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.

Trademarks

ISBN: 9781620764145

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: 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 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

05-DEC-2011
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 web site (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 "DSXXXXXA", where "XXXXX" 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 Wireless Security Remote Control Development Kit User's Guide. Items discussed in this chapter include:

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

DOCUMENT LAYOUT

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

- **Chapter 1. "Overview"** – This chapter describes the WSRCDK and how it works.
- **Chapter 2. "Getting Started"** – This chapter describes the procedures to demonstrate Microchip KEELOQ RKE solution on WSRCDK.
- **Chapter 3. "PIC12LF1840T39A Wireless Remote Key Fob"** – This chapter provides the hardware details of the wireless key fob.
- **Chapter 4. "SX1239 Receiver PICtail™ Daughter Board"** – This chapter provides the hardware details of the Receiver PICtail Daughter Board.
- **Chapter 5. "Embedded Security Development Board"** – This chapter provides the hardware details of the Embedded Security Development Board.

- **Chapter 6. "Developing with the Wireless Security Remote Control Development Kit"** – This chapter provides suggestions on the development based on Microchip RKE solution.
- **Appendix A. "PIC12LF1840T39A Wireless Remote Key Fob Schematics"** – This appendix provides the PCB layout, BOM and schematics.
- **Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics"** – This appendix provides the PCB layout, BOM and schematics.
- **Appendix C. "Embedded Security Development Board Schematics"** – This appendix provides the PCB layout, BOM and 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) { ... }`

WARRANTY REGISTRATION

Please complete the enclosed Warranty Registration Card and mail it promptly. Sending in the Warranty Registration Card entitles users to receive new product updates. Interim software releases are available at the Microchip web site.

RECOMMENDED READING

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

Readme Files

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

Application Notes

There are several application notes available from Microchip that help in understanding Microchip KEELOQ applications. These include:

- AN1259 *"KEELOQ® Microcontroller-based Code Hopping Encoder"*
- AN1265 *"KEELOQ® with AES Microcontroller-based Code Hopping Encoder"*
- AN743 "*Modular PIC® Mid-Range MCU Code Hopping Decoder*"
- AN745 "*Modular Mid-Range PIC® Decoder in C*"
- AN1275 "*KEELOQ® with AES Receiver/Decoder*"

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

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 web site 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, assemblers, linkers and other language tools. These include all MPLAB C compilers; all MPLAB assemblers (including MPASM™ assembler); all MPLAB linkers (including MPLINK™ object linker); and all MPLAB librarians (including MPLIB™ object librarian).
- **Emulators** – The latest information on Microchip in-circuit emulators.This includes the MPLAB REAL ICE™ and MPLAB ICE 2000 in-circuit emulators.
- **In-Circuit Debuggers** – The latest information on the Microchip in-circuit debuggers. This includes MPLAB ICD 3 in-circuit debuggers and PICkit™ 3 debug express.
- **MPLAB® IDE** – The latest information on Microchip MPLAB IDE, the Windows® Integrated Development Environment for development systems tools. This list is focused on the MPLAB IDE, MPLAB IDE Project Manager, MPLAB Editor and MPLAB SIM simulator, as well as general editing and debugging features.
- **Programmers** – The latest information on Microchip programmers. These include production programmers such as MPLAB REAL ICE in-circuit emulator, MPLAB ICD 3 in-circuit debugger and MPLAB PM3 device programmers. Also included are nonproduction development programmers such as PICSTART® Plus and PICkit 2 and 3.

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://www.microchip.com/support.

REVISION HISTORY

Revision A (July 2012)

- Initial Release of this Document.

NOTES:

Chapter 1. Overview

1.1 INTRODUCTION

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

The kit contains a four-button key fob transmitter based on the PIC12LF1840T39A, SX1239 Receiver PICtail™ Daughter Board, and the Embedded Security Development Board. The kits can be purchased in one of three transmit frequencies. See the next section for ordering part numbers.

- Wireless Security Remote Control Development Kit Contents
- Getting Started

1.2 WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT CONTENTS

The Wireless Security Remote Control Development Kits have three frequency choices:

- Wireless Security Remote Control Development Kit – 433.92 MHz (DM182017-1)
- Wireless Security Remote Control Development Kit – 868 MHz (DM182017-2)
- Wireless Security Remote Control Development Kit – 915 MHz (DM182017-3)

Each kit contains:

- PIC12LF1840T39A Wireless Remote Key Fob (**Chapter 3. "PIC12LF1840T39A Wireless Remote Key Fob"**, **Appendix A**)
- SX1239 Receiver PICtail Daughter Board (**Chapter 4. "SX1239 Receiver PICtail™ Daughter Board"**, **Appendix B**)
- Embedded Security Development Board (**Chapter 5. "Embedded Security Development Board"**, **Appendix C**)
- USB Cable
- CR2032 Coin Cell Battery

1.3 GETTING STARTED

Chapter 2. "Getting Started" provides a getting started tutorial to familiarize users with the Wireless Security Remote Control Development Kit.

NOTES:

Chapter 2. Getting Started

2.1 INTRODUCTION

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

The following topics are discussed in this chapter:

- Hardware Requirements
- Software Requirements
- Demo Setup
- Demo Operation

2.2 HARDWARE REQUIREMENTS

The following hardware is required to run the pre-programmed demo application:

- PIC12LF1840T39A Wireless Remote Key Fob
- SX1239 Receiver PICtail™ Daughter Board
- Embedded Security Development Board
- USB A to Mini-B Cable (to power the Embedded Security Development Board or power can also be provided by a bench power supply)

2.3 SOFTWARE REQUIREMENTS

The PIC12LF1840T39A Key Fob and Embedded Security Development Board are pre-programmed with a remote control demo program. The demo setup and operation are explained in the following sections.

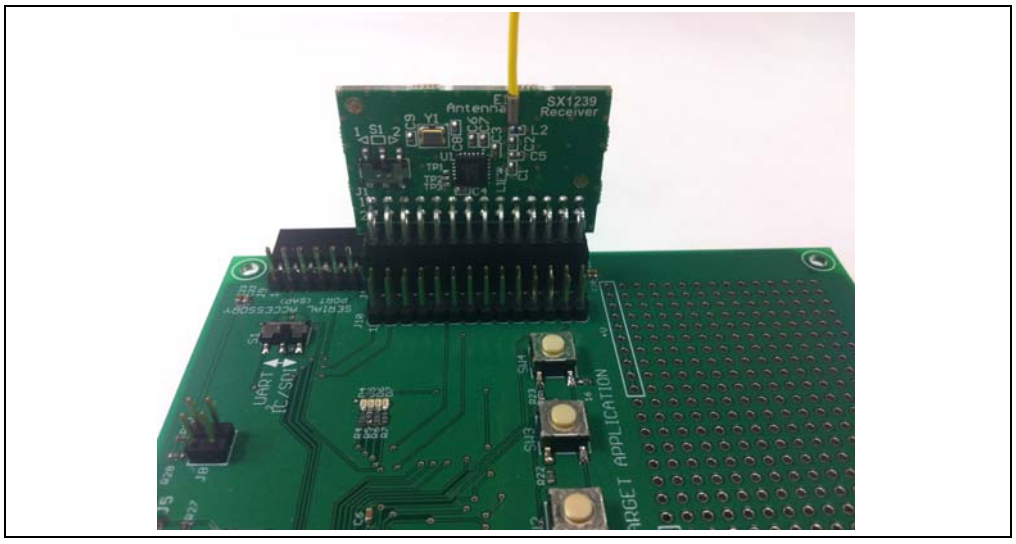
The source code for the demo is available from the Wireless Security Remote Control Development Kit product web page at http://www.microchip.com/security.

2.4 DEMO SETUP

This section describes how to set up the kit contents to operate the remote control demo program.

1. Obtain a CR2032 coin battery (if not included in the development kit)
2. Open the plastic enclosure of the red key fob by carefully prying apart the two halves. Remove the PCB board from the plastic enclosure carefully. Observe the correct battery polarity and insert the CR2032 coin battery into the battery holder. Put the PCB board back in the plastic enclosure and close the enclosure.
3. To verify that the key fob is properly installed, press any button and the LED should be flashing when the button is pressed.
4. Plug in the RF receiver daughter board on the PICtail slot of the Embedded Security Development Board. Make sure that the RF receiver daughter board has the side with RF receiver chip face the center, as shown in Figure 2-1.

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



5. 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 to the development board and an available USB port or USB power source. Set jumper J6 to pins 1-2. When using a USB port for power, there is no requirement to load the USB drivers.

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. Place jumper J6 to pins 2-3.

2.5 DEMO OPERATION

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

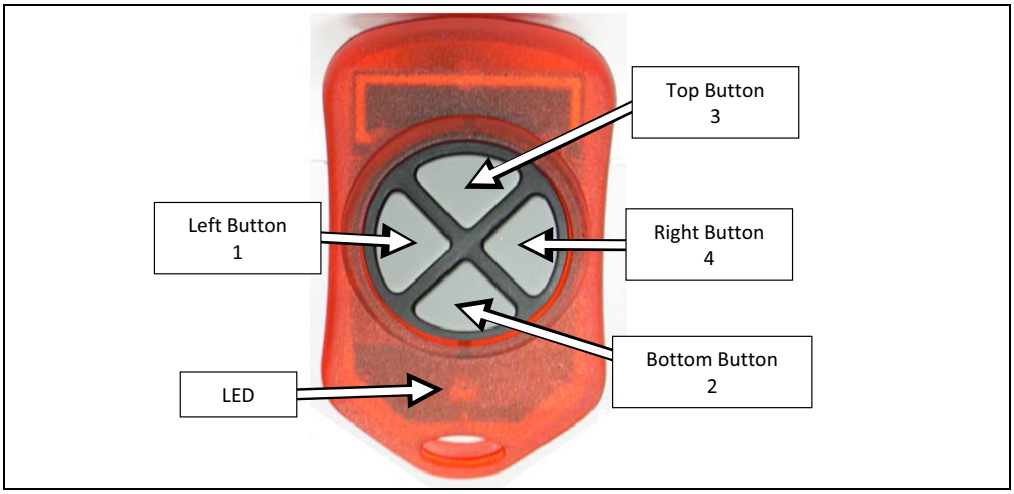
2.5.1 Key Fob as Transmitter

The pre-programmed demonstration shows how to secure information during data transmission. Pressing any one of four buttons on the red key fob, the information about the pressed button will be encrypted and transmitted. When data is being transmitted, the LED on the key fob will flash. Two ways to secure the information have been shown in this demo: KEELOQ Classic and KEELOQ AES. When button 1 or 2 (see Figure 2-2) is pressed, the information is secured with KEELOQ Classic before the transmission; when button 3 or 4 (see Figure 2-2) is pressed, the information is secured with KEELOQ AES before the transmission.

For details on KEELOQ Classic and KEELOQ AES, please refer to Microchip application notes AN1259, "*KEELOQ® Microcontroller-Based Code Hopping Encoder*" and AN1265 "*KEELOQ® with AES Microcontroller-Based Code Hopping Encoder*".

The key fob has four push buttons and is powered by a CR2032 coin battery. The key fob is shown in Figure 2-2, where the four buttons are labeled individually.

FIGURE 2-2: KEY FOB WITH FOUR PUSH BUTTONS



2.5.2 Embedded Security Development Board as 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 the cipher (KEELOQ Classic or KEELOQ AES) that is used to secure the data. The decryption process reveals the plain text, and the authentication process verifies whether the plain text is valid information.

2.5.2.1 KEELOQ CLASSIC

For KEELOQ Classic, only a message from a known transmitter can be accepted by the receiver. If a packet is received from an unknown transmitter, the message "**KLQ Transmitter Not Learned**" will be displayed on the LCD, as shown in Figure 2-3.

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

To learn a transmitter, the receiver initiates the learning process by pressing button SW4. The learning procedure will be started and the message "**Learn mode active**" will be displayed on the LCD, as shown in Figure 2-4.

FIGURE 2-4: START LEARN MODE

In the event no KEELOQ Classic packet from an unknown transmitter is received within 18 seconds, the KEELOQ Classic learn mode will time out and display the message "**Learn mode timeout**" on the LCD, as shown in Figure 2-5.

FIGURE 2-5: LEARN MODE TIMEOUT

The known transmitters and their latest counters are stored in the Nonvolatile Memory (NVM) space of the microcontroller. When all slots in the NVM space for transmitters are taken, the learning process will fail. Pressing and holding button SW3 for a few seconds will erase all transmitter records from the NVM, and then the display message "**Memory Erased**" on the LCD, as shown in Figure 2-6.

FIGURE 2-6: ERASE TRANSMITTER RECORDS FROM MEMORY

When a KEELOQ Classic packet is received from a known transmitter, the contents of the packet is displayed on the LCD, as shown in Figure 2-7. The following information from the KEELOQ Classic packet are available:

- Encoder: KLQ that represents KEELOQ Classic
- Serial number of the transmitter: 28-bit serial number (according to Figure 2-7*)* in this transmission
- Counter: 16-bit number (according to Figure 2-7) in this transmission
- Function Code: A bitmap of the pressed buttons (it will be 3 if both KLQ buttons are pressed), depending on the button pressed on the key fob

FIGURE 2-7: KEELOQ PACKET INFORMATION

2.5.2.2 KEELOQ AES

For KEELOQ AES, there is no requirement that a transmitter must be known to the receiver before a packet can be accepted, so there is no learning process for a packet that is encoded with KEELOQ AES cipher. When a KEELOQ AES packet is received, the contents of the packet is displayed on the LCD, as shown in Figure 2-8. The following information from the KEELOQ AES packet are available:

- Encoder: AES that represents KEELOQ AES
- Serial number of the transmitter: 32-bit serial number (according to Figure 2-8) in this transmission
- Counter: 32-bit counter (according to Figure 2-8) in this transmission
- Function Code: A bitmap of pressed buttons, depending on the button pressed on the key fob

FIGURE 2-8:

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 instruction of the hardware self-check is displayed on the LCD. The test result is either checked by firmware and display 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. Four individual hardware self-tests will then be performed one by one.

2.6.0.1 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.

2.6.0.2 LED TESTS

There are two sets, ten LEDs, which can be controlled by the host and target application microcontroller separately. When LED tests start, the message "**LEDs Flashing**" will be displayed on the first line of the LCD display. During the tests, two sets of LEDs will be flashing separately, while LEDs from the same set should be flashing together. 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.

2.6.0.3 RTCC TEST

When RTCC tests are initiated, the LCD display will show the clock and calendar. If no coin battery for RTCC has been installed, the time displayed will be close to the reset time of January 1, 2012. On the other hand, if a coin battery for RTCC is installed, the time displayed will be based on whatever is previously set, plus the time that has been 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.

2.6.0.4 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 be displayed; 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 work, the SPI test might show failure status. The reason is due to the expected values to be received from the SX1239.

Chapter 3. PIC12LF1840T39A Wireless Remote Key Fob

3.1 INTRODUCTION

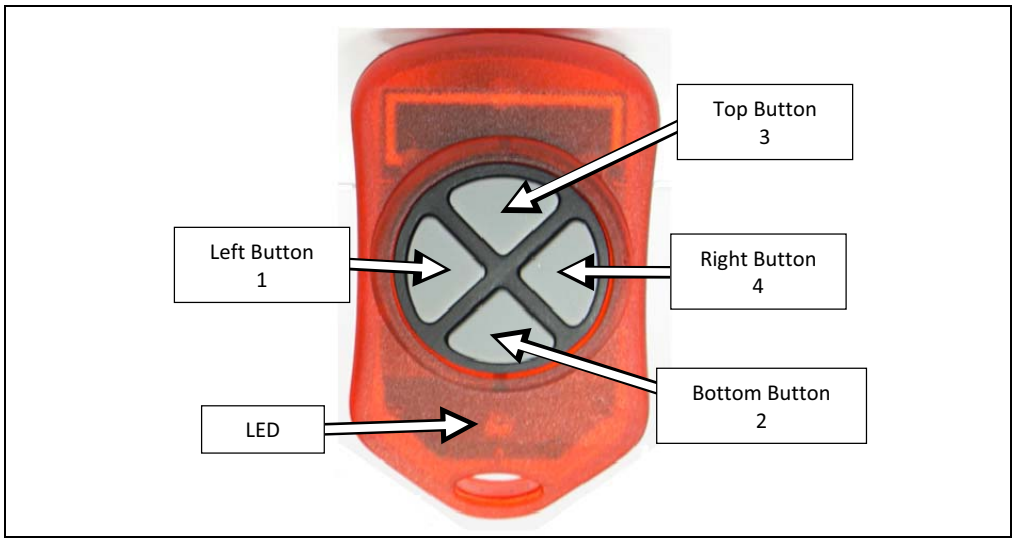
The PIC12LF1840T39A Wireless Remote Key Fob is a demonstration and development platform for wireless security remote control applications. This section gives a detailed description of the key fob.

3.2 HARDWARE DESCRIPTION

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

The schematic, PCB layout, and Bill of Materials are listed in **Appendix A. "PIC12LF1840T39A Wireless Remote Key Fob Schematics"**.

FIGURE 3-1: PIC12LF1840T39A WIRELESS REMOTE KEY FOB



3.3 PRINTED CIRCUIT BOARD DESCRIPTION

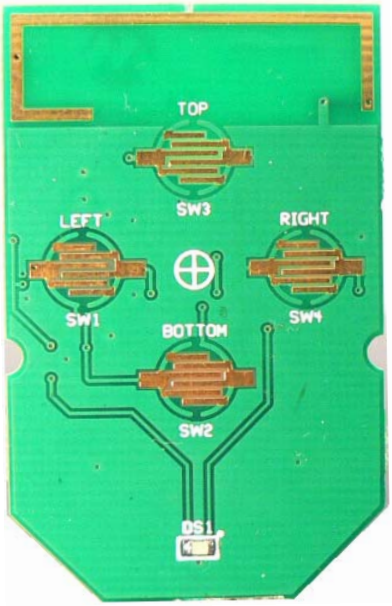
The key fob PCB is a two-layer, plated through hole, 0.031 inches (0.7874 millimeters) thick, FR4 material. Figure 3-2 shows the top layer of the PCB. All components, except the LED, are on the top layer. A PCB antenna is employed in the design for reduced cost and compactness. The PCB antenna is explained in more detail below.

P1 is the ICSP™ programming port. See **Chapter 6. "Developing with the Wireless Security Remote Control Development Kit"** for suggestions on developing and programming the key fob.

FIGURE 3-2: PCB TOP LAYER PHOTO

Figure 3-3 shows the bottom layer of the PCB. The bottom layer shows the PCB loop antenna and the PCB traces for the conductive push buttons from the plastic enclosure.

FIGURE 3-3: PCB BOTTOM LAYER PHOTO



3.4 PCB ANTENNA DESCRIPTION

The PCB antenna is a combination of top and bottom PCB layer traces, as shown in Figure 3-4. The feed point from the transmitter is on the right side of the figure. It is a top layer trace shown in red. It taps into the PCB loop antenna on the bottom layer shown in blue. The antenna loops to the left side of the PCB and is terminated to ground by a capacitor.

The PCB antenna is an "electrically small loop antenna." That is, the wavelength of the antenna is very much less than the one-quarter wavelength that antennas are normally designed to. This type of antenna has an extremely high quality factor (Q). Therefore, it is very susceptible to parasitic impedances and very challenging to impedance match to the transmitter.

Figure 3-4 is a design suggestion. The designer is cautioned that even though this design can be copied, the final product will require tuning. There are many factors that determine the performance of a PCB antenna: thickness of the copper layer, thickness of the PCB material, choice of the PCB material (e.g., FR4), and choice of the passive components used in the impedance matching circuit. The PCB antenna dimensions are not critical. Once the design has been tuned, what is important is the consistency of the manufacture.

FIGURE 3-4: PCB ANTENNA DIMENSIONS

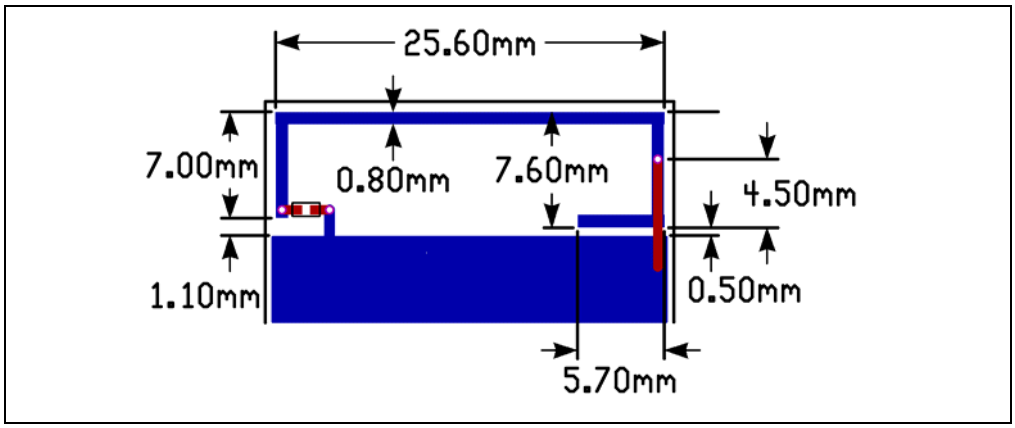


Figure 3-5 shows the simulated three-dimensional plot of the radiation patter from the antenna. Figure 3-6 shows the two-dimensional plots.

FIGURE 3-5: PCB ANTENNA 3D RADIATION PATTERN (SIMULATED)

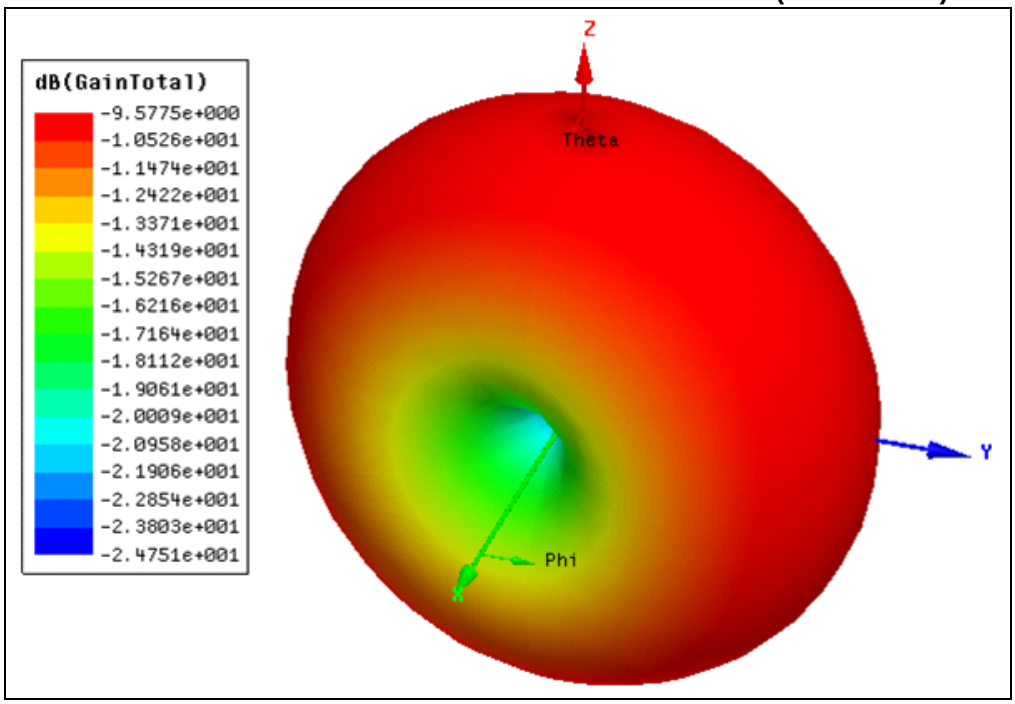
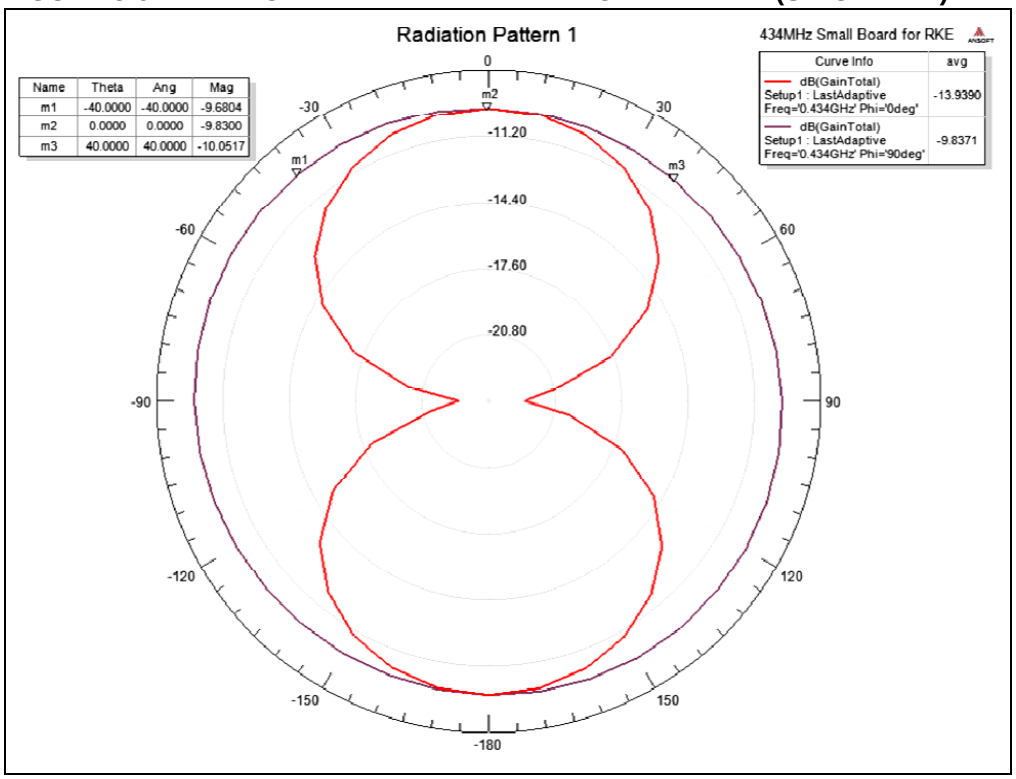


FIGURE 3-6: PCB ANTENNA 2D RADIATION PATTERN (SIMULATED)



Chapter 4. SX1239 Receiver PICtail™ Daughter Board

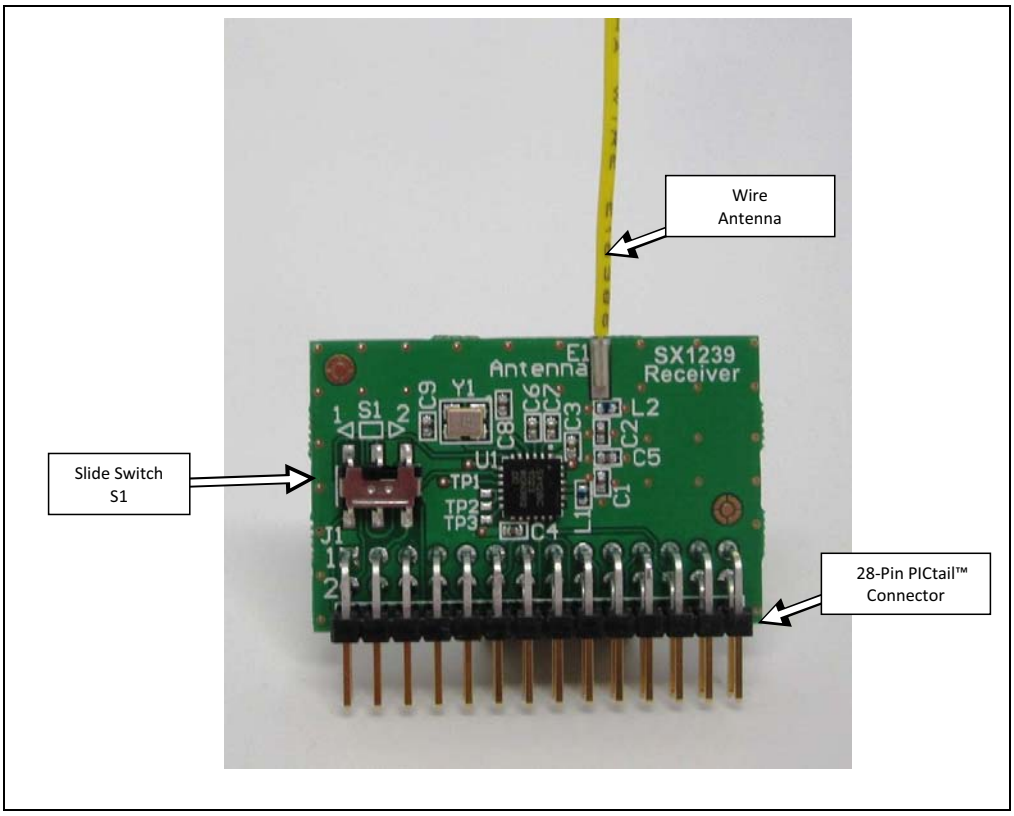
4.1 INTRODUCTION

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

4.2 HARDWARE DESCRIPTION

Figure 4-1 shows the SX1239 Receiver PICtail Daughter Board. The schematic, PCB layout, and Bill of Materials are listed in **Appendix B. "SX1239 Receiver PICtail™ Daughter Board Schematics"**.

FIGURE 4-1: SX1239 PICtail™ DAUGHTER BOARD



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

The antenna connection has a pin socket for plugging a wire antenna. This demonstrates a simple and low-cost antenna option. The length of the antenna should be approximately ¼ wavelength of the frequency of interest.

The antenna pin socket can be removed by heating it with a soldering iron and cleaning the connection. An SMA or reverse polarity SMA (RP-SMA) connector can be soldered in place on the PCB. A whip or sleeve dipole antenna can then be used.

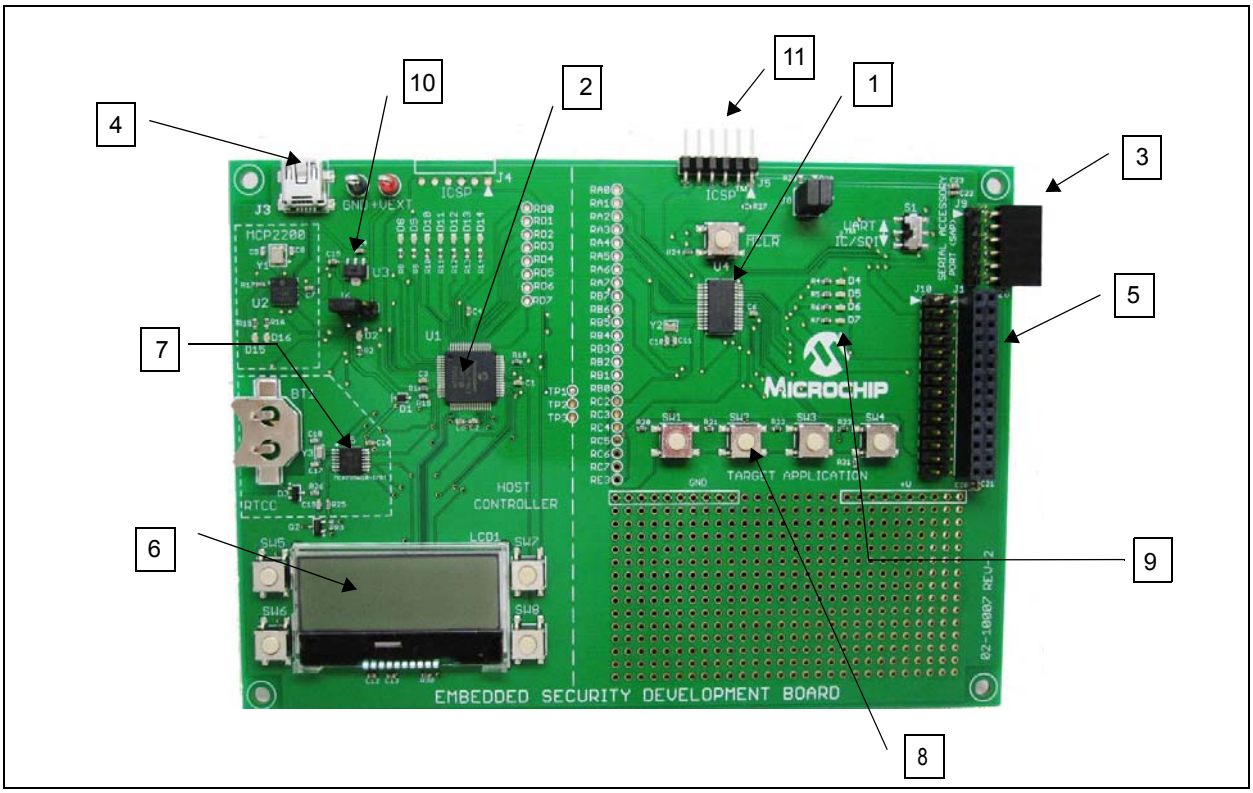
Chapter 5. Embedded Security Development Board

5.1 INTRODUCTION

The Embedded Security Development Board provides a demonstration and development environment for security and authentication products. This section gives a detailed description of the development board.

The layout of the Embedded Security Development Board is shown in Figure 5-1.

FIGURE 5-1: EMBEDDED SECURITY DEVELOPMENT BOARD



The following main blocks are defined on the Embedded Security Development Board:

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 HARDWARE DESCRIPTION

5.2.1 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 labeled 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 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/debugged via the ICSP™ header, J4. The host controller half schematic is shown in Appendix C as Figure C-2.

The target application half has a PIC16LF1398 microcontroller. The PIC16LF1398 microcontroller communicates with the 28-pin PICtail connector (J1), 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 half schematic is shown in Appendix C as Figure C-3.

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 sensor or accessory board. The partial list of Microchip boards with SAP capabilities includes the following:

- LCD Serial Accessary Board
- RS232 Serial Accessary 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
- I^2C™
- USART

The on-board switch "S1" selects these interfaces. Jumpers J7 and J8 pull-up resistors when I^2C is selected and the pull-up resistors are not available on the daughter board. Software modifications are expected to use those interfaces when pins are assigned different functionalities. For more information on the port pin assignment, see the schematic in Appendix C.

5.2.3 USB Interface Port

Microchip MCP2200 provides USB to UART support. MCP2200 provides automatic conversion between UART and full-speed USB 2.0 communication. At the same time, the USB interface port can be used to power the Embedded Security Development Board directly. For more information, please refer to the Microchip MCP2200 data sheet.

5.2.4 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 PICtail port, and perform different functionalities. Refer to the Microchip web site http://www.microchip.com for accessory daughter boards with PICtail port.

5.2.5 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. For details about the LCD display, refer to the data sheet of NHD-C0216CZ-FSW-FBW-3V3 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 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 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.

5.2.7 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 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 details of the push buttons design can be found in the schematics in Appendix C.

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 $\overline{\text{MCLR}}$ 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 also 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 target application microcontroller is configured to be a normal digital I/O pin; therefore, the $\overline{\text{MCLR}}$ push button is ineffective. Otherwise, if an SPI intercommunication is not required between the target application and host microcontroller, the pin can be configured as RESET and the $\overline{\text{MCLR}}$ button can be used.

5.2.8 LEDs

There are two sets of LEDs that are 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 six LEDs through digital output pins. The two sets of LEDs may be useful in the demo or debugging process.

Two LEDs (D15, D16) on the left half are used to identify the TX and RX operation of MCP2200. They cannot be controlled by the target application or host microcontroller. Similarly, LED D2 indicates the power availability. This LED cannot be controlled either by the target application or the host microcontroller.

5.2.9 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

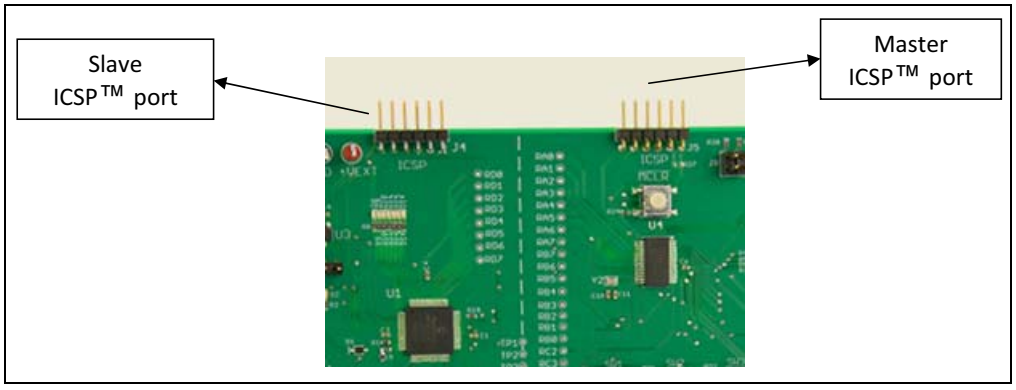
Jumper J6 is used to choose the power source. When the left side, pins 1-2 of J6, are closed, USB power is selected; when the right side, pins 2-3 of J6, are closed, external power source is selected.

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

5.2.10 ICSP™ Programming/Debugging Ports

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

FIGURE 5-2: ICSP™ PROGRAMMING/DEBUGGING PORTS



Chapter 6. Developing with the Wireless Security Remote Control Development Kit

6.1 INTRODUCTION

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

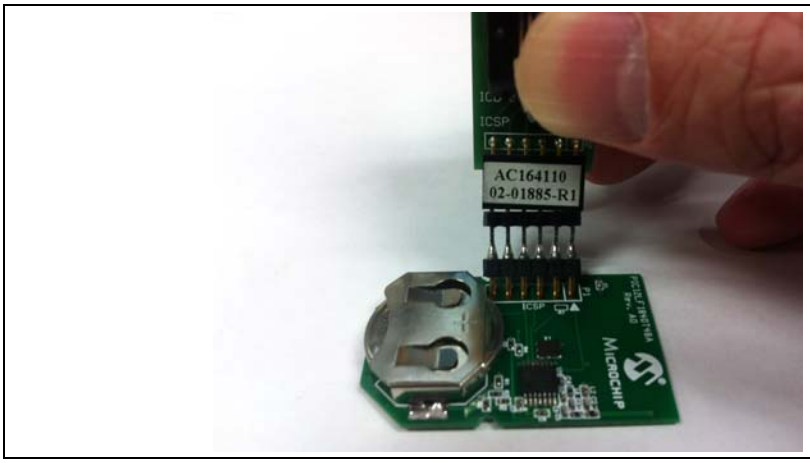
6.2 DEVELOPING WITH A KEY FOB AS TRANSMITTER

To modify the hex code in the key fob, the developer needs to open the red plastic enclosure. The ICSP™ port is available on the key fob PCB as six contact areas. To program the PIC12LF1840T39A on the PCB, the developer needs to perform the following steps:

- Remove the PCB board from the plastic enclosure and lay the PCB board on a nonconductive surface.
- Align the six ICSP pins to the contact areas on the PCB. Push the ICSP pins to the contact areas and avoid any movement during programming. Figure 6-1 shows how to program the key fob.
- When testing the key fob transmission when the plastic enclosure is open, avoid touching any PCB area with your finger.

Note: For simplicity, all key fobs in the demo share the same serial number.

FIGURE 6-1: PROGRAMMING THE KEY FOB



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 code-protect of the PIC® MCU memory.

The Microchip RKE demo uses PWM, driven by interrupt, in data whitening procedure. The transmission data rate over the air that can be achieved 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 has more current consumption. The real application may need compromise between higher data rate and faster processing speed to get the 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 on the target application microcontroller only, intercommunication between the target application and host microcontrollers can be ignored. The prototyping area under the four push buttons for target application controller can be used to prototype the application.

Same as 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 usually is powered by mains power, and power consumption is of less concern. It is possible to run the microcontroller faster to compensate higher data rate.

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

Appendix A. PIC12LF1840T39A Wireless Remote Key Fob Schematics

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

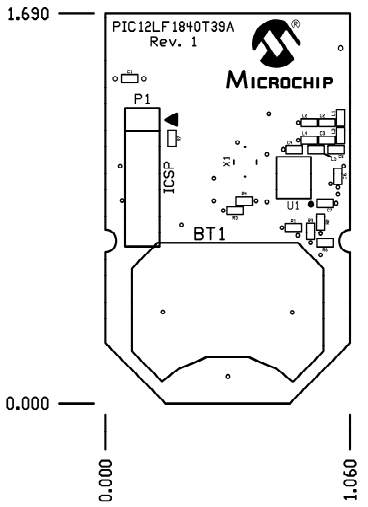


FIGURE A-2: KEY FOB PCB ASSEMBLY – TOP COPPER

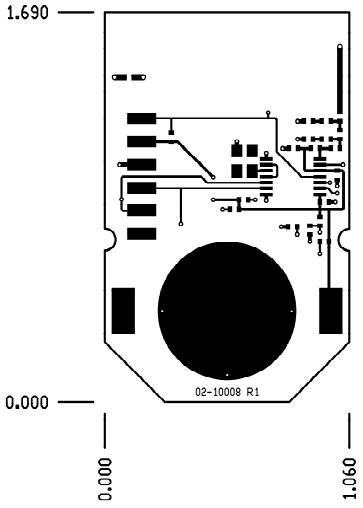


FIGURE A-3: KEY FOB PCB ASSEMBLY – BOTTOM COPPER

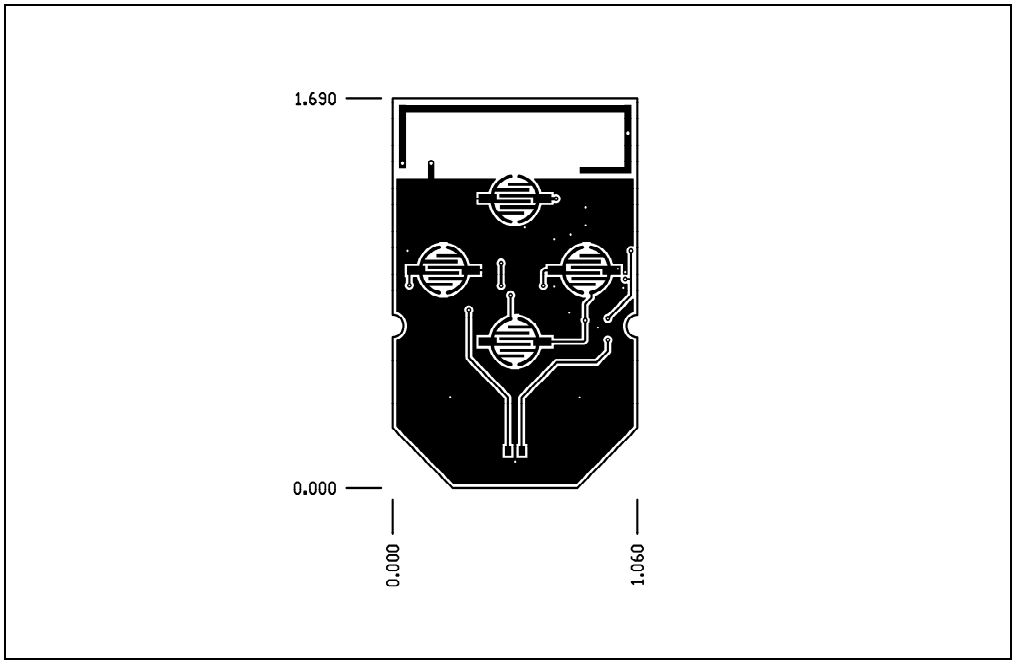


FIGURE A-4: KEY FOB PCB ASSEMBLY – BOTTOM SILKSCREEN

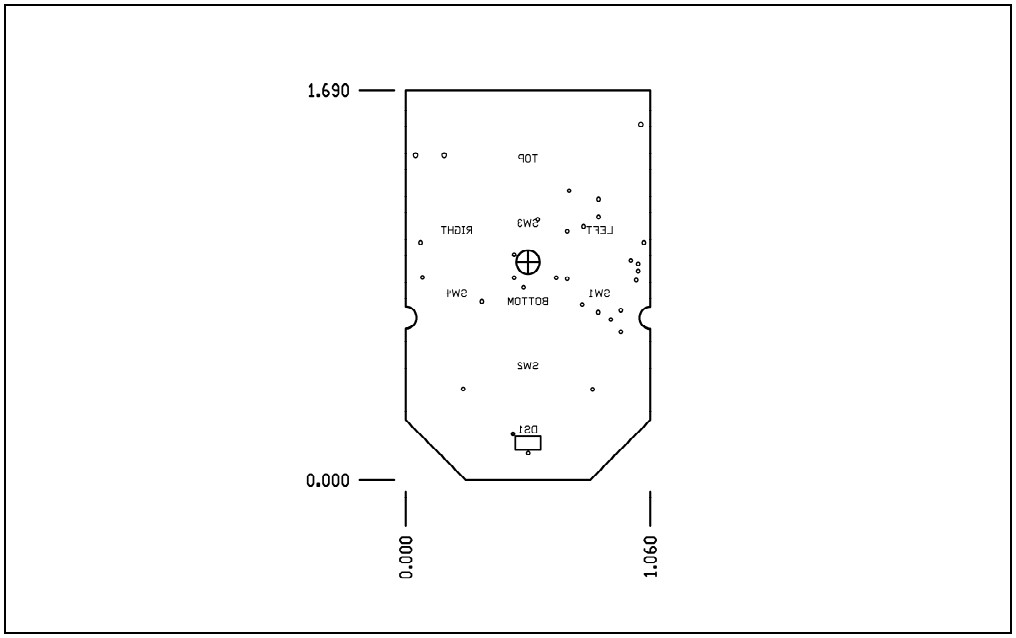


FIGURE A-5: KEY FOB SCHEMATIC

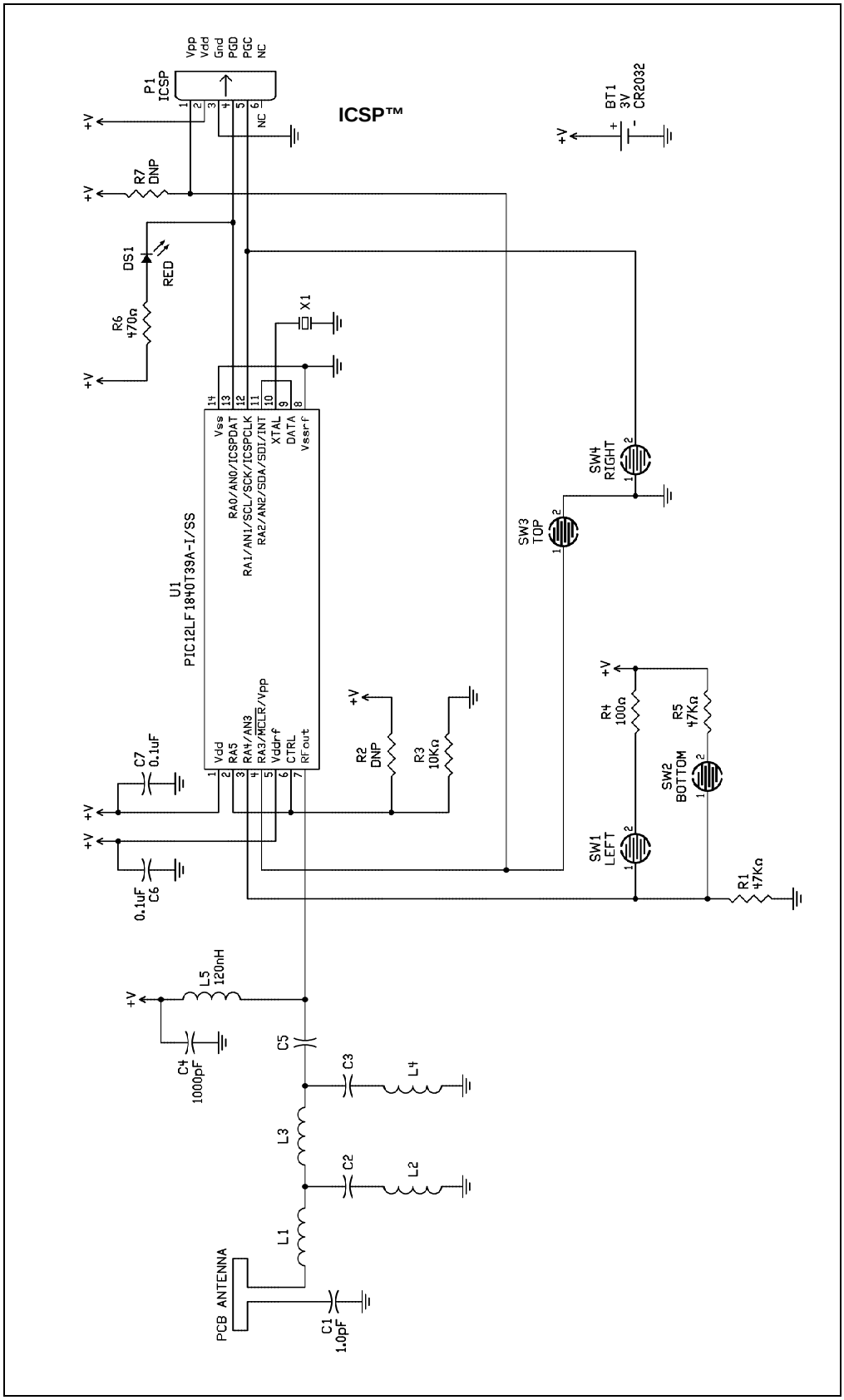


TABLE A-1: KEY FOB BOM

	Qty	Designator	Value	Description	Manufacturer	Manufacturer Part Number
Common	1	BT1		Holder Coin Cell 20MM SMD	Memory Protection Devices	BK-912
	1	@BT1		Battery Lithium Coin 3V 20mm	Panasonic – BSG	CR2032
	2	C6, C7	0.1 µF	Capacitor, Ceramic, 16V, +/-10%, X7R, SMT 0402	Murata Electronics North America	GRM155R71C104KA88D
	1	DS1	Red	Diode, Light Emitting	OSRAM	LS Q976-NR-1-0-20-R18
	1	R6	470 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-07470RL
	1	R3	10K Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-0710KL
	1	R4	100 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-07100RL
	2	R1, R5	47 kΩ	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-0747KL
	1	U1		Microcontroller with UHF Transmitter	Microchip Technology	PIC12LF1840T39A-I/SS
	1	enclosure		Enclosure, Key Fob, 4-button, Clear Red	Polycase	FB-20-4*9
	1	C1	1 pF	Capacitor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	GRM1555C1H1R0CA01D
	1	L5	120 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata	LQG15HSR12J02D
	1	C4	1000 pF	Capacitor, Ceramic,	Murata Electronics	GRM155R71H102KA01D
315 MHz	1	C5	1 nF	Capacitor, Ceramic,	Murata Electronics	GRM1555C1H102JA01D
	1	C3	0 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-070RL
	1	L4	39 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQG15HS39NJ02D
	1	L3	2.2 pF	Capacitor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	GRM1555C1H2R2CZ01D
	1	C2	DNP	Do not populate	—	—
	1	L2	DNP	Do not populate	—	—
	1	L1	0 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-070RL
	1	X1	24 MHz	CRYSTAL 24.000 MHz	Abracon Corporation	ABM8G-24.000MHZ-18-D2

TABLE A-1: KEY FOB BOM (CONTINUED)

433.92 MHz	1	C5	9.1 pF	Capacitor, Ceramic,	Johanson Technology	500R07S9R1CV4T
	1	C3	5.6 pF	Capacitor, Ceramic, 50V, ±0.1 pF, UHI-Q NP0, SMT 0402	Johanson Technology Inc	500R07S5R6CV4T
	1	L4	0 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-070RL
	1	L3	0 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-070RL
	1	C2	3 pF	Capacitor, Ceramic, 50V, ±0.1 pF, UHI-Q NP0, SMT 0402	Johanson Technology Inc	500R07S3R0BV4T
	1	L2	1 nH	Inductor, Ceramic, ±5%, SMT 0402	Johanson Technology Inc	L-07C1N0SV6T
	1	L1	47 nH	Inductor, Ceramic, ±5%, SMT 0402	Panasonic – ECG	ELJ-RF47NGFB
	1	X1	26 MHz	CRYSTAL 26.000 MHz	Abracon Corporation	ABM8G-26.000MHZ-18-D2
868 MHz	1	C5	100 pF	Capacitor, Ceramic,	Murata Electronics	GRM1555C1H101JZ01D
	1	C3	DNP	Do not populate	—	—
	1	L4	DNP	Do not populate	—	—
	1	L3	27 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQG15HS27NJ02D
	1	C2	1.8 pF	Capacitor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	GRM1555C1H1R8CZ01D
	1	L2	0 Ω	Resistor, 5%, ±100 ppm/C, SMT 0402	Yageo	RC0402JR-070RL
	1	L1	27 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQG15HS27NJ02D
	1	X1	26 MHz	CRYSTAL 26.000 MHz	Abracon Corporation	ABM8G-26.000MHZ-18-D2
915 MHz	1	C5	4.7 nH	Inductor, Ceramic, ±5%,	Murata Electronics	LQG15HS4N7S02D
	1	C3	4.7 pF	Capacitor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	GRM1555C1H4R7CZ01D
	1	L4	1.8 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQP15MN1N8B02D
	1	L3	2.7 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQG15HS2N7S02D
	1	C2	2.7 pF	Capacitor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	GRM1555C1H2R7CZ01D
	1	L2	1.8 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQP15MN1N8B02D
	1	L1	15 nH	Inductor, Ceramic, ±5%, SMT 0402	Murata Electronics North America	LQP15MN15NG02D
	1	X1	26 MHz	CRYSTAL 26.000 MHz	Abracon Corporation	ABM8G-26.000MHZ-18-D2

NOTES:

Appendix B. SX1239 Receiver PICtail™ Daughter Board Schematics

FIGURE B-1: SX1239 RECEIVER PICtail™ PCB ASSEMBLY

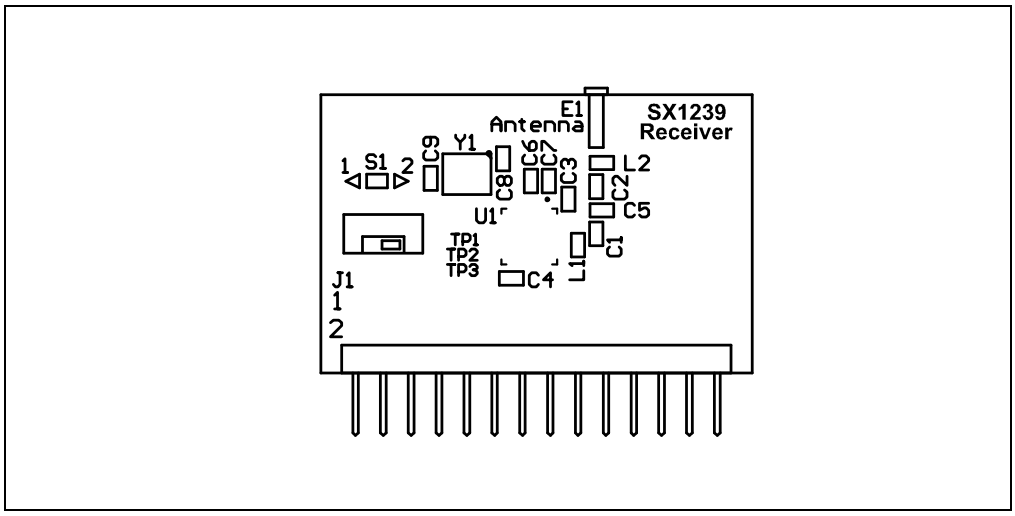


FIGURE B-2: RECEIVER PICtail™ SCHEMATIC

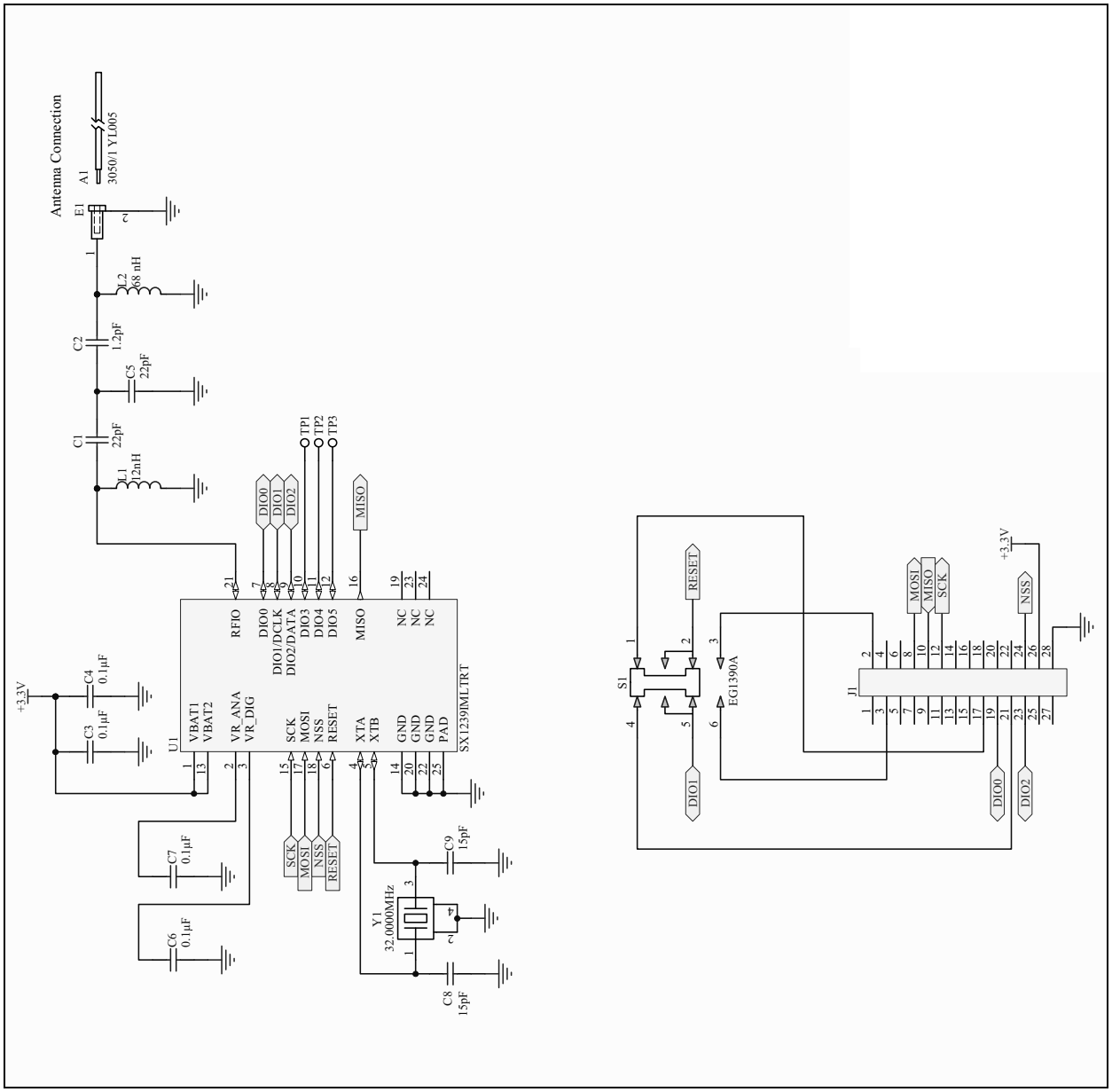


TABLE B-1: SX1239 RECEIVER PICtail™ BOM

	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, 0.1uF, 16V +/-10% X7R	Murata Electronics North America	GRM155R71C104KA88D
	4	C6, C7, C8, C9	15 pF	Cap, Ceramic, 15pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H150JZ01D
	1	E1		Pin Receptacle, .015/.025Dia, 0667 Series	Mill-Max Manufacturing Corp.	0667-0-15-01-30-27-10-0
	1	J1		Terminal strip, 2X14, 0.100sp, 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	SEMTECH	SX1239IMLTRT
	1	Y1	32 MHz	Crystal, 32.0000 MHz, 10pF, SMD TXC Series 7M	TXC CORPORATION	7M-32.000MEEQ-T
	1	C2	1.2 pF	Cap, Ceramic, 1.2pF, 50V +/-0.25pF COG	Murata Electronics North America	GRM1555C1H1R2CZ01D
	1	L2	68 nH	Inductor, 68nH, 140mA, Air Core, 5%	Murata Electronics North America	LQW15AN68NJ00D
315/434 MHz	2	C1, C5	22 pF	Cap, Ceramic, 22pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H220JZ01D
	1	L1	12 nH	Inductor, 12nH, 500mA, Air Core, 5%	Murata Electronics North America	LQG15HS12NJ02D
	Note: Designator A1 Wire Antenna: Cut to 6.75 in. OAL.					
868/915 MHz	1	C1	4.7 pF	Cap, Ceramic, 4.7pF, 50V	Murata Electronics	GRM1555C1H4R7CZ01D
	1	L1	13 nH	Inductor, 13nH, 500mA, Air Core, 5%	TDK Corporation	MLG1005S13NJ
	1	C5	3.6 pF	Cap, Ceramic, 3.6pF, 50V +/-5% COG	Murata Electronics North America	GRM1555C1H3R6CZ01D
	Note: Designator A1 Wire Antenna: Cut to 6.75 in. OAL.					

NOTES:

Appendix C. Embedded Security Development Board Schematics

FIGURE C-1: EMBEDDED SECURITY DEVELOPMENT BOARD PCB ASSEMBLY

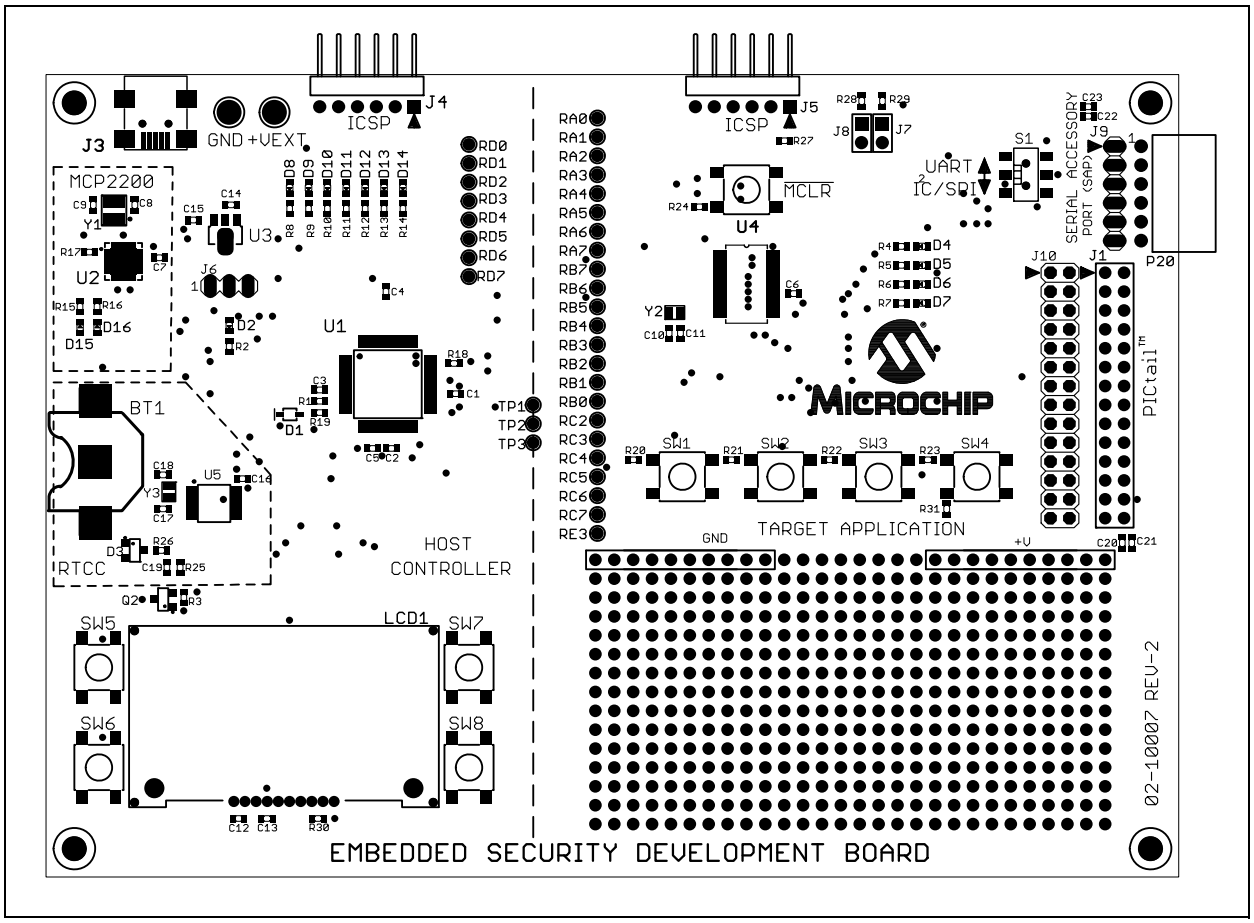


FIGURE C-2: EMBEDDED SECURITY DEVELOPMENT BOARD SCHEMATIC (1 OF 2)

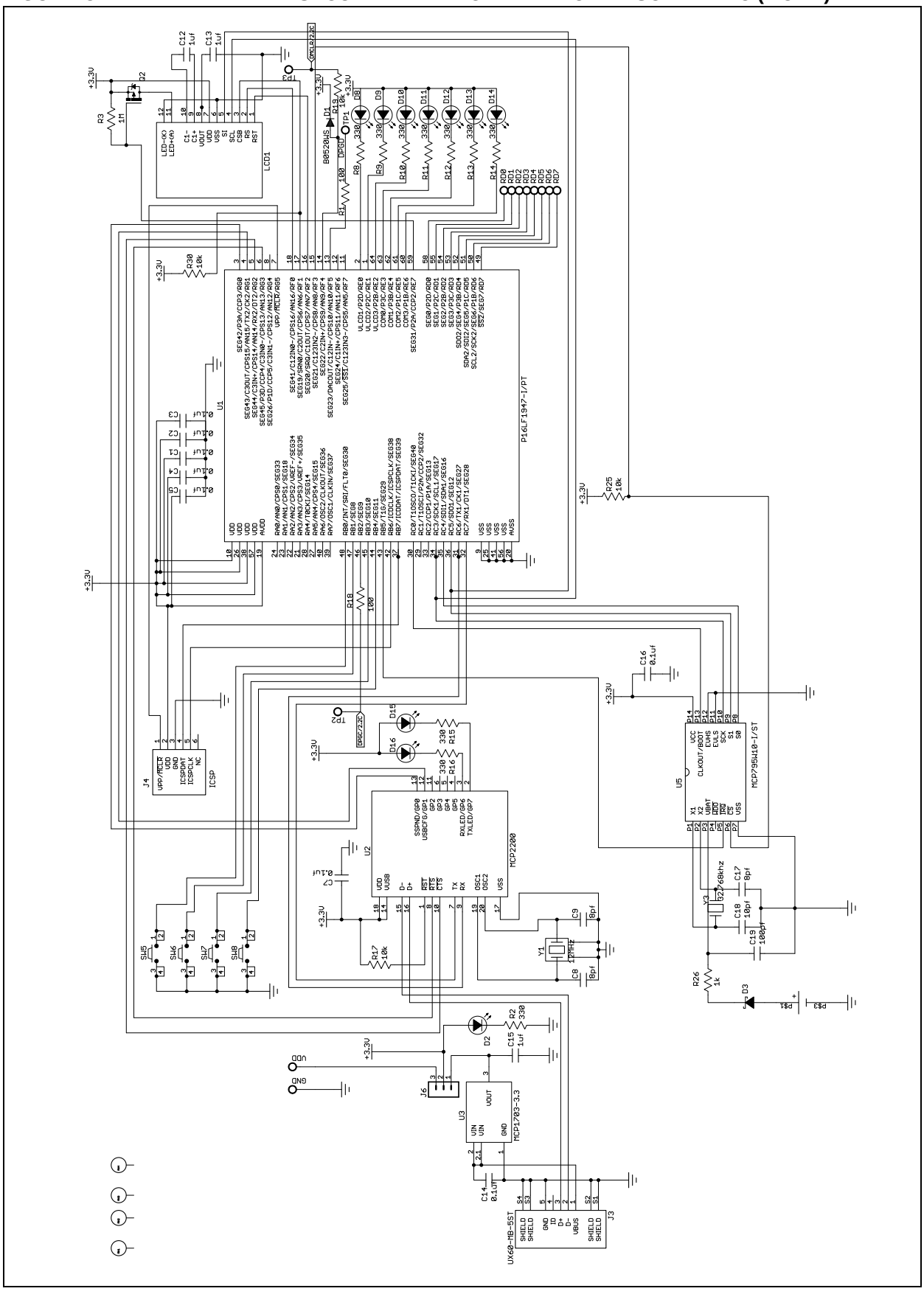


FIGURE C-3: EMBEDDED SECURITY DEVELOPMENT BOARD SCHEMATIC (2 OF 2)

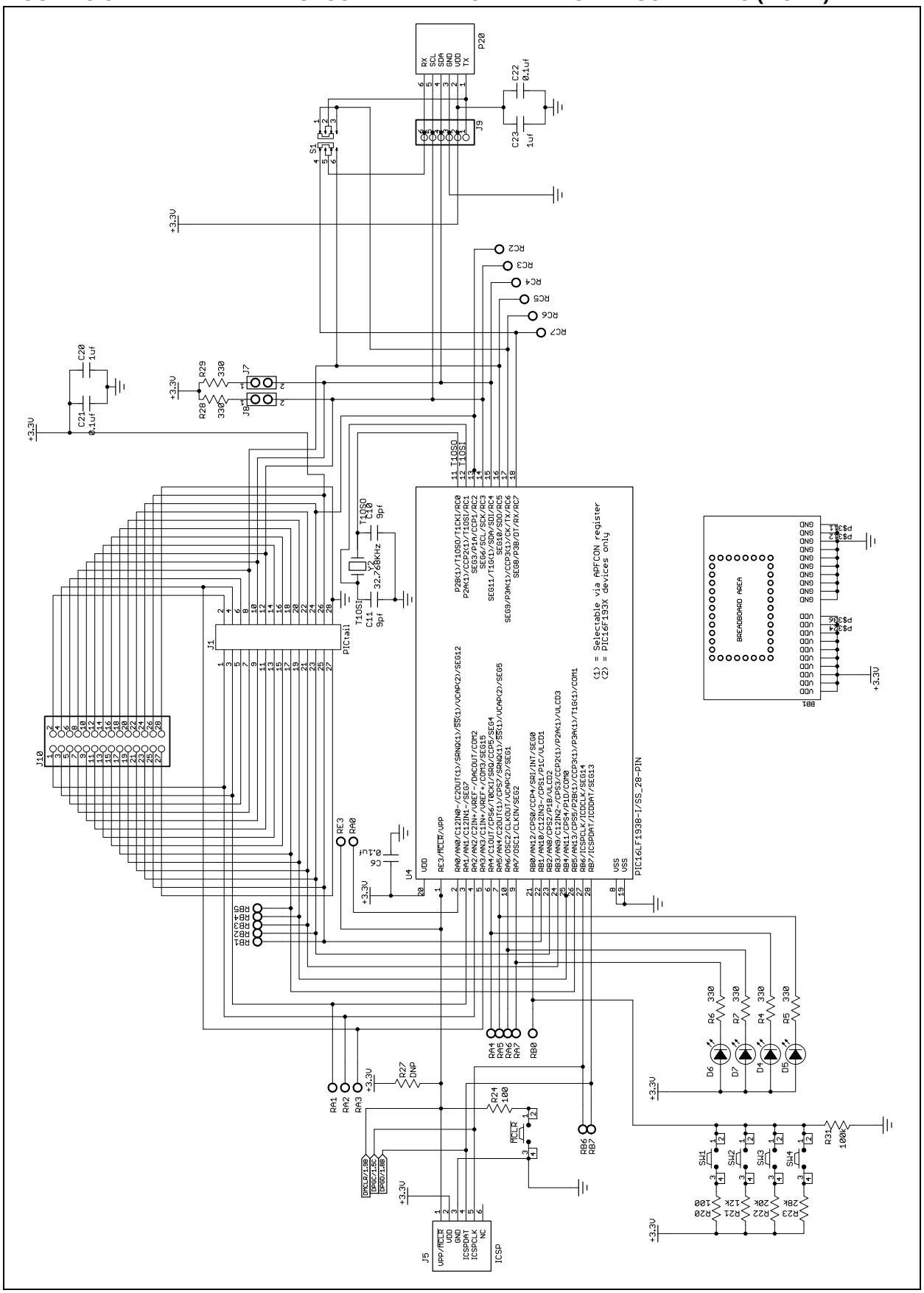


TABLE C-1: EMBEDDED SECURITY DEVELOPMENT BOARD BOM

Qty	Part	Value	Manufacturer	MFG Part Number
1	VDD	VDD	Keystone	5010
	GND	GND	Keystone	5011
1	BT1	BK-885	MPD (Memory Protection Devices)	BK-885
3	C8	8 pf	TDK Corporation	C1608C0G1H080D
	C9	8 pf	TDK Corporation	C1608C0G1H080D
	C17	8 pf	TDK Corporation	C1608C0G1H080D
2	C10	9 pf	TDK Corporation	C1608C0G1H090D
	C11	9 pf	TDK Corporation	C1608C0G1H090D
1	C18	10 pf	TDK Corporation	C1608C0G1H100D
1	C19	100 pf	TDK Corporation	C1608C0G1H101J
11	C1	0.1 µf	Murata	GRM188R71E104KA01D
	C2	0.1 µf	Murata	GRM188R71E104KA01D
	C3	0.1 µf	Murata	GRM188R71E104KA01D
	C4	0.1 µf	Murata	GRM188R71E104KA01D
	C5	0.1 µf	Murata	GRM188R71E104KA01D
	C6	0.1 µf	Murata	GRM188R71E104KA01D
	C7	0.1 µf	Murata	GRM188R71E104KA01D
	C14	0.1 µf	Murata	GRM188R71E104KA01D
	C16	0.1 µf	Murata	GRM188R71E104KA01D
	C21	0.1 µf	Murata	GRM188R71E104KA01D
	C22	0.1 µf	Murata	GRM188R71E104KA01D
5	C12	1 µf	Murata	GRM188R61A105MA61D
	C13	1 µf	Murata	GRM188R61A105MA61D
	C15	1 µf	Murata	GRM188R61A105MA61D
	C20	1 µf	Murata	GRM188R61A105MA61D
	C23	1 µf	Murata	GRM188R61A105MA61D
1	D1	B0520WS	Diodes Inc.	B0520WS-7-F
1	D3		Fairchild Semiconductor	BAT54
	D2		Lite-On	LTST-C191GKT
	D4		Lite-On	LTST-C191GKT
	D5		Lite-On	LTST-C191GKT
	D6		Lite-On	LTST-C191GKT
	D7		Lite-On	LTST-C191GKT
	D8		Lite-On	LTST-C191GKT
	D9		Lite-On	LTST-C191GKT
	D10		Lite-On	LTST-C191GKT

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

	D11		Lite-On	LTST-C191GKT
	D12		Lite-On	LTST-C191GKT
	D13		Lite-On	LTST-C191GKT
	D14		Lite-On	LTST-C191GKT
	D15		Lite-On	LTST-C191GKT
	D16		Lite-On	LTST-C191GKT
1	J1	PICtail™	Sullins	PPPC142LFBN-RC
1	J3	UX60-MB-5ST	Hirose Electric Co Ltd	UX60-MB-5ST
1	J4	DNP		Do Not Populate
1	J5	ICSP™	Sullins	PBC06SBAN
1	J6		Sullins	PBC03SAAN
1	J7, J8		Sullins	PBC02DAAN
1	J9		Sullins	PBC06SAAN
1	J10		Sullins	PBC14DAAN
1	LCD1		Newhaven Displays	C0216CZ-FSW-FBW-3V3
1	P20		Sullins	PPPC061LGBN-RC
1	Q2		International Rectifier	IRLML6302TRPBF
4	R1	100 Ω	Stackpole Electronics International	RMCF0603FT100R
	R18	100 Ω	Stackpole Electronics International	RMCF0603FT100R
	R20	100 Ω	Stackpole Electronics International	RMCF0603FT100R
	R24	100 Ω	Stackpole Electronics International	RMCF0603FT100R
16	R2	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R4	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R5	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R6	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R7	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R8	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R9	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R10	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R11	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R12	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R13	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R14	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R15	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R16	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R28	330 Ω	Stackpole Electronics International	RMCF0603FT330R
	R29	330 Ω	Stackpole Electronics International	RMCF0603FT330R
1	R26	1k Ω	Stackpole Electronics International	RMCF0603FT1K00

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

5	R17	10k Ω	Stackpole Electronics International	RMCF0603FT10K0
	R19	10k Ω	Stackpole Electronics International	RMCF0603FT10K0
	R25	10k Ω	Stackpole Electronics International	RMCF0603FT10K0
	R27	DNP Ω	Do not Populate	Do Not Populate
	R30	10k Ω	Stackpole Electronics International	RMCF0603FT10K0
1	R21	12k Ω	Stackpole Electronics International	RMCF0603FT12K0
1	R22	20k Ω	Stackpole Electronics International	RMCF0603FT20K0
1	R23	28k Ω	Stackpole Electronics International	RNCP0603FTD28K0
1	R31	100k Ω	Stackpole Electronics International	RMCF0603FT100K
1	R3	1M Ω	Stackpole Electronics International	RMCF0603FT1M00
1	S1		E-Switch	EG1390B
9	SW1		Omron	B3S-1000P
	SW2		Omron	B3S-1000P
	SW3		Omron	B3S-1000P
	SW4		Omron	B3S-1000P
	SW5		Omron	B3S-1000P
	SW6		Omron	B3S-1000P
	SW7		Omron	B3S-1000P
	SW8		Omron	B3S-1000P
	$\overline{\text{MCLR}}$		Omron	B3S-1000P
1	U1	P16LF1947-I/PT	Microchip Technology Inc.	PIC16LF1947-I/PT
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	32.768 kHz	Abracon	ABS06-32.768KHZ-T
	Y3	32.768 kHz	Abracon	ABS06-32.768KHZ-T

NOTES:

Worldwide Sales and Service

AMERICAS

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

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

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

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

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

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

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

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

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

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

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

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

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

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

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

China - Hangzhou
Tel: 86-571-2819-3187
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

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

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

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

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

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

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

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

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

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

ASIA/PACIFIC

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

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

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Osaka
Tel: 81-66-152-7160
Fax: 81-66-152-9310

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

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

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

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

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

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

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

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

Taiwan - Kaohsiung
Tel: 886-7-536-4818
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

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

EUROPE

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

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

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

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

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

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

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

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

11/29/11

Общество с ограниченной ответственностью «МосЧип» ИНН 7719860671 / КПП 771901001
Адрес: 105318, г.Москва, ул.Щербаковская д.3, офис 1107

Данный компонент на территории Российской Федерации

Вы можете приобрести в компании MosChip.

Для оперативного оформления запроса Вам необходимо перейти по данной ссылке:

http://moschip.ru/get-element

Вы можете разместить у нас заказ для любого Вашего проекта, будь то серийное производство или разработка единичного прибора.

В нашем ассортименте представлены ведущие мировые производители активных и пассивных электронных компонентов.

Нашей специализацией является поставка электронной компонентной базы двойного назначения, продукции таких производителей как XILINX, Intel (ex.ALTERA), Vicor, Microchip, Texas Instruments, Analog Devices, Mini-Circuits, Amphenol, Glenair.

Сотрудничество с глобальными дистрибьюторами электронных компонентов, предоставляет возможность заказывать и получать с международных складов практически любой перечень компонентов в оптимальные для Вас сроки.

На всех этапах разработки и производства наши партнеры могут получить квалифицированную поддержку опытных инженеров.

Система менеджмента качества компании отвечает требованиям в соответствии с ГОСТ Р ИСО 9001, ГОСТ РВ 0015-002 и ЭС РД 009

Офис по работе с юридическими лицами:

105318, г.Москва, ул.Щербаковская д.3, офис 1107, 1118, ДЦ «Щербаковский»

Телефон: +7 495 668-12-70 (многоканальный)

Факс: +7 495 668-12-70 (доб.304)

E-mail: info@moschip.ru

Skype отдела продаж:
moschip.ru
moschip.ru_4
moschip.ru_6
moschip.ru_9