C-Source Reference for Operating the DS28E50 Combined with a DS2477 from a Cortex-M4 Microcontroller

MAXREFDES9008

Introduction

The DS2477 is a 1-Wire® master that performs protocol conversion between the I²C master and any attached 1-Wire slaves. For 1-Wire line driving, the internal user-adjustable timers relieve the system host processor from generating time-critical 1-Wire waveforms, which supports both standard and overdrive communication speeds. The 1-Wire master has a selectable active or passive 1-Wire pullup. The strong pullup features support 1-Wire power delivery for 1-Wire devices that require additional current, such as electrically erasable programmable read-only memory (EEPROM) writes or cryptographic operations.

The DS2477 is also a SHA-3 coprocessor designed to operate with 1-Wire SHA3-256 secure authenticators, such as the DS28E50. The DS28E50 secure authenticator combines FIPS202-compliant secure hash algorithm (SHA-3) challenge and response authentication with Maxim's patented ChipDNA™ technology, a physically unclonable function (PUF), to provide a cost-effective solution with the ultimate protection against security attacks. The DS28E50 communicates over the single-contact 1-Wire® bus at both standard and overdrive speeds.

The MAXREFDES9008 reference design shows how to develop a secure application using a DS28E50 and DS2477 authentication scheme. Featured is an Arm® Cortex®-M4 host microcontroller to be used as the system's host processor. All hardware design files as well as C-code demonstration software are provided for this reference design in the *Design Resources* Section.

Other features include the following:

- 1-Wire DS28E50 provides SHA3-256 Challenge/Response Authentication
- DS2477 SHA3-256 Coprocessor stores a system secret securely and performs authentication
- 1-Wire Master DS2477 for Optimized 1-Wire I/O Communication
- Cotex-M4 compatible software libraries for the DS28E50 and DS2477
- C-Code example software to show how to fully authenticate devices

Designed–Built–Tested

A simple, cost-efficient, 1-Wire master and SHA3-256 coprocessor is demonstrated using the DS2477 for a secure authentication application using the MAX32660 host microcontroller and the DS28E50 1-Wire secure authenticator slave. This reference design includes the following major components: one each of MAX32660 Cortex-M4 microcontroller, DS2477 1-Wire master and secure SHA-3 coprocessor, and DS28E50 secure SHA-3 authenticator 1-Wire slave. This document describes the hardware shown in Figure 1 as well as its accompanying software. It provides a detailed, systematic technical guide to set up and understand the MAXREFDES9008 reference design. The system has been built and tested, details of which follow later in this document.

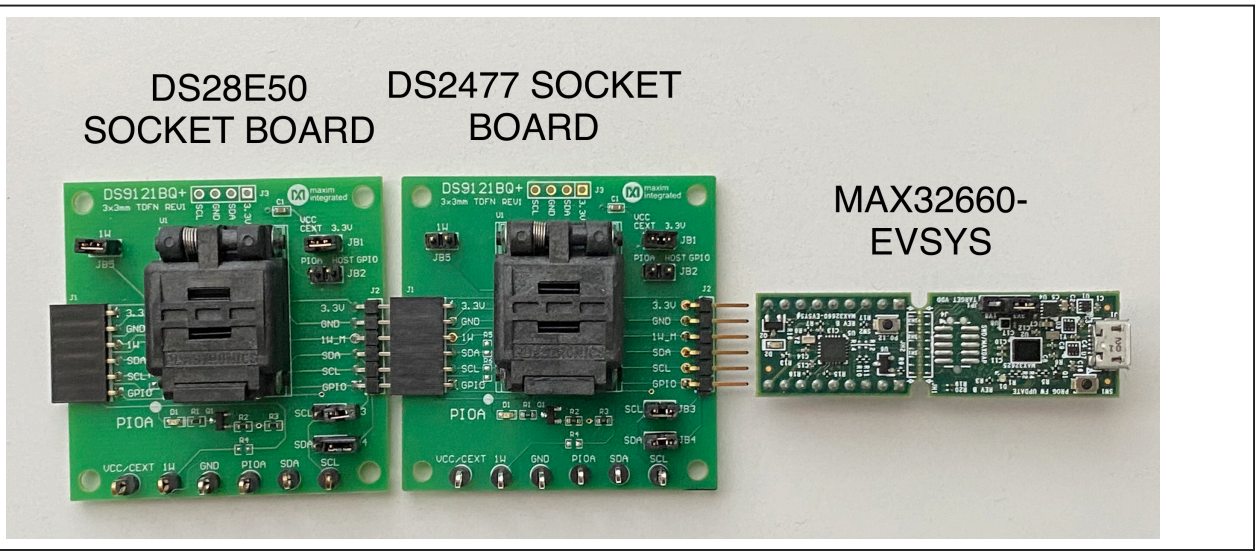

Figure 1. MAXREFDES9008 hardware.

1-Wire and Maxim Integrated are registered trademarks of Analog Devices, Inc.
ChipDNA is a trademark of Analog Devices Products, Inc.
Arm and Cortex are registered trademarks of Arm Limited.

One Analog Way, Wilmington, MA 01887 U.S.A. | Tel: 781.329.4700 |

Quick Start

This section includes a list of recommended equipment and instructions on how to set up the Windows®-based PC for the C-Demo software.

Required Equipment

- PC with a Windows 10, Windows 8, or Windows 7 operating system (64-bit or 32-bit) and a spare USB 2.0 or higher port
- Low-power Arm Micro Toolchain (Windows)
- C-Demo software
- DS28E50 EV Kit
- DS2477 Socket Board
- MAX32660-EVSYS
- Terminal Program such as PuTTY

Procedure

Follow the steps below to set up the demo software:

1) Download the **ARMCortexToolchain.exe** file.
2) Double-click on **ARMCortexToolchain.exe** to begin the installation as shown in Figure 2.

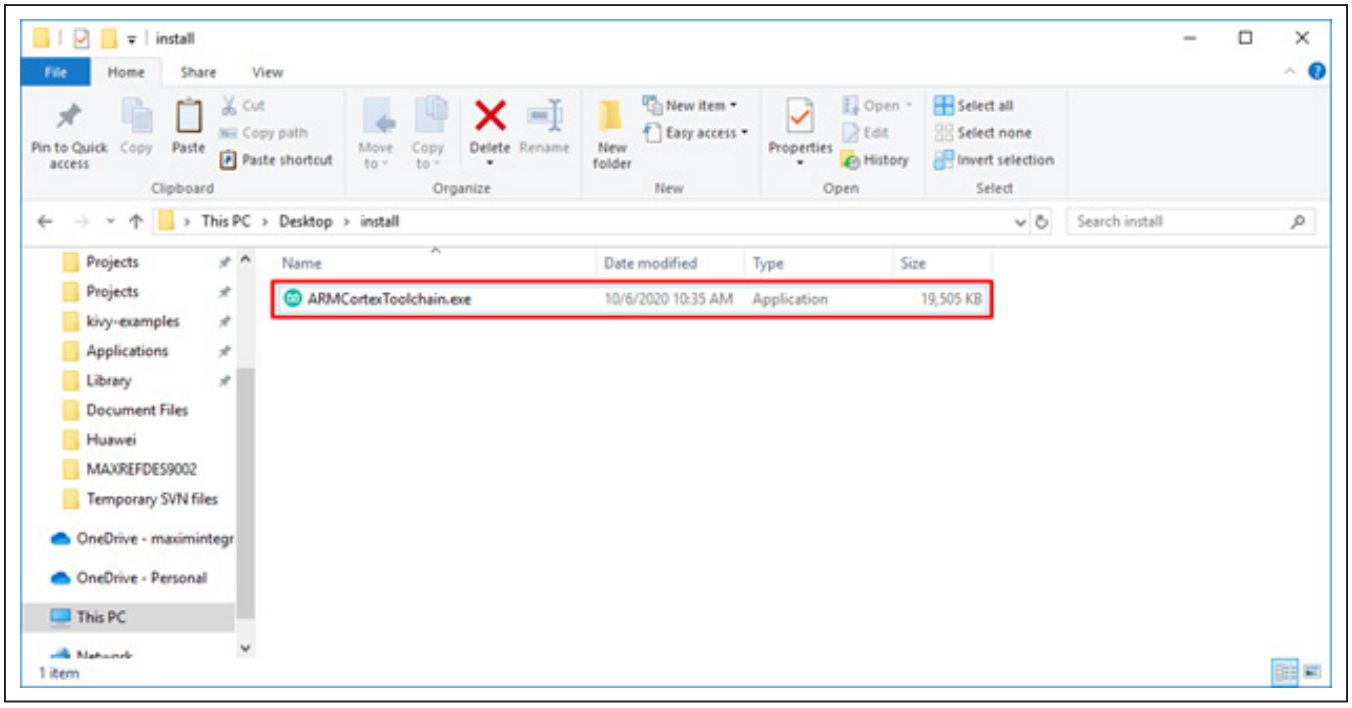

Figure 2. File viewer.

Windows is a registered trademark and service mark of Microsoft Corp.

3) Follow the prompts in the setup wizard to finish the installation as shown in Figure 3.

4) Navigate to the toolchain's install directory, open the **Eclipse** folder, and run Eclipse.bat to launch the Eclipse IDE as shown in Figure 4.

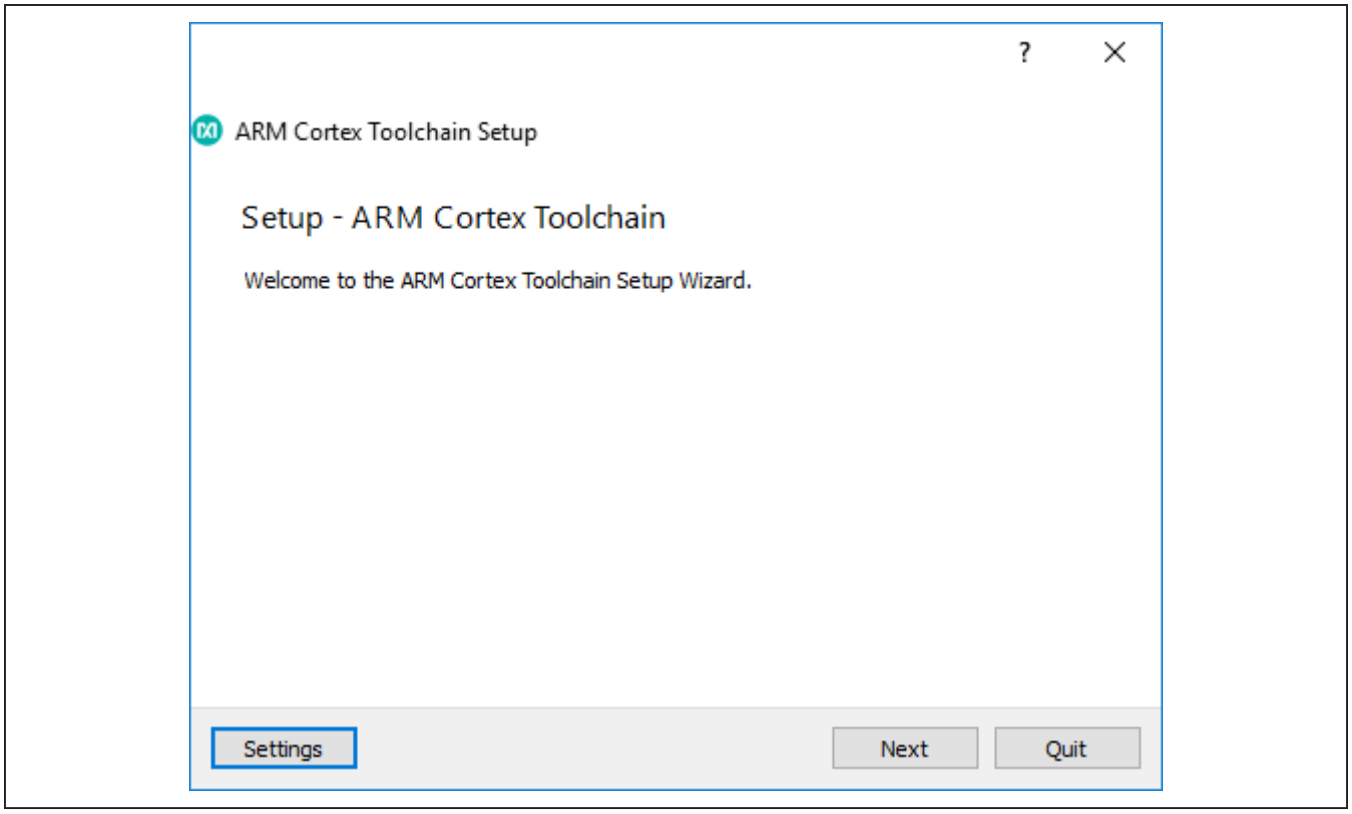

Figure 3. Toolchain setup wizard.

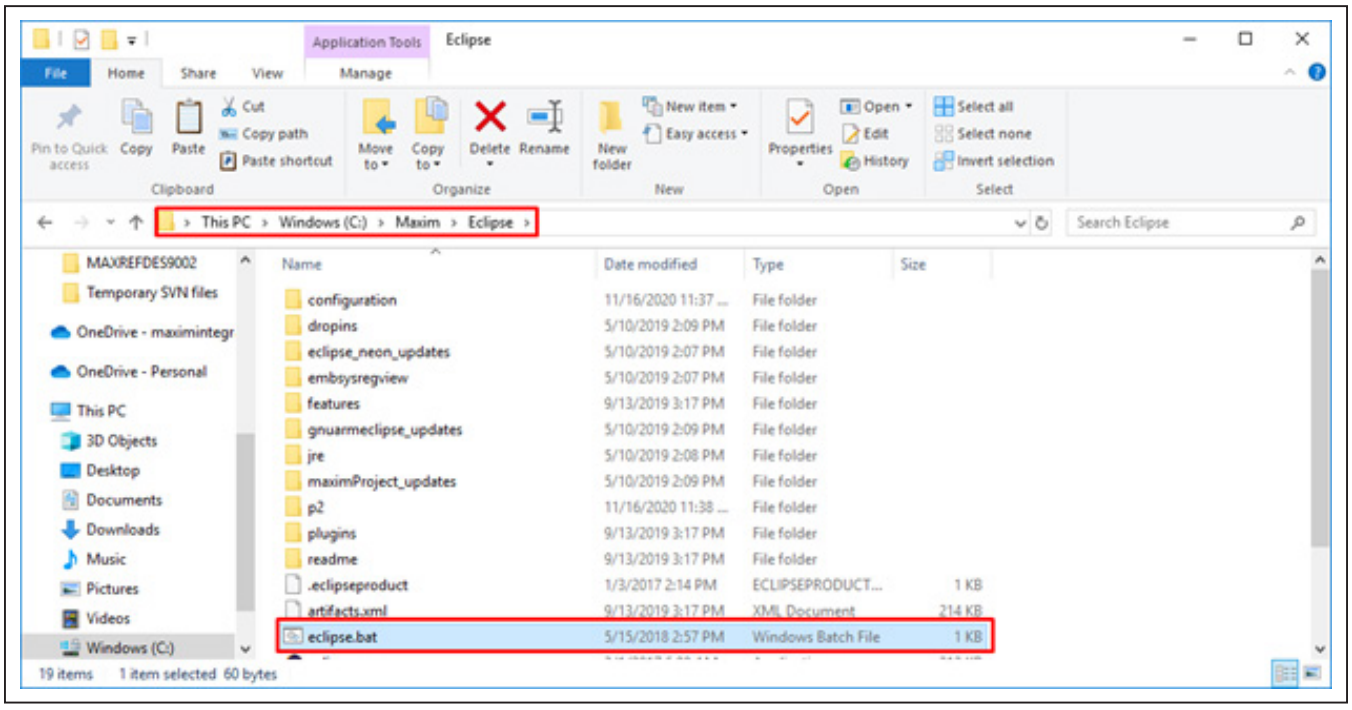

Figure 4. Eclipse launch location.

5) Create a workspace in a desired location as shown in Figure 5.

6) Download and extract the **MAXREFDES9008_Software_V1.0.0** file, in any location as shown in Figure 6.

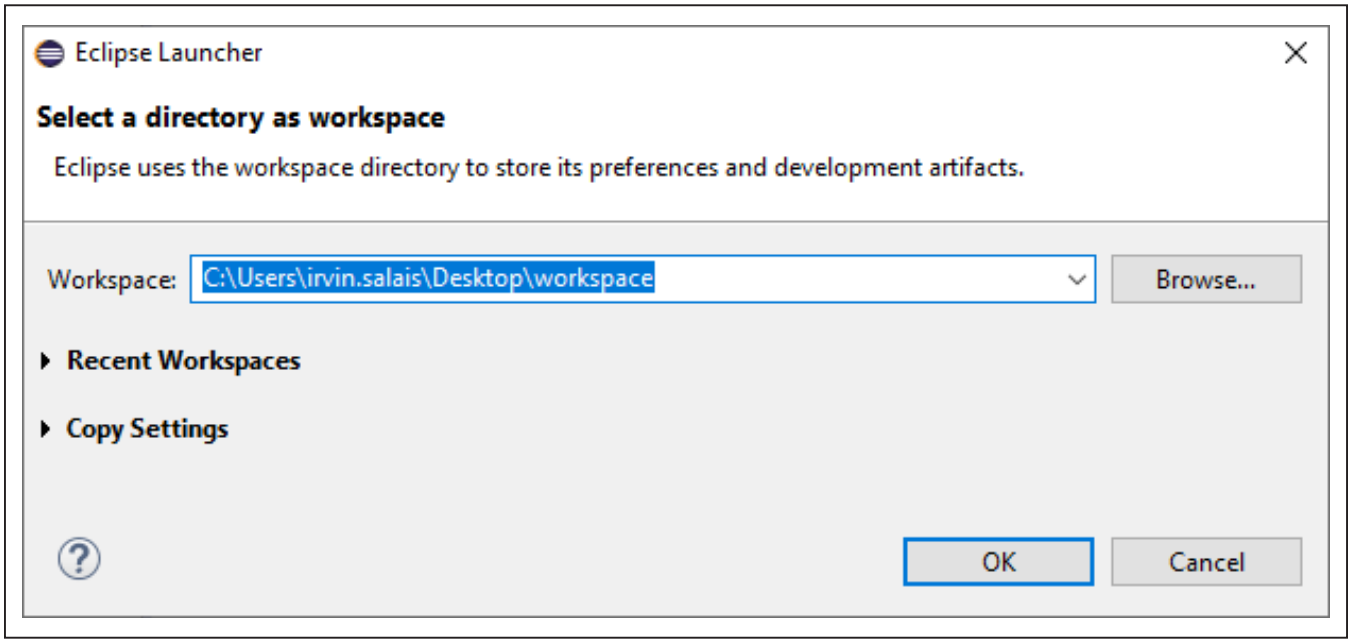

Figure 5. Eclipse workspace creation.

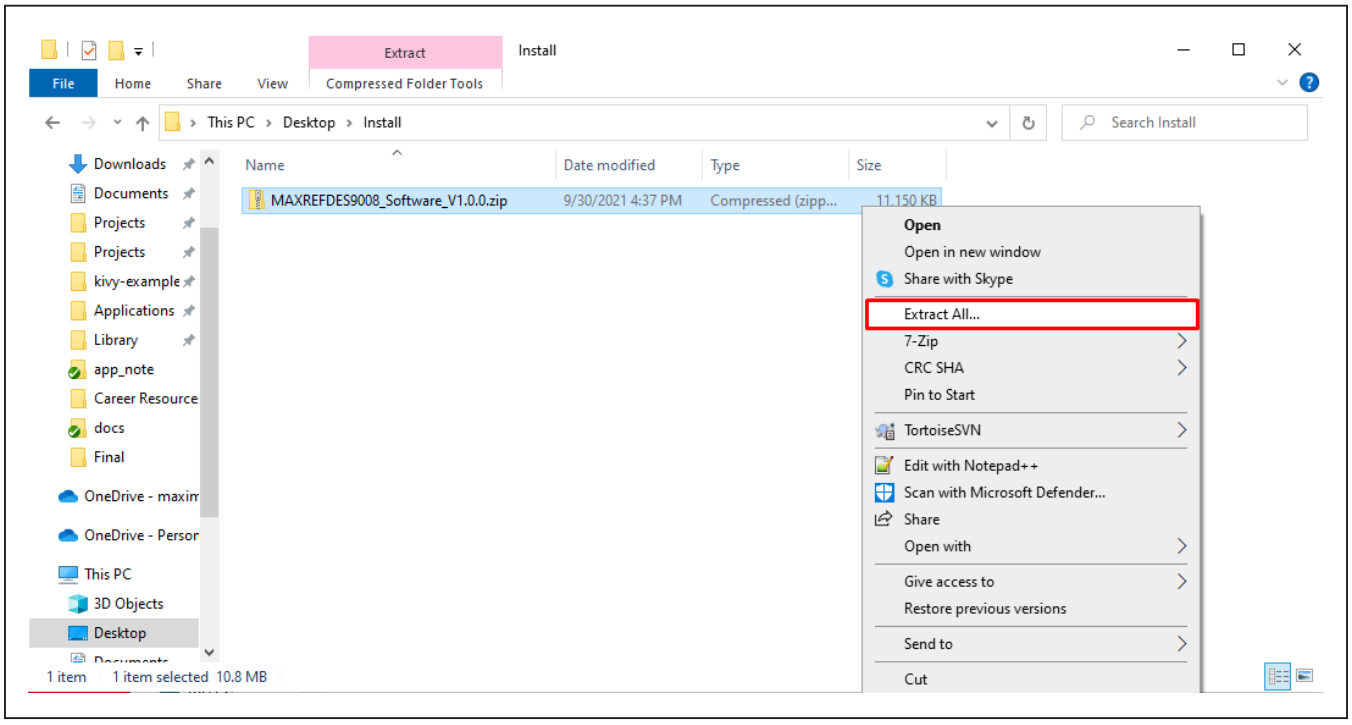

Figure 6. C-Demo extraction.

7) Open the **MAXREFDES9008_Software_V1.0.0** folder and copy the **demos** and **libraries** folder into the workspace location as shown in Figure 7.

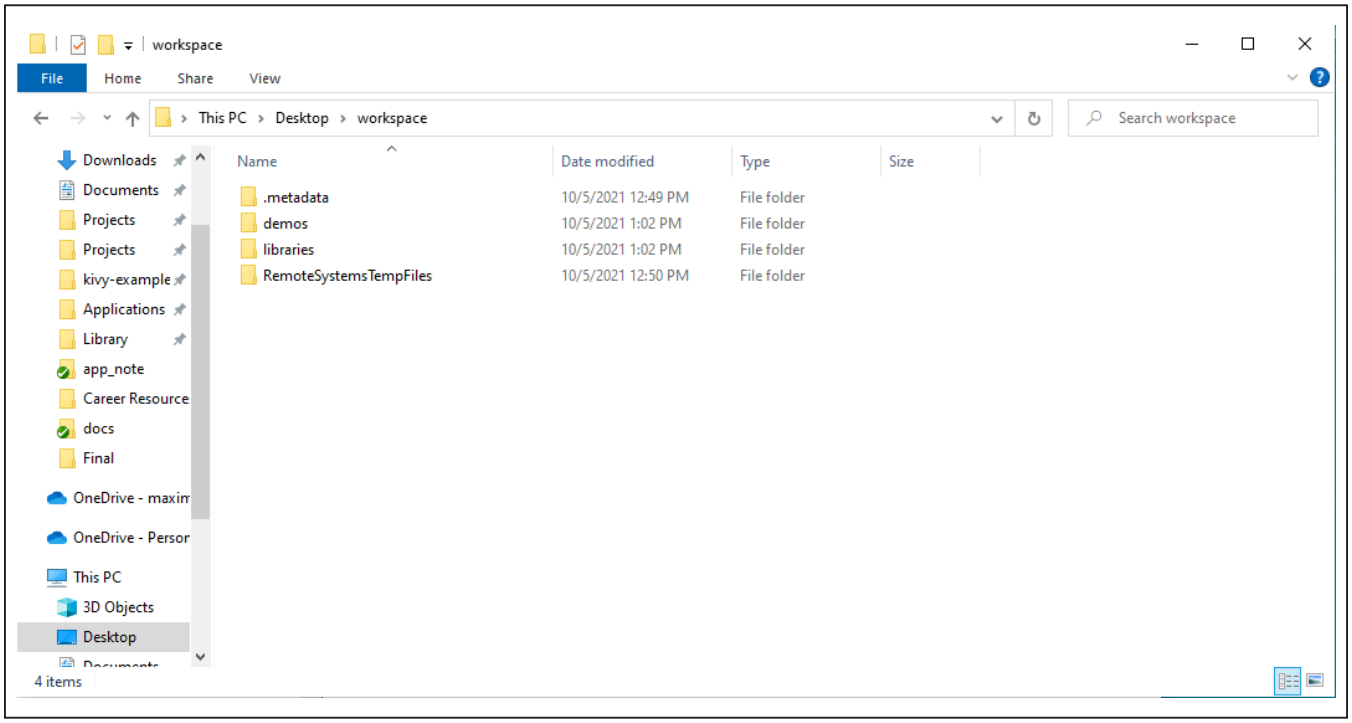

Figure 7. Software workspace.

8) From the **Eclipse** dialog box > **File** menu, select the **File > Open Projects from File System…** as shown in Figure 8.

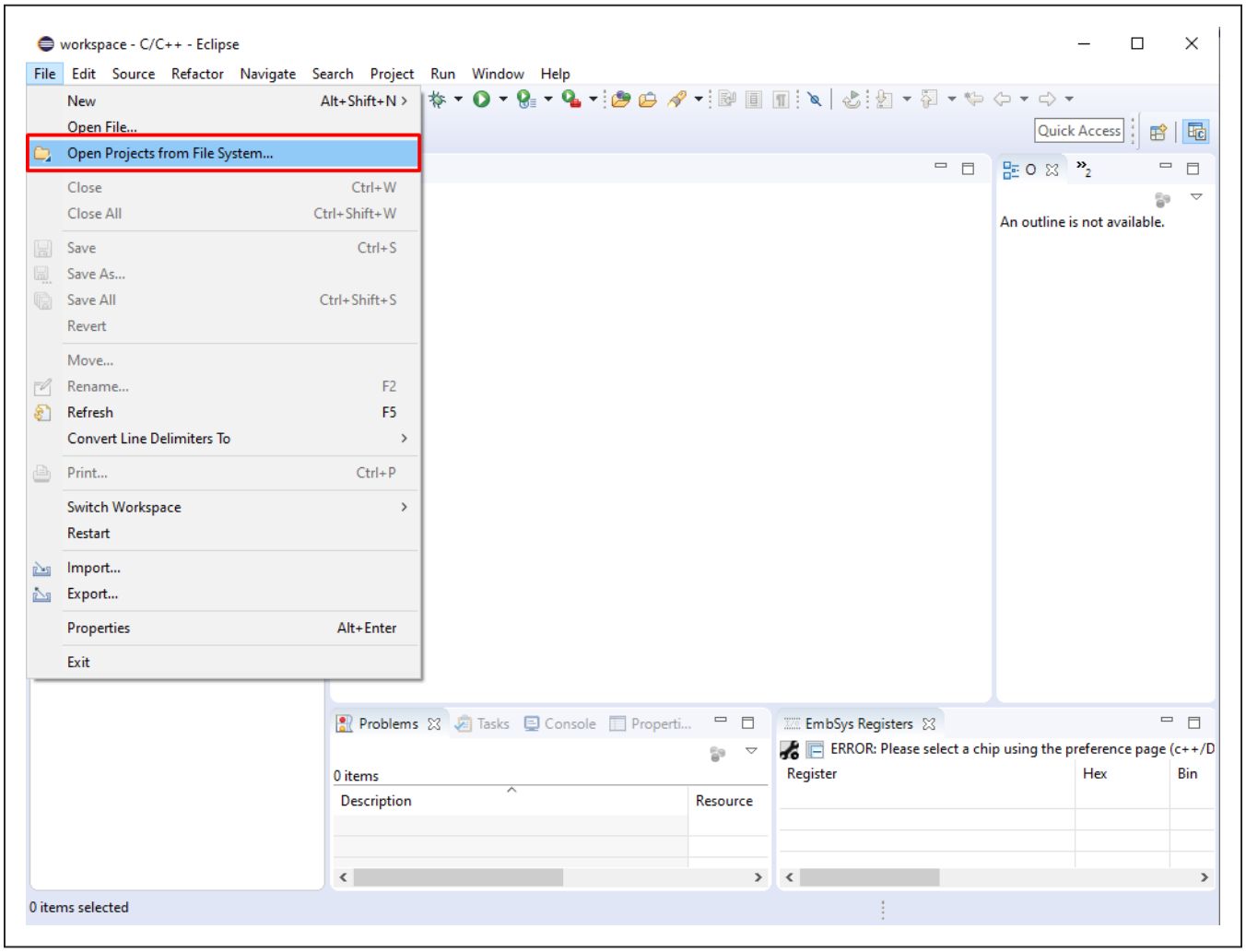

Figure 8. Eclipse Open Projects.

9) From the **Import Projects from File System or Archive** dialog box, click **Directory…** button and navigate to the **Demos** folder within the workspace location and click **Finish** as shown in Figure 9.

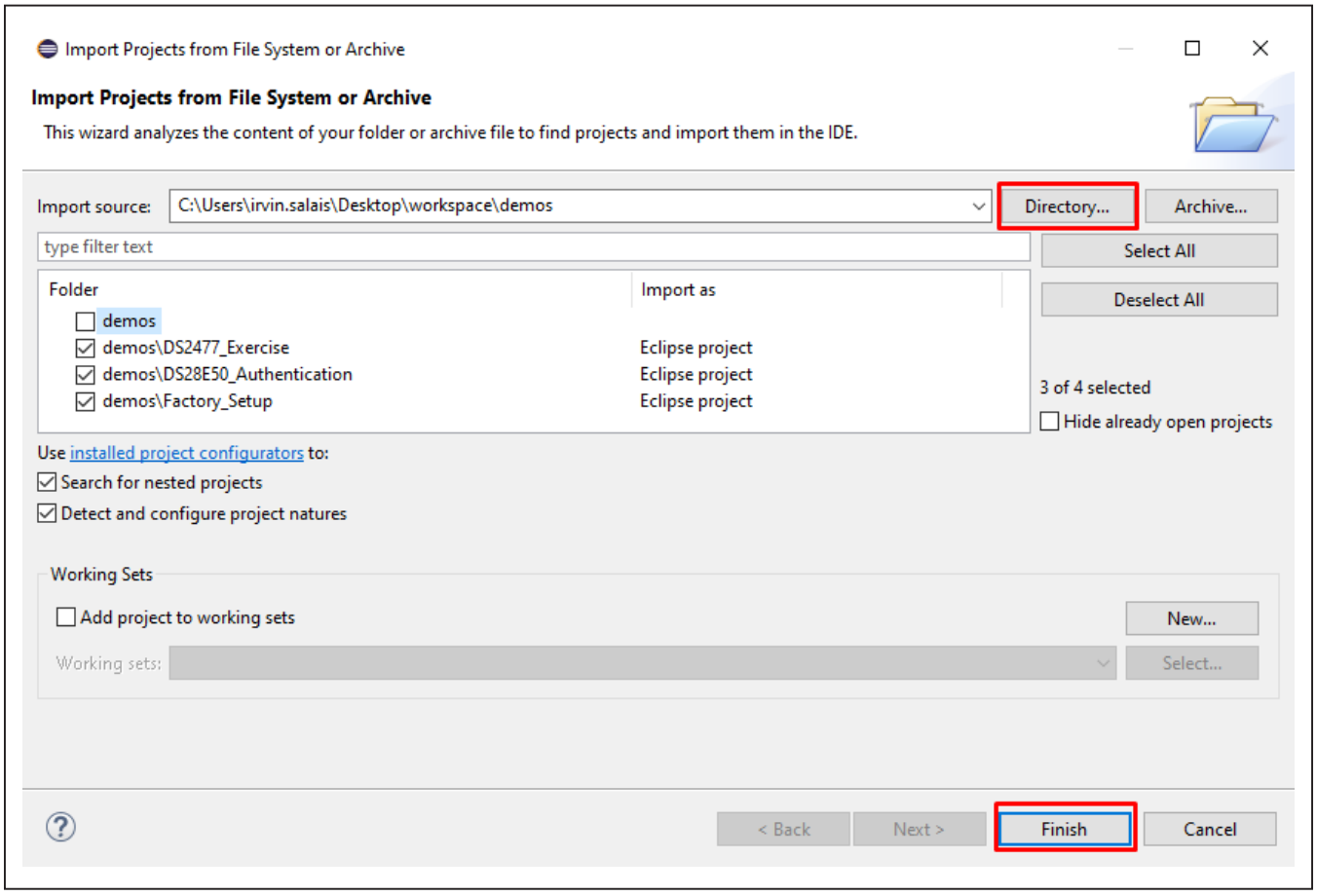

Figure 9. Eclipse Open Projects.

10) From the **Putty Configuration** dialog box, open up a terminal and connect it to the MAX32660's corresponding serial COM port as shown in Figure 10.

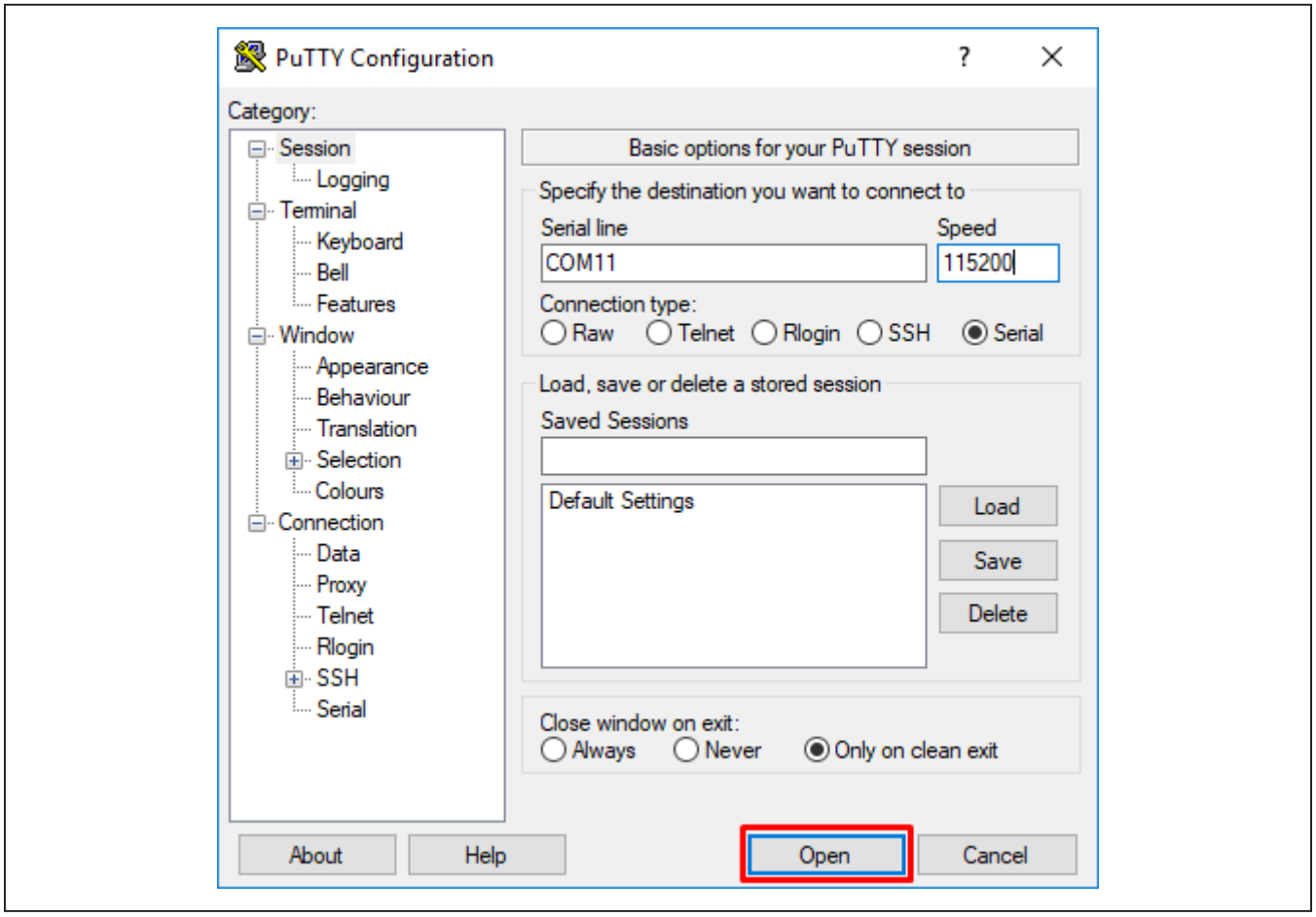

Figure 10. Opening a serial console.

11) From the **Eclipse** dialog box, select the example program to run under the drop-down box located next to the green **Run** button as shown in Figure 11. The output appears on the serial console as shown in Figure 12.

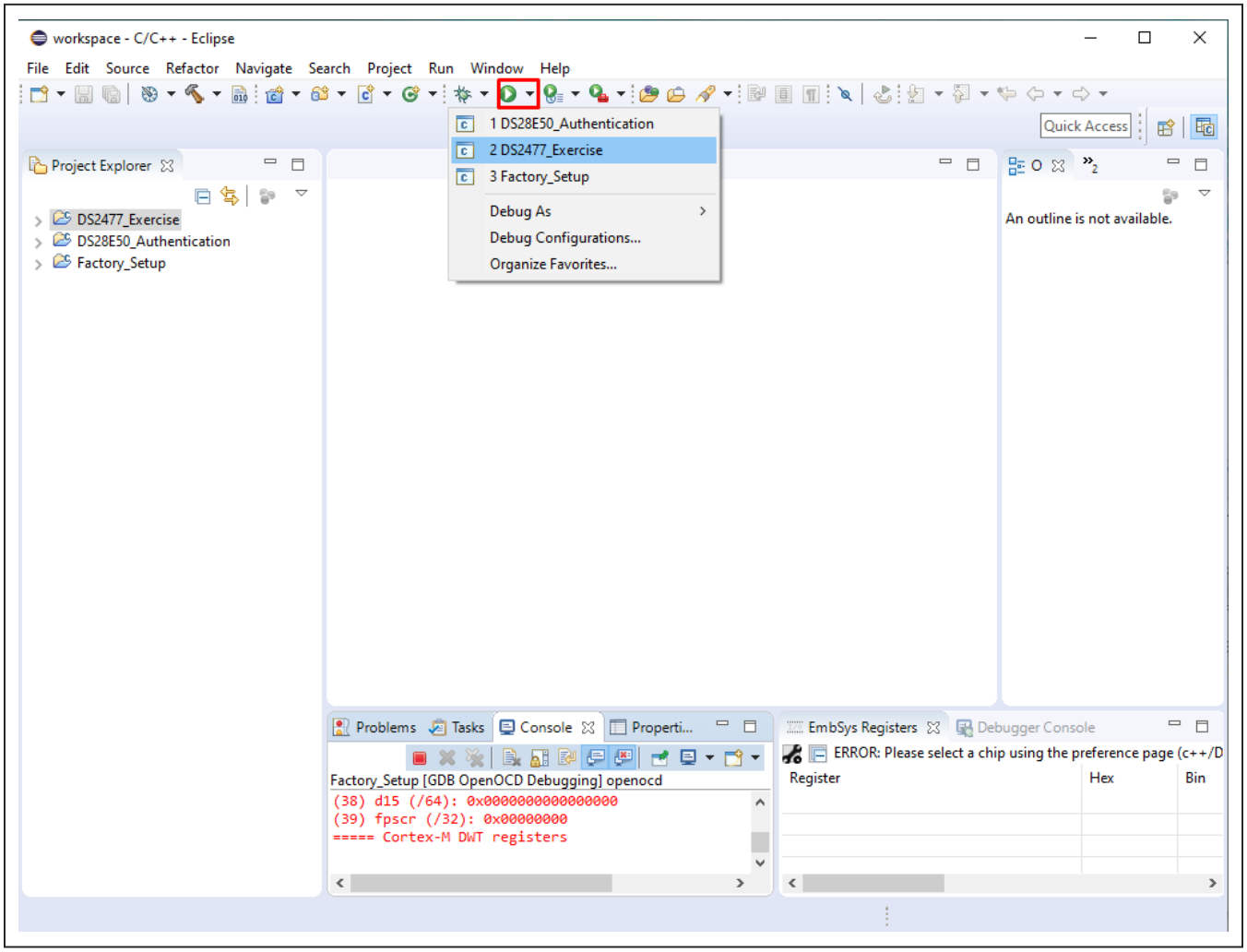

Figure 11. Running the demo program.

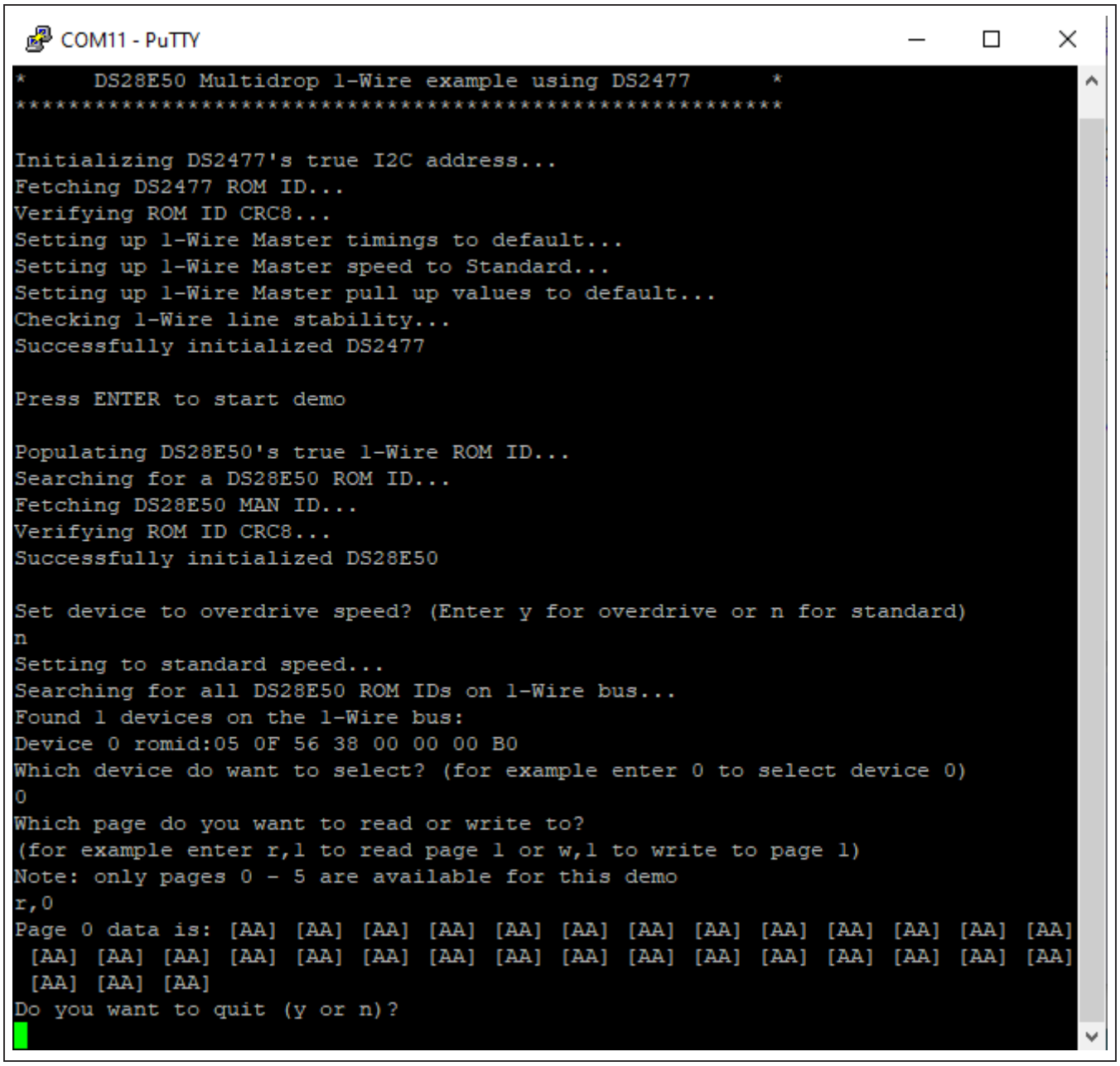

Figure 12. Console output for the demo program.

Detailed Description of Hardware

A detailed block diagram of the MAXREFDES9008 hardware is shown in Figure 13. A Maxim Integrated® MAX32660 Cortex M4 microcontroller is used as the system's host controller for the DS2477 through its I2C peripheral. The MAX32660's I2C port pins, P0_8 and P0_9, are connected to the DS2477's SDA and SCL pins, respectively, each with a 10kΩ external pullup resistor connected to 3.3V. The DS2477 bridges 1-Wire communication to a DS28E50 secure authenticator device by connecting the DS2477's and DS28E50's IO pins together.

Detailed Description of Software

The MAXREFDES9008 software consists of C-code demonstration programs for using the DS2477 and DS28E50 SHA3-256 authentication schemes. For a detailed list of available C-programs, see Table 1. The software is supported on the MAXREFDES9008 hardware and includes the firmware and source files for programming an Arm Cortex-M4 processor-based microcontroller like the MAX32660. This C-Demo software utilizes the DS2477 and DS28E50 APIs for convenient interfacing within the system. The software is compatible with the Maxim toolchain, that can be found in the Design Resources tab of the MAX32660 and can be directly imported into an Eclipse IDE workspace. For details on how to set up the C-Demo software, see the *Quick Start* Section.

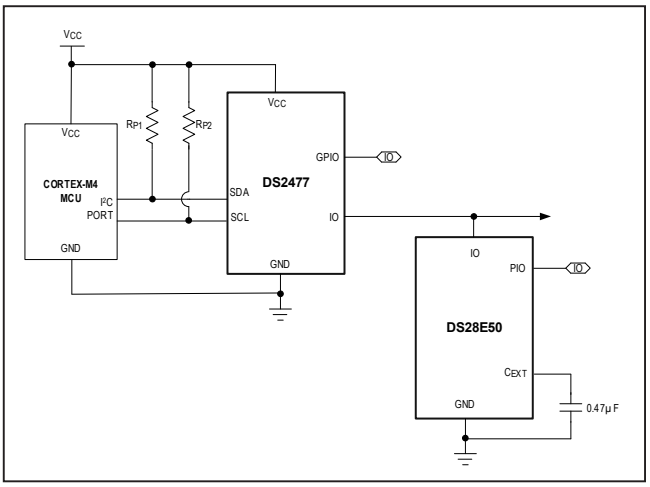

Figure 13. MAXREFDES9008 detailed block diagram.

Table 1. Demos Overview

DEMO PROGRAM	DESCRIPTION
DS2477_Exercise	Designed to get familiarized with the DS2477 and its 1-Wire master capabilities.
Factory Setup	For programming both the DS28E50 and the DS2477 in preparation for an authentication.
DS28E50_Authentication	For authenticating the DS28E50 target device. Computes unique secret for the DS28E50 1-Wire SHA-3 authenticator device and performs and verifies a Compute and Read Page Authentication on a preprogrammed device page. The DS28E50 and the DS2477 must first be setup with the 'Factory Setup' demo.

DS2477 API

Table 2 shows a brief overview of the DS2477 API. This API allows the MAX32660 to interface with the DS2477 through I²C and provides access to its commands.

DS28E50 API

The C-Demo software also provides a DS28E50 API. A brief overview of the DS28E50 API is shown in Table 3. This API makes it easy to exercise all the features of the DS28E50.

Table 2. DS2477 API Overview

FUNCTION	DESCRIPTION
DS2477_WriteMemory	DS2477 performs a 'Write Memory' command.
DS2477_ReadMemory	DS2477 performs a 'Read Memory' command.
DS2477_ReadStatus	DS2477 performs a 'Read Status' command.
DS2477_ReadRNG	DS2477 performs a 'Read RNG' command.
DS2477_SetPageProtection	DS2477 performs a 'Set Page Protection' command.
DS2477_EncryptedReadMemory	DS2477 performs a 'Encrypted Read Memory' command.
DS2477_ComputeAndLockSecret	DS2477 performs a 'Compute and Lock Secret' command.
DS2477_ComputeSessionKey	DS2477 performs a 'Compute Session Key' command.
DS2477_ComputeHMAC	DS2477 performs a 'Compute HMAC' command.
DS2477_ComputeSHA3	DS2477 performs a 'Compute SHA3' command.
DS2477_ReadOneWirePortConfig	DS2477 performs a 'Read 1-Wire Port Config' command.
DS2477_WriteOneWirePortConfig	DS2477 performs a 'Write 1-Wire Port Config' command.
DS2477_MasterReset	DS2477 performs a 'Master Reset' command.
DS2477_OneWireCommand	DS2477 performs a '1-Wire Command' command.
DS2477_OneWireBlock	DS2477 performs a '1-Wire Block' command.
DS2477_OneWireWriteBlock	DS2477 performs a '1-Wire Write Block' command.
DS2477_OneWireReadBlock	DS2477 performs a '1-Wire Read Block' command.
DS2477_OneWireSearch	DS2477 performs a '1-Wire Search' command.
DS2477_FullCommandSequence	DS2477 performs a 'Full Command Sequence' command.
DS2477_ComputeCrc16	DS2477 performs a 'Compute CRC16' command.

Table 3. DS28E50 API Overview

FUNCTION	DESCRIPTION
DS28E50_Initialize	Populates the ROM ID for all DS28E50 devices found on the 1-Wire bus.
DS28E50_WriteMemory	DS28E50 performs a 'Write Memory' command.
DS28E50_WriteMemoryEX	DS28E50 performs a 'Write Memory EX' command.
DS28E50_ReadMemory	DS28E50 performs a 'Read Memory' command.
DS28E50_ReadStatus	DS28E50 performs a 'Read Status' command.
DS28E50_SetPageProtection	DS28E50 performs a 'Set Page Protection' command.
DS28E50_ReadRNG	DS28E50 performs a 'Read RNG' command.
DS28E50_EncryptedReadMemory	DS28E50 performs a 'Encrypted Read Memory' command.
DS28E50_ComputeAndReadPageAuthentication	DS28E50 performs a 'Compute and Read Page Authentication' command.
DS28E50_AuthenticatedWriteMemory	DS28E50 performs a 'Authenticated Write Memory' command.
DS28E50_ComputeAndLockSecret	DS28E50 performs a 'Compute and Lock Secret' command.
DS28E50_DecrementCounter	DS28E50 performs a 'Decrement Counter' command.
DS28E50_Device_Disable	DS28E50 performs a 'Device Disable' command.

Design Resources

Download the complete set of **Design Resources** including the schematics, bill of materials, PCB layout, and C-demo software.

Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	2/22	Initial release	—