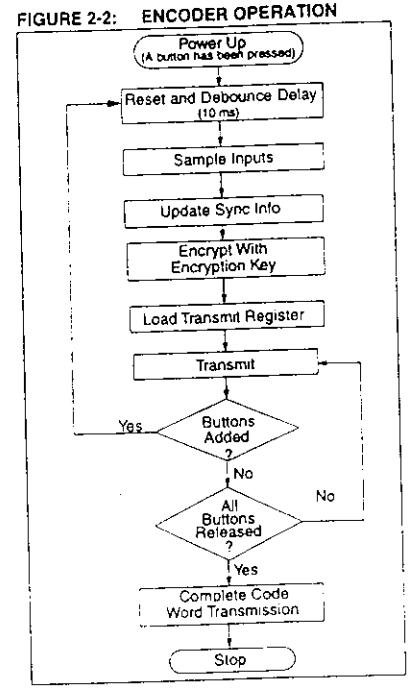
TABLE 2-1: PIN DESCRIPTIONS

Name	Pin Number	Description
S0	1	Switch input 0
S1	2	Switch input 1
S2	3	Switch input 2/Can also be clock pin when in programming mode
S3	4	Switch input 3/Clock pin when in programming mode
VSS	5	Ground reference connection
PWM	6	Pulse width modulation (PWM) output pin/Data pin for programming mode
LED	7	Cathode connection for directly driving LED during transmission
VDD	8	Positive supply voltage connection

The high security level of the HCS300 is based on the patented KEELOQ technology. A block cipher type of 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 coded transmission will change. The HCS300 will wake up upon detecting a switch closure and then delay approximately 10 ms for switch debounce (Figure 2-2). The synchronized 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 18 years of typical use before a code is repeated based on 10 operations per day. Overflow information programmed into 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 ccurrent code word will be completed and the power down will occur.

FIGURE 2-2: ENCODER OPERATION



3.0 EEPROM MEMORY ORGANIZATION

The HCS300 contains 192 bits (12 x 16-bit words) of EEPROM memory (Table 3-1). This EEPROM array is used to store the encryption key information, synchronization value, etc. Further descriptions of the memory array is given in the following sections.

TABLE 3-1: EEPROM MEMORY MAP

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

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

3.1 Key_0 - Key_3 (64-Bit Encryption Key)

The 64-bit encryption key is used by the transmitter to create the encrypted message transmitted to the receiver. This key is created and programmed at the time of production using a key generation algorithm. 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. Although there are 32 bits allocated for the serial number, only the lower order 28 bits are transmitted. The serial number is meant to be unique for every transmitter. The most significant bit of the serial number (Bit 31) is used to turn the auto shutoff timer on or off.

3.3.1 AUTO SHUTOFF TIMER SELECT

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

3.4 SEED_0, SEED_1 (Seed Word)

This is the two word (32 bits) seed code that will be transmitted when all four 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 EN_Key (Envelope Encryption Key)

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

3.6 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	Overflow Bit 0 (OVR0)
11	Overflow Bit 1 (OVR1)
12	Low Voltage Trip Point Select
13	Baudrate Select Bit 0 (BSL0)
14	Baudrate Select Bit 1 (BSL1)
15	Envelope Encryption Select (EENC)

3.6.1 DISCRIMINATION VALUE (DISC0 TO DISC9)

The discrimination value can be programmed with any value to serve as a post decryption check on the decoder end. In a typical system, this will be programmed with the 10 least significant bits of the serial number, 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.

3.6.2 OVERFLOW BITS (OVR0 AND OVR1)

The overflow bits are used to extend the number of possible synchronization values. The synchronization counter is 16 bits in length, yielding 65,536 values before the cycle repeats. Under typical use of 10 operations a day, this will provide nearly 18 years of use before a repeated value will be used. Should the system designer conclude that is not adequate, then the overflow bits can be utilized to extend the number of unique values. This can be done by programming OVR0 and OVR1 to 1s at the time of production. The encoder will automatically clear OVR0 the first time that the synchronization value wraps from 0xFFFF to 0x0000 and clear OVR1 the second time the counter wraps. Once cleared, OVR0 and OVR1 cannot be set again, thereby creating a permanent record of the counter overflow. This prevents fast cycling of 64K counter. If the decoder system is programmed to track the overflow bits, then the effective number of unique synchronization values can be extended to 196,608. If programmed to zero, the system will be compatible with the NTQ104/5/6 devices (i.e., no overflow with discrimination bits set to zero).

3.6.3 ENVELOPE ENCRYPTION (EENC)

If the EENC bit is set to a 1, the 32-bit fixed code part of the transmission will also be encrypted so that it will appear to be random. The 16-bit envelope key and envelope algorithm will be used for encryption.

3.6.4 BAUDRATE SELECT BITS (BSL0, BSL1)

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

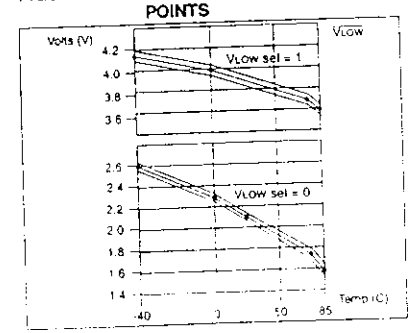
TABLE 3-3: BAUDRATE SELECT

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

3.6.5 LOW VOLTAGE TRIP POINT SELECT

The low voltage trip point select bit is used to tell the HCS300 what VDD 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 VDD level is assumed to be operating from a 5 volt or 6 volt VDD level. If the bit is set low, then the VDD level is assumed to be 3.0 volts. Refer to Figure 3-1 for voltage trip point. VLOW is tested at 6.3V at -25°C and +85°C and 2.0V at -25°C and +85°C

FIGURE 3-1: TYPICAL VOLTAGE TRIP POINTS



4.0 TRANSMITTED WORD

4.1 Transmission Format (PWM)

The HCS300 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 (or S3), the device enters synchronous transmission mode. In this mode, it functions as a normal transmitter, with the exception that the timing of the PWM data string is controlled externally and 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 or S3. The timing of the PWM data string is controlled by supplying a clock on S2 or S3 and should not exceed 20 KHz. The code word is the same as in PWM mode with 16 reserved bits at the end of the word. The reserved bits can be ignored. When in synchronous transmission mode S2 or S3 should not be toggled until all internal processing has been completed as shown in Figure 4-4.

4.3 Code Word Organization

The HCS300 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 button bits, two overflow counter bits, ten discrimination bits, and the 16-bit synchronization value (Figure 8-4).

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

FIGURE 4-1: CODE WORD TRANSMISSION FORMAT

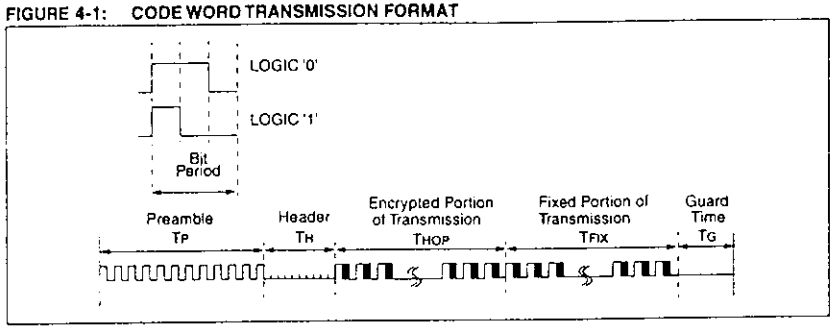


FIGURE 4-2: CODE WORD ORGANIZATION

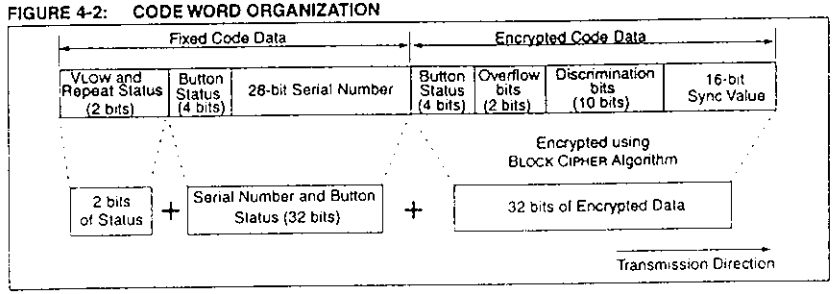


FIGURE 4-3: SYNCHRONOUS TRANSMISSION MODE

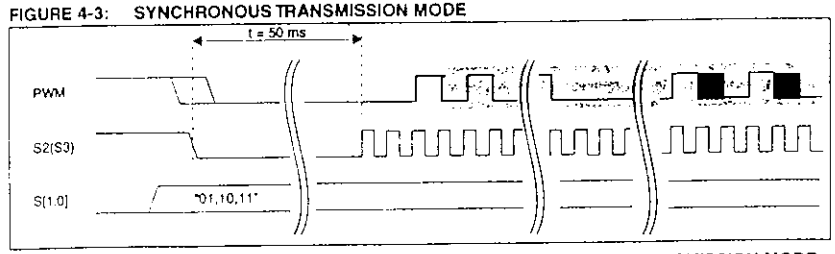
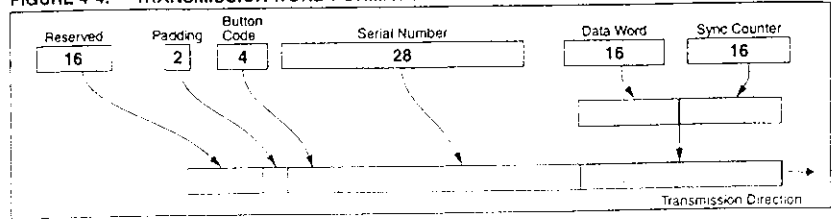


FIGURE 4-4: TRANSMISSION WORD FORMAT DURING SYNCHRONOUS TRANSMISSION MODE



5.0 SPECIAL FEATURES

5.1 Code Word Completion

Code word completion is an automatic feature that makes sure that the entire code word is transmitted, even if the button is released before the transmission is complete. The HCS300 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. Blank Alternate Code Word (BACW) is used for reducing the average power of a transmission (Figure 5-1). This is a selectable feature that is determined in conjunction with the baudrate selection bits BSL0 and BSL1. Using the BACW allows the user to transmit a higher amplitude transmission if the transmission length is shorter. The FCC puts constraints on the average power that can be transmitted by a device, and BACW effectively prevents continuous transmission by only allowing the transmission of every second or every fourth code word. This reduces the average power transmitted and hence, assists in FCC approval of a transmitter device.

5.3 Envelope Encryption Option

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

5.4 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 HCS300 which is stored in EEPROM and can only be transmitted when all four 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.

TABLE 5-1: PIN ACTIVATION TABLE

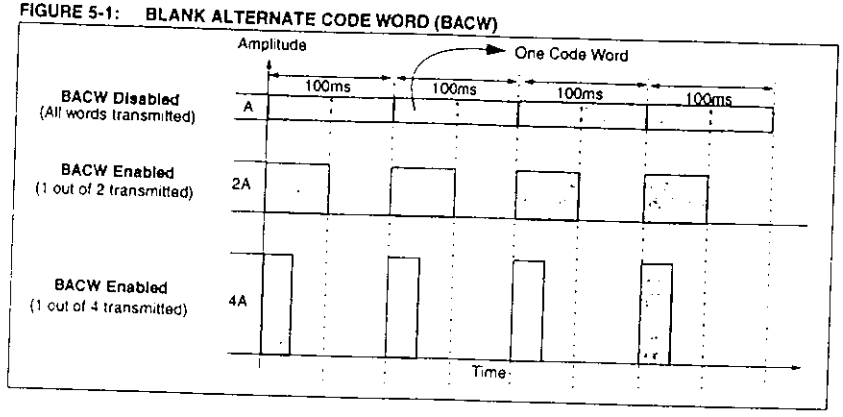
	S3	S2	S1	S0	Notes
1	0	0	0	1	1
2	0	0	1	0	1
3	0	0	1	1	1
4	0	1	0	0	1
5	0	1	0	1	1
6	0	1	1	0	1
7	0	1	1	1	1
8	1	0	0	0	1
9	1	0	0	1	1
10	1	0	1	0	1
11	1	0	1	1	1
12	1	1	0	0	1
13	1	1	0	1	1
14	1	1	1	0	1
15	1	1	1	1	2

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

5.5 Auto-shutoff

The Auto-shutoff function automatically stops the device from transmitting if a button inadvertently gets pressed for a long period of time. This will prevent the device from draining the battery if a button gets pressed while the transmitter is in a pocket or purse. This function can be enabled or disabled and is selected by setting or clearing the Auto-shutoff bit (see Section 3.3.1). Setting this bit high will enable the function (turn Auto-shutoff function on) and setting the bit low will disable the function. Time-out period is approximately 25 seconds.

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



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 between two values, based on the battery voltage being used. See Section 3.6.5 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 (Section 5.8).

5.7 RPT: Repeat Indicator

This bit will be low for the first transmitted word. If a button is held down for more than one transmitted code word, this bit will be set to indicate a repeated code word and remain set until the button is released (Figure 8-4).

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

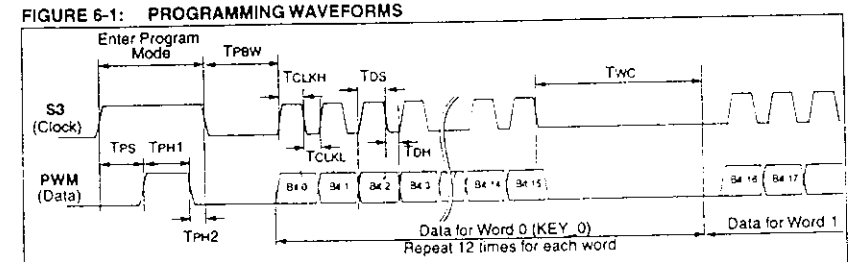
During normal transmission the $\overline{\text{LED}}$ output is LOW. If the supply voltage drops below the low voltage trip point, the $\overline{\text{LED}}$ output will be toggled at approximately 5Hz during the transmission (Section 3.6.5).

6.0 PROGRAMMING THE HCS300

When using the HCS300 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 S3 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 S3 as the clock line and PWM as the data in line. After each 16-bit word is loaded, a programming delay is required for the internal program cycle to complete. This delay can take up to Twc. At the end of the programming cycle, the device can be verified (Figure 6-2) by reading back the EEPROM. Reading is done by clocking the S3 line and reading the data bits on PWM. For security reasons, it is not possible to execute a verify function without first programming the EEPROM. **A verify operation can only be done once, immediately following the program cycle.**

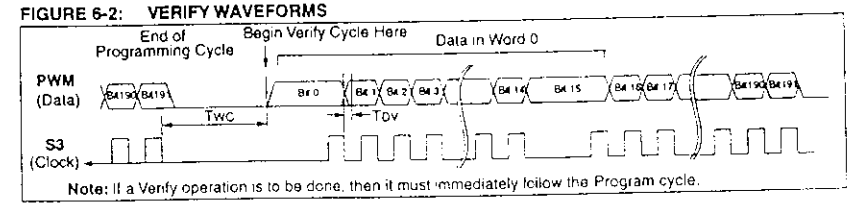
Note: To ensure that the device does not accidentally enter programming mode, PWM should never be pulled high by the circuit connected to it. Special care should be taken when driving PNP RF transistors.

FIGURE 6-1: PROGRAMMING WAVEFORMS



Note 1: Unused button inputs to be held to ground during the entire programming sequence.
Note 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.

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}	3.5	4.5	ms
Hold time 1	T_{PH1}	3.5	—	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

7.0 INTEGRATING THE HCS300 INTO A SYSTEM

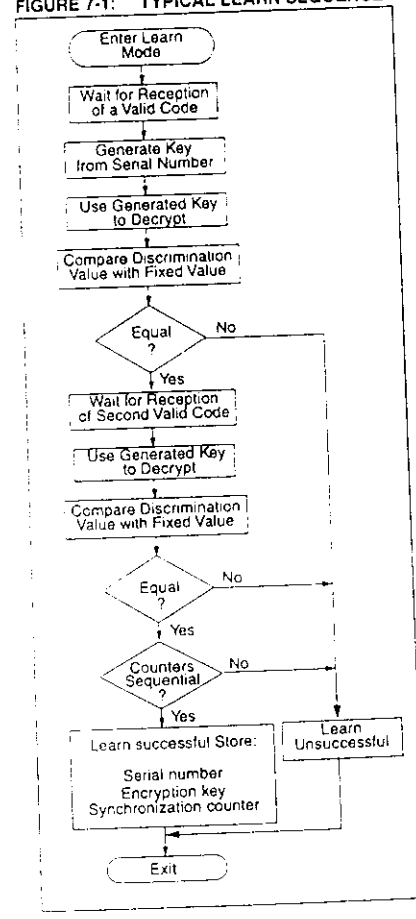
Use of the HCS300 in a system requires a compatible decoder. This decoder is typically a microcontroller with compatible firmware. Microchip will provide (via a license agreement) firmware routines that accept transmissions from the HCS300 and decrypt the hopping code portion of the data stream. These 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.

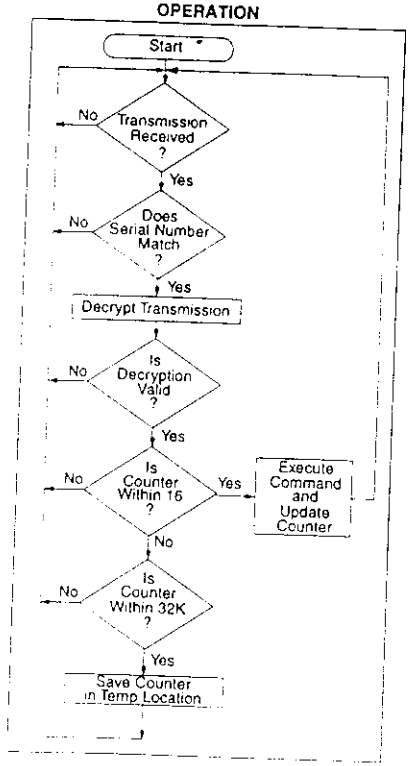
FIGURE 7-1: TYPICAL LEARN SEQUENCE



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

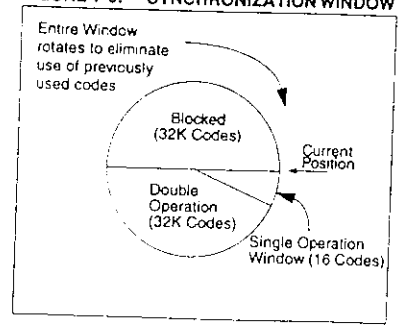


7.3 Synchronization with Decoder

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
VDD	Supply voltage	-0.3 to 6.6	V
VIN	Input voltage	-0.3 to VDD + 0.3	V
VOUT	Output voltage	-0.3 to VDD + 0.3	V
IOUT	Max output current	50	mA
TSTG	Storage temperature	-55 to +125	C (Note)
TLSOL	Lead soldering temp	300	C (Note)
VESD	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

		2.0V < VDD < 3.0			3.0 < VDD < 6.3				
Parameter	Sym.	Min	Typ[1]	Max	Min	Typ[1]	Max	Unit	Conditions
Operating current (avg)[2]	ICC		0.2	0.5				mA	VDD = 3.0V
						0.7	1.4	mA	VDD = 6.3V
Standby current	ICCS		0.1	1.0		0.1	1.0	µA	
Auto-shutoff current[3,4]	ICCS		40	75		160	650	µA	
High level input voltage	VIH	0.55VDD		VDD+0.3	0.55VDD		VDD+0.3	V	
Low level input voltage	VIL	-0.3		0.15VDD	-0.3		0.15VDD	V	
High level output voltage	VOH	0.7VDD			0.7VDD			V	IOH = -1.0 mA VDD = 2.0V
								V	IOH = -2.0 mA VDD = 6.3V
Low level output voltage	VOL			0.08VDD			0.08VDD	V	IOL = 1.0 mA VDD = 2.0V
								V	IOL = 2.0 mA VDD = 6.3V
LED sink current[5]	ILED	1.0	1.8	2.5				mA	VLED[6] = 1.5V VDD = 3.0V
					2.0	2.7	3.7	mA	VLED[6] = 1.5V VDD = 6.3V
Resistance; S0-S3	RS0-3	40	60	80	40	60	80	kΩ	VDD = 4.0V
Resistance; PWM	RPWM	80	120	160	80	120	160	kΩ	VDD = 4.0V

Note 1: Typical values are at 25°C.
2: No load.
3: Auto-shutoff current specification does not include the current through the input pulldown resistors.
4: Auto-shutoff current is periodically sampled and not 100% tested.
5: With VLOW Sel = 0 for operation from 2.0V to 3.0V and VLOW Sel = 1 for operation from 3.0V to 6.3V.
6: VLED is the voltage drop across the terminals of the LED.

FIGURE 8-1: POWER UP AND TRANSMIT TIMING

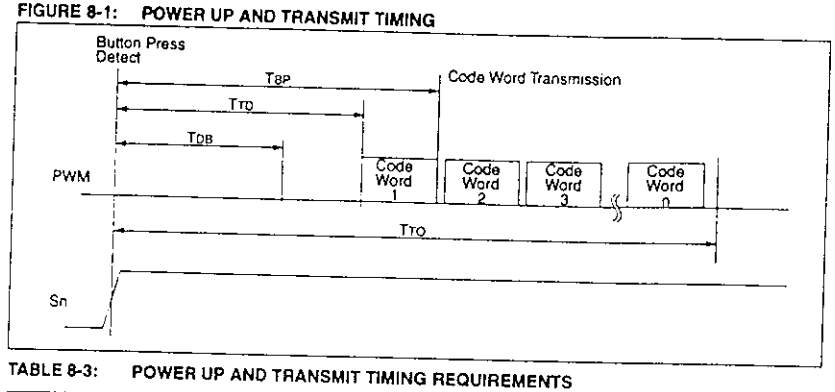


TABLE 8-3: POWER UP AND TRANSMIT TIMING REQUIREMENTS

VDD = +2.0 to 6.3V
Commercial (C): Tamb = 0°C to +70°C
Industrial (I): Tamb = -40°C to +85°C

Parameter	Symbol	Min	Max	Unit	Remarks
Time to second button press	TBP	10 + Code Word Time	26 + Code Word Time	ms	(Note 1)
Transmit delay from button detect	TTD	10	26	ms	
Debounce delay	TDB	6	13	ms	
Auto-shutoff time-out period	TTO	20	35	s	(Note 2)

Note 1: TBP is the time in which a second button can be pressed without completion of the first code word and the intention was to press the combination of buttons.
2: The auto shutoff timeout period is not tested.

FIGURE 8-2: PWM FORMAT

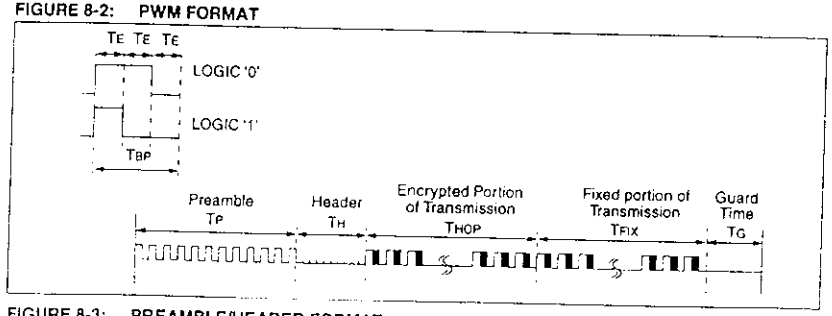


FIGURE 8-3: PREAMBLE/HEADER FORMAT

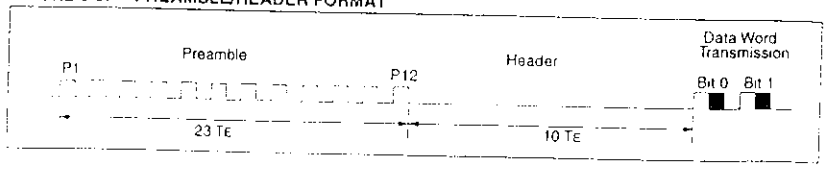


FIGURE 8-4: DATA WORD FORMAT

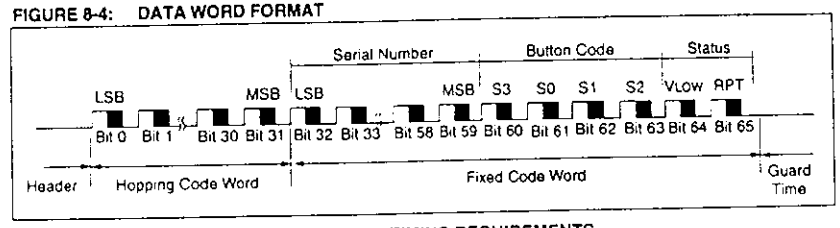


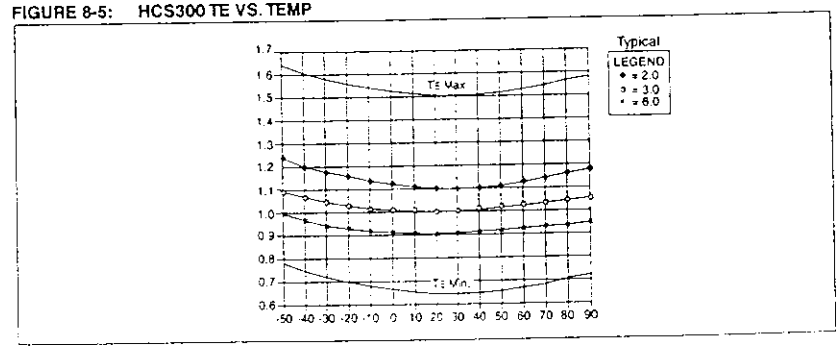
TABLE 8-4: CODE WORD TRANSMISSION TIMING REQUIREMENTS

VDD = +2.0 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			1 out of 4			
Symbol	Characteristic	Number of TE	Min.	Typ.	Max.	Min.	Typ.	Max.	Min.	Typ.	Max.	Units
TE	Basic pulse element	1	260	400	660	130	200	330	65	100	165	µs
TBP	PWM bit pulse width	3	780	1200	1980	390	600	990	195	300	495	µs
TP	Preamble duration	23	6.0	9.2	15.2	3.0	4.6	7.6	1.5	2.3	3.8	ms
TH	Header duration	10	2.6	4.0	6.6	1.3	2.0	3.3	0.7	1.0	1.7	ms
THOP	Hopping code duration	96	25.0	38.4	63.4	12.5	19.2	31.7	6.2	9.6	15.8	ms
TFIX	Fixed code duration	102	26.5	40.8	67.3	13.3	20.4	33.7	6.6	10.2	16.8	ms
TG	Guard Time	39	10.1	15.6	25.7	5.1	7.8	12.9	2.5	3.9	6.4	ms
—	Total Transmit Time	270	70.2	108.0	178.2	35.1	54.0	89.1	17.6	27.0	44.6	ms
—	PWM data rate	—	1282	833	505	2564	1667	1010	5128	3333	2020	bps

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

FIGURE 8-5: HCS300 TE VS. TEMP



HCS300 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.

HCS300 - /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:	HCS300	Code Hopping Encoder
		HCS300T	Code Hopping Encoder (Tape and Reel)

Sales and Support

Products supported by a preliminary Data Sheet may possibly 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 (see next page)
2. The Microchip Corporate Literature Center U.S. FAX: (602) 786-7277
3. The Microchip's Bulletin Board, via your local CompuServe number (CompuServe membership NOT required).

Please specify which device, revision of silicon and Data Sheet (include Literature #) you are using.
For latest version information and upgrade kits for Microchip Development Tools, please call 1-800-755-2345 or 1-602-786-7302.

MICROCHIP

HCS301

KEELOQ® Code Hopping Encoder*

FEATURES

Security

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

Operating

- 3.5V - 13.0V operation
- Four button inputs
  - 15 functions available
- Selectable baud rate
- Automatic code word completion
- Battery low signal transmitted to receiver
- Battery low indication on LED
- Non-volatile synchronization data

Other

- Functionally identical to HCS300
- Easy to use programming interface
- On-chip EEPROM
- On-chip oscillator and timing components
- Button inputs have internal pulldown resistors
- Current limiting on LED output
- Low external component cost

Typical Applications

The HCS301 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

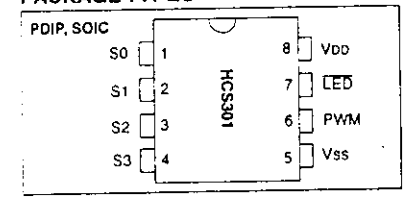
- Automotive RKE systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage door openers
- Identity tokens
- Burglar alarm systems

DESCRIPTION

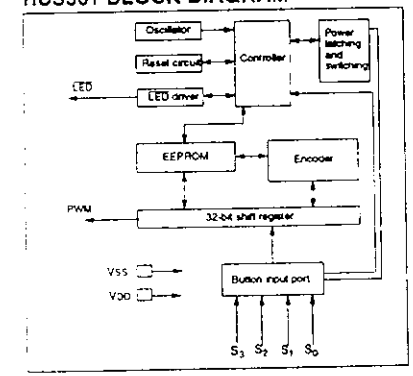
The HCS301, from Microchip Technology Inc., is a code hopping encoder designed for secure Remote Keyless Entry (RKE) systems. The HCS301 utilizes the KEELOQ code hopping technology, which incorporates high security, a small package outline, and low cost, to make this device a perfect solution for unidirectional remote keyless entry systems and access control systems.

PACKAGE TYPES

PDIP, SOIC



HCS301 BLOCK DIAGRAM



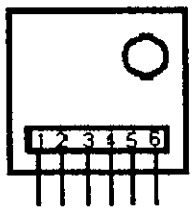
The HCS301 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and six status bits to create a 66-bit transmission stream. The length of the transmission eliminates the threat of code scanning and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend (code grabbing) schemes useless.

The 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.

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

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

WIRELESS TRANSMITTER MODULE
FT-COM-TX2 - 433.92MHZ



PIN DETAILS

PIN 1	RF OUT
PIN 2	Vcc
PIN 3	GND
PIN 4	GND
PIN 5	DATA IN
PIN 6	GND

DIMENSION:-

Dimension of Transmitter Module FT-COM-TX2:- 26mm*27mm

FEATURES:

- Complete RF solution
- No external components required (except antenna).
  Easy integration and no production tuning
- High performance SAW based architecture
  150 feet range (for 102 dBm receiver sensitivity with ¼ wave with antenna)
  4800 bps max. data rate
- Direct interface
  Logic level I/O, interface directly to microprocessors
  encoder/decoder and rolling code chips.
- Ultra low power consumption
  Low voltage capacity and minimal power consumption are
  ideally suited for battery operated devices.

APPLICATIONS :

- Wireless Remote control systems.
- Keyless entry for cars and automobiles.
- Home security systems.
- Wireless Gate and Garage door openers.
- Lighting control.
- Personal Assistance / Paging Devices.
- Remote status / position sensing.
- Access Control Systems (RFID).
- Wireless serial data transmission.