Chipsmall

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

MICRF114 Wireless Security 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.

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

Object of Declaration: MICRF114 Wireless Security Remote Control Development Kit

EU Declaration of Conformity

Manufacturer: Microchip Technology Inc.
                       2355 W. Chandler Blvd.
                       Chandler, Arizona, 85224-6199
                       USA

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 a Finished Appliance, nor is it intended for incorporation into Finished Appliances that are made commercially available as single functional units to end users under 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.

This development/evaluation tool, when incorporating wireless and radio-telecom functionality, is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC and the FCC rules as stated in the declaration of conformity provided in the module datasheet and the module product page available at www.microchip.com.

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   12-Sep-14
Derek Carlson   Date
VP Development Tools

NOTES:

MICRF114 WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT USER'S GUIDE

Table of Contents

NOTES:

Preface

NOTICE TO CUSTOMERS

All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our website (www.microchip.com) to obtain the latest documentation available.

Documents are identified with a "DS" number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is "DSXXXXXXXXA", where "XXXXXXXX" is the document number and "A" is the revision level of the document.

For the most up-to-date information on development tools, see the MPLAB® IDE online help. Select the Help menu, and then Topics to open a list of available online help files.

INTRODUCTION

This chapter contains general information that will be useful to know before using the MICRF114 Wireless Security Remote Control Development Kit. Items discussed in this chapter include:

- Document Layout
- Conventions Used in this Guide
- Recommended Reading
- The Microchip Website
- Development Systems Customer Change Notification Service
- Customer Support
- Document Revision History

DOCUMENT LAYOUT

This document describes how to use the MICRF114 Wireless Security Remote Control Development Kit to evaluate and experiment with Microchip KEELOQ® Remote Keyless Entry (RKE) solutions. The document is organized as follows:

- **Chapter 1. "Overview"** – This chapter describes the MICRF114 Wireless Security Remote Control Development Kit and its contents.
- **Chapter 2. "Getting Started"** – This chapter provides the requirements and demonstration setup to start using the MICRF114 Wireless Security Remote Control Development Kit.
- **Chapter 3. "MICRF114 Wireless Remote Key Fob"** – This chapter provides the hardware details of the MICRF114 Wireless Remote Key Fob.
- **Chapter 4. "SX1239 Receiver PICtail™ Daughter Board"** – This chapter provides the hardware details of the SX1239 Receiver PICtail™ Daughter Board.
- **Chapter 5. "Embedded Security Development Board"** – This chapter provides the hardware details of the Embedded Security Development Board.

- **Chapter 6. "Wireless Security Remote Control Development Kit"** – This chapter describes the Wireless Security Remote Control Development Kit and provides the general design for the transmitter and receiver.
- **Appendix A. "MICRF114 Wireless Remote Key Fob Schematics"** – This appendix provides the PCB layout, schematic, and Bill of Materials (BOM).
- **Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics"** – This appendix provides the PCB layout, schematic, and Bill of Materials.
- **Appendix C. "Embedded Security Development Board Schematics"** – This appendix provides the PCB layout, schematic, and Bill of Materials.

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 MICRF114 Wireless Security Remote Control Development Kit. Other useful document is listed below. The following Microchip document is recommended as a supplemental reference resource:

MICRF114 Low-Power Integrated Sub-GHz Wireless RF Transmitter Data Sheet (DS50002416)

This data sheet provides the technical specifications for the MICRF114 RF transmitter and is available for download from the Microchip website at www.microchip.com.

THE MICROCHIP WEBSITE

Microchip provides online support via our website at www.microchip.com. This website is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the website 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, and Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, and listings of Microchip sales offices, distributors and factory representatives

DEVELOPMENT SYSTEMS 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 website at www.microchip.com, click on Customer Change Notification and follow the registration instructions.

The Development Systems product group categories are:

- **Compilers** – The latest information on Microchip C compilers and other language tools
- **Emulators** – The latest information on the Microchip MPLAB® REAL ICE™ in-circuit emulator
- **In-Circuit Debuggers** – The latest information on the Microchip in-circuit debugger. This includes MPLAB ICD 3 in-circuit debuggers and PICkit™ 3 debug express.
- **MPLAB X IDE** – The latest information on Microchip MPLAB X IDE, the Windows® Integrated Development Environment for development systems tools
- **Programmers** – The latest information on Microchip programmers including the PICkit 3 development programmer

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 website at: http://www.microchip.com/support.

DOCUMENT REVISION HISTORY

Revision A (November 2015)

This is the initial release of this document.

Chapter 1. Overview

1.1   INTRODUCTION

The MICRF114 Wireless Security Remote Control Development Kit is a demonstration and development platform for wireless security remote control applications. The kit demonstrates two security protocols, KEELOQ® Classic and KEELOQ AES.

The kit contains a four-button key fob transmitter based on the MICRF114 RF transmitter, an SX1239 Receiver PICtail™ Daughter Board, and an Embedded Security Development Board.

1.2   WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT CONTENTS

The MICRF114 Wireless Security Remote Control Development Kit operates on 433.92 MHz (DM182017-5).

Each kit contains the following items:

- MICRF114 Wireless Remote Key Fob

  Refer to **Chapter 3. "MICRF114 Wireless Remote Key Fob"** and **Appendix A. "MICRF114 Wireless Remote Key Fob Schematics"**.

- SX1239 Receiver PICtail Daughter Board

  Refer to **Chapter 4. "SX1239 Receiver PICtail™ Daughter Board"** and **Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics"**.

- Embedded Security Development Board

  Refer to **Chapter 5. "Embedded Security Development Board"** and **Appendix C. "Embedded Security Development Board Schematics"**.

- USB Cable
- CR2032 Coin Cell Battery

NOTES:

Chapter 2. Getting Started

2.1 INTRODUCTION

This chapter provides a getting started tutorial to familiarize users with the MICRF114 Wireless Security Remote Control Development Kit.

This chapter includes the following topics:

- Hardware Requirements
- Software Requirements
- Demo Setup
- Demo Operation
- Embedded Security Development Board Hardware Self-Check

2.2 HARDWARE REQUIREMENTS

The following hardware is required to run the preprogrammed demo application:

- MICRF114 Wireless Remote Key Fob
- CR2032 Coin Cell Battery
- SX1239 Receiver PICtail Daughter Board
- Embedded Security Development Board
- USB-A to Mini-B Cable

  This cable is used to power the Embedded Security Development Board. Power can also be provided by a bench power supply.

2.3 SOFTWARE REQUIREMENTS

The MICRF114 Wireless Remote Key Fob and Embedded Security Development Board are preprogrammed with a remote control demo program. **Section 2.4 "Demo Setup"** and **Section 2.5 "Demo Operation"** explain the demo setup and operation.

For additional information related to the demo, visit the MICRF114 product web page at www.microchip.com/MICRF114.

2.4 DEMO SETUP

To setup and operate the remote control demo program, perform the following steps:

1. Open the plastic enclosure of the red key fob by carefully prying apart the two sections. Carefully remove the Printed Circuit Board (PCB) from the plastic enclosure. Observe the correct battery polarity and insert the CR2032 coin battery into the battery holder. Put the PCB back into the plastic enclosure and then close the enclosure.
2. Press any push button to verify that the key fob is properly installed. The LED flashes when the button is pressed.
3. Plug in the RF receiver daughter board into the PICtail socket of the Embedded Security Development Board. Ensure that the RF receiver chip side faces the center as shown in Figure 2-1.

FIGURE 2-1: PLUG THE SX1239 RECEIVER PICtail™ DAUGHTER BOARD
INTO THE EMBEDDED SECURITY DEVELOPMENT BOARD

4. Power-up the Embedded Security Development Board.

    To power the Embedded Security Development Board from the USB port, con-
    nect the USB-A to Mini-B cable and an available USB port or USB power source
    to the development board. Set jumper J6 to pins 1-2. When using a USB port for
    power, loading the USB drivers is *not* required.

    To power the Embedded Security Development Board from an external power
    supply, connect test points labeled +V_{EXT} and GND to a bench power supply set
    to 3.3 VDC. Set jumper J6 to pins 2-3.

    Once the Embedded Security Development Board is powered up, the messages
    "Security and Auth Development Kit" followed by "KEELOQ 3 Demo 433.92 MHz"
    appears on the LCD display. If the second message did *not* appear within five
    seconds, press the MCLR button located on the upper right quarter of the board.

2.5   DEMO OPERATION

The preprogrammed demo is used to demonstrate the basic operation of Microchip
Remote Keyless Entry (RKE) solutions. The demo highlights the capabilities of secure
data transmission over the air. Two different methods of securing information before
transmission, KEELOQ Classic and KEELOQ AES, are used in this demo.

2.5.1   Key Fob as a Transmitter

The preprogrammed demonstration shows how to secure information during data
transmission. The red key fob has four push buttons and is powered by a CR2032 coin
battery. By pressing any of the four buttons, the information on the pressed button is
encrypted and transmitted. During data transmission, the LED on the key fob is flash-
ing. The two methods to secure the information before the transmission are KEELOQ
Classic and KEELOQ AES. Press button 1 or button 2 to secure the information with
KEELOQ Classic and button 3 or button 4 to secure the information with KEELOQ AES.
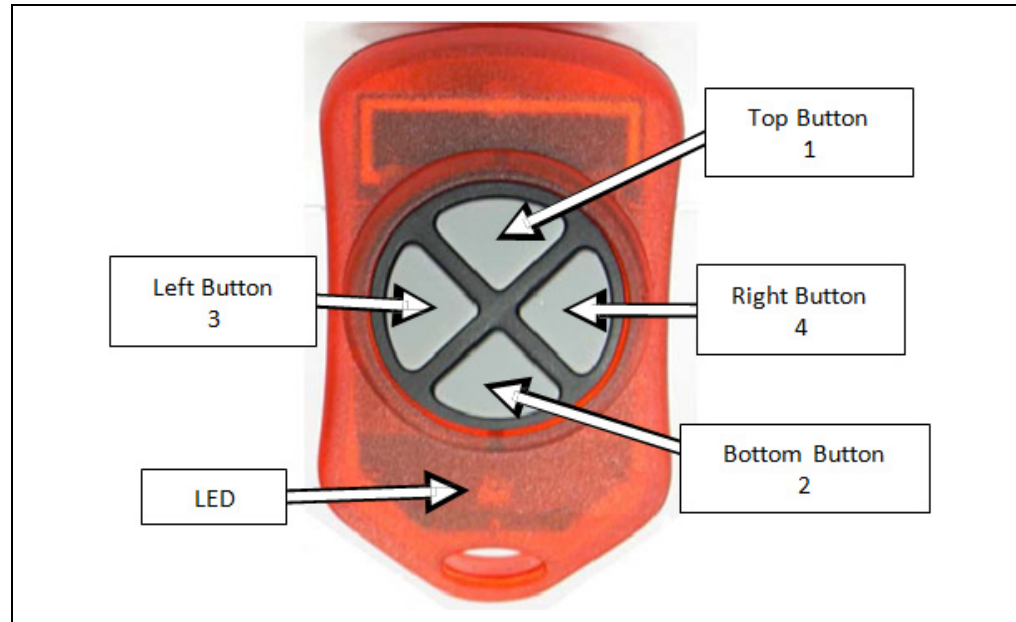Refer to Figure 2-2.

For more information on KEELOQ Classic and KEELOQ AES, refer to the following Microchip Technology Application Notes:

- *AN1259 KEELOQ® Microcontroller-Based Code Hopping Encoder* (DS01259)
- *AN1265 KEELOQ® with AES Microcontroller-Based Code Hopping Encoder* (DS01265)

FIGURE 2-2: **KEY FOB WITH FOUR PUSH BUTTONS**

2.5.2 Embedded Security Development Board as a Receiver

When the SX1239 Receiver PICtail Daughter Board receives a secured packet, the content of the packet is acquired by the target application microcontroller. Based on the length of the received packet, the target application microcontroller decides what cipher (KEELOQ Classic or KEELOQ AES) to use in securing the data. The decryption process reveals the plain text, and the authentication process verifies whether the plain text contains valid information.

2.5.2.1 KEELOQ® CLASSIC

For KEELOQ Classic, the receiver accepts messages only from a known transmitter. The known transmitters and their latest counters are stored in the Nonvolatile Memory (NVM) space of the microcontroller. If a packet is received from an unknown transmitter, the message "KLQ: (serial number) Not Learned!" displays on the LCD as shown in Figure 2-3.

FIGURE 2-3: **ERROR MESSAGE OF RECEIVING PACKET FROM AN UNKNOWN TRANSMITTER**

To learn a transmitter, press the **SW4** button to make the receiver initiate the learning process. The message "Learn mode active" displays on the LCD, as shown in Figure 2-4.

FIGURE 2-4:   **START LEARN MODE**

If the received packet is from a known transmitter, the NVM remains untouched. If a relearn is performed to resynchronize the hop counter of a transmitter, the NVM must be erased first. If no KEELOQ Classic packet from an unknown transmitter is received within 18 seconds, the KEELOQ Classic Learn mode timeouts and displays the message "Learn mode timeout" on the LCD as shown in Figure 2-5.

FIGURE 2-5:   **LEARN MODE TIMEOUT**

When all slots in the NVM space for transmitters are taken, the learning process fail. Press and hold **SW4** button for about ten seconds to erase all transmitter records from the NVM. The message "Memory Erased" displays on the LCD as shown in Figure 2-6. After erasing records from the NVM, reset the board by removing and reinserting J6.

FIGURE 2-6:   **ERASE TRANSMITTER RECORDS FROM MEMORY**

When a KEELOQ Classic packet is received from a known transmitter, the contents of the packet displays on the LCD as shown in Figure 2-7. The LED D7 flashes during a valid packet reception.

Figure 2-7 shows the following information from a sample KEELOQ Classic packet:

- Encoder: KLQ representing KEELOQ Classic
- Serial number of the transmitter: a 28-bit serial number
- Counter (C): a 16-bit number
- Function Code (F): a bitmap of the pressed buttons on the key fob. Number 3 displays if both KLQ buttons (1 and 2) are pressed.

FIGURE 2-7:   KEELOQ® PACKET INFORMATION

2.5.2.2   KEELOQ® AES

For KEELOQ AES, it is *not* required that a transmitter must be known to the receiver before a packet can be accepted. Therefore, there is no learning process for a packet encoded with KEELOQ AES cipher. When a KEELOQ AES packet is received, the content of the packet displays on the LCD as shown in Figure 2-8. The LED D7 flashes during a valid packet reception.

Figure 2-8 shows the following information from a sample KEELOQ AES packet:

- Encoder: AES representing KEELOQ AES
- Serial number of the transmitter: a 32-bit serial number
- Counter (C): a 32-bit counter
- Function Code (F): a bitmap of the pressed buttons, depending on the button pressed on the key fob.

FIGURE 2-8:   KEELOQ® AES PACKET INFORMATION

2.6   EMBEDDED SECURITY DEVELOPMENT BOARD HARDWARE SELF-CHECK

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

To initiate the hardware self-check, press and hold the **SW1** button before powering up the Embedded Security Development Board. Release the **SW1** button only when the message "HDW Self Tests" displays on the LCD screen.

The four individual hardware self-tests are performed in the following sequence:

2.6.1   Button Test

"Button Test" displays in the first line of the LCD display, while the test instructions are displayed in the second line.

Once the required button is pressed, the test instruction message changes for the next push button. Once all buttons have been tested, press **SW1** button to move forward to the LED test.

2.6.2   LED Tests

When the LED tests start, the message "LEDs Flashing" displays in the first line of the LCD display. During the tests, the two sets of LEDs are flashing separately, while LEDs from the same set must be flashing together at roughly one second intervals. Once the user verifies the LED test, press **SW1** button to move forward to the Real-Time Clock and Calendar (RTCC) test.

2.6.3   RTCC Test

When RTCC test is initiated, the LCD display shows the clock and the calendar. If there is no coin battery installed for RTCC, the time displayed is close to the reset time of January 1, 2012. If a coin battery for RTCC is installed, the time displayed is based on the previously set time, plus the time that has passed. Observe that the clock shows the time in advance. Once the RTCC test is done, press **SW1** button to move forward to the SPI test.

2.6.4   SPI Test

The SPI test in hardware self-check is performed on the SPI bus that connects the target application microcontroller and the SX1239 Receiver PICtail Daughter Board. Therefore, the SX1239 Receiver PICtail Daughter Board must be plugged in before starting the test. Once the SPI test starts, the target application microcontroller requests specific information from the SX1239 receiver through the SPI bus. The "Successful" status displays if the expected response is received. Otherwise, expect the "Fail" status message.

Note: If a PICtail daughter board other than the SX1239 Receiver PICtail Daughter Board is plugged into the PICtail connector, the SPI bus may still work, but the SPI test may show a failure status. It is due to the expected values to be received specifically from the SX1239.

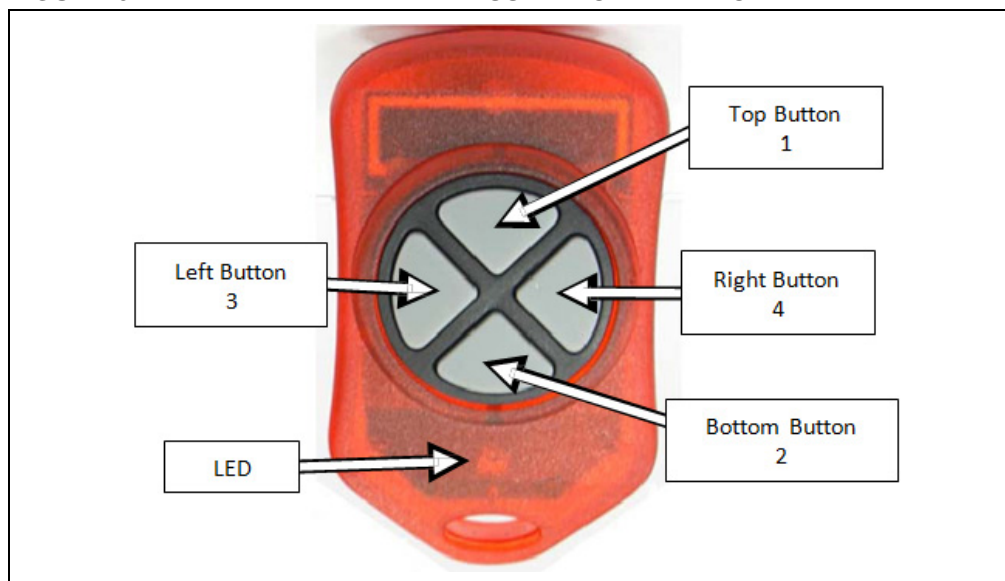# Chapter 3. MICRF114 Wireless Remote Key Fob

3.1   INTRODUCTION

The MICRF114 Wireless Remote Key Fob is a demonstration and development platform for wireless security remote control applications. This chapter provides a detailed description of the key fob.

3.2   HARDWARE DESCRIPTION

Figure 3-1 shows the key fob. The enclosure is an off-the-shelf key fob from Polycase (http://www.polycase.com/). The enclosure houses a two-sided PCB.

 Appendix A. "MICRF114 Wireless Remote Key Fob Schematics" provides the PCB layout, schematic, and Bill of Materials (BOM).

FIGURE 3-1:   **MICRF114 WIRELESS REMOTE KEY FOB**

3.3   PCB DESCRIPTION

The key fob PCB is a two layer, plated through hole, 1/24 inches (1 millimeter) thick, FR4 material. Figure 3-2 and Figure 3-3 show the top and the bottom view of the PCB. All components, except the coin battery, are on the top side. These components are the PCB antenna, conductive push button footprints (SW1-SW4), LED (LD1), MICRF114 transmitter (IC1), RF matching network (C5-C8, L1-L3), and PIC12LF1840 microcontroller. A PCB antenna is used in the design for reduced cost and compactness. Refer to **Section 3.4 "PCB Antenna Description"** for more information on the PCB antenna. An ICSP™ Programming Capability is also available on the board.

Refer to **Chapter 6."Wireless Security Remote Control Development Kit"** for suggestions on developing and programming the key fob.

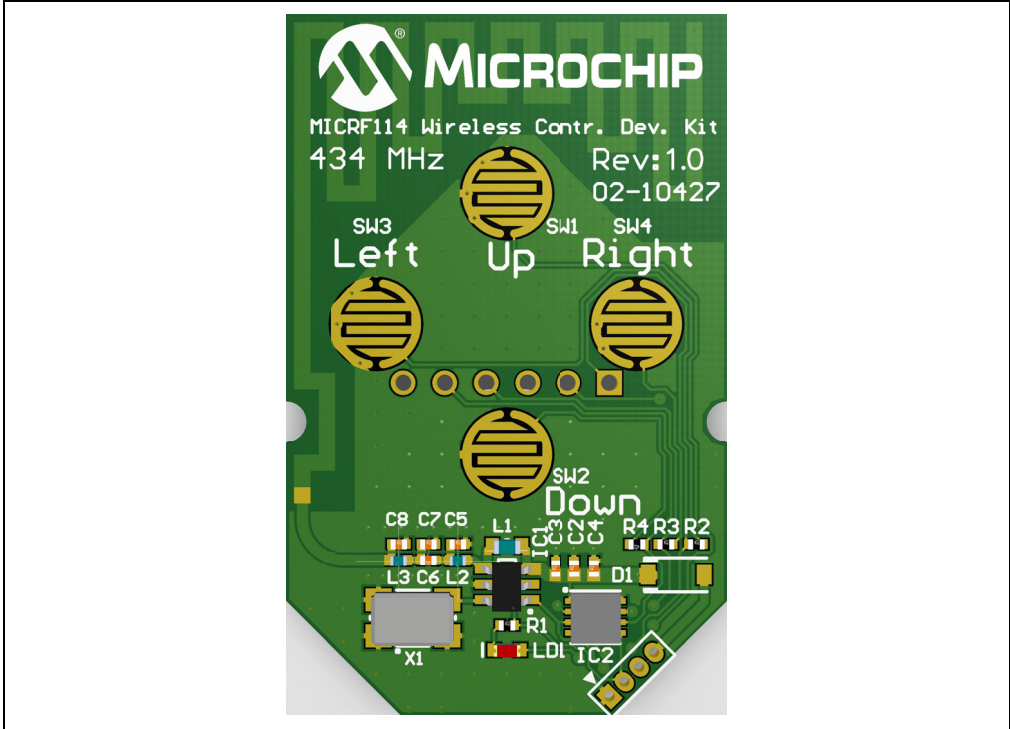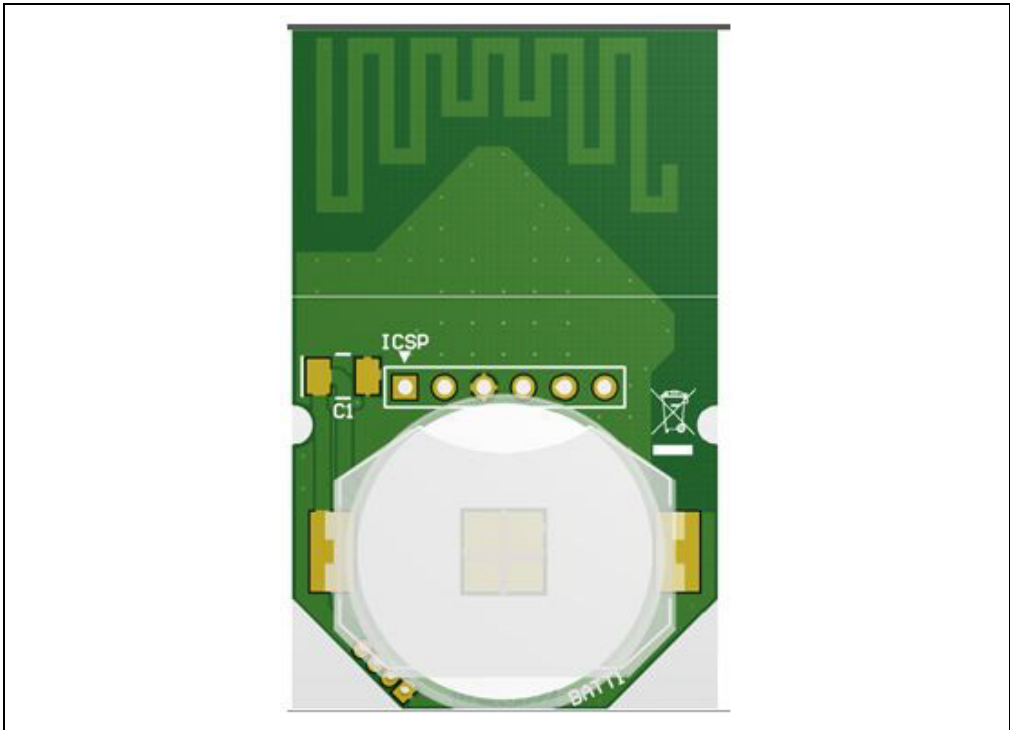**FIGURE 3-2:** **PCB TOP SIDE**
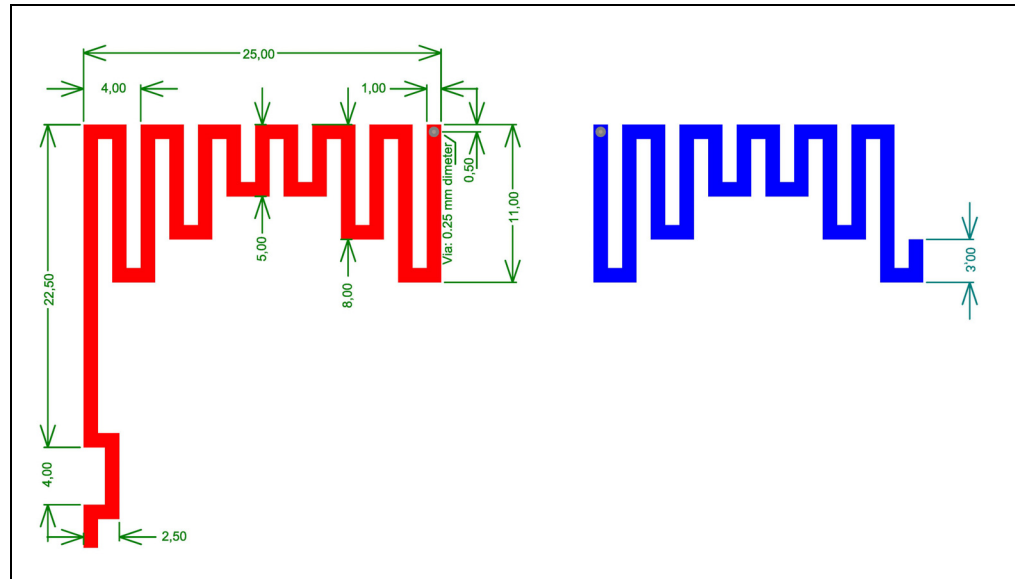

FIGURE 3-3: **PCB BOTTOM SIDE**

3.4   PCB ANTENNA DESCRIPTION

The on-board antenna of the key fob is a meander shaped PCB antenna in which impedance and resonant frequency are determined by electromagnetic (EM) simulations and laboratory fine tuning. This design leads to a modest antenna gain (about -18 dBi), which is usual in the case of small PCB sizes. On the other hand, it does *not* require any external impedance matching component as the impedance of the antenna are set to 50 ohms by simulation and fine tuning.

The designer is cautioned that although this design is constructed to be ETSI/FCC certifiable, the final product may require fine tuning. It is the responsibility of the designer to ensure that the final design satisfies ETSI or FCC recommendations, or both. There are some factors that determine the performance of a PCB antenna, such as the thickness of the copper layers, thickness of the PCB material, choice of PCB material (FR4 as an example), and choice of passive components used.

Figure 3-4 shows the used antenna dimensions on both top copper and bottom copper layers.

FIGURE 3-4:   PCB ANTENNA DIMENSIONS

NOTES:

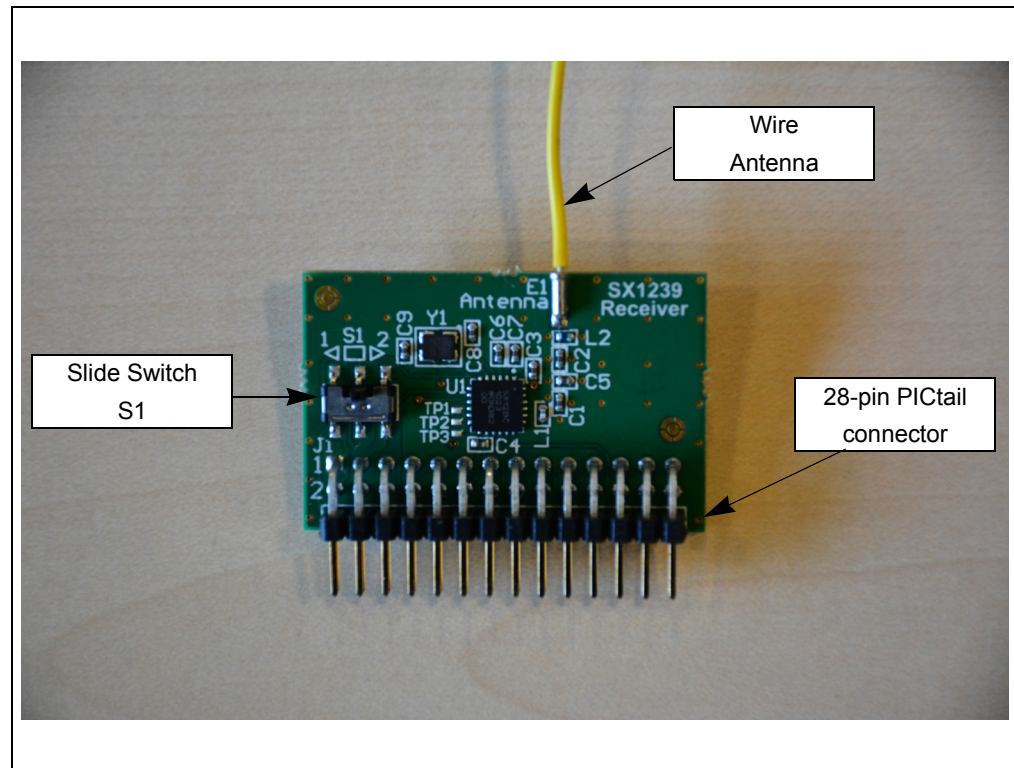# Chapter 4. SX1239 Receiver PICtail™ Daughter Board

4.1   INTRODUCTION

The SX1239 Receiver PICtail Daughter Board is a demonstration and development platform for wireless security remote control applications. This chapter provides a detailed description of the receiver daughter board.

4.2   HARDWARE DESCRIPTION

Figure 4-1 shows the SX1239 Receiver PICtail Daughter Board.

Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics" provides the PCB layout, schematic, and BOM.

FIGURE 4-1:   SX1239 RECEIVER PICtail™ DAUGHTER BOARD

The daughter board features the SX1239 Low-Power Integrated UHF Receiver (http://www.semtech.com/wireless-rf/rf-receivers/sx1239/).The PICtail daughter board can be plugged into the 28-pin PICtail connector featured on many Microchip development tools.

The antenna connection has a pin socket for plugging in a wire antenna. This demonstrates a simple and low-cost antenna option. The length of the antenna must be approximately 1/4 wavelength of the frequency of interest.

If a whip or sleeve dipole antenna having an SMA connector must be used instead of the wire antenna, the antenna pin can be replaced with a mating SMA socket by removing the wire antenna pin and using the SMA footprint on the same place.

Chapter 5. Embedded Security Development Board

5.1   INTRODUCTION

The Embedded Security Development Board provides a demonstration and development environment for security and authentication products. This chapter provides a detailed description of the development board. **Appendix C. "Embedded Security Development Board Schematics"** provides the PCB layout, schematic, and BOM.

The Embedded Security Development Board has the following main blocks as represented in Figure 5-1:

1. Target Application (Master) microcontroller (U4)
2. Host (Slave) microcontroller (U1)
3. Serial Accessory Port (P20)
4. USB Interface Port (J3)
5. PICtail connector (J1)
6. 16x2 character LCD display (LCD1)
7. Real-Time Clock and Calendar (RTCC) module (U5)
8. Push Buttons (SW1-SW4 and SW5-SW8)
9. LEDs (D4-D7)
10. Voltage Regulator (U3)
11. ICSP Programming Ports (J4 for Host and J5 for Target Application)
12. MCP2200 USB to UART communications IC (U2)

FIGURE 5-1:   EMBEDDED SECURITY DEVELOPMENT BOARD