MICROCHIP

AN1259

KEELOQ® Microcontroller-based Code Hopping Encoder

Author: *Enrique Aleman*
Microchip Technology Inc.

INTRODUCTION

This application note describes the design of a Microcontroller-based KEELOQ® Hopping Encoder. This encoder is implemented on Microchip PIC16F636 microcontroller. A description of the encoding process, the encoding hardware and description of the software modules are included within this application note. The software was designed to emulate an HCS365 dual encoder. As it is, this design can be used to implement a secure system transmitter that will have the flexibility to be designed into various types of KEELOQ receiver/ decoders.

The software used in this implementation makes use of the PIC16F636 internal encryption engine to generate the hopping codes required for transmission.

TRANSMITTER OVERVIEW

As this is an emulation of the HCS365, the transmitter has the following key features:

Security:

- Two programmable 32-bit serial numbers
- Two programmable 64-bit encryption keys
- Two programmable 60-bit seed values
- Each transmitter is unique
- 67/69-bit transmission code length
- 32-bit hopping code

Operation:

- 2.0-5.5V operation
- Four button inputs
- 15 functions available
- Four selectable baud rates
- Selectable minimum code word completion
- Battery low signal transmitted to receiver
- Nonvolatile synchronization data
- PWM, VPWM, PPM, and Manchester modulation
- Button queue information transmitted
- Dual Encoder functionality

DUAL ENCODER OPERATION

This firmware contains two transmitter configurations with separate serial numbers, encoder keys, discrimination values, counters and seed values. This means that the transmitter can be used as two independent systems. The SHIFT(S3) input pin is used to select between encoder configurations. A low on this pin will select Encoder 1, and a high will select Encoder 2.

FUNCTIONAL INPUTS AND OUTPUTS

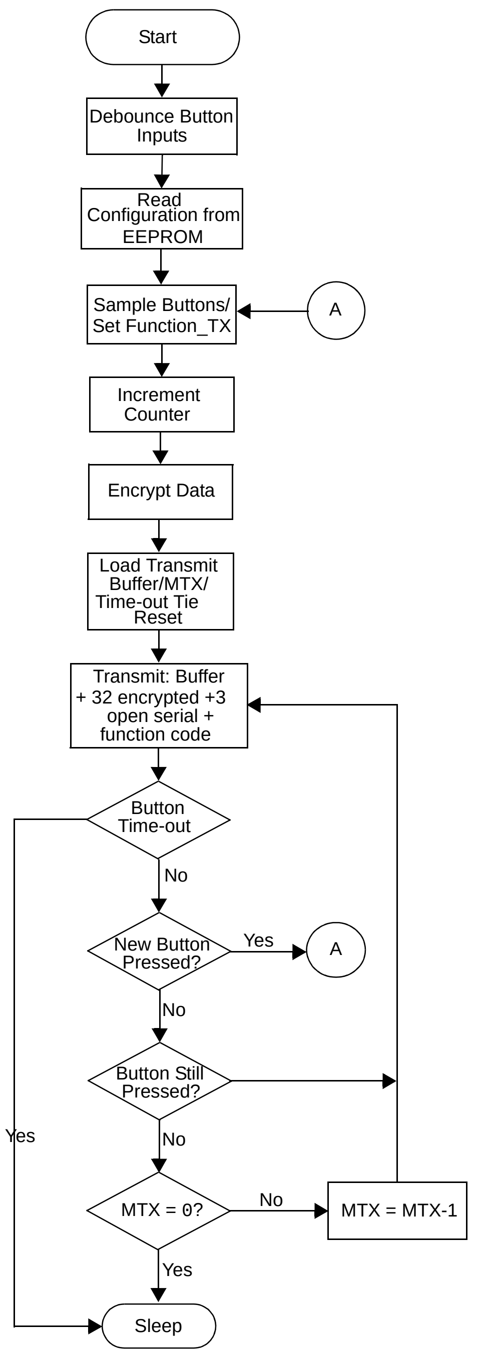
The software implementation makes use of the following pin designations:

TABLE 1: FUNCTIONAL INPUTS AND OUTPUTS

Label	Pin Number	Input/Output	Function
S0	2 (RA5)	Input	Switch Input S0
S1	3 (RA4)	Input	Switch input S1
S2	4 (RA3)	Input	Switch Input S2
S3	5 (RA2)	Input	Switch Input S3
RF_OUT	6 (RA1)	Output	Encoded transmitter signal output
LED	7(RA0)	Output	LED On/Off

OPERATION FLOW DIAGRAM

FIGURE 1: OPERATION FLOW DIAGRAM



SAMPLE BUTTONS/WAKE-UP

Upon power-up, the transmitter verifies the state of the buttons inputs and determines if a button is pressed. If no button pressed is detected, the transmitter will go to Sleep mode. The transmitter will wake up whenever a button is pressed. Wake-up is achieved by configuring the input port to generate an interrupt-on-change. After the wake event, the input buttons are debounced for 20 ms to make a determination on which buttons have been pressed. The button input values are then placed in the transmission buffer, in the appropriate section.

LOAD SYSTEM CONFIGURATION

After waking up and debouncing the input switches, the firmware will read the system Configuration bytes. These Configuration bytes will determine what data and modulation format will be for the transmission.

All the system Configuration bytes are stored in the EEPROM. Below is the EEPROM mapping for the PIC16F636 transmitter showing the configuration and data bits stored.

TABLE 2: EEPROM MAPPING FOR THE PIC16F636 TRANSMITTER

Offset	Bits								
Bytes	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**MNEMONIC**
0x00	Sync Counter Transmitter #0, stored in Pseudo-Gray Code								EE_CNT0
0x01	Sync Counter Transmitter #0, stored in Pseudo-Gray Code								
0x02	Sync Counter Transmitter #0, stored in Pseudo-Gray Code								
0x03	Sync Counter Transmitter #0 Checksum AB								
0x04	Sync Counter Transmitter #0 Checksum BC								
0x05	Sync Counter Transmitter #0 Checksum AC								
0x06	—								
0x07	—	—	—	—	—	—	—		EE_VLOWL
0x08	Sync Counter Transmitter #1, stored in Pseudo-Gray Code								EE_CNT1
0x09	Sync Counter Transmitter #1, stored in Pseudo-Gray Code								
0x0A	Sync Counter Transmitter #1, stored in Pseudo-Gray Code								
0x0B	Sync Counter Transmitter #1 Checksum AB								
0x0C	Sync Counter Transmitter #1 Checksum BC								
0x0D	Sync Counter Transmitter #1 Checksum AC								
0x0E	—								
0x0F	—	—	—	—	SD_FLG	—	TST_FLG		
0x10	32-BIT SERIAL NUMBER for TX#0 (MSB)								EE_SER
0x11	32-BIT SERIAL NUMBER for TX#0								
0x12	32-BIT SERIAL NUMBER for TX#0								
0x13	32-BIT SERIAL NUMBER for TX#0 (LSB)								
0x14	4-BIT SEED CODE TX#0				60-BIT SEED_0 VALUE (MS-NIBBLE)				EE_SEED
0x15	60-BIT SEED VALUE (MSB) for TX #0								
0x16	60-BIT SEED VALUE for TX #0								
0x17	60-BIT SEED VALUE for TX #0								
0x18	60-BIT SEED VALUE for TX #0								
0x19	60-BIT SEED VALUE for TX #0								
0x1A	60-BIT SEED VALUE for TX #0								
0x1B	60-BIT SEED VALUE (LSB) for TX #0								
0x1C	STRTSEL_0	QUEN_0	XSER_0	HEADER_0	TMOD_0		DISC_0 (MS-BITS)		EE_DISC
0x1D	DISC_0 (Lower 8 bits)								
0x1E	64-BIT KEY (MSB) for TX #0								EE_KEY
0x1F	64-BIT KEY for TX #0								
0x20	64-BIT KEY for TX #0								
0x21	64-BIT KEY for TX #0								
0x22	64-BIT KEY for TX #0								
0x23	64-BIT KEY for TX #0								
0x24	64-BIT KEY for TX #0								

TABLE 2: EEPROM MAPPING FOR THE PIC16F636 TRANSMITTER (CONTINUED)

0x25	64-BIT KEY-0 (LSB) for TX #0								
0x26	32-BIT SERIAL NUMBER for TX#1 (MSB)								B_EE_SER
0x27	32-BIT SERIAL NUMBER for TX#1								
0x28	32-BIT SERIAL NUMBER for TX#1								
0x29	32-BIT SERIAL NUMBER for TX#1 (LSB)								
0x2A	4-BIT SEED CODE TX#1				60-BIT SEED_1 VALUE (MS-NIBBLE)				B_EE_SEED
0x2B	60-BIT SEED VALUE (MSB) for TX#1								
0x2C	60-BIT SEED VALUE for TX#1								
0x2D	60-BIT SEED VALUE for TX#1								
0x2E	60-BIT SEED VALUE for TX#1								
0x2F	60-BIT SEED VALUE for TX#1								
0x30	60-BIT SEED VALUE for TX#1								
0x31	60-BIT SEED VALUE (LSB) for TX#1								
0x32	DISC_1 (MS-BITS)		STRTSEL_1	QUEN_1	XSER_1	HEADER_1	TMOD_1		B_EE_DISC
0x33	DISC_1 (Lower 8 bits)								
0x34	64-BIT KEY (MSB) for TX#1								B_EE_KEY
0x35	64-BIT KEY for TX#1								
0x36	64-BIT KEY for TX#1								
0x37	64-BIT KEY for TX#1								
0x38	64-BIT KEY for TX#1								
0x39	64-BIT KEY for TX#1								
0x3A	64-BIT KEY for TX#1								
0x3B	64-BIT KEY (LSB) for TX#1								
0x3C	GSEL_0		BSEL_0		SDTM_0		SDMD_0	SDLM_0	EE_CFG3
0x3D	LEDOS_1	LEDBL_1	TSEL		RFENO	INDESEL	MTX		EE_CFG2
0x3E	GSEL_1		BSEL_1		SDTM_1		SDMD_1	SDLM_1	EE_CFG1
0x3F	LEDOS_0	LEDBL_0	PLLSEL	VLOWSEL	VLOWL	CNTSEL	WAKE		EE_CFG0

CONFIGURATION WORDS DESCRIPTION

TABLE 3: TX0_CFG0 (FOR TRANSMITTER 0, FOR TRANSMITTER 1 USE TX1_CFG0)

BIT	Field	Description	Values
0	DISC:8	Upper two bits of Discrimination	Discrimination bits 9:8
1	DISC:9		
2	TMOD:0	Transmission Modulation Format	00 = PWM 01 = Manchester 10 = VPWM 11 = PPM
3	TMOD:1		
4	HEADER	Time Length of Transmission Header	0 = 4*Te 1 = 10*Te
5	XSER	Extended Serial Number Select	0 = 28 bits 1 = 32 bits
6	QUEN	Queue Counter Enable	0 = Disable 1 = Enable
7	STRTSEL	Start/Stop Pulse Enable	0 = Disable 1 = Enable

TABLE 4: TX0_CFG1 (FOR TRANSMITTER 0, FOR TRANSMITTER 1 USE TX1_CFG1)

BIT	Field	Description	Values
0	SDLM	Limited Seed Enable	0 = Disable 1 = Enable
1	SDMD	Seed Mode	0 = User 1 = Production
2	SDTM <3:2>	Time Before Seed Code Word	00 = 0.0 sec 01 = 0.8 sec 10 = 1.6 sec 11 = 3.2 sec
3			
4	BSEL <5:4>	Transmission Baud Rate Select	00 = 100 µs 01 = 200 µs 10 = 400 µs 11 = 800 µs
5			
6	GSEL <7:6>	Guard Time Select	00 = 0.0 ms 01 = 6.4 ms 10 = 51.2 ms 11 = 102.4 ms
7			

TABLE 5: SYSCFG0

BIT	Field	Description	Values
0	WAKE <1:0>	Wake-up	00 = No wake-up 01 = 75ms 50% 10 = 50ms 33% 11 = 100ms 16.6%
1			
2	CNTSEL	Counter Select	0 = 16 bits 1 = 20 bits
3	VLOWL	Low-Voltage Latch Enable	0 = Disable 1 = Enable
4	VLOWSEL	Low-Voltage Trip Level	0 = 2.2V 1 = 3.2V
5	PLLSEL	PLL interface Select	0 = ASK 1 = FSK
6	LEDBL_0	Low-Voltage LED Blink	0 = Continuous 1 = Once
7	LEDOS_0	LED On Time Select	0 = 50 ms 1 = 100 ms

TABLE 6: SYSCFG1

BIT	Field	Description	Values
0	MTX <1:0>	Maximum Code Words	00 = 1 01 = 2 10 = 4 11 = 8
1			
2	INDESEL	Dual Encoder Enable	0 = Disable 1 = Enable
3	RFEN0	RF Enable Output Select	0 = Disable 1 = Enable
4	TSEL	Time-out Select	00 = Disabled 01 = 0.8 sec 10 = 3.2 sec 11 = 25.6 sec
5			
6	LEDBL_1	Low-Voltage LED Blink	0 = Continuous 1 = Once
7	LEDOS_1	LED On-Time Select	0 = 50 ms 1 = 100 ms

SER_0 AND SER_1

SER_0 stores the 4 bytes of the 32-bit serial number for transmitter 1 (SER_1 for transmitter 2). There are 32 bits allocated for the serial number and a selectable Configuration bit determines whether 32 or 28 bits will be transmitted. The serial number is meant to be unique for every transmitter.

SEED_ 0 AND SEED_1

This is the 60-bit seed code that will be transmitted when seed transmission is selected. SEED_0 for transmitter 0 and SEED_1 for transmitter 1. This allows for the implementation of the secure learning scheme.

KEY_0 (TRANSMITTER 0 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 using a key generation algorithm. The inputs to the key generation algorithm are the secret manufacturer's code, the serial number, and/or the SEED value. The user may elect to use the algorithm supplied by Microchip or to create their own method of key generation.

COUNTER-CODE DESCRIPTION

The following addresses save the counter checksum values. The counter value is converted to Pseudo-Gray code and stored in the Counter locations (COUNTA, COUNTB, COUNTC) described on the EEPROM table. These checksum values are used to validate the current value of the counter and allows recovery from any brown-out events. This code is contained in module CounterCode.inc.

ENCRYPTION ENGINE

The encryption portion of the firmware makes use of the encryption engine internal to the PIC16F636. In essence, the data to be encrypted is loaded into the module, the number of cycles through the engine is set and, after running, the encryption module places the encrypted data into the registers CSRDATA<3:0>. Please read technical Brief TB076, "*Using the KEELOQ Cryptographical Module*" for more information on the use of this module.

BUTTON PRESS DURING TRANSMIT

If the device is in the process of transmitting and detects that a new button is pressed, the current transmission will be aborted, a new code word will be generated based on the new button information and transmitted. If all the buttons are released, a minimum number of code words will be completed. If the time for transmitting the minimum code words is longer than the time-out time, or the button is pressed for that long, the device will time-out.

CODE TRANSMISSION FORMAT

The following is the data stream format transmitted:

TABLE 7: DATA STREAM FORMAT TRANSMITTED

Unencrypted (bits)/Fixed Code					Encrypted (32 bits)		
CRC (2 bits)	VLOW (1 bit)	Repeat (1 bit)	Function Code (4 bits)	Serial Number (28 bits)	Function Code (4 bits)	Discrimination (12 bits)	Counter (16 bits)

Data transmitted LSb-first

A KEELOQ transmission consists of 32 bits of hopping code data, 32 bits of fixed code data and 3 to 5 bits of status information.

HOPPING CODE PORTION

The hopping code portion is calculated by encrypting the counter, discrimination value, and function code with the Encoder Key (KEY). A new hopping code is calculated every time a button press is pressed.

The synchronization counter can be either a 16- or a 10-bit counter as selected by the Counter Select option (CNTSEL).

The discrimination value can be programmed with any fixed value to serve as a post decryption check on the receiver end.

FIXED CODE PORTION

The 32 bits of fixed code consist of 28 bits of serial number and a copy of the 4-bit function code.

Each code word contains a preamble, header and data, and is separated from another code by guard time. The Guard Time Select (GSEL) configuration option can select a time period of 0ms, 6.4ms, 51.2ms or 102.4ms.

All other timing specifications are based on the timing element (Te). This *Te* can be set to 100 µs, 200 µs, 400 µs or 800 µs with the Baud Rate select (BSEL) configuration. The calibration header time can be set to 4*Te or 10*Te with the Header Select (HEADER) configuration option.

The firmware has four different transmission modulation formats available. The Modulation select (TMOD) configuration option is used to select between:

- Pulse-Width Modulation (PWM)
- Manchester (MAN)
- Variable Pulse-Width Modulation (VPWM)
- Pulse Position Modulation (PPM)

FIGURE 2: PULSE-WIDTH MODULATION (PWM)

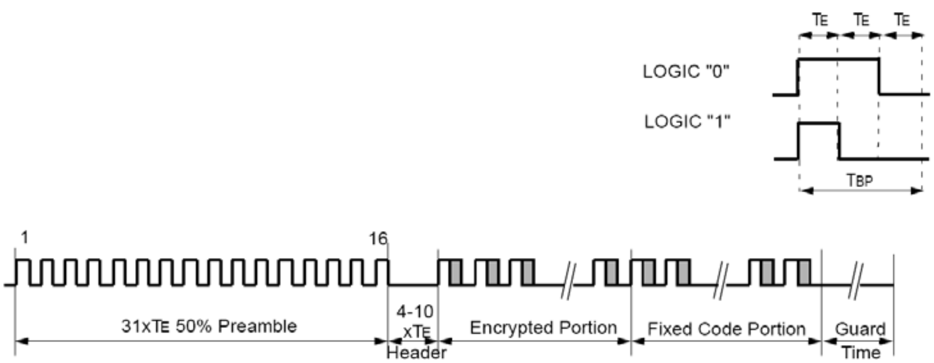


FIGURE 3: MANCHESTER (MAN)

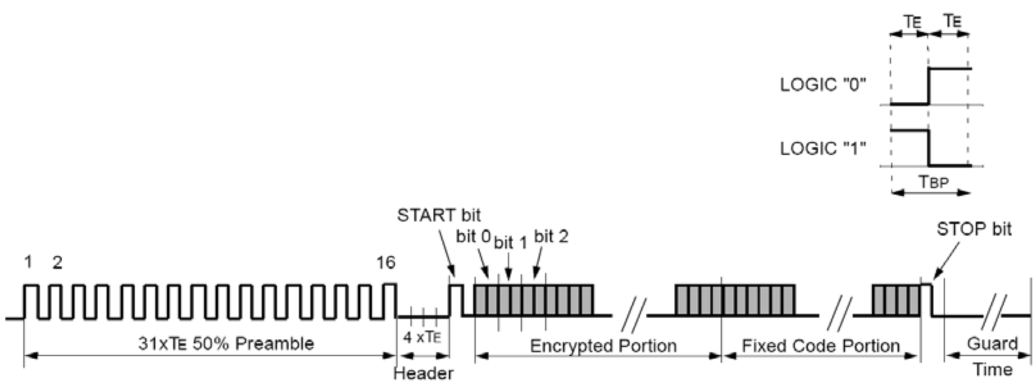


FIGURE 4: VARIABLE PULSE-WIDTH MODULATION (VPWM)

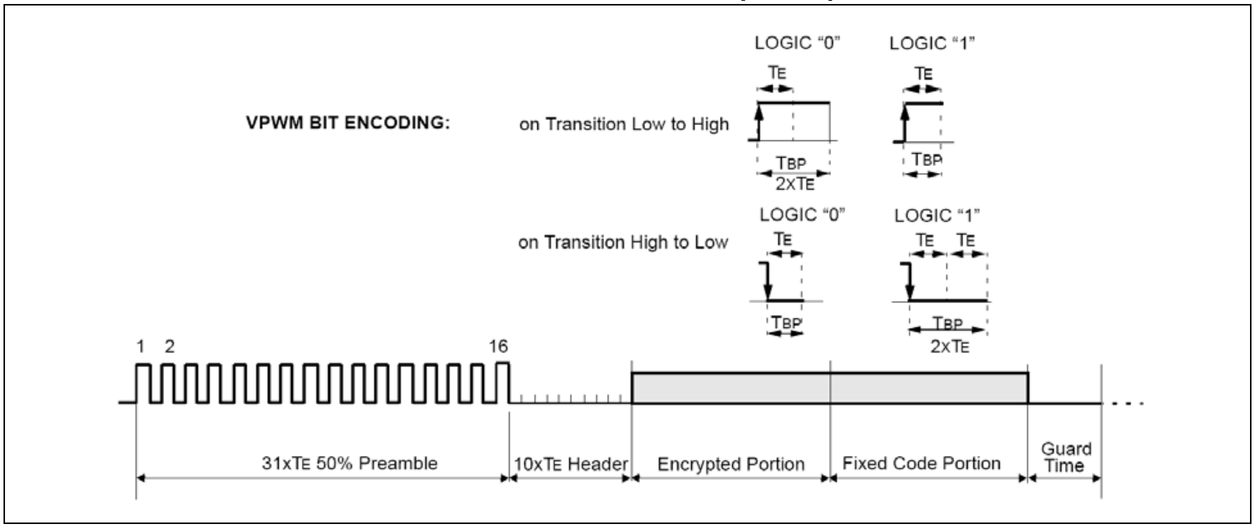
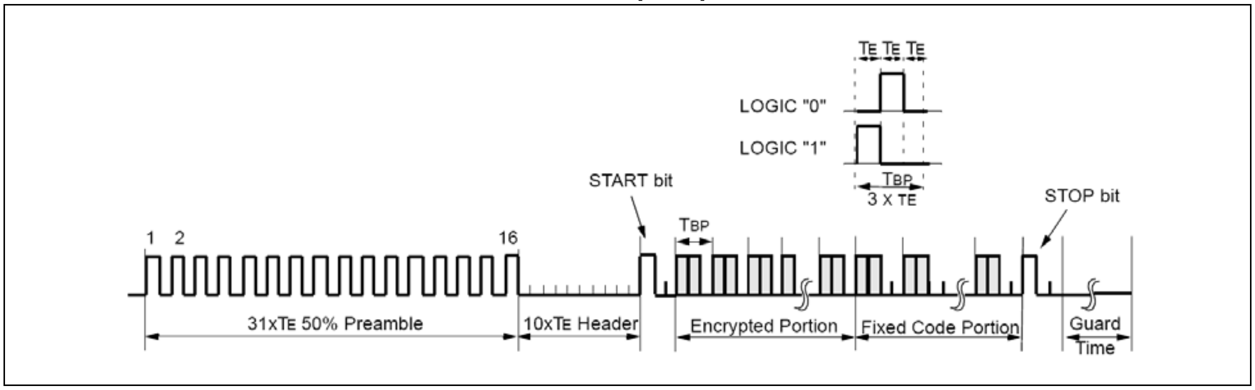


FIGURE 5: PULSE POSITION MODULATION (PPM)



If the Start/Stop Pulse Enable (STEN) configuration option is enabled, the software will place a leading and trailing '1' on each code word. This bit is necessary for modulation formats such as Manchester and PPM to interpret the first and last data bit.

A receiver wake-up sequence can be transmitted before the transmission starts. The wake-up sequence is configured with the Wake-up (WAKE) configuration option and can be disabled or set to 50 ms, 75 ms, or 100 ms of pulses of Te width.

FIRMWARE MODULES

The following files make up the KEELOQ transmitter firmware:

- TX_16F636.asm: this file contains the main loop routine as well as the wake-up, debounce, read configuration, load transmit buffer and transmit routines.
- Encrypt636.inc: this file runs the KEELOQ encryption engine.
- TX_eeprom.inc: this file contains the EEPROM data as specified on the EEPROM data map.
- CounterCode.inc: Calculates the checksums and confirms the validity of the counter.

CONCLUSION

This KEELOQ transmitter firmware has all the features of a standard hardware encoder. What makes this firmware implementation useful to the designer is that it gives the designer the power and flexibility of modifying the encoding and/or transmission formats and parameters to suit their security system.

ADDITIONAL INFORMATION

Microchip's Secure Data Products are covered by some or all of the following:

Code hopping encoder patents issued in European countries and U.S.A.

Secure learning patents issued in European countries, U.S.A. and R.S.A.

REVISION HISTORY

Revision B (June 2011)

- Added new section **Additional Information**
- Minor formatting and text changes were incorporated throughout the document

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.

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2009

Trademarks

Printed on recycled paper.

ISBN: 978-1-61341-266-4

Microchip received ISO/TS-16949:2002 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

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
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

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

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

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario, Canada
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: 852-2401-1200
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: 86-571-2819-3180
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2401-1200
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: 86-755-8203-2660
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: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

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: 886-3-6578-300
Fax: 886-3-6578-370

Taiwan - Kaohsiung
Tel: 886-7-213-7830
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
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 - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

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

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

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

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

05/02/11