MCS3122

MCS3122 Advanced KEELOQ® Technology Encoder Data Sheet

Features Overview

- Advanced KEELOQ® Technology:
  - Programmable 32-bit serial number
  - Programmable 32-bit serial number for seed transmissions
  - AES-128 block cipher
  - Programmable 128-bit crypt key
  - 160/192-bit transmission code length:
    - 32-bit unencrypted portion
    - 128-bit encrypted, code hopping portion
    - 32-bit authorization check (optional)
- Operating Features:
  - 2.0 to 3.7V operation
  - Three switch inputs
  - Seven functions available
  - One active-low $\overline{\text{LED}}$ drive
  - Configurable maximum code word
- RF:
  - Configurable bit rate
  - Configurable modulation, supporting FSK and OOK
  - Configurable data modulation, supporting PWM and Manchester
- Other:
  - Button inputs have internal pull-up resistors

Typical Applications

MCS3122 is ideal for Remote Keyless Entry (RKE) applications. These applications include:

- Automotive RKE Systems
- Automotive Alarm Systems
- Gate and Garage Door Openers
- Home Security Systems
- Security and Safety Sensors
- Remote Control
- Remote Keypad
- Wireless Sensors

Package Type

- 14-Pin TSSOP

FIGURE 1: 14-PIN TSSOP

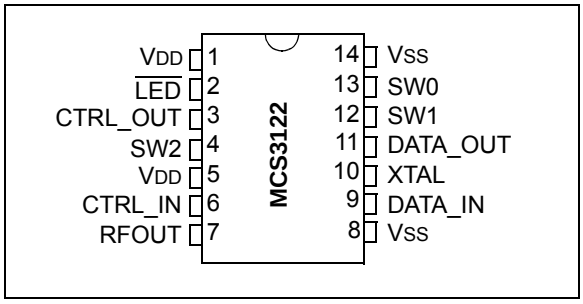


TABLE 1: PIN DESCRIPTION

Name	14-Pin TSSOP	Input Type	Output Type	Description
VDD	1	Power	—	Power
$\overline{\text{LED}}$	2	—	TTL	LED Output (active-low)
CTRL_OUT	3	—	TTL	Transmitter Clock
SW2	4	TTL	—	Switch 2 Input
VDD	5	Power	—	Power
CTRL_IN	6	TTL	—	Transmitter Clock
RFOUT	7	—	RF	Transmitter Output
VSS	8	Power	—	Power
DATA_IN	9	TTL	—	Transmitter Data
XTAL	10	Analog	—	Transmitter Reference Oscillator
DATA_OUT	11	—	TTL	Transmitter Data
SW1	12	TTL	—	Switch 1 Input
SW0	13	TTL	—	Switch 0 Input
VSS	14	Power	—	Power

© 2014 Microchip Technology Inc.

Table of Contents

1.0 General Description 3
2.0 Device Description 4
3.0 Memory Organization 5
4.0 Advanced KEELOQ® Technology Operation 9
5.0 Transmitter Operation 12
6.0 Integrating MCS3122 into a System 15
7.0 Electrical Specifications 17
8.0 Packaging Information 18
The Microchip Web Site 23
Customer Change Notification Service 23
Customer Support 23
Product Identification System 24

TO OUR VALUED CUSTOMERS

It is our intention to provide our valued customers with the best documentation possible to ensure successful use of your Microchip products. To this end, we will continue to improve our publications to better suit your needs. Our publications will be refined and enhanced as new volumes and updates are introduced.

If you have any questions or comments regarding this publication, please contact the Marketing Communications Department via E-mail at **docerrors@microchip.com**. We welcome your feedback.

Most Current Data Sheet

To obtain the most up-to-date version of this data sheet, please register at our Worldwide Web site at:

http://www.microchip.com

You can determine the version of a data sheet by examining its literature number found on the bottom outside corner of any page. The last character of the literature number is the version number, (e.g., DS30000000A is version A of document DS30000000).

Errata

An errata sheet, describing minor operational differences from the data sheet and recommended workarounds, may exist for current devices. As device/documentation issues become known to us, we will publish an errata sheet. The errata will specify the revision of silicon and revision of document to which it applies.

To determine if an errata sheet exists for a particular device, please check with one of the following:

- Microchip's Worldwide Web site; **http://www.microchip.com**
- Your local Microchip sales office (see last page)

When contacting a sales office, please specify which device, revision of silicon and data sheet (include literature number) you are using.

Customer Notification System

Register on our web site at **www.microchip.com** to receive the most current information on all of our products.

© 2014 Microchip Technology Inc.

1.0 GENERAL DESCRIPTION

MCS3122 is a KEELOQ encoder, designed for secure Remote Keyless Entry (RKE) and secure remote control systems. MCS3122 utilizes the Advanced KEELOQ code hopping technology. The encoder incorporates a high- security, low-cost small package outline to make this device the perfect solution for unidirectional authentication systems and access control systems.

The Advanced KEELOQ technology uses the industry standard AES-128 encryption algorithm, a serial number and a message counter which continuously increments with each button press.

The crypt key, serial number and configuration data are stored in a Flash array which is not accessible via any external connection. The Flash data is programmable but read-protected. The data can be verified only after an automatic erase and programming operation. This protects against attempts to gain access to keys or manipulate synchronization values. In addition, MCS3122 provides an easy to use serial interface for programming the necessary keys, system parameters and configuration data.

1.1 Key Terms

The following is a list of key terms used throughout this data sheet. For additional information on KEELOQ technology and code hopping, refer to "*An Introduction to KEELOQ® Code Hopping*" Technical Brief (DS91002).

- **RKE**: Remote Keyless Entry
- **Function Code**: It indicates what button input(s) activated the transmission. It encompasses the function code bits.
- **Code Hopping**: A method by which a code, viewed externally to the system, appears to change unpredictably each time it is transmitted.
- **Code Word**: A block of data that is repeatedly transmitted upon button activation.
- **Transmission**: A data stream consisting of repeating code words.
- **Crypt Key**: A unique and secret number (128-bit for Advanced KEELOQ technology) used to encrypt and decrypt data. In a symmetrical block cipher such as those used on MCS3122, the encryption and decryption keys are equal and, therefore, will generally be referred to as the crypt key.
- **Encoder**: A device that generates and encodes data.
- **Encryption Algorithm**: A method whereby data is scrambled using a crypt key. The data can only be interpreted by the respective decryption algorithm using the same crypt key.
- **Decoder**: A device that decodes data received from an encoder.
- **Decryption Algorithm**: A recipe whereby data, scrambled by an encryption algorithm, can be unscrambled using the same crypt key.
- **Learn**: Learning involves the receiver calculating the transmitter's appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter or timer value, and crypt key in EEPROM. The KEELOQ technology product family facilitates several learning strategies to be implemented on the decoder. The following are examples of what can be done:
  - **Simple Learning**: The receiver uses a fixed crypt key. The crypt key is common to every component used by the same manufacturer.
  - **Normal Learning**: The receiver derives a crypt key from the encoder serial number. Every transmitter has a unique crypt key.
  - **Secure Learning**: The receiver derives a crypt key from the encoder seed value. Every encoder has a unique seed value that is only transmitted by a special button combination.
- **Manufacturer's Code**: A unique and secret number (128-bit for Advanced KEELOQ technology) used to derive crypt keys. Each encoder is programmed with a crypt key that is a function of the manufacturer's code. Each decoder is programmed with the manufacturer's code itself.

The MCS3122 code hopping encoder is designed specifically for keyless entry systems. Typical applications include vehicles and home garage door openers. The encoder portion of a keyless entry system is integrated into a transmitter carried by the user. The transmitter is operated to gain access to a vehicle or a restricted area. MCS3122 is meant to be a cost-effective, yet secure solution to such systems, requiring very few external components (see Figure 2-1).

Most low-end keyless entry transmitters are given a fixed identification code that is transmitted every time a button is pushed. The number of unique identification codes in a low-end system is usually a relatively small number. These shortcomings provide an opportunity for a sophisticated thief to create a device that 'grabs' a transmission and retransmits it later, or a device that quickly 'scans' all possible identification codes until the correct one is found.

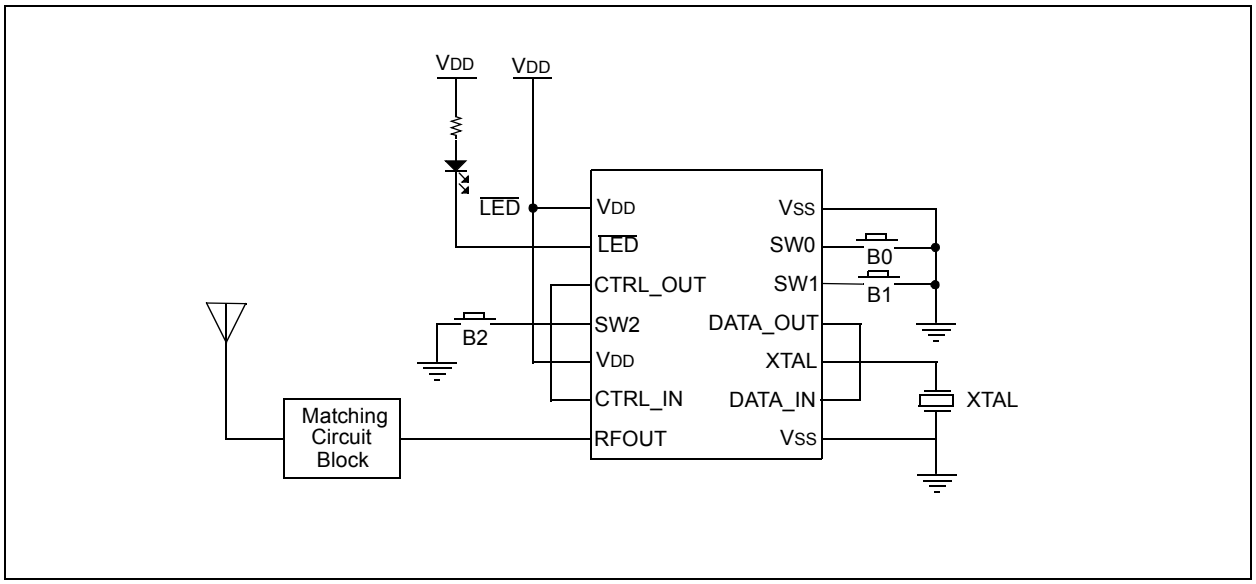
Advanced KEELOQ technology uses the industry standard AES-128 encryption algorithm to obscure data using 128 bits for both its block and key length. In addition to the security of Advanced KEELOQ technology, the encoder sends a message authorization block which is used to separate the message encryption from the message authentication.

© 2014 Microchip Technology Inc.

2.0 DEVICE DESCRIPTION

As shown in the typical application circuit (Figure 2-1), MCS3122 is a simple device to use. It requires only the addition of up to three buttons, a transmitter reference oscillator, and RF circuitry for use as the transmitter in the security application. See Table 1 for a description of each pin.

FIGURE 2-1: TYPICAL CIRCUIT



© 2014 Microchip Technology Inc.

3.0 MEMORY ORGANIZATION

MCS3122 has 64 bytes of configuration data. In general, the Configuration bytes can be divided into two categories: those options related to the Advanced KEELOQ technology encoder and those related to the transmitter and device operation.

TABLE 3-1: CONFIGURATION REGISTERS

Address	Size (Bytes)	Description
0x00-0x02	3	Synchronization Counter, Copy A
0x03	1	Synchronization Counter Checksum
0x04-0x07	4	Reserved (set to 0xFF)
0x08-0x0A	3	Synchronization Counter, Copy B
0x0B	1	Reserved (set to 0xFF)
0x0C-0x0F	4	Seed Transmission Serial Number (usually set to 0xFFFFFFFF)
0x10-0x1F	16	Encryption Key
0x20-0x2F	16	Authorization Key
0x30-0x33	4	Serial Number
0x34-0x35	2	Transmitter Settings
0x36-0x37	2	Reserved (set to 0xFF)
0x38-0x3F	8	Seed Value

3.1 Counter and Protection

The synchronization counter is read, checked for integrity, updated (incremented) and saved back to Flash during normal operation of the device. The special operation prevents against data loss from unexpected power loss. An 8-bit checksum is calculated and stored alongside the synchronization counter. The checksum is calculated as a two's complement checksum. If there is a mismatch, the second copy of the synchronization counter is read instead. Example 3-1 illustrates how to compute this value.

EXAMPLE 3-1: CHECKSUM CALCULATION

```
static uint8_t crc(const uint8_t* buffer, size_t len){
     uint8_t bitcount;
     uint8_t checksum = 0xFF;

     while(len--)
     {
         c = c + *buffer++;

     }
     return 0-c;
}
```

3.2 Configuration Byte Details

The following tables describe Configuration bytes in detail.

TABLE 3-2: ADVANCED KEELOQ® TECHNOLOGY SYNCHRONIZATION REGISTERS, COPY A

Byte Address	Bit	Description	Values
0x00	7:0	Synchronization Counter, Copy A	Byte 0 of the synchronization counter (LSB)
0x01	7:0		Byte 1 of the synchronization counter
0x02	7:0		Byte 2 of the synchronization counter (MSB)
0x03	7:0	Checksum	Checksum of the synchronization counter

TABLE 3-3: ADVANCED KEELOQ® TECHNOLOGY SYNCHRONIZATION REGISTERS, COPY B

Byte Address	Bit	Description	Values
0x08	7:0	Synchronization Counter, Copy B	Byte 0 of the synchronization counter (LSB)
0x09	7:0		Byte 1 of the synchronization counter
0x0A	7:0		Byte 2 of the synchronization counter (MSB)

TABLE 3-4: ADVANCED KEELOQ® TECHNOLOGY SEED SERIAL NUMBER REGISTERS

Byte Address	Bit	Description	Values
0x0C	7:0	Seed Serial Number	Byte 0 of the seed serial number (LSB)
0x0D	7:0		Byte 1 of the seed serial number
0x0E	7:0		Byte 2 of the seed serial number
0x0F	7:0		Byte 3 of the seed serial number (MSB)

TABLE 3-5: ADVANCED KEELOQ® TECHNOLOGY CRYPT KEY REGISTERS

Byte Address	Bit	Description	Values
0x10	7:0	Crypt Key	Byte 0 of the crypt key (LSB)
0x11	7:0		Byte 1 of the crypt key
0x12	7:0		Byte 2 of the crypt key
0x13	7:0		Byte 3 of the crypt key
0x14	7:0		Byte 4 of the crypt key
0x15	7:0		Byte 5 of the crypt key
0x16	7:0		Byte 6 of the crypt key
0x17	7:0		Byte 7 of the crypt key
0x18	7:0		Byte 8 of the crypt key
0x19	7:0		Byte 9 of the crypt key
0x1A	7:0		Byte 10 of the crypt key
0x1B	7:0		Byte 11 of the crypt key
0x1C	7:0		Byte 12 of the crypt key
0x1D	7:0		Byte 13 of the crypt key
0x1E	7:0		Byte 14 of the crypt key
0x1F	7:0		Byte 15 of the crypt key (MSB)

© 2014 Microchip Technology Inc.

TABLE 3-6: ADVANCED KEELOQ® TECHNOLOGY AUTHORIZATION KEY REGISTERS

Byte Address	Bit	Description	Values
0x20	7:0	Authorization Key	Byte 0 of the authorization key (LSB)
0x21	7:0		Byte 1 of the authorization key
0x22	7:0		Byte 2 of the authorization key
0x23	7:0		Byte 3 of the authorization key
0x24	7:0		Byte 4 of the authorization key
0x25	7:0		Byte 5 of the authorization key
0x26	7:0		Byte 6 of the authorization key
0x27	7:0		Byte 7 of the authorization key
0x28	7:0		Byte 8 of the authorization key
0x29	7:0		Byte 9 of the authorization key
0x2A	7:0		Byte 10 of the authorization key
0x2B	7:0		Byte 11 of the authorization key
0x2C	7:0		Byte 12 of the authorization key
0x2D	7:0		Byte 13 of the authorization key
0x2E	7:0		Byte 14 of the authorization key
0x2F	7:0		Byte 15 of the authorization key (MSB)

TABLE 3-7: ADVANCED KEELOQ® TECHNOLOGY SERIAL NUMBER REGISTERS

Byte Address	Bit	Description	Values
0x30	7:0	Serial Number	Byte 0 of the serial number (LSB)
0x31	7:0		Byte 1 of the serial number
0x32	7:0		Byte 2 of the serial number
0x33	7:0		Byte 3 of the serial number (MSB)

TABLE 3-8: TRANSMITTER CONFIGURATION REGISTERS

Byte Address	Bit	Description	Values
0x34	7:6	FSK Frequency Deviation	11 – 200 kHz 10 – 100 kHz 01 – 75 kHz 10 – 50 kHz
	5	Output Power	0 – 0 dBm 1 – 10 dBm
	4	Encoding	1 – PWM 0 – Manchester
	3	Modulation	1 – OOK 0 – FSK
	2:0	Frequency Select	000 – 315.00 MHz (only with 24 MHz crystal) 001 – 390.00 MHz 010 – 418.00 MHz 011 – 433.92 MHz 100 – 868.30 MHz 101 – 868.65 MHz 110 – 868.95 MHz 111 – 915.00 MHz
0x35	3 and 1:0	Seed Button Configuration	111 – Disabled, no seed option 110 – SW0 101 – SW1 100 – SW1 and SW0 011 – SW2 010 – SW2 and SW0 001 – SW2 and SW1 000 – SW3, SW2 and SW1
	2	Authorization Code Enable	1 – Enabled 0 – Disabled
	5:4	Baud Rate	11 – 200 µS 10 – 150 µS 11 – 100 µS 11 – 50 µS
	7:6	Maximum Code Words	11 – 234 words 10 – 80 words 01 – 4 words 00 – No maximum limit

TABLE 3-9: ADVANCED KEELOQ® TECHNOLOGY SEED CONFIGURATION REGISTERS

Byte Address	Bit	Description	Values
0x38	7:0	Seed Value	Byte 0 of the seed value (LSB)
0x39	7:0		Byte 1 of the seed value
0x3A	7:0		Byte 2 of the seed value
0x3B	7:0		Byte 3 of the seed value
0x3C	7:0		Byte 4 of the seed value
0x3D	7:0		Byte 5 of the seed value
0x3E	7:0		Byte 6 of the seed value
0x3F	7:0		Byte 7 of the seed value (MSB)

© 2014 Microchip Technology Inc.

4.0 ADVANCED KEELOQ® TECHNOLOGY OPERATION

4.1 Synchronization Counter

This is the 24-bit synchronization value that is used to create the hopping code for transmission. This value will be incremented after every transmission. The initial value of the synchronization counter may be set via the Synchronization Counter Initial Value registers (see Table 3-2 and Table 3-3).

4.2 Function Code (Button Status Code)

The function code is a bitmapped representation of the state of each button on the transmitter. States are active-high.

TABLE 4-1: ADVANCED KEELOQ® BUTTON CODE TRANSLATION

Button	Function Code
SW0	xx1
SW1	x1x
SW2	1xx

4.3 Serial Number

Each Advanced KEELOQ encoder transmits its 32-bit serial number with each transmission. It is intended that this serial number be unique to a system. It is set in the Serial Number Configuration registers, listed in Table 3-7.

4.4 Seed Code Serial Number

The transmitter has the possibility to set the serial number which will be transmitted with a seed transmission. In a typical system, this serial number is transmitted as 0xFFFFFFFF; however, the user can configure this according to the actual application. The seed code serial number is set in the Seed Code Configuration registers, listed in Table 3-4.

© 2014 Microchip Technology Inc.

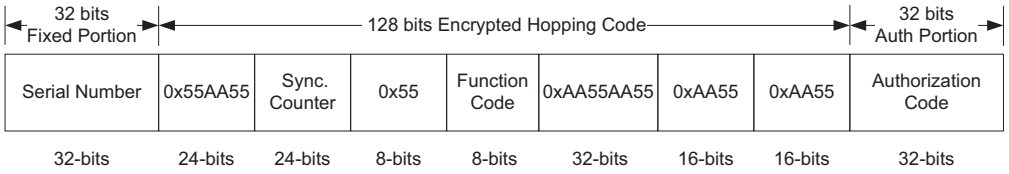
4.5 Code Word Format

The Advanced KEELOQ code word is either 160 or 192-bit long. It comprises three sections (see Figure 4-1):

- 32 Bits of the Encoder's Serial Number
- 128 Bits of the Encrypted Hopping Code
- 32 Bits of the Authorization Code (optional)

These segments are described in detail in the following sections.

FIGURE 4-1: ADVANCED KEELOQ® CODE WORD FORMAT



Note: The data is sent LSB first (in this figure from right to left).

4.5.1 FIXED CODE PORTION

The fixed code portion consists of 32 bits of the serial number.

4.5.2 HOPPING CODE PORTION

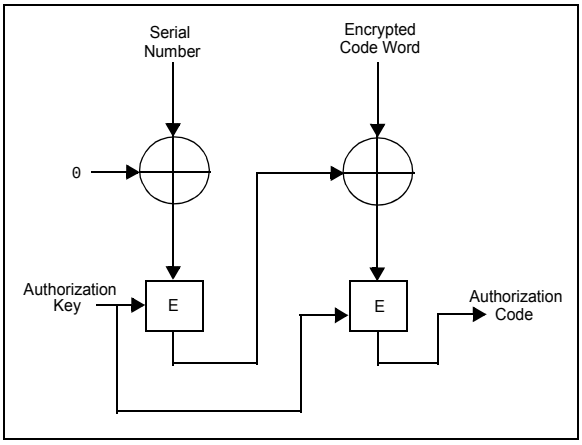
The hopping code portion is calculated by encrypting the synchronization counter and function code with the encoder key. The hopping code is calculated when a button press is registered.

4.5.3 AUTHORIZATION CODE PORTION

The authorization code is a cryptographically-strong industry standard representation of the code word suitable for authentication and integrity verification. It is generated by using the on-board AES encryption algorithm in CBC-MAC mode. The calculation takes place over the entire code word, including the encrypted and unencrypted portions, using the authorization key as input. Figure 4-2 shows a representation of how this calculation is performed. This calculation is truncated to its Least Significant 32 bits for transmission.

The authorization code requires a shared secret called the authorization key. This key is set in the Authorization Key Configuration register, listed in Table 3-6.

FIGURE 4-2: AUTHORIZATION CODE CALCULATION



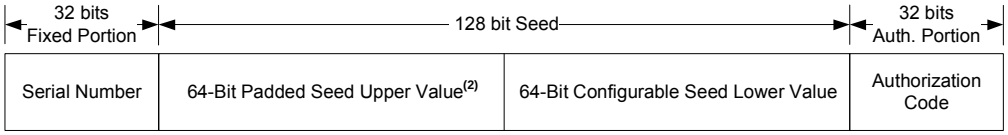
The authorization code portion consists of the 32-bit Least Significant bits of the authorization code.

© 2014 Microchip Technology Inc.

4.5.4 SEED WORD FORMAT

The seed word is used when pairing the transmitter to a receiver using a secure learn methodology. The seed code word format is shown is Figure 4-3. While the MCS3122 Flash data contains user-configurable 64-bit seed data, the encoder will send 128-bit seed code. The 128-bit seed code is constructed using the user-configured seed code for the lower 64 bits of the seed. The upper 64 bits are added by MCS3122 as 8 bytes with a 0x12 value.

FIGURE 4-3: ADVANCED KEELOQ® SEED WORD FORMAT(1)



Note 1: MCS3122 can set a different serial number for the seed packet. This is typically set to 0xFFFFFFFF.

2: The padded value is 0x1212121212121212.

3: The data is sent LSB first (in this figure from right to left.

5.0 TRANSMITTER OPERATION

5.1 Data Modulation Format and Baud Rate

A transmission is made up of several code words. Each code word contains a preamble, header and data. A code word is separated from another code word by guard time.

All timing specifications for the modulation formats are based on a basic Time Element, described as TE. See **Section 5.2 "Baud Rate"** for details on baud rate calculation. This timing element can be set to a wide range of values. The length of the preamble, header and guard is fixed. The guard time is fixed to a typical 18.5 ms.

FIGURE 5-1: PWM TRANSMISSION FORMAT

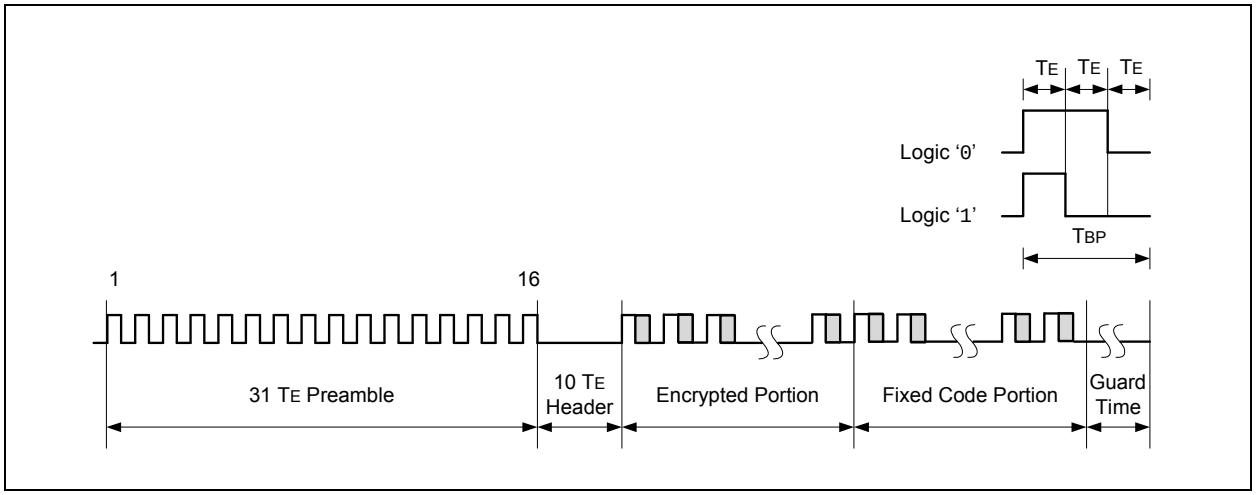
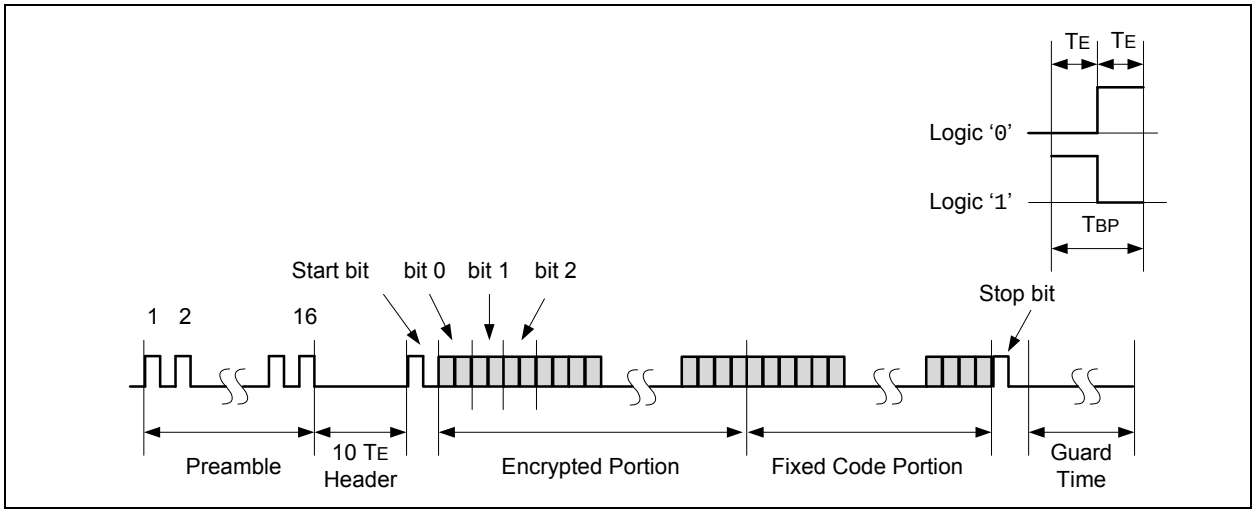


FIGURE 5-2: MANCHESTER TRANSMISSION FORMAT



© 2014 Microchip Technology Inc.

5.2 Baud Rate

The baud rate of an encoder's transmission is highly configurable using the two bits in the Transmitter Setting Byte 1 register (0x35).

TABLE 5-1: BAUD RATE SELECTION OPTIONS

T_E (µS)	Bits <5:4>
200	1:1
150	1:4
100	1:4
50	1:16

5.3 Transmission Modulation Format

The RF transmission can be configured to modulate using Frequency-Shift Keying (FSK) or On-Off Keying (OOK). The selection is done using one bit in the Transmitter Settings Byte 0 register (0x34).

TABLE 5-2: MODULATION FORMAT SELECTION OPTIONS

Modulation	Bit <3>
FSK	0
OOK	1

5.4 Frequency and Band Selection

The RF frequency configuration is performed by selecting the appropriate bits in the Transmitter Settings Byte 0 register (0x34).

TABLE 5-3: FREQUENCY SELECTION OPTIONS

Frequency	Bits <2:0>
315.00 MHz(1)	000
390.00 MHz	001
418.00 MHz	010
433.92 MHz	011
868.30 MHz	100
868.65 MHz	101
868.90 MHz	110
915.00 MHz	111

Note 1: For 315.00 MHz operation, a 24 MHz crystal is required. All the other frequency settings will require a 26 MHz crystal.

5.5 Deviation Selection

When using FSK modulation, the frequency deviation can be configured using bits <7:6> in the Transmitter Settings Byte 0 register (0x34).

TABLE 5-4: FREQUENCY DEVIATION SELECTION OPTIONS

Deviation	Bits <7:6>
200 kHz	11
100 kHz	10
75 kHz	01
50 kHz	00

5.6 Power Output

The RF output power can be configured to either 0 dBm or 10 dBm. The setting is done using bit <5> in the Transmitter Settings Byte 0 register (0x34).

TABLE 5-5: OUTPUT POWER SELECTION OPTIONS

Out Power	Bit <5>
0 dBm	0
10 dBm	1

5.7 Crystal Selection

Once the frequency band has been selected, the choice of crystal frequency is flexible provided the crystal meets the specifications summarized in Table 5-6, the boundaries of the Encoder Frequency Configuration value are followed and the RF transmit frequency error is acceptable to the system design.

TABLE 5-6: CRYSTAL RESONATOR SPECIFICATIONS

Symbol	Description	Min.	Typ.	Max.	Unit
f_{REF}	Crystal Frequency	—	26 or 24(1)	—	MHz
C_L	Load Capacitance	—	15	—	pF
ESR	Equivalent Series Resistance	—	—	100	Ω

Note 1: When selecting the 315.000 MHz frequency, a 24 MHz crystal is required.

5.8 Seed Button Configuration

The MCS3122 allows the user to select which button combination will output the seed transmission instead of the normal data packet. Table 5-7 lists all the possible button combinations.

TABLE 5-7: SEED BUTTON CONFIGURATION OPTIONS

SW2	SW1	SW0	Bit Settings <3> and <1:0>
Closed	Closed	Closed	000
Closed	Closed	Open	001
Closed	Open	Closed	010
Closed	Open	Open	011
Open	Closed	Closed	100
Open	Closed	Open	101
Open	Open	Closed	110
Open	Open	Open	111(1)

Note 1: The button combination corresponding to the setting '111' will not generate a seed combination since it corresponds to all buttons not pressed. Setting the bits to this value will disable the seed packet sending (i.e., no button combination will send a seed code).

5.9 Code Word Completion

MCS3122 always ensures that a full and complete code word is transmitted even if all buttons are released before transmission is complete.

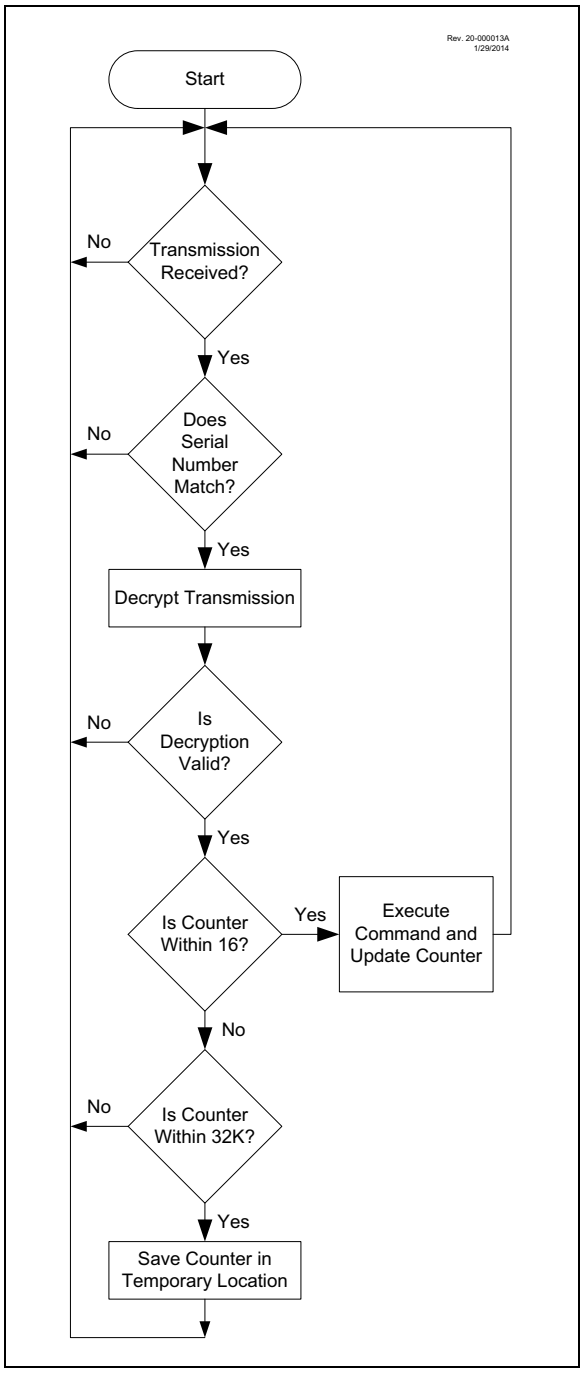
5.10 Maximum Code Words

This feature sets a maximum number of code words transmitted by a button configuration. If a button is kept pressed, the maximum allowed code words will be transmitted. If a new button is pressed or a new button press combination is used, the process will be restarted and the maximum number of words will be transmitted.

© 2014 Microchip Technology Inc.

6.0 INTEGRATING MCS3122 INTO A SYSTEM

FIGURE 6-1: TYPICAL DECODER OPERATION



6.1 Decoder Operation

The decoder waits until a transmission is received. The received serial number is compared to the EEPROM table of learned transmitters to first determine if this transmitter's use is allowed in the system. If from a paired transmitter, the transmission is decrypted using the stored crypt key and authenticated via the Discrimination bits for appropriate crypt key usage. If the decryption is valid, the synchronization value is evaluated (see Figure 6-1).

6.2 Synchronization with a Decoder

Note:	The synchronization method described in this section is an exemplar method. It may be altered to fit the needs and capabilities of a particular system.

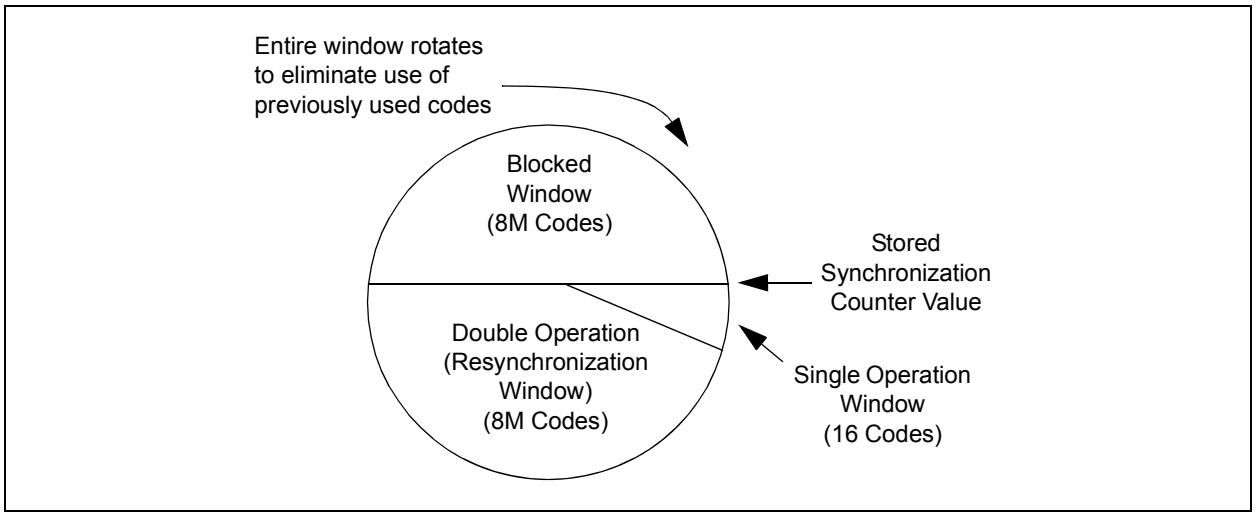
The KEELOQ technology includes a sophisticated synchronization technique that does not require the calculation and storage of future codes. The technique securely blocks invalid transmission while providing transparent resynchronization to transmitters inadvertently activated away from the receiver.

Figure 6-2 shows a three-partition, rotating Synchronization window. The size of each window is optional but the technique is fundamental. Each time a transmission is authenticated, the intended function is executed and the transmission's synchronization counter value is stored in EEPROM. From the currently stored counter value there is an initial Single Operation Forward window of 16 codes. If the difference between a received synchronization counter and the last stored counter is within 16, the intended function will be executed on a single button press and the new synchronization counter will be stored. Storing the new synchronization counter value effectively rotates the entire Synchronization window.

A Double Operation (Resynchronization) window further exists from the Single Operation window up to 8M code forward of the currently stored counter value. It is referred to as Double Operation because a transmission with a synchronization counter in this window will require an additional, sequential counter transmission prior to executing the intended function. Upon receiving the sequential transmission the decoder executes the intended function and stores the synchronization counter value. This resynchronization occurs transparently to the user, as it is human nature to press the button a second time if the first was unsuccessful.

The third window is a Blocked window ranging from the Double Operation window to the currently stored synchronization counter value. Any transmission with synchronization counter value within this window will be ignored. This window excludes previously used code-grabbed transmissions from accessing the system.

FIGURE 6-2: SYNCHRONIZATION WINDOW



6.3 Security Considerations

The strength of this security is based on keeping a secret inside the transmitter that can be verified by encrypted transmissions to a trained receiver. The transmitter's secret is the manufacturer's key, not the encryption algorithm. If that key is compromised, then a smart transceiver can capture any serial number, create a valid code word and trick all receivers trained with that serial number. The key cannot be read from the EEPROM without costly die probing, but it can be calculated by brute force decryption attacks on transmitted code words. The cost for these attacks should exceed what the manufacturer would want to protect.

To protect the security of other receivers with the same manufacturer's code, the manufacturer should use the random seed for secure learn. It is a second secret that is unique for each transmitter. If a manufacturer's key is compromised, clone transmitters can be created, but without the unique seed, they have to be relearned by the receiver. In the same way, if the transmissions are decrypted by brute force on a computer, the random seed hides the manufacturer's key and prevents more than one transmitter from being compromised.

The length of the code word at these baud rates make brute force attacks that guess the hopping code take years. To make the receiver less susceptible to this attack, it should test *all* bits in the decrypted code for the correct value, not just the low counter bits and function code.

The main benefit of hopping codes is to prevent the retransmission of captured code words. This works very well for code words which the receiver decodes. Its weakness is that, if a code is captured when the receiver misses it, the code may trick the receiver once if it is used before the next valid transmission. The receiver should increment the counter on questionable code word receptions. The transmitter should use separate buttons for lock and unlock functions. A different method would be to require two different buttons in sequence to gain access.

There are more ways to make KEELOQ systems more secure, but they all have trade-offs. The user should find a balance between security, design effort and usability, particularly in failure modes. For example, if a button sticks or kids play with it, the counter should not advance into the Blocked Code window, rendering the transmitter useless or requiring retraining.

© 2014 Microchip Technology Inc.

7.0 ELECTRICAL SPECIFICATIONS

7.1 Absolute Maximum Ratings(†)

Ambient temperature under bias ..... -40°C to +85°C
Storage temperature ..... -55°C to +150°C
Voltage on pins with respect to V_{SS}
on V_{DD} pin 0-3.9V
on all other pins ..... -0.3V to (V_{DD} + 0.3V)
Maximum current
on any output pin ..... ±25 mA

† 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 above maximum rating conditions for extended periods may affect device reliability.

7.2 Standard Operating Conditions

The standard operating conditions for any device are defined as:

Operating Voltage: $V_{DDMIN} \le V_{DD} \le V_{DDMAX}$
Operating Temperature: $T_{A_MIN} \le T_A \le T_{A_MAX}$

V_{DD} — Operating Supply Voltage
V_{DDMIN} ..... +2.0V
V_{DDMAX} ..... +3.7V

T_A — Operating Ambient Temperature Range
T_{A_MIN} ..... -40°C
T_{A_MAX} ..... +85°C

I_{DD} — Supply Current
At 315 MHz, +10 dBm, FSK, typical(1) ..... +15 mA
At 315 MHz, +10 dBm, OOK, typical(1) ..... +11 mA
At 315 MHz, +0 dBm, FSK, typical(1) ..... +9 mA
At 915 MHz, +10 dBm, FSK, typical(1) ..... +17.5 mA
At 915 MHz, +0 dBm, FSK, typical(1) ..... +10.5 mA

I_{PD} — Standby Current
V_{DD} = 3V, typical(1) ..... +0.23 µA

V_{IH} — Input High Voltage, minimum ..... 0.25 V_{DD} + 0.8V

V_{IL} — Input Low Voltage, maximum ..... 0.15 V_{DD}

V_{OH} — Output High Voltage
I_{OH} = 3 mA, V_{DD} = 3.3V, minimum ..... V_{DD} – 0.7V

V_{OL} — Output Low Voltage
I_{OL} = 6 mA, V_{DD} = 3.3V, maximum ..... +0.6V

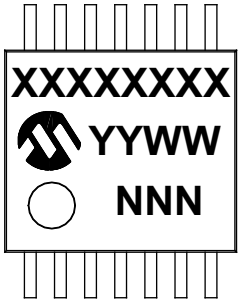
I_{LED} — $\overline{\text{LED}}$ Sink Current, maximum ..... +25 mA

Note 1: Typical values are at 25°C.

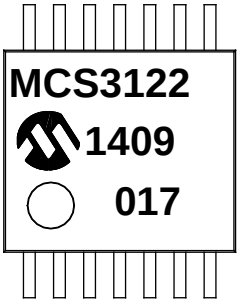
8.0 PACKAGING INFORMATION

8.1 Package Marking Information

14-Lead TSSOP (4.4 mm)



Example



Legend:	XX...X	Customer-specific information
	Y	Year code (last digit of calendar year)
	YY	Year code (last 2 digits of calendar year)
	WW	Week code (week of January 1 is week ‘01’)
	NNN	Alphanumeric traceability code
	(e3)	Pb-free JEDEC® designator for Matte Tin (Sn)
	*	This package is Pb-free. The Pb-free JEDEC designator ((e3)) can be found on the outer packaging for this package.

Note: In the event the full Microchip part number cannot be marked on one line, it will be carried over to the next line, thus limiting the number of available characters for customer-specific information.

***** Standard PIC® device marking consists of Microchip part number, year code, week code, and traceability code. For PIC device marking beyond this, certain price adders apply. Please check with your Microchip Sales Office. For QTP devices, any special marking adders are included in QTP price.

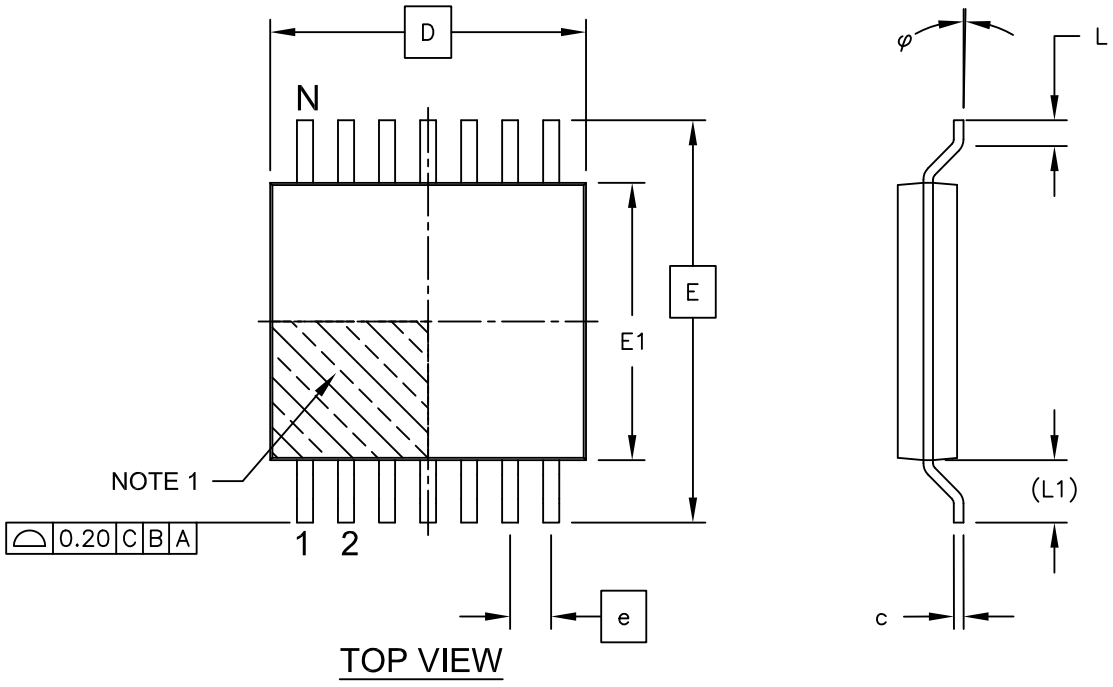
© 2014 Microchip Technology Inc.

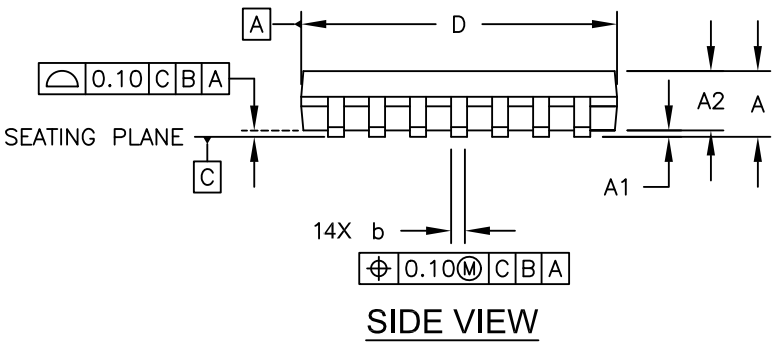
8.2 Package Details

The following sections give the technical details of the packages.

14-Lead Plastic Thin Shrink Small Outline (ST) - 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging

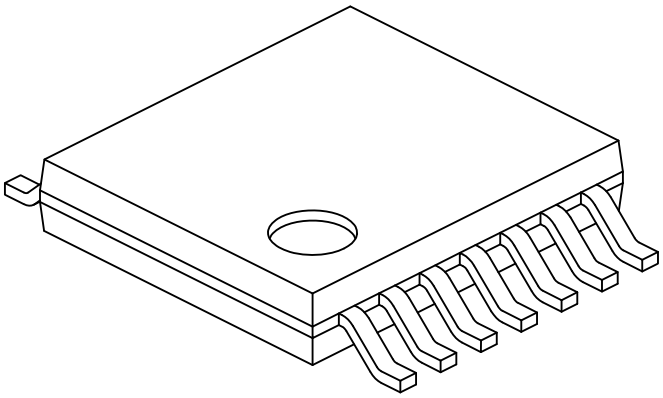




Microchip Technology Drawing C04-087C Sheet 1 of 2

14-Lead Plastic Thin Shrink Small Outline (ST) - 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		14	
Pitch	e		0.65 BSC	
Overall Height	A	-	-	1.20
Molded Package Thickness	A2	0.80	1.00	1.05
Standoff	A1	0.05	-	0.15
Overall Width	E		6.40 BSC	
Molded Package Width	E1	4.30	4.40	4.50
Molded Package Length	D	4.90	5.00	5.10
Foot Length	L	0.45	0.60	0.75
Footprint	(L1)		1.00 REF	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.09	-	0.20
Lead Width	b	0.19	-	0.30

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
3. Dimensioning and tolerancing per ASME Y14.5M

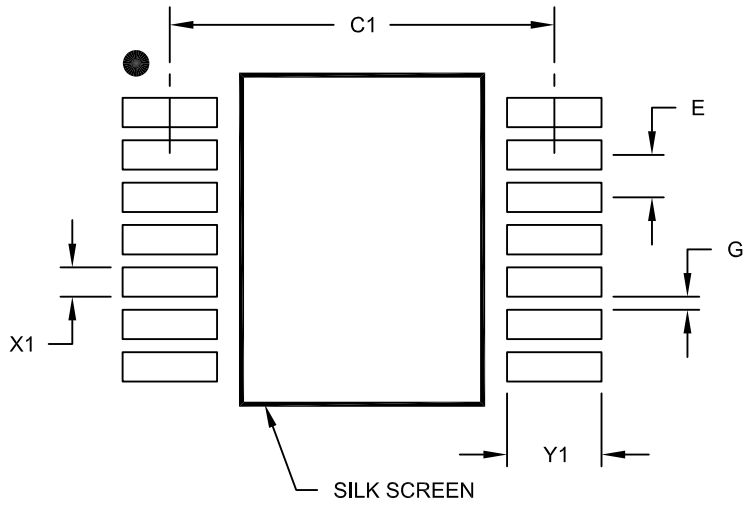
BSC: Basic Dimension. Theoretically exact value shown without tolerances.
REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing No. C04-087C Sheet 2 of 2

© 2014 Microchip Technology Inc.

14-Lead Plastic Thin Shrink Small Outline (ST) - 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.65 BSC	
Contact Pad Spacing	C1		5.90	
Contact Pad Width (X14)	X1			0.45
Contact Pad Length (X14)	Y1			1.45
Distance Between Pads	G	0.20		

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2087A

© 2014 Microchip Technology Inc.

APPENDIX A: REVISION HISTORY

Revision A (October 2014)

Initial release of this document.

© 2014 Microchip Technology Inc.

THE MICROCHIP WEB SITE

Microchip provides online support via our WWW site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://microchip.com/support.

PRODUCT IDENTIFICATION SYSTEM

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

PART NO.	[X](1)	-	X	/XX	XXX
Device	Tape and Reel Option		Temperature Range	Package	Pattern

Device:	MCS3122
Tape and Reel Option:	Blank = Standard packaging (tube or tray) T = Tape and Reel(1)
Temperature Range:	I = -40°C to +85°C (Industrial)
Package:(2)	ST = TSSOP
Pattern:	QTP, SQTP, Code or Special Requirements (blank otherwise)

Examples:

a) MCS3122 - I/ST
Industrial temperature,
TSSOP package

Note 1: Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.

2: For other small form-factor package availability and marking information, please visit www.microchip.com/packaging or contact your local sales office.

© 2014 Microchip Technology Inc.

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, FlashFlex, flexPWR, JukeBlox, KEELOQ, KEELOQ logo, Kleer, LANCheck, MediaLB, MOST, MOST logo, MPLAB, OptoLyzer, PIC, PICSTART, PIC^{32} logo, RightTouch, SpyNIC, SST, SST Logo, SuperFlash and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

The Embedded Control Solutions Company and mTouch are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, BodyCom, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, ECAN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, KleerNet, KleerNet logo, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, RightTouch logo, REAL ICE, SQI, Serial Quad I/O, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademarks of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2014, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 978-1-63276-724-0

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
═ ISO/TS 16949 ═

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110

Canada - Toronto
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2943-5100
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-8792-8115
Fax: 86-571-8792-8116

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Dusseldorf
Tel: 49-2129-3766400

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Pforzheim
Tel: 49-7231-424750

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Venice
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Poland - Warsaw
Tel: 48-22-3325737

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820

03/25/14

© 2014 Microchip Technology Inc.