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.

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in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates.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 unless otherwise stated.

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

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, motorBench, 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 trademark 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.

ISBN: 978-1-5224-0030-1

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: 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
Derek Carlson
VP Development Tools

12-Sep-14
Date

NOTES:

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.

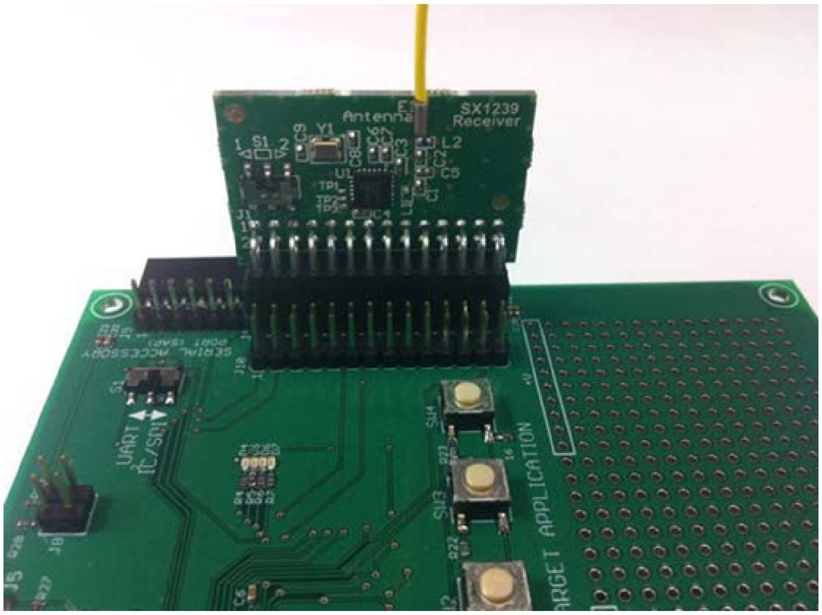
For additional information related to the demo, visit the MICRF114 product web page at www.microchip.com/MICRF114.

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, connect 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 +VEXT 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 $\overline{\text{MCLR}}$ 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.

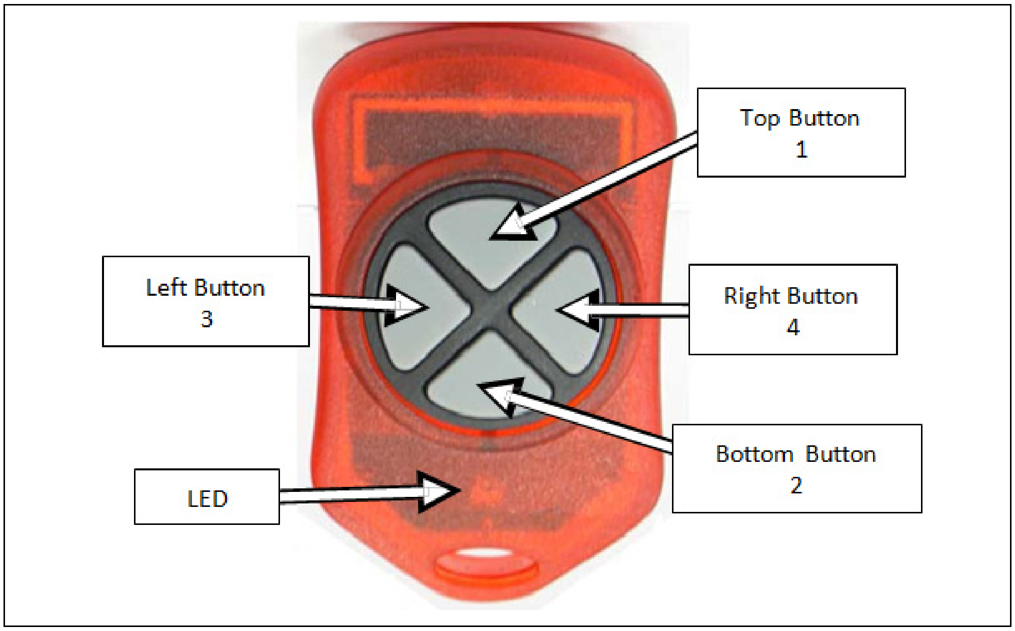
2.5.1 Key Fob as a Transmitter

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 flashing. 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



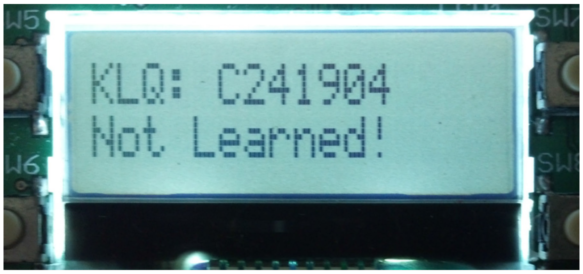
2.5.2 Embedded Security Development Board as a Receiver

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

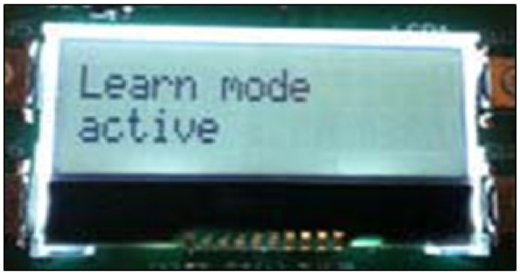
For KEELOQ Classic, the receiver accepts messages only from a known transmitter. The known transmitters and their latest counters are stored in the Nonvolatile Memory (NVM) space of the microcontroller. If a packet is received from an unknown transmitter, the message “KLQ: (serial number) Not Learned!”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

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


KLQ: C241904
Not Learned!

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.

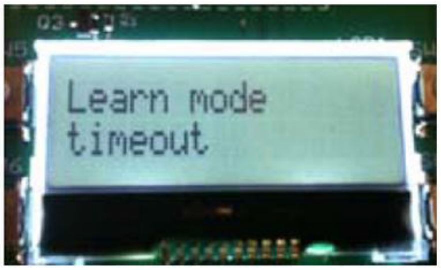
FIGURE 2-4: START LEARN MODE



Learn mode
active

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.

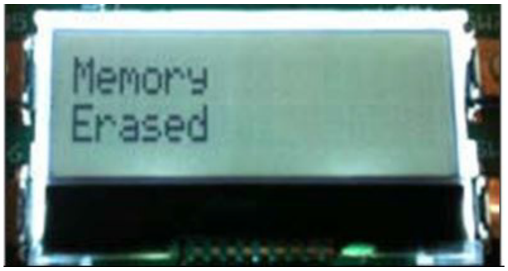
FIGURE 2-5: LEARN MODE TIMEOUT



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



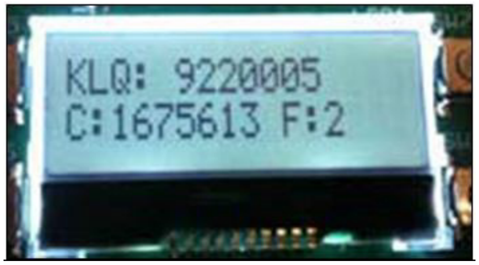
Memory
Erased

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



```
KLQ: 9220005
C:1675613 F:2
```

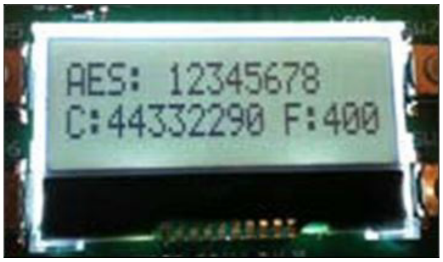
2.5.2.2 KEELOQ® AES

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



```
AES: 12345678
C:44332290 F:400
```

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

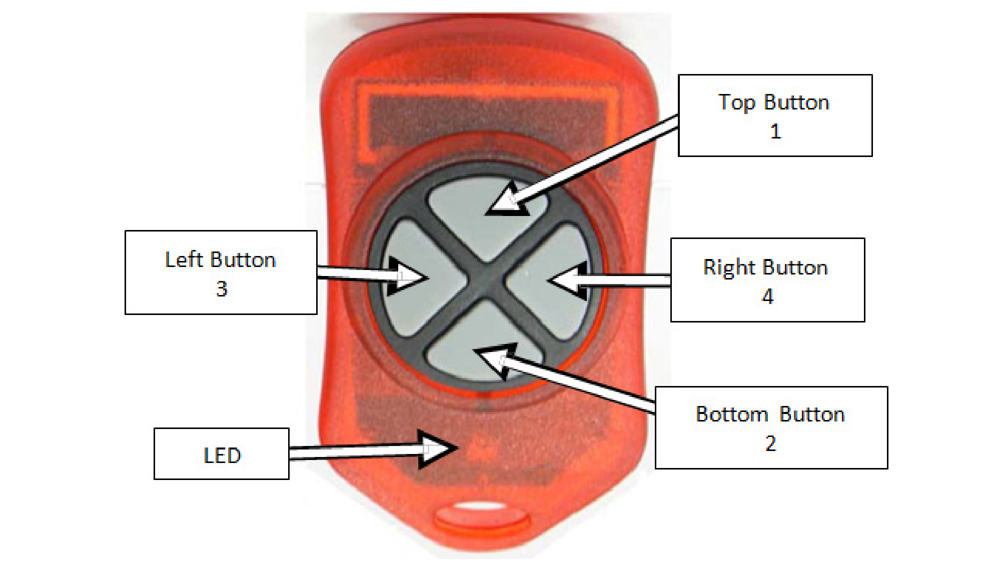
The MICRF114 Wireless Remote Key Fob is a demonstration and development platform for wireless security remote control applications. This chapter provides a detailed description of the key fob.

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

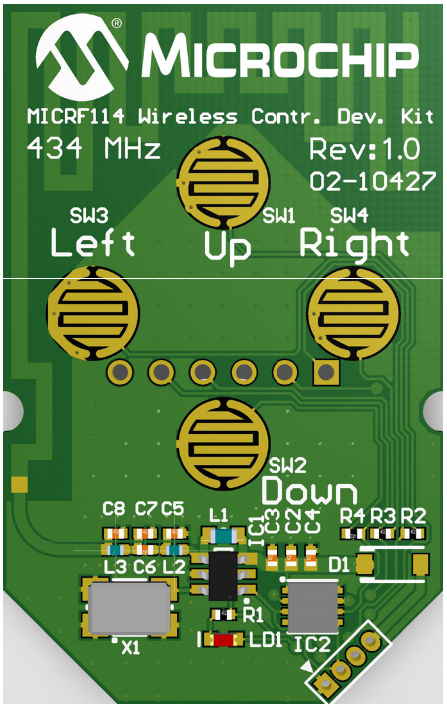
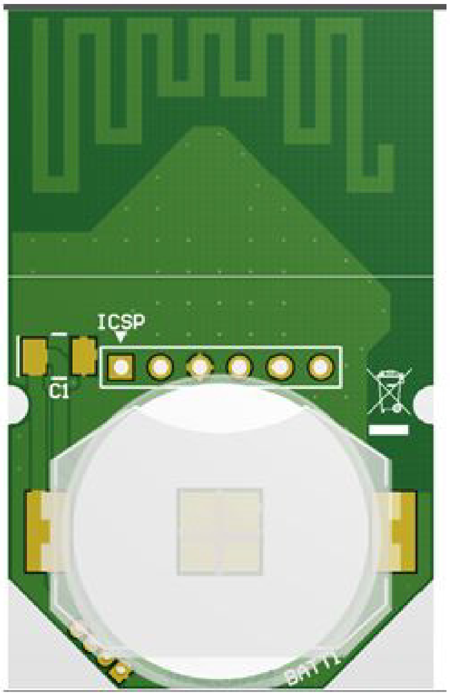


FIGURE 3-3: PCB BOTTOM SIDE



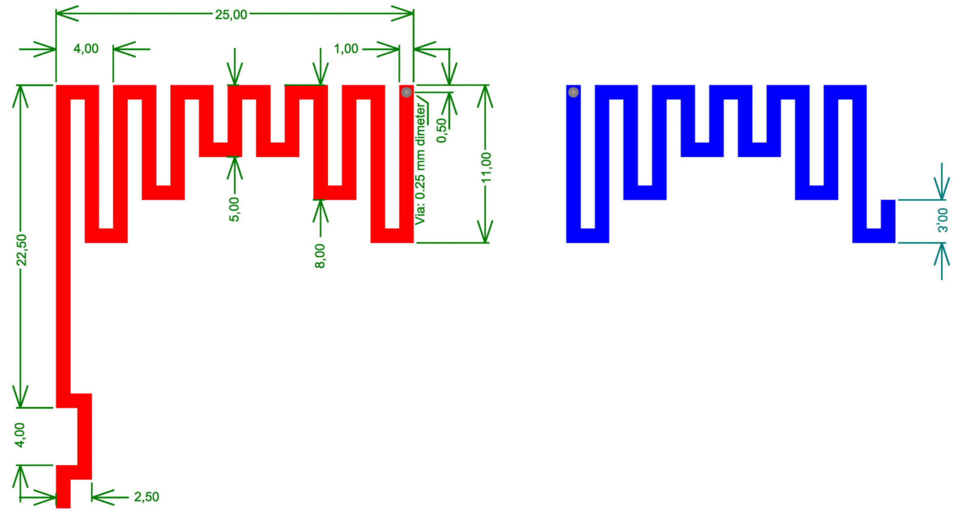
3.4 PCB ANTENNA DESCRIPTION

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

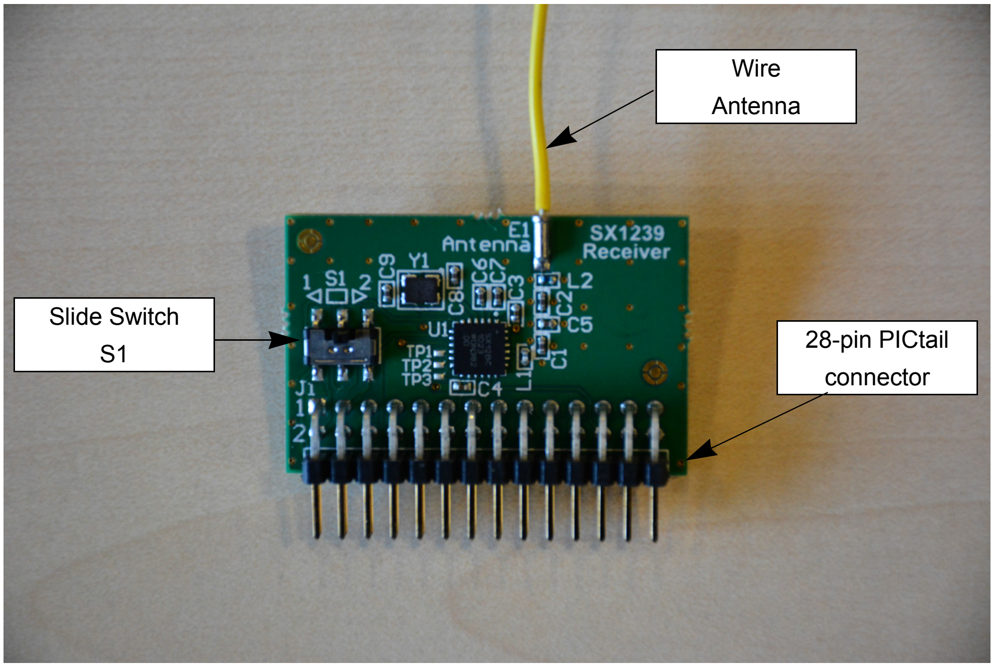
The SX1239 Receiver PICtail Daughter Board is a demonstration and development platform for wireless security remote control applications. This chapter provides a detailed description of the receiver daughter board.

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

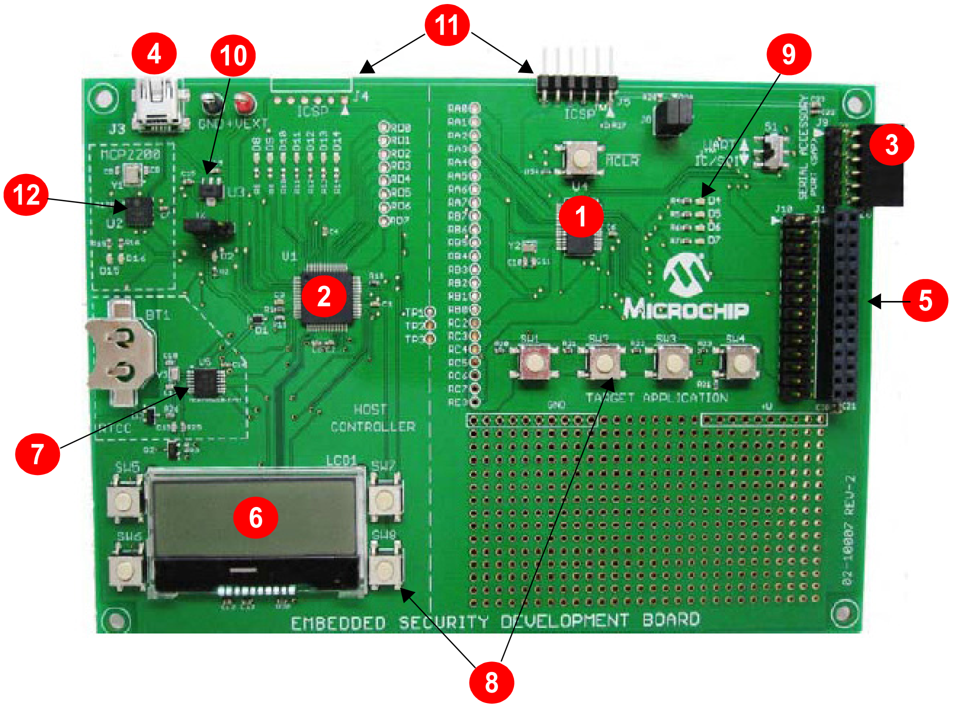
5.1 INTRODUCTION

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



5.2 HARDWARE DESCRIPTION

5.2.1 Serial Communications Connections

The Embedded Security Development Board is divided into two sections. The left section is the host controller and the right section is the target application. The two sections are connected by three wires labeled as TP1, TP2, and TP3. Table 5-1 lists the respective microcontroller I/O port connections.

TABLE 5-1: SERIAL COMMUNICATIONS CONNECTIONS

Host Controller PIC16LF1947 (Slave)	Test Points	Target Application PIC16LF1398 (Master)
RF5	TP1	RB7/ICSPDAT
RB2	TP2	RB6/ICSPCLK
RF4	TP3	RE3/$\overline{\text{MCLR}}$/VPP

The host controller section 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/debugged via the ICSP header (J4). The host controller section schematic is shown in Figure C-2 of **Appendix C. "Embedded Security Development Board Schematics"**.

The target application section has a PIC16LF1398 microcontroller. The PIC16LF1398 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 PIC16LF1398 microcontroller can be programmed/debugged via the ICSP header (J5). The target application section schematic is shown in Figure C-1 of **Appendix C. "Embedded Security Development Board Schematics"**.

5.2.2 Serial Accessory Port (P20)

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

- LCD Serial Accessory Board
- RS232 Serial Accessory Board

For more information on the available accessory boards, visit the Microchip website at www.microchip.com or refer to the *RS232 Serial Accessory Board User's Guide* (DS70649).

The Serial Accessory Port supports the following interfaces:

- 3- or 4-wire SPI
- I^{2}C
- USART

The on-board switch, S1, selects these interfaces. Jumpers J7 and J8 connect the pull-up resistors when I^{2}C is selected and the pull-up resistors are unavailable on the daughter board. Software modifications are expected to use those interfaces when different functionalities are assigned to the pins.

For more information on the port pin assignment, refer to the schematic in **Appendix C. "Embedded Security Development Board Schematics"**.

5.2.3 USB Interface Port

Microchip MCP2200 provides USB to UART support. MCP2200 provides automatic conversion between UART and a full-speed USB 2.0 communication. At the same time, the USB interface port can be used to directly power the Embedded Security Development Board. For more information, refer to the *MCP2200 Data Sheet* (DS22228).

5.2.4 PICtail Port

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

- 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 must also check the schematics before assigning functions to any port pin.

There are many Microchip accessory daughter boards with a PICtail port connectivity. When unused as one of the components in the Wireless Security Remote Control Development Kit, the Embedded Security Development Board can be connected to any daughter board with a PICtail port and perform different functionalities.

For more information on the accessory daughter boards with a PICtail port, refer to the Microchip website at www.microchip.com.

5.2.5 LCD Display

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

For more information on the LCD display, refer to the "*NHD-C0216CZ-FSW-FBW-3V3*" specification by Newhaven Display (http://www.newhavendisplay.com).

5.2.6 Real-Time Clock and Calendar (RTCC) Module

The Embedded Security Development Board RTCC module can be used to precisely set and track clock and calendar. The RTCC functionality is achieved with the Microchip MCP795W10 device. The RTCC module is controlled by the host microcontroller through the SPI interface. 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 unavailable.

For details on operating the RTCC module, refer to the *"MCP795W1X/MCP795W2X SPI RTCC with Enhanced Features and Battery Switchover Data Sheet"* (DS22280C) at http://www.microchip.com/MCP795W10.

5.2.7 Push Buttons

The Embedded Security Development Board has two sets of push buttons. Each set consists of four individual push buttons and serves as input to the host and target application microcontrollers.

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 resistor values, the input analog voltages to the master microcontroller are different. Therefore, the pressed button can be identified through the ADC on the target application microcontroller. Such design is used to save I/O pin requirement for the target application microcontroller.

For more information on the design of the push buttons, refer to the schematics in **Appendix C. "Embedded Security Development Board Schematics"**.

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. All buttons are assigned to the individual interrupt lines of the microcontroller and are *not* driven by external pull-up circuitry to save on power consumption. The user software must enable the PORTB pull-ups of the microcontroller before evaluating the button state.

The **$\overline{\text{MCLR}}$** push button is connected to the RE3/$\overline{\text{MCLR}}$ pin of the target application microcontroller. The RE3/$\overline{\text{MCLR}}$ pin of the target application microcontroller is one of the SPI lines that control the host microcontroller. When the target application and host microcontrollers are interconnected, the RE3/$\overline{\text{MCLR}}$ pin of the target application microcontroller is configured to be a normal digital I/O pin. Therefore, the **$\overline{\text{MCLR}}$** push button is ineffective. However, if an SPI communication is *not* required between the target application and host microcontroller, the pin can be configured as Reset by using the **$\overline{\text{MCLR}}$** push button.

5.2.8 LEDs

There are two sets of LEDs controlled by the target application and 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 seven LEDs through digital output pins. The two sets of LEDs are useful in the demo or debugging process.

In addition, two LEDs, D15 and D16, on the left section of the Embedded Security Development Board are used to identify the TX and RX operation of the MCP2200. LED D2 indicates the power availability. These LEDs cannot be controlled by either the target application or the host microcontroller.

5.2.9 Power Supply

The Embedded Security Development Board is powered by one of these two sources:

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

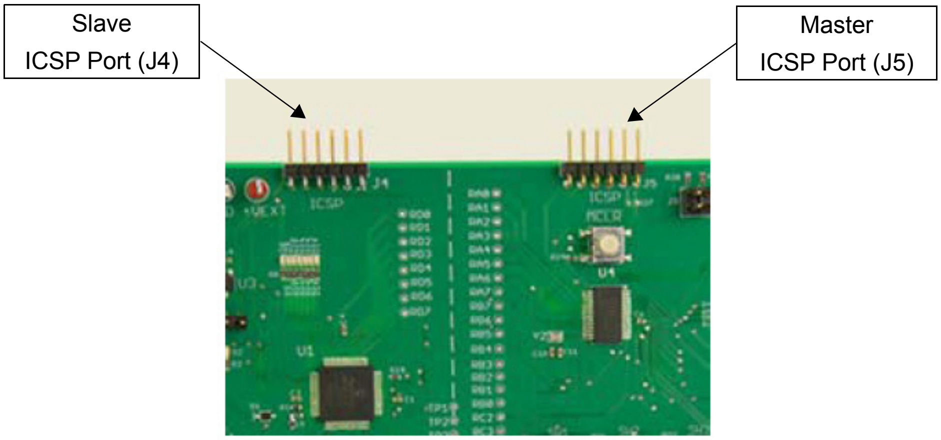
Set jumper J6 to pins 1-2 to power the Embedded Security Development Board from the USB port, and set J6 to pins 3-4 to power from an external power source.

When the USB port is used to power the board, the input voltage is stabilized by Microchip MCP1703, 250 mA, 3.3V, and low quiescent current LDO regulator (U3).

5.2.10 ICSP™ Programming Capability

Figure 5-2 shows that there are two ICSP programming/debugging ports on the Embedded Security Development Board. The ICSP port on the left side, J4, is used to program the host microcontroller. The ICSP port on the right, J5, is used to program the target application microcontroller.

FIGURE 5-2: ICSP PROGRAMMING/DEBUGGING PORTS



Note: J4 is *not* populated by default.

NOTES:

Chapter 6. Wireless Security Remote Control Development Kit

6.1 INTRODUCTION

This chapter provides recommendations regarding the development of an RKE solution on the Wireless Security Remote Control Development Kit. General design considerations are also provided for both the transmitter and receiver side.

6.2 DEVELOPING WITH THE KEY FOB AS TRANSMITTER

To modify the hex code in the key fob, the developer must open the red plastic enclosure. The ICSP port is available on the key fob PCB as six through-hole pads. The developer can access the MCU either by soldering a 6-pin header into the holes or by pushing the ICSP header in the ICSP through-hole pads. Slightly tilt and force the ICSP header to ensure proper connection and then start programming. Be careful as *not* to make short to the coin battery.

Note: When testing the key fob transmission with an open plastic enclosure, avoid touching the PCB area with your finger. For simplicity, all key fobs in the demo share the same serial number.

As a secured RKE system, KEELOQ® security keys, especially the manufacturer key is essential to the security of the whole system. It is highly recommended to use the code protection of the PIC® MCU memory.

The Microchip RKE demo uses pulse-width modulation (PWM), driven by interrupt, in data whitening procedure. The achievable transmission data rate over the air is tightly related to the operation speed of the microcontroller. Higher data rate requires faster processing speed. Higher transmission data rate may reduce the total active time for each transmission. However, higher microcontroller processing speed generally results in higher current consumption. The real application may need a compromise between higher data rate and faster processing speed to achieve optimal battery life.

6.3 DEVELOPING WITH THE EMBEDDED SECURITY DEVELOPMENT BOARD AS RECEIVER

The Embedded Security Development Board acts as a receiver in the Wireless Security Remote Control Development Kit. The target application microcontroller on the right side of the development board is the driving host for the receiver. All data receiving and KEELOQ security functionalities are performed by the target application microcontroller. On the other hand, the host microcontroller is mainly used to drive the LCD display in this demo.

If the developer decides to develop the application only on the target application microcontroller, intercommunication between the target application and the host microcontroller can be ignored. The prototyping area under the four push buttons of the target application controller can be used to prototype the application.

Similar to the transmitter, when Continuous mode is used to receive data, the data rate is tightly associated with the processing speed of the microcontroller. Unlike the transmitter, which is usually powered by battery, the receiving side is usually powered by main power, and power consumption is of less concern. It is possible to run the microcontroller faster to achieve higher data rate.

On the other hand, if the developer also decides to use the host microcontroller, then the intercommunication between the two microcontrollers may need attention. The host microcontroller is an SPI slave, and thus requires a faster response to the SPI command. Generally, if no SPI delay is applied by the target application controller side, the operation speed of the host microcontroller must double the speed of the target application microcontroller.

Normally, the $\overline{\mathbf{MCLR}}$ button is *not* functioning as a **Reset** button due to the RE3/$\overline{\text{MCLR}}$ pin is configured as a general-purpose input and is used for the Master-Slave communication. To debug the application, the Reset functionality must be enabled by modifying the appropriate Configuration bit and installing R27. In this case, communication between the Master and the Slave MCUs is lost.

Appendix A. MICRF114 Wireless Remote Key Fob Schematics

A.1 INTRODUCTION

This appendix provides the following information:

- Key Fob PCB Assembly top and bottom silkscreen (Figure A-1 and Figure A-2)
- Key Fob PCB Assembly top and bottom copper (Figure A-3 and Figure A-4)
- MICRF114 Wireless Remote Key Fob Schematic (Figure A-5)
- Key Fob Bill of Materials (BOM) (Table A-1.)

FIGURE A-1: KEY FOB PCB ASSEMBLY - TOP SILKSCREEN

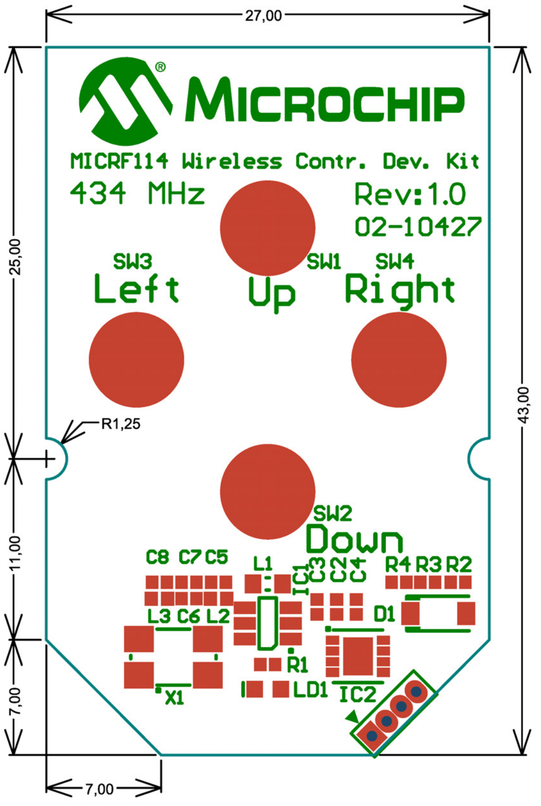


FIGURE A-2: KEY FOB PCB ASSEMBLY – BOTTOM SILKSCREEN

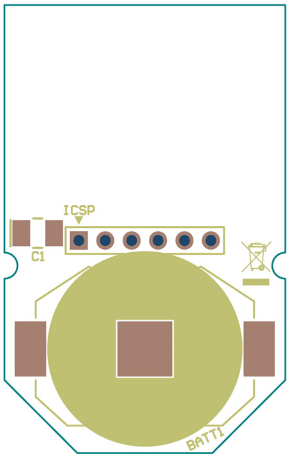


FIGURE A-3: KEY FOB PCB ASSEMBLY - TOP COPPER

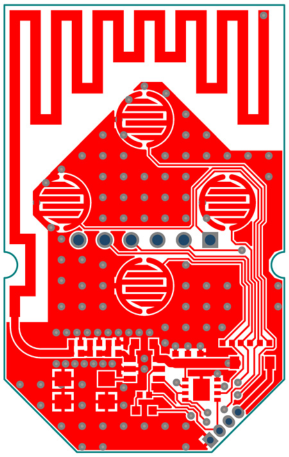


FIGURE A-4: KEY FOB PCB ASSEMBLY - BOTTOM COPPER

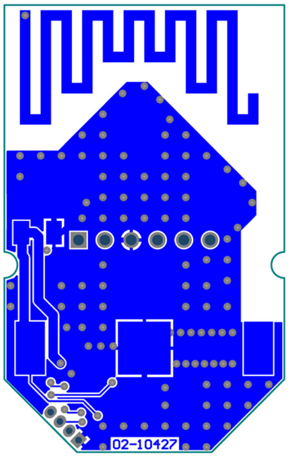


FIGURE A-5: MICRF114 WIRELESS REMOTE KEY FOB SCHEMATIC

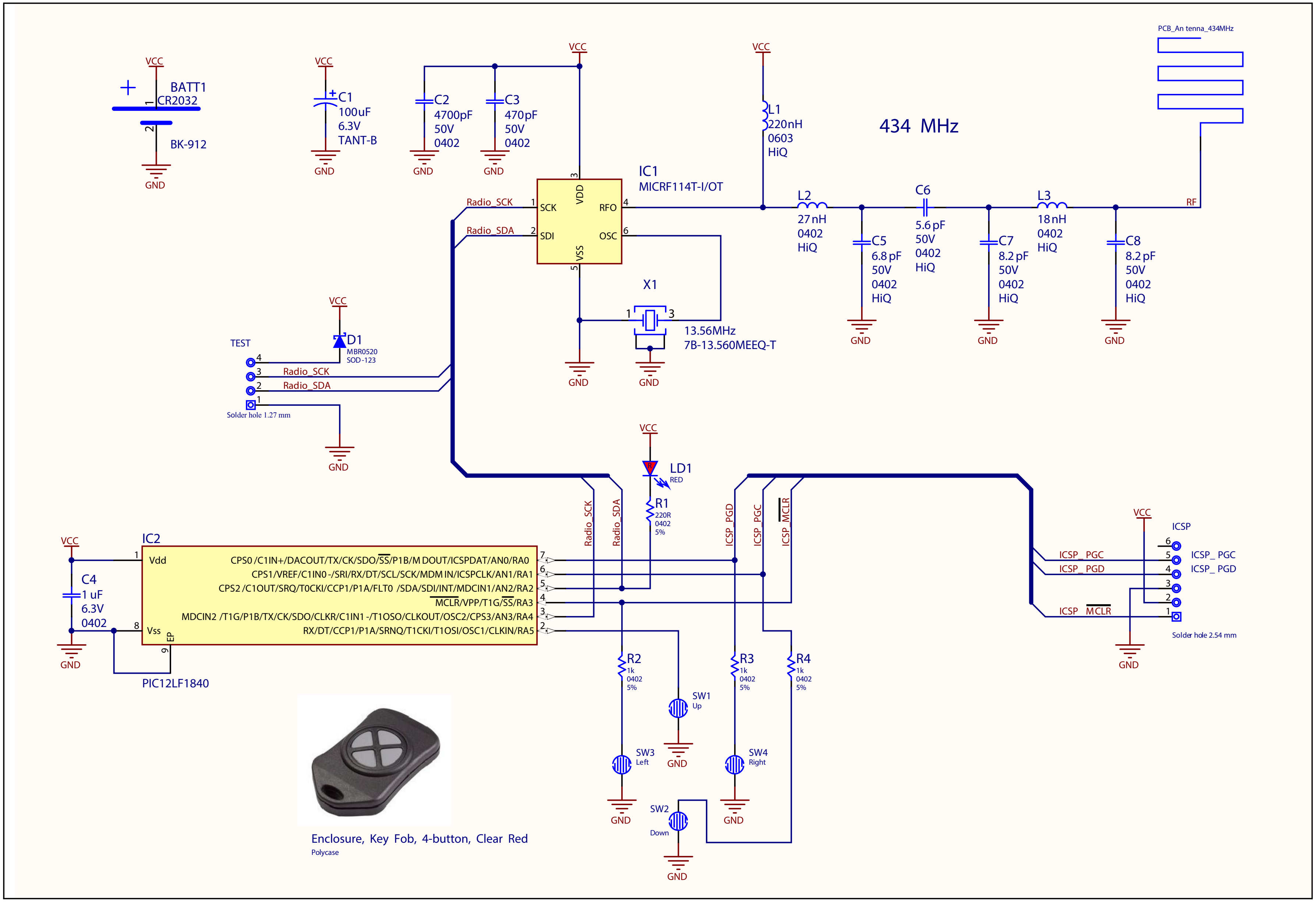


TABLE A-1: KEY FOB BOM

Qty	Designator	Value	Description	Manufacturer	Manufacturer Part Number
1	BT1	—	Holder Coin Cell 20 mm SMD	Memory Protection Devices	BK-912
1	@BT1	—	Battery Lithium Coin 3V 20 mm	Panasonic - BSG	CR2032
1	C1	100 µF Do Not Populate	Capacitor, Tantalum, 6.3V, +/-10%, SMT 1210	AVX Corporation	TPSB107K006R0400
1	C2	4.7 nF	Capacitor, Ceramic, 50V, +/-10%, X7R, SMT	Murata Electronics North America	GRM155R71H472KA01J
1	C3	470 pF	Capacitor, Ceramic, 50V, +/-10%, NP0, SMT	Murata Electronics North America	GRM1555C1H471JA01D
1	C4	1 µF	Capacitor, Ceramic, 50V, +/-10%, X5R, SMT	Murata Electronics North America	GRM155R60J105KE19D
1	LD1	Red	Diode, Light Emitting, Red, Clear	Kingbright	APTD1608SURCK
1	D1	MBR0520LT1G Do Not Populate	Diode, Schottky, 20V, 500 mA, SMT SOD123	On Semiconductor	MBR0520LT1G
1	R1	220Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-07220RL
3	R2, R3, R4	1 kΩ	Resistor, 5%, ±100 ppm/C, SMT 0402	Panasonic Electronic Components	ERJ-2GEJ102X
1	enclosure	—	Enclosure, Key Fob, 4-button, Clear Red	Polycase	FB-20-4*9
1	IC1	MICRF114T-I/OT	IC RF MICRF114T-I-OT Sub GHz transmitter SOT 23-6	Microchip Technology Inc.	MICRF114T-I/OT
1	IC2	PIC12LF1840T-I/MF	IC MCHP MCU 8-BIT 32 MHz 7 kB 256B DFN-8	Microchip Technology Inc.	PIC12LF1840T-I/MF
1	L1	220 nH	Inductor, Ceramic, ±5%,SMT 0603	Johanson Technology Inc.	L-14CR22JV4T
1	L2	5.6 nH	Inductor, Ceramic, ±5%,SMT 0402	Johanson Technology Inc.	L-07C27NJV6T
1	L3	18 nH	Inductor, Ceramic, ±5%,SMT 0402	Johanson Technology Inc.	L-07C18NJV6T
1	C5	6.8 pF	Capacitor, Ceramic, 50V 0.25 pF NP0 0402	Johanson Technology Inc.	500R07S6R8CV4T
1	C6	5.6 pF	Capacitor, Ceramic, 50V 0.25 pF NP0 0402	Johanson Technology Inc.	500R07S5R6CV4T
2	C7, C8	8.2 pF	Capacitor, Ceramic, 50V 0.25 pF NP0 0402	Johanson Technology Inc.	500R07S8R2CV4T
1	X1	13.56 MHz	CRYSTAL 13.56 MHz 10 pF SMD L5.2W3.5H0.9	TXC CORPORATION	7B-13.560MEEQ-T

Appendix B. SX1239 Receiver PICtail™ Daughter Board Schematics

B.1 INTRODUCTION

This appendix provides the following information:

- SX1239 Receiver PICtail™ Daughter Board PCB Assembly (Figure B-1)
- SX1239 Receiver PICtail Daughter Board Schematic (Figure B-2)
- SX1239 Receiver PICtail Daughter Board BOM (Table B-1)

FIGURE B-1: SX1239 RECEIVER PICtail™ DAUGHTER BOARD PCB ASSEMBLY

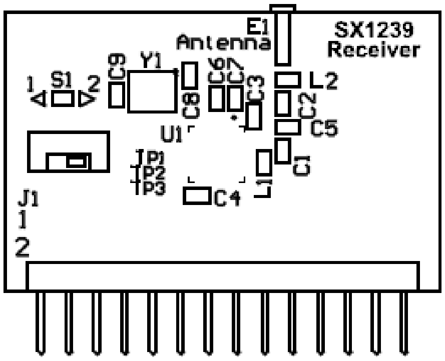


FIGURE B-2: SX1239 RECEIVER PICtail™ DAUGHTER BOARD SCHEMATIC

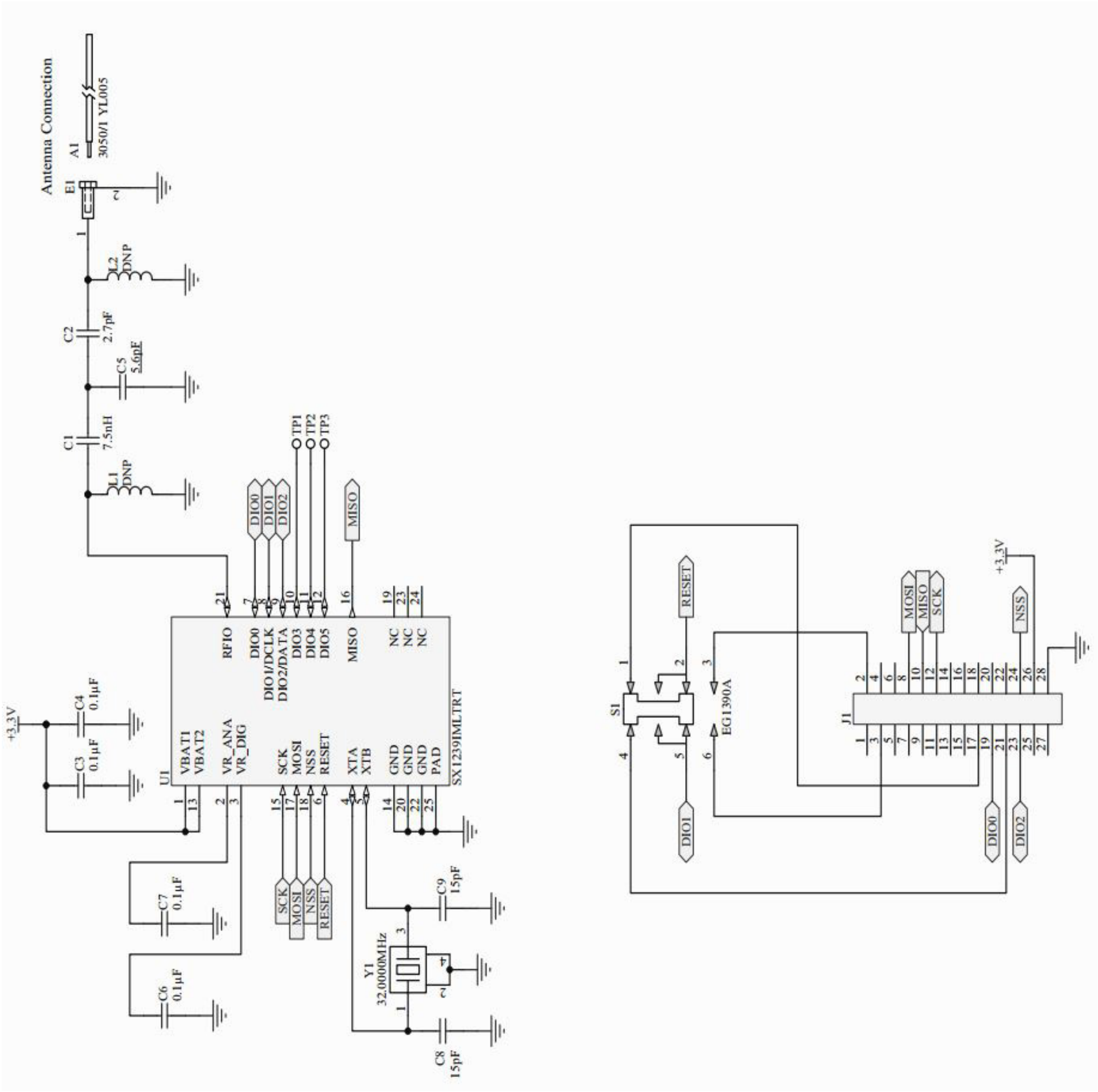


TABLE B-1: SX1239 RECEIVER PICtail™ DAUGHTER BOARD BOM

Band Select	Qty	Designator	Value	Description	Manufacturer	Manufacturer Part Number
Common	1	A1	—	Wire, 24AWG, Solid, PVC Insul, Yellow	Alpha Wire	3050/1 YL005
	1	C3, C4	0.1 µF	Cap, Ceramic, 0.1 µF, 16V +/-10% X7R	Murata Electronics North America	GRM155R71C104KA88D
	4	C6, C7, C8, C9	15 pF	Cap, Ceramic, 15 pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H150JZ01D
	1	E1	—	Pin Receptacle, .015/.025 Dia, 0667 Series	Mill-Max Manufacturing Corp.	0667-0-15-01-30-27-10-0
	1	J1	—	Terminal strip, 2X14, 0.100 sp, Rt Angle, 0.025 sq post	SAMTEC	TSW-114-08-F-D-RA
	1	S1	—	Switch, DPDT, Miniature Slide, Vert, SMD	E-Switch	EG1390A
	1	U1	—	RF Transceiver, 433/868/915 MHz, Low Power, QFN24	Microchip Technology Inc.	SX1239T - I/LY
	1	Y1	32 MHz	Crystal, 32.0000 MHz, 10 pF, SMD TXC Series 7M	TXC CORPORATION	7M-32.000MEEQ-T
	1	C2	1.2 pF	Cap, Ceramic, 1.2 pF, 50V +/-0.25 pF COG	Murata Electronics North America	GRM1555C1H1R2CZ01D
	1	L2	68 nH	Inductor, 68 nH, 140 mA, Air Core, 5%	Murata Electronics North America	LQW15AN68NJ00D
315/434 MHz	2	C1, C5	22 pF	Cap, Ceramic, 22 pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H220JZ01D
	1	L1	12 nH	Inductor, 12 nH, 500 mA, Air Core, 5%	Murata Electronics North America	LQG15HS12NJ02D
868/915 MHz	1	C1	4.7 pF	Cap, Ceramic, 4.7 pF, 50V	Murata Electronics North America	GRM1555C1H4R7CZ01D
	1	L1	13 nH	Inductor, 13 nH, 500 mA, Air Core, 5%	TDK Corporation	MLG1005S13NJ
	1	C5	3.6 pF	Cap, Ceramic, 3.6 pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H3R6CZ01D

Note: Designator A1 Wire Antenna: Cut to 6.75 inches Overall Length (OAL).

NOTES:

Appendix C. Embedded Security Development Board Schematics

C.1 INTRODUCTION

This appendix provides the following information:

- Embedded Security Development Board PCB Assembly (Figure C-1)
- Embedded Security Development Board Schematics (Figure C-2 and Figure C-3)
- Embedded Security Development Board BOM (Table C-1)

FIGURE C-1: EMBEDDED SECURITY DEVELOPMENT BOARD PCB ASSEMBLY

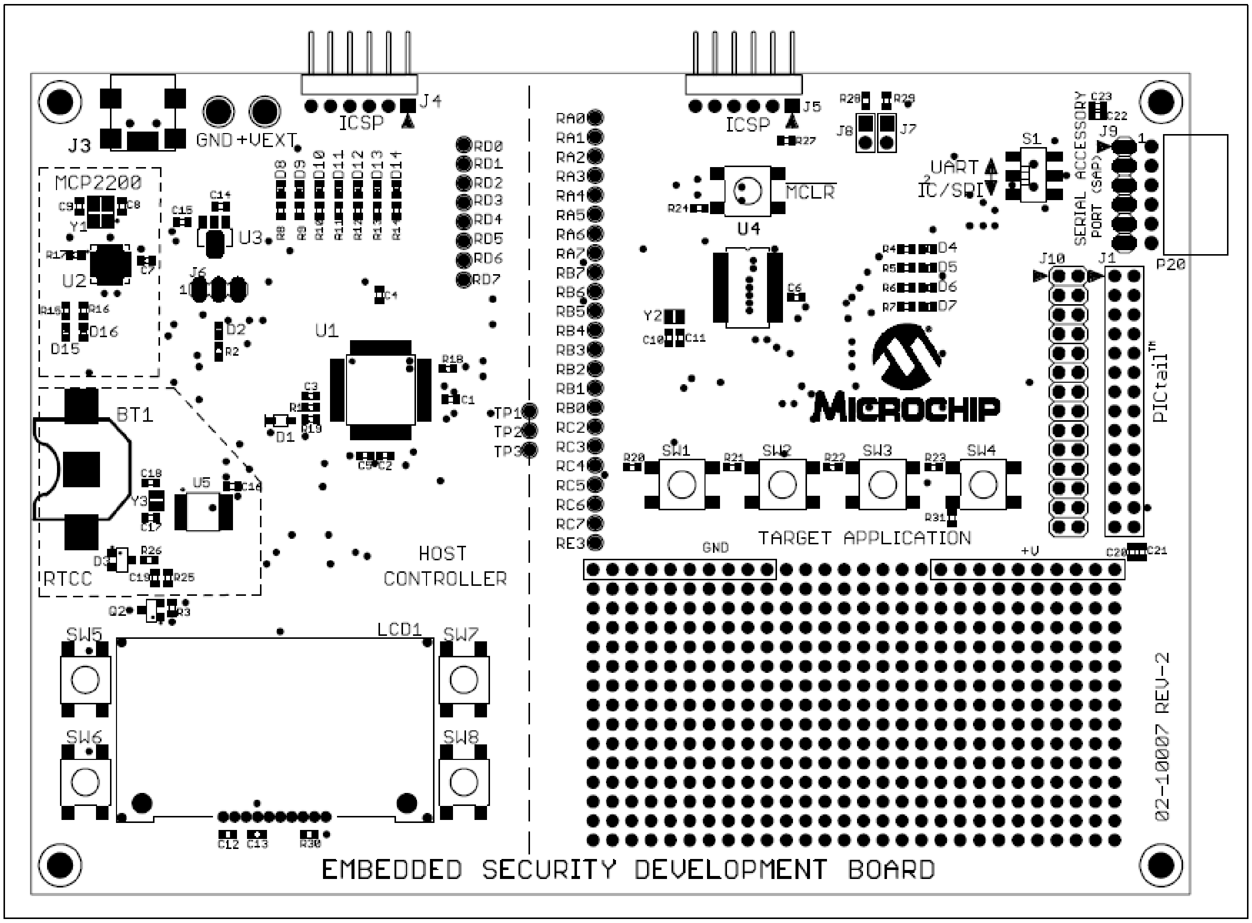


FIGURE C-2: EMBEDDED SECURITY DEVELOPMENT BOARD SCHEMATIC (1 OF 2)

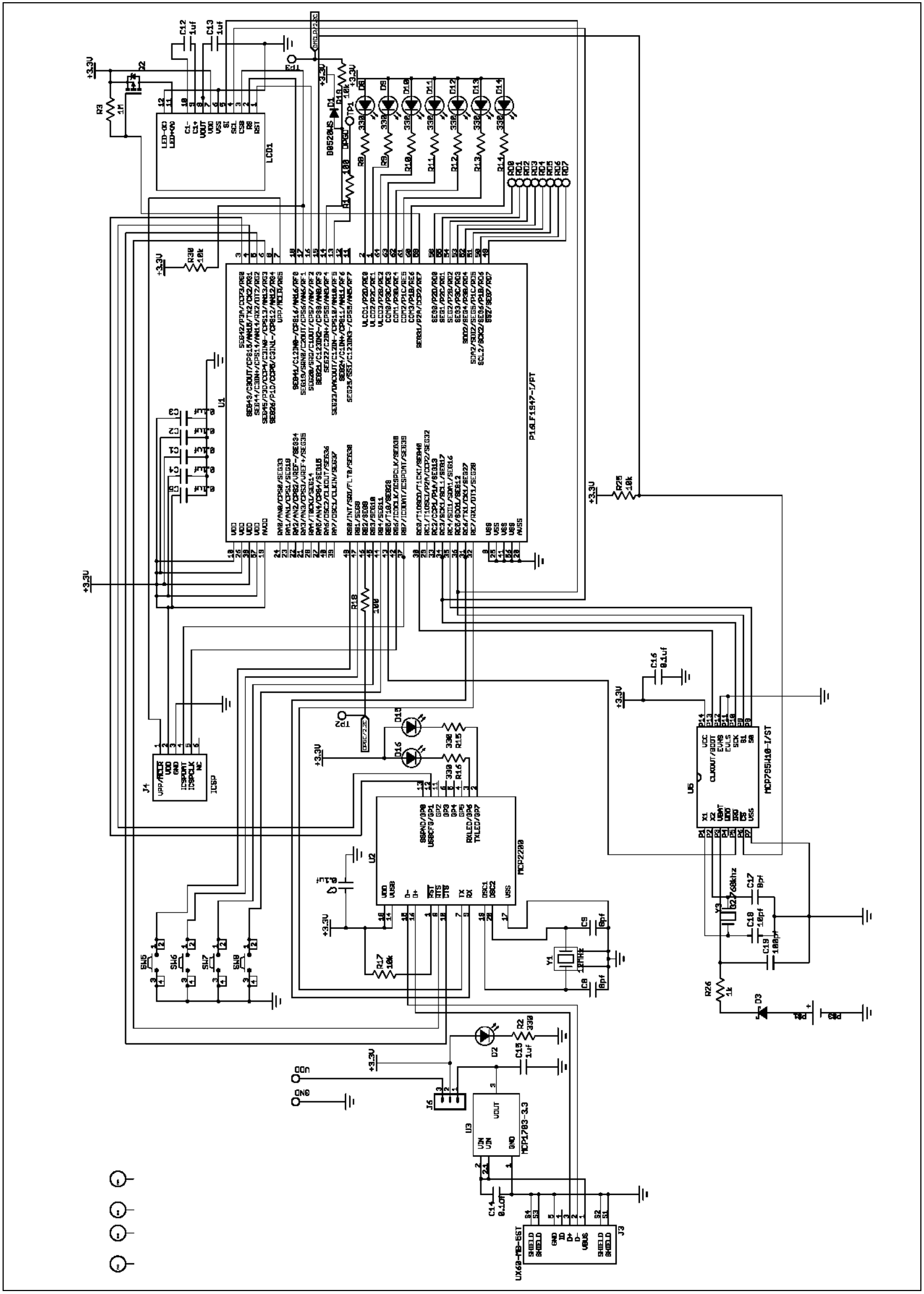


FIGURE C-3: EMBEDDED SECURITY DEVELOPMENT BOARD SCHEMATIC (2 OF 2)

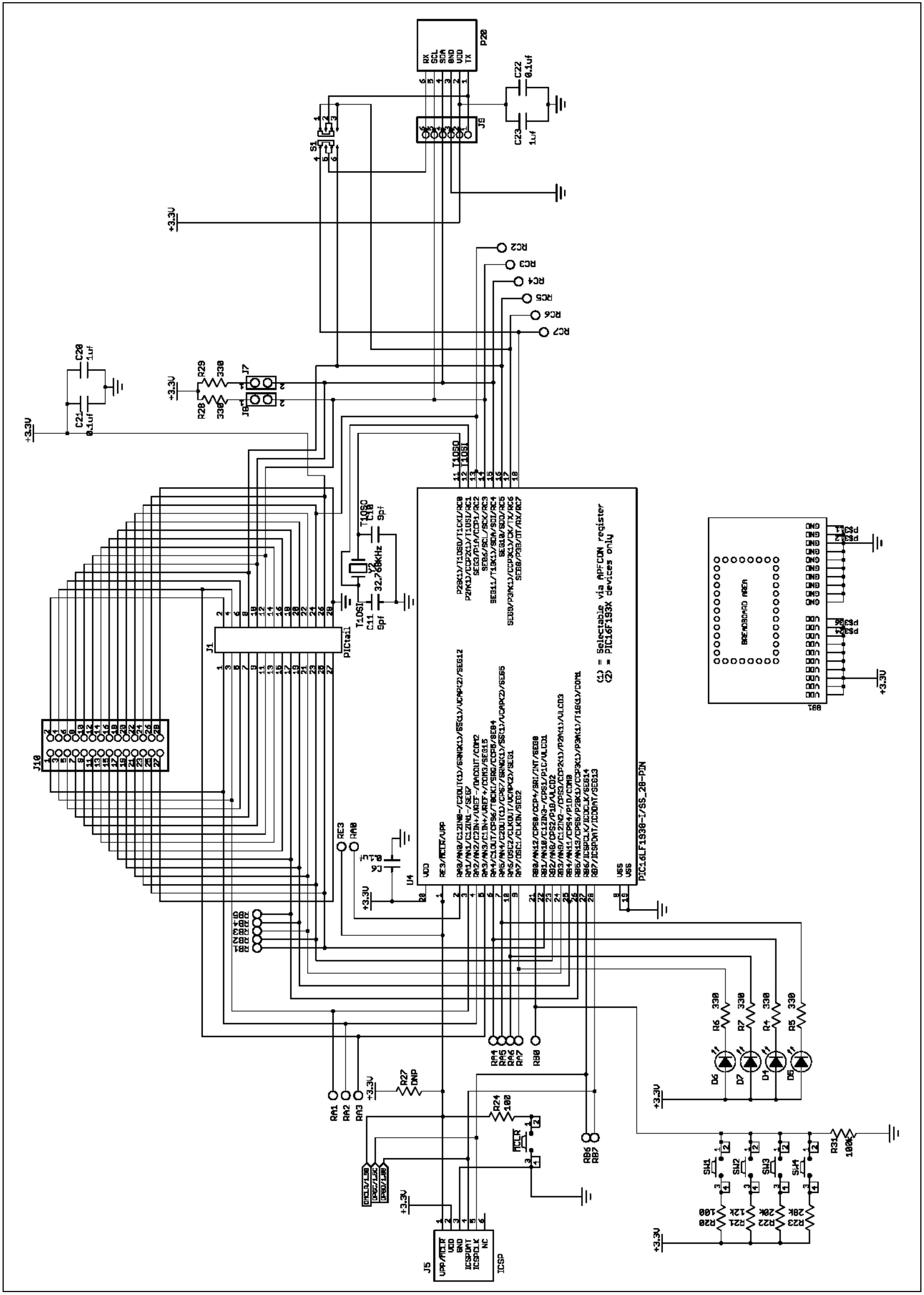


TABLE C-1: EMBEDDED SECURITY DEVELOPMENT BOARD BOM

Qty	Designator	Value	Manufacturer	Manufacturer Part Number
1	VDD	VDD	Keystone	5010
1	GND	GND	Keystone	5011
1	BT1	BK-885	MPD (Memory Protection Devices)	BK-885
3	C8, C9, C17	8 pF	TDK Corporation	C1608C0G1H080D
2	C10, C11	9 pF	TDK Corporation	C1608C0G1H090D
1	C18	10 pF	TDK Corporation	C1608C0G1H100D
1	C19	100 pF	TDK Corporation	C1608C0G1H101J
11	C1-C7, C14, C16, C21, C22	0.1 µF	Murata Electronics North America	GRM188R71E104KA01D
5	C12, C13, C15, C20, C23	1 µF	Murata Electronics North America	GRM188R61A105MA61D
1	D1	B0520WS	Diodes Inc.	B0520WS-7-F
1	D3	BAT54	Fairchild Semiconductor	BAT54
14	D2, D4-D16	LTST-C191GKT	Lite-On	LTST-C191GKT
1	J1	—	Sullins	PPPC142LFBN-RC
1	J3	UX60-MB-5ST	Hirose Electric Co Ltd	UX60-MB-5ST
1	J4	Do Not Populate	Sullins	PBC06SBAN
1	J5	—	Sullins	PBC06SBAN
1	J6	—	Sullins	PBC03SAAN
2	J7, J8	—	Sullins	PBC02DAAN
1	J9	—	Sullins	PBC06SAAN
1	J10	—	Sullins	PBC14DAAN
1	LCD1	C0216CZ-FSW-FBW-3V3	Newhaven Displays	C0216CZ-FSW-FBW-3V3
1	P20		Sullins	PPPC061LGBN-RC
1	Q2	IRLML6302TRPBF	International Rectifier	IRLML6302TRPBF
4	R1, R18, R20, R24	100Ω	Stackpole Electronics International	RMCF0603FT100R
16	R2, R4-R16, R28-R29	330Ω	Stackpole Electronics International	RMCF0603FT330R
1	R26	1 kΩ	Stackpole Electronics International	RMCF0603FT1K00
5	R17, R19, R25, R30	10 kΩ	Stackpole Electronics International	RMCF0603FT10K0
1	R27	10 kW Do Not Populate	Stackpole Electronics International	RMCF0603FT10K0
1	R21	12 kΩ	Stackpole Electronics International	RMCF0603FT12K0
1	R22	20 kΩ	Stackpole Electronics International	RMCF0603FT20K0
1	R23	28 kΩ	Stackpole Electronics International	RNCP0603FTD28K0
1	R31	100 kΩ	Stackpole Electronics International	RMCF0603FT100K
1	R3	1 MΩ	Stackpole Electronics International	RMCF0603FT1M00
1	S1	—	E-Switch	EG1390B
9	SW1-SW8, $\overline{\text{MCLR}}$	—	Omron	B3S-1000P
1	U1	P16LF1947-I/PT	Microchip Technology Inc.	PIC16LF1947-I/PT

TABLE C-1: EMBEDDED SECURITY DEVELOPMENT BOARD BOM (CONTINUED)

Qty	Designator	Value	Manufacturer	Manufacturer Part Number
1	U2	MCP2200	Microchip Technology Inc.	MCP2200-I/MQ
1	U3	MCP1703-3.3	Microchip Technology Inc.	MCP1703T-3302E/MB
1	U4	PIC16LF1938-I/SS_28-PIN	Microchip Technology Inc.	PIC16LF1938-I/SS
1	U5	MCP795W10-I/ST	Microchip Technology Inc.	MCP795W10-I/ST
1	Y1	12 MHz	NDK	NX3225SA-12.000000MHZ
2	Y2, Y3	32.768 kHz	Abracon	ABS06-32.768KHZ-T

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 - Dongguan
Tel: 86-769-8702-9880

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

ASIA/PACIFIC

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

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

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: 886-7-213-7828

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 - Karlsruhe
Tel: 49-721-625370

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

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

07/14/15