

FEATURES

- Demonstrates the capabilities of the DS2704 1280 bit EEPROM with SHA-1 Authentication Device, including:
 - Secure Challenge and Response Authentication using the SHA-1 Algorithm
 - 5 Lockable 32 Byte Pages of EEPROM with DS2502 Compatibility
 - Identification
- Interfaces to the USB Port of a PC running Windows OS that supports USB operation

INDEX

Evaluation Kit Contents
Equipment Needed
Introduction
Setup and Installation
 Board Connections
 Software Installation
Menus
 SHA-1 Tools
SHA-1 Tab
Memory Tab

INTRODUCTION

The DS2704K Evaluation Kit makes performance evaluation, software development, and prototyping with the DS2704 1280 bit EEPROM with SHA-1 Authentication easy. The evaluation board interfaces to a PC through a DS9123O USB Adapter and RJ-11 cable connection. The provided CD ROM contains all related data sheets along with the evaluation software, which can be run under any Windows operating system that supports USB operation.

The DS2704K evaluation software gives the user complete control of all SHA-1 and Memory functions of the DS2704 as well as the various other commands.

The evaluation board circuit is designed to provide the DS2704 with a stable environment to perform SHA-1 Calculations and program and read the DS2704. Kit demonstration boards will vary as they are improved upon over time. For information on the demonstration board circuits refer to the documentation directory on the DS2704K CD ROM.

EVALUATION KIT CONTENTS

- 1 pc. TSSOP Evaluation Board
- 1 pc. DS9123O USB Adapter
- 1 pc. RJ-11 Phone Cable
- 1 pc. DS2704K CD containing:
 - DS2704K Evaluation Software
 - DS2704 Related Data Sheets

REQUIRED EQUIPMENT

1. A PC running Windows 2000 or newer with a CD ROM drive and an available USB port.
2. A battery or power supply.
3. Cables with mini-grabber style clips or the ability to solder directly to connection pads.

SETUP AND INSTALLATION

BOARD CONNECTIONS

Connections to the demonstration board are best made either by soldering directly to the pads or by using cables with mini-grabber clips. Communication to the board can be accomplished through the RJ-11 jack by connecting the provided standard six conductor RJ-11 cord to the DS9123O USB Adapter. Simply attach the Bat+/Bat- terminals to a battery or power supply and the DS2704K software can communicate with the DS2704 for performing SHA-1 Calculations and accessing the memory.



Figure 1: DS2704K Evaluation Board (PD091605) Connections

SOFTWARE INSTALLATION

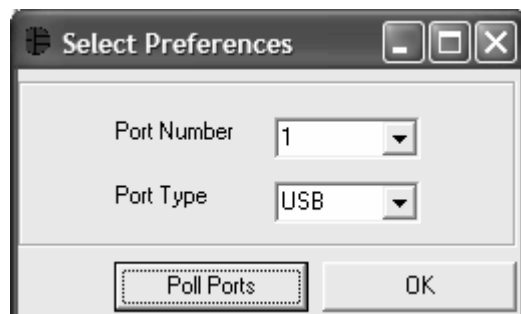
To install the DS2704K software, exit all programs currently running and insert the DS2704K software CD into your computer's CD ROM. The user can run SETUP.EXE from the setup directory and the installation process begins. Follow the prompts to complete the installation. The DS2704K software can be uninstalled in the Add/Remove Programs tool in the Control Panel. After the installation is complete, open the DS2704K folder and run DS2704K.EXE or select DS2704K from the program menu. A splash screen containing information about the evaluation kit appears as the program is being loaded.

The Documentation directory also located on the CD contains all relevant data sheets and application notes on the DS2704 and DS2704K. They are stored in Adobe Acrobat format for easy viewing.

SELECTING THE COM PORT

If the DS9123O is connected when the DS2704K is started, the software will start up automatically. If it is not connected, the Select Preferences window will open. This software will also operate with the DS9123 Serial Port Adapter.

In this window, select either serial port or USB communication and the port number; then hit OK. The DS2704K software saves this port selection and automatically uses the selection each time the program starts. To change the port later, click the Preferences option on the menu bar, select Edit Preferences, and then select the appropriate port. To attempt to automatically locate the DS9123O or DS9123, click the Poll Ports button. Warning - automatically polling for the DS9123 can disrupt other devices connected to your computer's COM ports.



MENUS

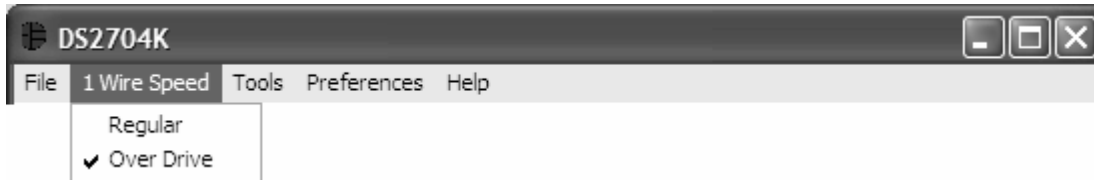
Several pull down menu options have been provided to simplify use of the DS2704K software for the user. Their functions are individually detailed below.

FILE MENU



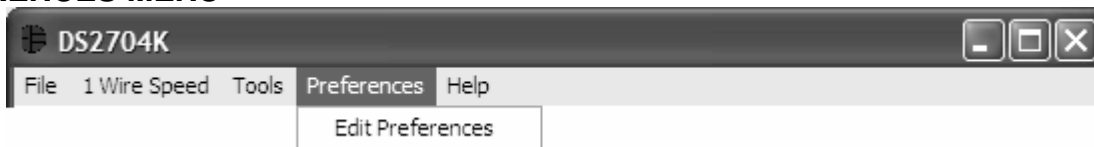
The File Menu allows the user to save the contents of the 160 bytes of EEPROM to a file so that other DS2704's can easily be programmed with the same data. To save the EEPROM values to a file, select Save Memory Set Up and enter a filename and select the location to store the file. This will store the contents of all of the text boxes on the Memory Tab to the selected file. To load the values from a file into the text boxes on the Memory Tab, select Load Memory Set Up and select the desired file.

1 WIRE SPEED MENU



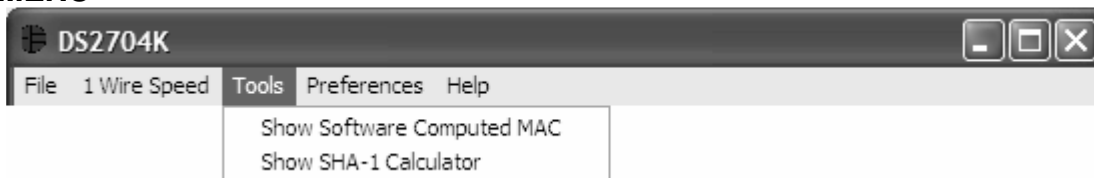
The 1 Wire Speed Menu allows the user to set the 1 Wire speed that the software uses. The DS2704 is capable of communicating at Regular and Over Drive speeds, so it is possible that the software will be communicating in one speed and the DS2704 will be in the other speed. This menu allows the user to specify which speed the software will use, but it will not make any changes to the device. The software will attempt to identify the correct speed of the device at startup, but in the event that the software and the device get out of sync, this Menu will allow the user to correct the problem. A check mark will be next to the speed that is currently in use by the software.

PREFERENCES MENU



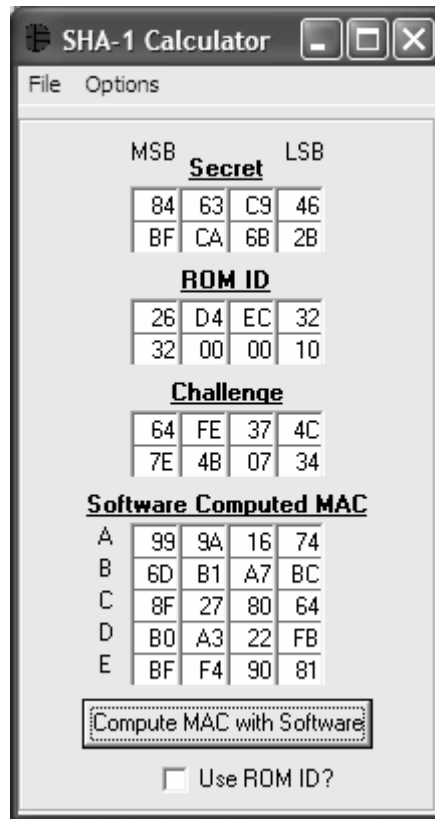
The Preferences Menu allows the user to change port settings at any time. Edit Preferences opens the Select Preferences window. See Selecting the COM Port above.

TOOLS MENU



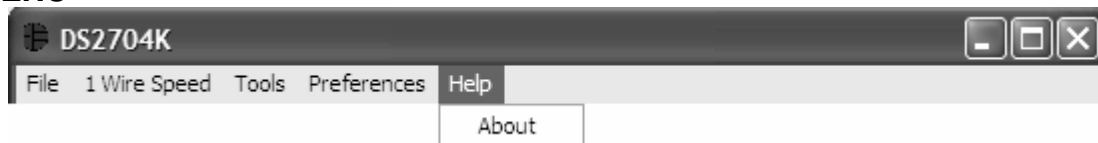
The software provides 2 tools to evaluate the SHA-1 calculations, a method to view the Software Computed MAC and a SHA-1 Calculator. Left-clicking on the Show Software Computed MAC Menu Item will expand the Main Window to show the MAC computed by the software. See the SHA-1 Tab section below for more details.

The SHA-1 Calculator



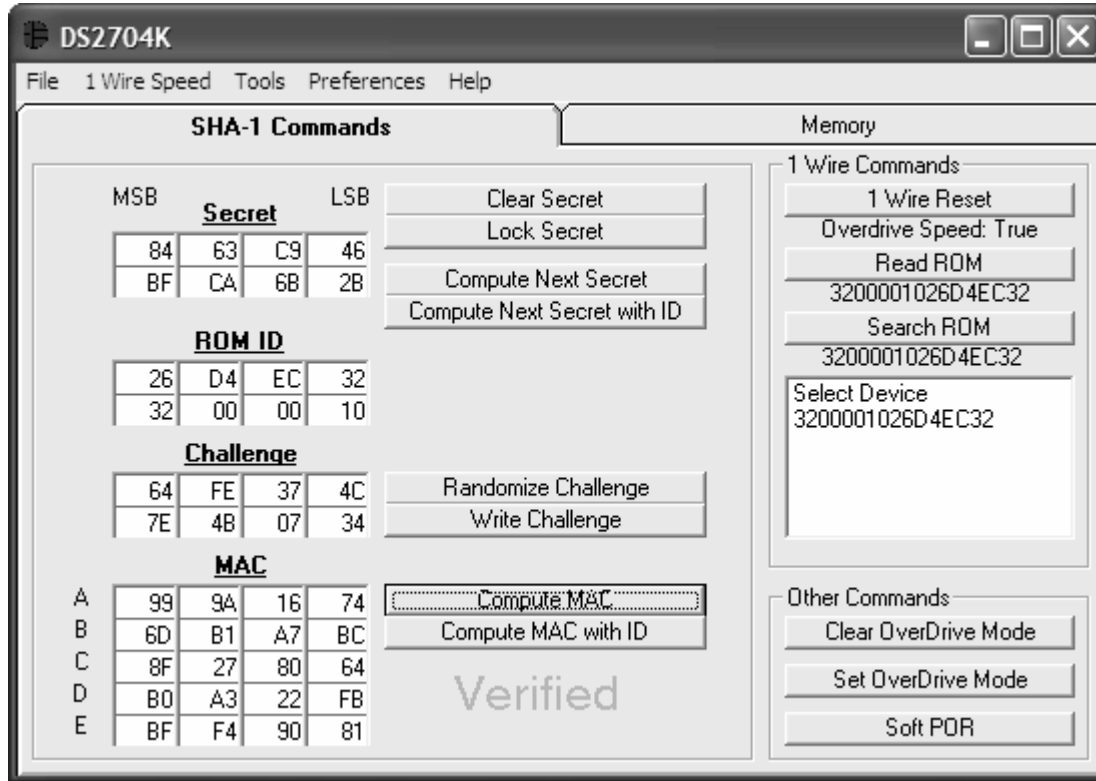
Left-clicking on the Show SHA-1 Calculator Menu Item will open a new window that will allow the user to perform SHA-1 calculations independent of the DS2704. Simply fill in the text boxes with the desired values and left-click on the Compute MAC with Software button. If the ROM ID is to be used in Computing the MAC, then check the Use ROM ID? check box. Use the Option – Fill with Values from Main Form Menu Item to fill the Secret, ROM ID and Challenge text boxes with values from the Main Program Window.

HELP MENU



Selecting the About topic from the Help Menu will open a window containing information about this program and Dallas Semiconductor.

SHA-1 Commands Tab

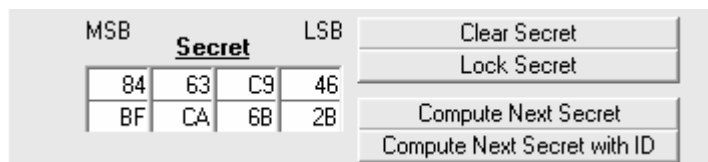


The functions of the DS2704 shown on the SHA-1 Commands Tab are divided into three sections: SHA-1 Commands, 1 Wire Commands, and Other Commands.

SHA-1 COMMANDS

The DS2704 uses an 8 byte Secret, the 8 byte ROM ID code of the device and an 8 byte Challenge to generate a 20 byte Message Digest (also called the MAC) using the SHA-1 encryption algorithm.

The Secret



The user is able to clear the 8 bytes of the Secret by left-clicking on the Clear Secret button. The top-right text box is the LSB of the Secret, and the bottom-left text box is the MSB of the Secret. (All text boxes are displayed in this same format.)

The user can also permanently lock the Secret by left-clicking on the Lock Secret button. Once the Secret is locked, it cannot be changed and cannot be read from the DS2704. The software will prompt the user to make sure the Secret is ready to be permanently locked.

Another feature of the DS2704 is to generate the Next Secret from the existing Secret, ROM ID and Challenge. It is important to Write the Challenge (see below) before left-clicking the Compute Next Secret or Compute Next Secret with ID button. The device will perform the SHA-1 calculation and create the Next Secret. The software will perform a SHA-1 calculation based on the values in the text

boxes for the Secret, ROM ID (if desired) and Challenge and place the new Secret, as calculated by software, in the Secret text boxes. The new Secret is never read back from the device.

It is important for the software and the DS2704 to have identical Secrets, ROM ID's, and Challenges so that the software can properly verify the operation of the DS2704. If the software is not in sync with the device, simply clear the Secret to get the software and hardware back in sync.

The DS2704 has 2 commands to compute the Next Secret. The Compute Next Secret with ID command uses the Secret, the ROM ID and the Challenge to perform the SHA-1 encryption algorithm. The Compute Next Secret command uses the Secret and the Challenge, but replaces the ROM ID with 0xFF's to perform the algorithm. The user can select which command is used by left-clicking on the appropriate button.

The ROM ID

ROM ID			
26	D4	EC	32
32	00	00	10

The ROM ID code is unique for each DS2704 device and cannot be changed by the User. The user can load the ROM ID of the device into the ROM ID text boxes by using the Read ROM or Search ROM functions described in the 1 Wire Commands section.

The Challenge

Challenge			
64	FE	37	4C
7E	4B	07	34

The Challenge is a random 8 byte block that is used by the DS2704 to perform the SHA-1 encryption algorithm. Each time the SHA-1 is performed, either during a Compute Next Secret or a Compute MAC (see below) the Challenge is left in an undefined state. Therefore the user must left-click on the Write Challenge button prior to each computation in order to get a proper SHA-1 calculation.

The user can left-click on the Randomize Challenge button to load a random challenge into the Challenge text boxes. Left-clicking this button does not write the Challenge to the device. It is still required that the user left-click on the Write Challenge button to write the challenge to the device.

The MAC

	MAC			
A	99	9A	16	74
B	6D	B1	A7	BC
C	8F	27	80	64
D	B0	A3	22	FB
E	BF	F4	90	81

Verified

The MAC is the 20 byte message digest that is the result of the SHA-1 encryption algorithm. When the Secret has been loaded properly, the ROM ID has been read, and the Challenge has been written to the device, left-clicking on the Compute MAC or Compute MAC with ID button will perform the SHA-1 calculation, read back the results, and then display them in the MAC text boxes.

The software will also perform the SHA-1 calculations based on the Secret, ROM ID (if desired) and Challenge text box values and compare its results to the results read back from the DS2704. If the MAC computed by the software and MAC read back from the DS2704 match, then the software will display “Verified”. If they do not match, “Not Verified” will be displayed. The user can view the Software Computed MAC by using the Tools Menu – Show Software Computed MAC. The user also can compute the MAC with the DS2704, then change 1 bit in one of the text boxes of the Secret, and then Compute the MAC with software to see how big of a difference changing 1 bit will make.

Software Computed MAC				
A	99	9A	16	74
B	6D	B1	A7	BC
C	8F	27	80	64
D	B0	A3	22	FB
E	BF	F4	90	81

Compute Software MAC

Compute Software MAC with ID

If the MAC is “Not Verified”, make sure that the Challenge was written prior to computing the MAC. If the “Not Verified” error continues, perhaps the Secret in the device does not match what is in the Secret text boxes and the user will need to clear the Secret of the DS2704.

1 WIRE COMMANDS

1 Wire Commands

1 Wire Reset

Overdrive Speed: True

Read ROM

3200001026D4EC32

Search ROM

3200001026D4EC32

Select Device

3200001026D4EC32

1 Wire Reset

All communication to the DS2704 occurs over the 1-Wire bus, but the device can be configured to communicate at Regular 1-Wire Speed or at Over Drive Speed. The user can left-click on the 1-Wire Reset button and a 1-Wire Reset will be generated at the proper 1-Wire speed. The caption below the 1-Wire Reset button will display which 1-Wire Speed is used. It will also indicate whether a device on the bus responded to the 1-Wire Reset with a Presence Detect pulse at the proper 1-Wire speed.

Read ROM

The user can left-click on the Read ROM button to perform the Read ROM function. The result of the Read ROM will be displayed in the caption below the button. If a single 1-Wire device is located on the bus, the device’s ROM ID will be displayed. If more than one 1-Wire device is on the bus, the result will be a logical AND of the ROM ID’s of all of the devices on the bus. The result will also be displayed in the ROM ID text boxes in the SHA-1 Commands Sections.

Search ROM

If one or more 1-Wire devices are on the bus, the user can left-click on the Search ROM button to perform the Search ROM Routine. This will find all 1-Wire devices on the 1-Wire bus communicating at

the specified 1-Wire speed and will display the results in the list box. The user can left-click on any of the ROM ID's in the text box to select that device. The selected ROM will appear in the caption below the Search ROM button as well as be displayed in the ROM ID text boxes in the SHA-1 Commands Sections. This ROM ID will be used for the Match ROM portion of the communication. If no ROM ID is selected, a Skip ROM command will be used.

OTHER COMMANDS



The Other Commands Section contains 3 other commands of the DS2704: Clear Over Drive Mode, Set Over Drive Mode, and Soft POR.

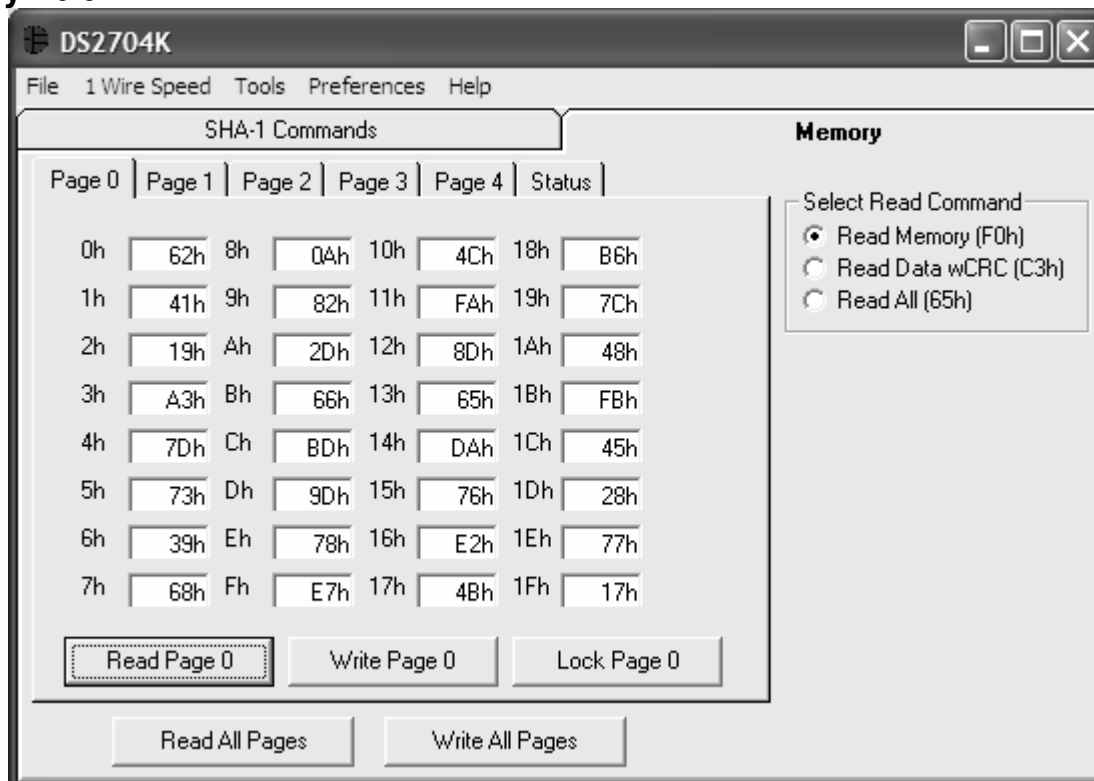
Set/Clear Over Drive Mode

The user can left-click on the Clear Over Drive Mode or Set Over Drive Mode to send the command to the device to configure the device to communicate in Regular 1-Wire Speed or in Over Drive Speed. It is important that the software and the device are communicating at the same speed in order for these commands to have any affect. After either of these buttons has been clicked, the software will send the command at the current 1-Wire speed, and then will switch the software to the appropriate speed.

Soft POR

The final button in this section is the Soft POR button. The user can left-click on the Soft POR button to send the command to the device, which causes the device to be internally reset. The part goes through its Power On Reset procedure without actually cycling the power on the device.

Memory Tab



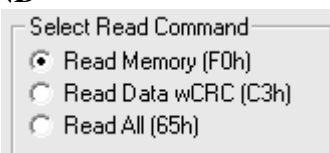
The Memory Tab contains a sub-tab which allows the user to access the 5 pages of EEPROM and the Status Page. Each sub-tab provides Read/Write Access to the memory locations displayed on that single page as well as the ability to permanently lock each Page of EEPROM.

When the EEPROM is written, it is read back to verify it was written properly. If the data that is read back is incorrect, an error message will be displayed. One reason to see this error is if the page is locked prior to writing.

When a Lock Page button is clicked, the page will be permanently locked. The user will be prompted before the page is locked. The pages of EEPROM can also be locked by writing the Write Protection byte on the Status sub-tab.

The Read Every Page button and Write Every Page button allow for all the pages to be read or written at one time.

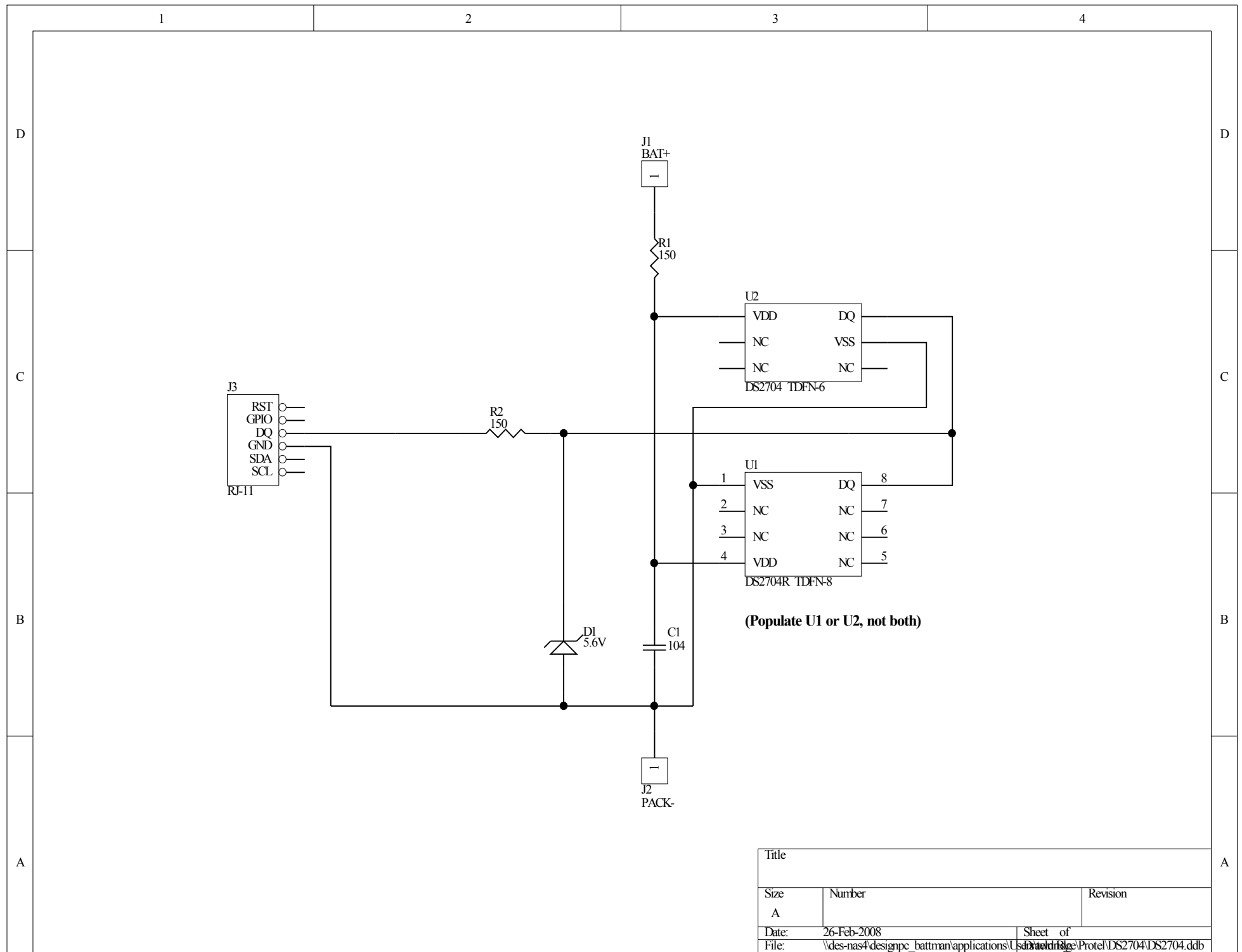
SELECTING THE READ COMMAND



There are three commands available to read the memory of the DS2704. The Read Memory Command (F0h) and the Read Data with CRC Command (C3h) are identical to the same commands of the DS2502. The DS2502 only has Pages 0, 1, 2, and 3, so these commands only allow access to these pages. To read Page 4, use the Read All Command (65h). The Read All Command can be used to read all five pages of EEPROM. See the DS2704 Datasheet for more information on the various commands.

To select a Read Command, simply click the radio button next to the desired command in the Select Read Command section. Clicking any of the Read Page buttons or the Read Every Page button will use the selected command to read the memory.

A CRC of the data read from memory is read from the DS2704 following the reading of certain memory locations which is different for each read command. The Read Memory Command reads a CRC following memory location 7Fh. The Read Data with CRC Command reads a CRC following the end of each page. The Read All Command reads a CRC following a read of memory location 9Fh. Each time the CRC is read it will be displayed at the bottom of the sub-tab.



Title		
Size	Number	Revision
A		
Date:	26-Feb-2008	Sheet of
File:	\\des-nas4\design\pc_battman\applications\Substrate\Protel\DS2704\DS2704.ddb	