Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

MCS3142 Dual KEELOQ® Encoder Wireless Remote Control Development Kit User's Guide

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.

Trademarks

Printed on recycled paper.

ISBN: 9781620779422

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.

Object of Declaration: MCS3142 Dual KEELOQ® Encoder Wireless Remote Control Development Kit

EU Declaration of Conformity

This declaration of conformity is issued by the manufacturer.
The development/evaluation tool is designed to be used for research and development in a laboratory environment. This development/evaluation tool is not intended to be a finished appliance, nor is it intended for incorporation into finished appliances that are made commercially available as single functional units to end users. This development/evaluation tool complies with EU EMC Directive 2004/108/EC and as supported by the European Commission's Guide for the EMC Directive 2004/108/EC (8th February 2010).
This development/evaluation tool complies with EU RoHS2 Directive 2011/65/EU.
For information regarding the exclusive, limited warranties applicable to Microchip products, please see Microchip's standard terms and conditions of sale, which are printed on our sales documentation and available at www.microchip.com.
Signed for and on behalf of Microchip Technology Inc. at Chandler, Arizona, USA

Derek Carlson
VP Development Tools

16-July-2013
Date

MCS3142 DUAL KEELOQ® ENCODER WIRELESS REMOTE CONTROL DEVELOPMENT KIT USER'S GUIDE

Table of Contents

Preface

INTRODUCTION

This chapter contains general information that will be useful to know before using the MCS3142 Dual KEELOQ® Encoder Wireless Remote Control Development Kit. Items discussed in this chapter include:

- Document Layout
- Conventions Used in this Guide
- Recommended Reading
- The Microchip Web Site
- Customer Support
- Document Revision History

DOCUMENT LAYOUT

This document describes how to use the MCS3142 Dual KEELOQ Encoder Wireless Remote Control Development Kit as a development tool to emulate and debug firmware on a target board. The manual layout is as follows:

- **Chapter 1. "Overview"**
- **Chapter 2. "Quick Start"**
- **Chapter 3. "Hardware Self-Test"**
- **Chapter 4. "MCS3142 Wireless Remote Key Fob"**
- **Chapter 5. "Embedded Security Development Board"**
- **Chapter 6. "Developing with the MCS3142 Wireless Security Remote Control Development Kit"**
- **Chapter 7. "KEELOQ MPLAB X Plugin"**
- **Chapter 8. "PC Application"**
- **Appendix A. "MCS3142 Transmitter Fob Schematic"**
- **Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics"**
- **Appendix C. "Embedded Security Development Board Schematics"**

CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

DOCUMENTATION CONVENTIONS

Description	Represents	Examples
Arial font:		
Italic characters	Referenced books	*MPLAB® IDE User's Guide*
	Emphasized text	...is the *only* compiler...
Initial caps	A window	the Output window
	A dialog	the Settings dialog
	A menu selection	select Enable Programmer
Quotes	A field name in a window or dialog	"Save project before build"
Underlined, italic text with right angle bracket	A menu path	*File>Save*
Bold characters	A dialog button	Click **OK**
	A tab	Click the **Power** tab
N'Rnnnn	A number in verilog format, where N is the total number of digits, R is the radix and n is a digit.	4'b0010, 2'hF1
Text in angle brackets < >	A key on the keyboard	Press <Enter>, <F1>
Courier New font:		
Plain Courier New	Sample source code	`#define START`
	Filenames	`autoexec.bat`
	File paths	`c:\mcc18\h`
	Keywords	`_asm, _endasm, static`
	Command-line options	`-Opa+, -Opa-`
	Bit values	`0, 1`
	Constants	`0xFF, 'A'`
Italic Courier New	A variable argument	*`file`*`.o`, where *`file`* can be any valid filename
Square brackets [ ]	Optional arguments	`mcc18 [options]` *`file`* `[options]`
Curly brackets and pipe character: { | }	Choice of mutually exclusive arguments; an OR selection	`errorlevel {0|1}`
Ellipses...	Replaces repeated text	`var_name [, var_name...]`
	Represents code supplied by user	`void main (void) { ... }`

RECOMMENDED READING

This user's guide describes how to use the MCS3142 Dual KEELOQ Encoder Wireless Remote Control Development Kit. Other useful documents are listed below. The following Microchip documents are available and recommended as supplemental reference resources.

Read me Files

For the latest information on using other tools, read the tool-specific Readme files in the Readmes subdirectory of the MPLAB X® IDE installation directory. The Readme files contain update information and known issues that may not be included in this user's guide.

Design Center

Microchip has a KEELOQ design center which can be found on **www.microchip.com/keeloq**.

THE MICROCHIP WEB SITE

Microchip provides online support via our web 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 (FAQs), 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 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://support.microchip.com

DOCUMENT REVISION HISTORY

Revision A (February 2014)

- Initial Release of this Document.

Chapter 1. Overview

1.1 INTRODUCTION

This document details how to use the stand-alone MCS3142 development kit, as well as the associated PC application and the MPLAB X plugin. The addition of a PC application allows much greater flexibility in accessing and viewing the captured wireless data. The MPLAB X plugin provides programming support for the MCS3142 as well as for the other KEELOQ devices.

The MCS3142 Dual KEELOQ Encoder Wireless Remote Kit contains a receiver platform and MCS3142 transmitter that are used in conjunction with each other to showcase the various technologies of KEELOQ: Classic KEELOQ and Ultimate KEELOQ.

For details on Classic KEELOQ and Ultimate KEELOQ, please refer to Microchip application notes AN1259, "*KEELOQ® Microcontroller-Based Code Hopping Encoder*".

1.2 KIT CONTENTS

- Embedded Security Development Board
- MCS3142 Wireless Remote Key Fob
- SX1239 Receiver PICtail™ Daughter Board
- USB A to Mini-B Cable
- CR2032 Coin Cell Battery

1.2.1 Downloadable Content

The following latest software builds should be obtained from the Microchip web site:

- Embedded Security Development Board source code
- MPLAB X Integrated Development Environment
  - KEELOQ Plugin (see **Chapter 7. "KEELOQ MPLAB X Plugin"**)
- KEELOQ Graphical Interface for the Embedded Security Development Board

Chapter 2. Quick Start

2.1 INTRODUCTION

The MCS3142 Dual KEELOQ Encoder Wireless Remote Control Development Kit uses an identical receiver module and demo board as seen in the Wireless Security Remote Control Development Kit User's Guide. (http://ww1.microchip.com/downloads/en/DeviceDoc/41646A.pdf). This chapter will explain how to setup the board and show the general operation.

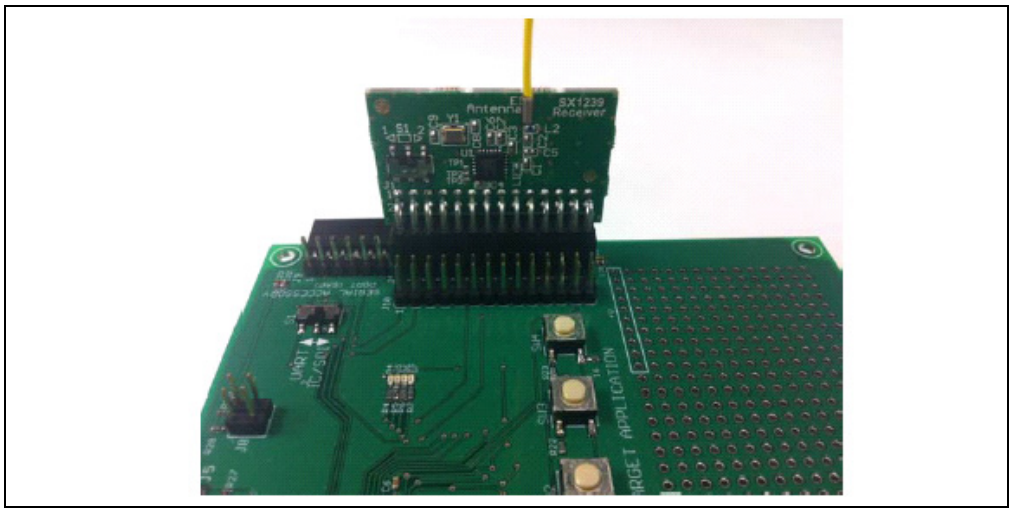
2.2 USING THE STAND-ALONE DEMO

2.2.1 Setup

There are only a few steps to perform to get the stand-alone demo working:

1. Open the plastic enclosure of the red key fob by carefully prying apart the two halves with a flat-head screw driver. Observe the correct battery polarity and insert the coin battery into the holder. Put the key fob back together.
2. To verify that the key fob is properly installed, press any button and the LED should flash when a button is pressed.
3. Plug in the RF receiver daughter board on the PICtail slot of the demo board. Make sure that the RF receiver daughter board has the side with the RF receiver chip facing the center, as shown in Figure 2-1.

FIGURE 2-1: ORIENTATION OF THE SX1239 RECEIVER PICtail™ DAUGHTER CARD



The board can be powered either from a USB cable or external power source.

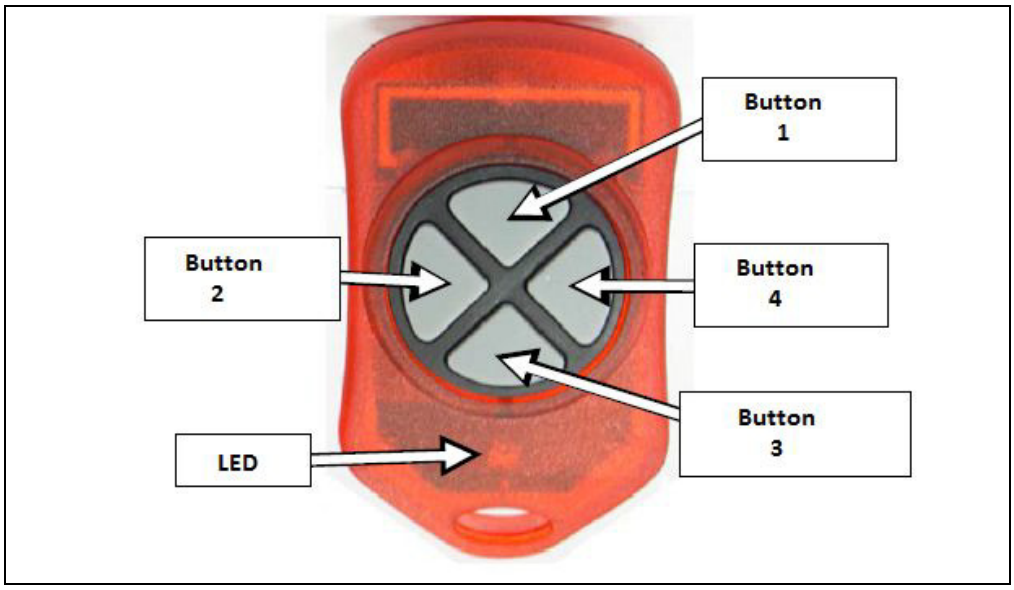
- To power by USB, connect a USB A to mini-B cable to the development board and an available USB port. Set jumper J6 to pins 1-2. No drivers are required to power the board; however, the MCP2200 driver may need to be installed for the PC to Board communication (see **Section 8.2 "Installation"**)
- To power from an external power supply, place jumper J6 to pins 2-3. Connect the test points labeled +VEXT and GND to a bench power supply that is set to 3.3 VDC.

2.2.2 Operation

The pre-programmed demo is used to demonstrate the operation of Microchip Remote Keyless Entry (RKE) solutions. The demo highlights the capabilities of transmitting and receiving secured data wirelessly. Two different methods, Classic KEELOQ and Ultimate KEELOQ, are used in this demo.

The pre-programmed demonstration shows how to secure information during data transmission.The transmitter sends out two types of packets. A Typical packet contains the device serial number, button code, synchronization counter, timer (Ultimate KEELOQ only) and various other parameters used in the decryption and validation process. A Seed packet contains special data related to the encoder's encryption key. A Seed packet is sent infrequently, and only used when pairing a transmitter to a receiver.

FIGURE 2-2: MCS3142 KEY FOB



Pressing any one of the four buttons on the red key fob will start the encryption process and eventual transmission of a KEELOQ packet. The LED will flash momentarily to indicate a transmission.Table 2-1 describes the transmitter buttons and their functions.

TABLE 2-1: TRANSMITTER BUTTONS AND FUNCTIONS

Button Combination	Description
Button 1	Transmit a Classic KEELOQ® Typical Packet
Button 2	Transmit a Classic KEELOQ Typical Packet
Button 3	Transmit an Ultimate KEELOQ Typical Packet
Button 4	Transmit an Ultimate KEELOQ Typical Packet
Button 1 + Button 2 simultaneously	Transmit a Classic KEELOQ Seed Packet
Button 3 + Button 4 simultaneously	Transmit an Ultimate KEELOQ Typical Packet

The kit is configured to use the Secure Learn pairing mechanism. This requires the encoders to transmit a special packet, called a Seed packet, with special information the receiver needs to properly decrypt transmissions. This kit is configured to transmit a Seed transmission with both buttons assigned to a particular encoder are pressed. The pairing phase also requires a Typical transmission to complete the pairing process.

To pair a transmitter to the receiver using Secure learn:

1. Press SW3, the **Secure Learn** button on the Embedded Security Development Board to enable Secure Learn mode.
2. If learning the Classic KEELOQ encoder, press both buttons **1** and **2**. If learning the Ultimate KEELOQ encoder, press both buttons **3** and **4**. This will cause the special Seed packet to be sent.
3. The receiver will indicate reception of the Seed transmission.
4. If learning the Ultimate KEELOQ encoder, press either button **3** or **4** to send a Typical transmission.
5. The receiver will indicate successful pairing.

The kit also includes the SX1239 Receiver PICtail Daughter Board. It houses the Semtech SX1239 wideband receiver. The target application configured the receiver on start-up.

2.3 KEELOQ SCREENS

This section describes all of the LCD screens when used with the MCS3142 transmitter.

Note:	The receiver will always display the encoder serial number associated with a transmission, regardless of the transmitter's status with the receiver.

Only a message from a paired transmitter can be accepted by the receiver. If a packet is received from an unknown transmitter, the message '`Not Learned`' will be displayed on the LCD, as shown in Figure 2-3 and Figure 2-4. The type of transmission and the transmitter's serial number are also displayed on the screen.

FIGURE 2-3: CLASSIC KEELOQ® ENCODER NOT LEARNED

FIGURE 2-4: ULTIMATE KEELOQ® ENCODER NOT LEARNED

When a Classic KEELOQ packet is received from a paired transmitter, the contents of the packet is displayed on the LCD, as shown in Figure 2-5. Table 2-2 describes the data displayed on the screen.

TABLE 2-2: CLASSIC KEELOQ® TYPICAL TRANSMISSION DATA

'KLQ'	Indicates a Classic KEELOQ® encoder
'7989002'	The encoder's serial number
'C: 1008'	The encoder's synchronization counter value
'F: 2'	The encoder's function code

FIGURE 2-5: TYPICAL CLASSIC KEELOQ® TRANSMISSION

When a Classic KEELOQ packet is received from a paired transmitter, the contents of the packet is displayed on the LCD, as shown in Figure 2-6. Table 2-3 describes the data displayed on the screen.

TABLE 2-3: ULTIMATE KEELOQ® TYPICAL TRANSMISSION DATA

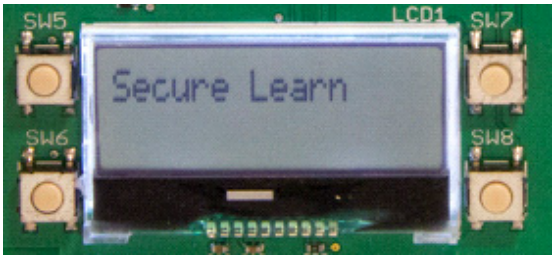
'ULT'	Indicates an Ultimate KEELOQ® encoder
'12345666'	The encoder's serial number
'T: 00330A1F'	The encoder's time-stamp
'F: 04'	The encoder's function code

FIGURE 2-6: TYPICAL ULTIMATE KEELOQ® TRANSMISSION

The kit can pair transmitters using Normal Learn or Secure Learn (note, though, that the included transmitters are configured to pair only using Secure Learn). When the receiver enters Normal Learn mode, text similar to Figure 2-7 is displayed. For Secure Learn, text similar to Figure 2-8 is shown.

FIGURE 2-7: ENTER NORMAL LEARN MODE

FIGURE 2-8: ENTER SECURE LEARN MODE



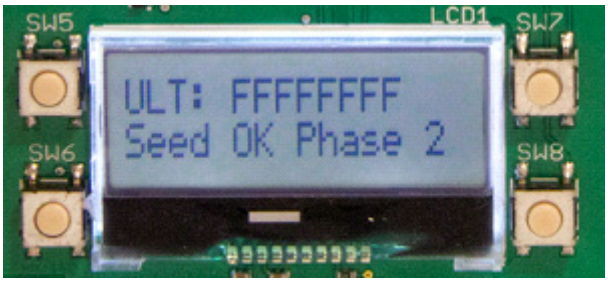
The receiver must complete the learn process within a fixed window. If the necessary data is not received from the transmitters within this window, the process will abort and a message similar to Figure 2-9 is displayed.

FIGURE 2-9: LEARN MODE TIMEOUT

Secure Learn requires a Seed transmission from the encoder. Once received, a message similar to Figure 2-10 is displayed for Classic KEELOQ or Figure 2-11 for Ultimate KEELOQ.

FIGURE 2-10: CLASSIC KEELOQ® SEED RECEIVED

FIGURE 2-11: ULTIMATE KEELOQ® SEED RECEIVED



Ultimate KEELOQ requires an explicit transmission of a Typical packet. Once received, a message similar to the one shown in Figure 2-12 is displayed.

FIGURE 2-12: ULTIMATE KEELOQ® PAIRING COMPLETE

A message similar to Figure 2-13 is shown if an otherwise valid Classic KEELOQ packet is received, but is not a Seed transmission.

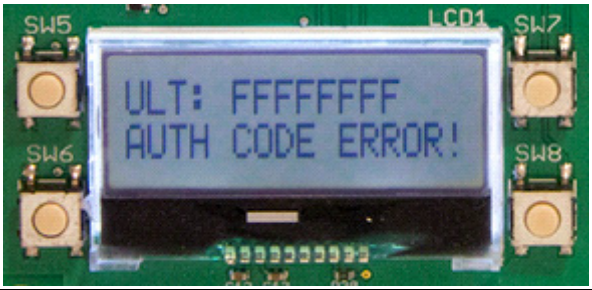
FIGURE 2-13: CLASSIC KEELOQ® NO SEED TRANSMISSION

The synchronization counter is used to validate Classic KEELOQ transmissions. If the transmitted value falls outside the acceptable boundaries of the receiver's copy, an error similar to Figure 2-14 is displayed.

FIGURE 2-14: CLASSIC KEELOQ SYNCHRONIZATION ERROR

Packets from Ultimate KEELOQ encoders are always validated initially by confirming the Authorization Code portion of the transmission. If this check fails, a message similar to Figure 2-15 is displayed. Note that, this may be seen while completing the Secure Learn process and does not necessarily indicate an error.

FIGURE 2-15: AUTHORIZATION CODE INVALID



The kit allows the user to erase, or 'forget', all paired transmitters. If done, the LCD will display a message similar to Figure 2-16.

FIGURE 2-16: DELETE EEPROM

Chapter 3. Hardware Self-Test

3.1 INTRODUCTION

A hardware self-check can be performed to ensure the hardware integrity of the Embedded Security Development Board. The instruction of the hardware self-check is displayed on the LCD. The test result is either checked by firmware and displayed on the LCD, or verified by user observation.

To initiate the hardware self-check, press and hold push button **SW1** before powering-up the Embedded Security Development Board. SW1 can then be released when "`HDW Self Tests`" is displayed on the LCD screen.

3.2 BUTTON TESTS

"`Button Test`" will be displayed on the first line of the LCD display. Test instructions of pressing individual buttons will be displayed on the second line of the LCD display. Once a required push button is pressed, the test instruction message will be changed for the next push button. Once all push buttons have been tested, **SW1** needs to be pressed to move forward to the LED test.

3.3 LED TESTS

There are two sets of LEDs. When the LED tests start, the message "`LEDs Flashing`" will be displayed on the first line of the LCD display. During the tests, two sets four LEDs (D4-D7) and seven LEDs (D8-D14) will flash in a pattern. The user should observe that all LEDs are turned on and off with flashing intervals of roughly one second. Once the user has verified the LED test, SW1 needs to be pressed to move forward to the RTCC test.

3.4 RTCC TEST

When RTCC tests are initiated, the LCD display will show the clock and calendar. If no coin battery for the RTCC has been installed, the time displayed will be close to the reset time of January the 1st, 2012. If a coin battery for RTCC is installed, the time displayed will be based on whatever was previously set, plus the time that has passed. Observe that the clock is advancing. Once the RTCC test is done, SW1 needs to be pressed to move forward to the SPI test.

3.5 SPI TEST

The SPI test in hardware self-check is performed to the SPI bus that connects the target application microcontroller and the SX1239 Receiver PICtail Daughter Board. Therefore, the SX1239 Receiver PICtail Daughter Board must have been plugged in before this test starts. Once the SPI test starts, the target application microcontroller requests specific information from the SX1239 receiver through the SPI bus. If the expected response is received, then the "`Successful`" status will appear; otherwise, the "`Fail`" status will be displayed.

Note: If a PICtail daughter board, other than the SX1239 Receiver PICtail™ Daughter Board, is plugged into the PICtail connector (even though the SPI bus may still be working), the SPI test might show failure status. The demo board expects an SX1239 to be identified on the SPI interface.

Chapter 4. MCS3142 Wireless Remote Key Fob

4.1 INTRODUCTION

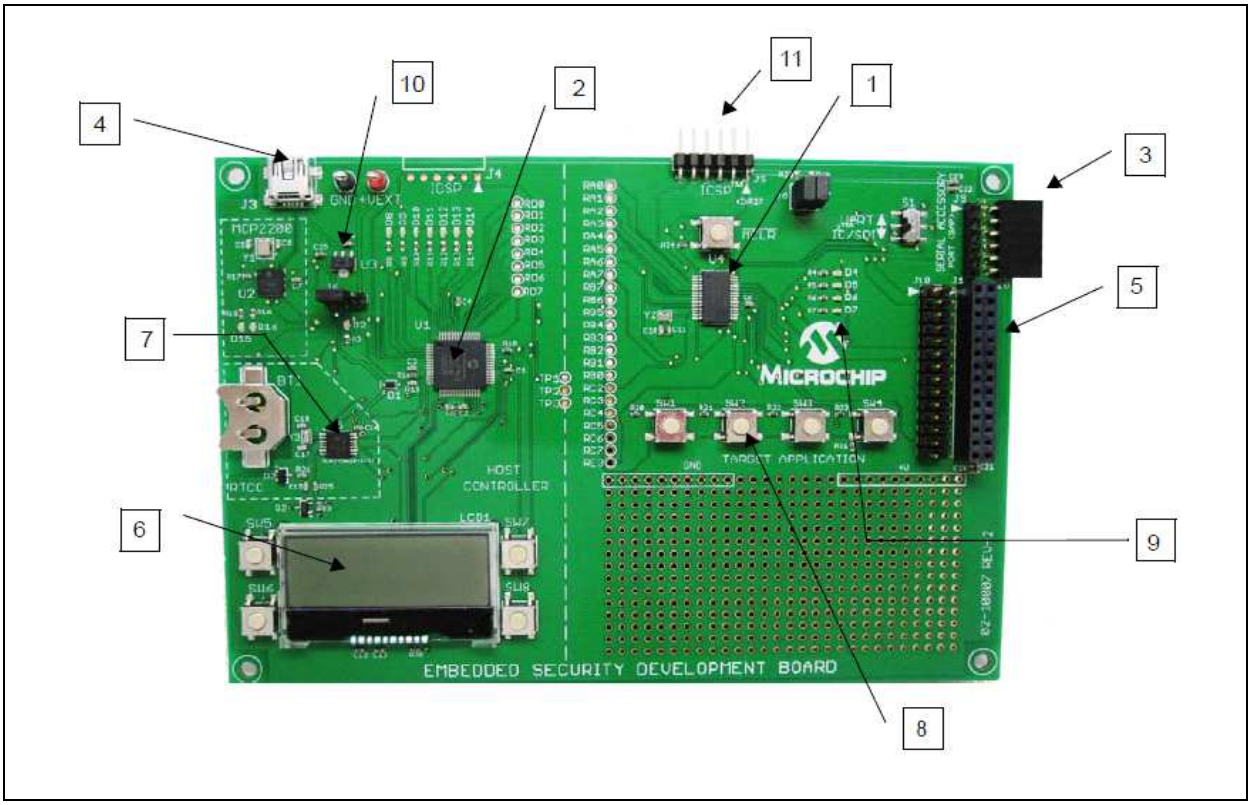
The MCS3142 Wireless Remote Key Fob is a demonstration and development platform for wireless security remote control applications. Please see http://ww1.microchip.com/downloads/en/DeviceDoc/41646A.pdf for similar information about the transmitter printed circuit board and its antenna design.

Chapter 5. Embedded Security Development Board

5.1 INTRODUCTION

This section gives a detailed description of the development board. The layout can be seen in Figure 5-1.

FIGURE 5-1: EMBEDDED SECURITY DEVELOPMENT BOARD



The following main blocks are defined on the Embedded Security Development Board in Table 5-1:

TABLE 5-1: EMBEDDED SECURITY MODULE DEFINITIONS

1	Target Application microcontroller U4
2	Host microcontroller U1
3	Serial Accessory Port P20
4	USB Interface Port J3
5	PICtail™ Connector J1
6	16x2 character LCD display
7	Real-Time Clock and Calendar (RTCC) module U5
8	Push Buttons
9	LEDs
10	Voltage Regulator
11	ICSP™ Programming Ports, J4 for Host; J5 for Target Application

5.2 SERIAL COMMUNICATIONS CONNECTIONS

The Embedded Security Development Board is divided into two halves. The left side is the host controller half. The right side is the target application half. The two halves are connected by three wires, easily accessible by test points, labeled TP1, TP2 and TP3. Table 5-2 lists the respective microcontroller I/O port connections:

TABLE 5-2: SERIAL CONNECTIONS BETWEEN DEVICES

Host Controller MCS3142	Test Points	Target Application PIC16LF1947 (Master)
RF5	TP1	RB7/ICSPDAT
RB2	TP2	RB6/ICSPCLK
RF4	TP3	RE3/$\overline{\text{MCLR}}$/VPP

The host side half is controlled by a PIC16LF1947 microcontroller. The PIC16LF1947 microcontroller communicates with a 16x2 character LCD display (LCD1), an MCP2200 USB to UART communications IC (U2), an MCP795W10 SPI Real-Time Clock Calendar IC (U5), four push button switches (SW5-SW8), and seven LEDs (D8-D14). The PIC16LF1947 microcontroller can be programmed and debugged via the ICSP™ header (J4).

The target application half has a PIC16LF1938 microcontroller. The PIC16LF1938 microcontroller communicates with the 28-pin PICtail connector (J1), the Serial Accessory Port (P20), four push button switches (SW1-SW4), and four LEDs (D4-D7). The PIC16LF1938 microcontroller can be programmed/debugged via the ICSP (J5). The Embedded Security Development Board schematic is shown in **Appendix C. "Embedded Security Development Board Schematics"** as Figure C-2.

5.3 SERIAL ACCESSORY PORT (P20)

The Serial Accessory Port provides a simple serial interface for the external modules. These modules may be either an external sensor or an accessory board. The partial list of Microchip boards with SAP capabilities includes the following:

- LCD Serial Accessory Board
- RS-232 Serial Accessory Board

For more information about the existing accessory boards, visit http://www.microchip.com or refer to the "*RS-232 Serial Accessory Board User's Guide*" (DS70649). The following interfaces are supported by the Serial Accessory Port:

- 3 or 4-wire SPI
- I²C™
- USART

Jumpers J7 and J8 connect pull-up resistors, typically useful when I²C is selected and the pull-up resistors are not available on the daughter board.

5.4 USB INTERFACE PORT

The Microchip MCP2200 provides USB to UART support. The USB interface port can also be used to power the Embedded Security Development Board directly. Please see **Section 8.2 "Installation"** for more information about connecting the board to a PC.

5.5 PICtail™ PORT

The PICtail port is a 28-pin interface port that supports Microchip's RF-based daughter cards. The PICtail port provides the following interfaces to the daughter cards:

- Power Supply
- SPI interface
- Interrupt request lines
- Other digital/analog I/O lines

> **Note:** The user must be careful about the PICtail port pins that share different functions of the board. The user needs to check the schematics before assigning functions for any port pin.

There are many Microchip accessory daughter cards, which have PICtail port connectivity. When not used as one of the components in the Wireless Security Remote Control Development Kit, the Embedded Security Development Board can be connected with any daughter board with the PICtail port, and perform different functionalities. Refer to the Microchip web site http://www.microchip.com for accessory daughter boards with PICtail port.

5.6 LCD DISPLAY

The Embedded Security Development Board supports 16x2 character LCD display with backlight. The LCD is controlled by the host microcontroller through the SPI port.

5.7 REAL-TIME CLOCK AND CALENDAR (RTCC) MODULE

The Embedded Security Development Board RTCC module can be used to set and track clock and calendar precisely. The RTCC functionality is achieved with the Microchip MCP795W10. The RTCC module is controlled by the host microcontroller through the SPI interface. The RTCC is commonly used with Ultimate KEELOQ, which relies on the system clock as part of its security.

The RTCC module can be powered either by the 3.3V power from the Embedded Security Development Board, or by a separate coin battery when external power is not available. For details on operating this RTCC module, refer to the data sheet of the MCP795W10 at http://www.microchip.com/MCP795W10.

5.8 PUSH BUTTONS

The Embedded Security Development Board has two sets of push buttons. **SW1**-**SW4** on the target application side and SW5 on the host controller side.

The four push buttons for the target application microcontroller are read as a single analog input. Depending on the different ratios of pull-up and pull-down resister values, the input analog voltages to the master microcontroller are different. Therefore, through the ADC on the target application microcontroller, the button that is pressed can be identified. Such design is used to save I/O pin requirement for the target application microcontroller.

The four push buttons for the host microcontroller are four separate digital inputs to the slave microcontroller, due to the abundant I/O pin availability for the slave microcontroller. All buttons are assigned to the individual interrupt lines of the microcontroller and are not driven by external pull-up circuitry to save power consumption. The user software must enable the PORTB pull-ups of the microcontroller before evaluating the button state.

The **MCLR** push button is connected to the RE3/MCLR pin of the target application microcontroller. The RE3/MCLR pin of the target application microcontroller is also one of the SPI lines that control the host microcontroller. When the target application and host microcontrollers are interconnected, the RE3/MCLR pin of target application microcontroller is configured to be a normal digital I/O pin; therefore, the **MCLR** push button is ineffective. Otherwise, if an I^2C intercommunication is not required between the target application and host microcontroller, the pin can be configured as Reset and the **MCLR** button can be used.

5.9 LEDS

There are two sets of LEDs that are controlled by the target application and the host microcontrollers, respectively. The target application MCU controls a set of four LEDs through the digital output pins. The host MCU controls a set of six LEDs through digital output pins. The two sets of LEDs may be useful in the demo or debugging process.

LEDs D15 and D16 on the left half are used to identify the TX and RX operation of MCP2200. The default configuration of the MCP2200 does not enable this feature, but it may be enabled using the MCP2200 configuration utility (see **Section 7.2 "Install"**). LEDs D12 and D13 are used by the preprogrammed demo firmware to identify the TX and RX communication between the host and target microcontrollers.

LED D2 indicates the power availability. This LED cannot be controlled by the target application or by the host microcontroller.

5.10 POWER SUPPLY

The Embedded Security Development Board can be powered by one of the following two sources:

- USB port
- External 3.3V power source through GND and +VEXT connectors

Jumper J6 is used to choose the power source. When the left side, pins 1-2 of J6 are closed, USB power is selected; when the right side, pins 2-3 of J6 are closed, external power source is selected.

When the USB port is used to power the board, the input voltage is stabilized by a Microchip MCP1703, LDO regulator U3.