Release Notes for CrossCore Serial Flash Programmer 1.2.0

http://www.analog.com
processor.tools.support@analog.com

Contents

1 Introduction

The CrossCore Serial Flash Programmer (CCSFP) is a Windows utility for programming the flash memory of supported Analog Devices processors via a UART serial port.

The installer allows the user to choose the install location. By default, CCSFP is installed at *C:\Analog Devices\CrossCore Serial Flash Programmer 1.2.0*. A start menu entry is created under *Analog Devices\CrossCore Tools*. Settings are stored in *Analog Devices\Cross Core Serial Flash Programmer.ini* within the current user's local settings directory.

2 News

Release 1.2.0 adds support for ADSP-CM41x parts.

3 Technical support

You can reach Analog Devices software and tools technical support in the following ways:

- Post your questions in the software and development tools support community at EngineerZone®.
- E-mail your questions to processor.tools.support@analog.com.
- E-mail your questions about processors and processor applications to processor.support@analog.com.
- Submit your questions to technical support directly via http://www.analog.com/support.
- Contact your Analog Devices sales office or authorized distributor.

4 File formats

CCSFP supports Intel Hex (*.hex*) and plain binary (*.bin*) as flash image file formats. In *IAR Embedded Workbench* projects, generation of an Intel Hex file or a binary file can be enabled on the *Output Converter* pane of the project options.

For Intel Hex files, CCSFP checks addresses covered in the file against the flash address range of the target processor. Any other files are treated as binary files assumed to start at the flash start address, while their size is checked against the target flash size. The use of Intel Hex files is recommended for the additional address checking.

CCSFP does not support ELF executables. If given one as an input file, it will treat it as a binary file and write its entire content including bookkeeping information such as section headers and symbol table to flash, so the code in the ELF will not run as expected.

5 Supported parts

CCSFP 1.2.0 supports ADSP-CM40x, ADSP-CM41x and ADuCM302x parts.

5.1 ADSP-CM40x

ADSP-CM40x parts from revision G onwards are supported.

The ADSP-CM40x boot ROM does not directly support flash programming. Therefore, CCSFP works by first downloading a second stage kernel to RAM, which then receives and programs the actual flash image.

This requires the UART slave boot mode to be active, which is boot mode number 3. The boot mode is selected by the two BMODE pins, which are connected to a rotary switch on ADSP-CM40x EZ-KIT boards. The boot mode becomes active on reset.

In UART slave boot mode, the boot ROM receives a boot loader stream via UART0, which is connected to the RS232 socket on EZ-KIT boards. The *ADSP-CM40x-FlashProgrammer.ldr* file in the CCSFP install is the loader stream containing the second stage kernel. Its source code can be found in the *src\ADSP-CM40x* directory.

Booting an application that has been programmed into flash requires boot mode 1 to be selected.

5.1.1 Example

The *examples* directory of the CCSFP install contains example flash application images for ADSP-CM403F and ADSP-CM408F EZ-KIT boards: *ADSP-CM403F-Button.hex* and *ADSP-CM408F-Button.hex*. These are builds of the Button_LED_GPIO example from the *ADSP-CM40x Enablement Software Package* (ESP) version 2.1.0.

The following instructions assume that the flash is blank or that it contains a valid image without security features enabled.

1. Connect the host to the EZ-KIT's RS232 port socket, either directly from a serial port or via a USB-to-Serial adapter.
2. Select boot mode 3 on the board.
3. Reset the board.
4. Open CrossCore Serial Flash Programmer.
5. Select *ADSP-CM40x* as the target and the appropriate serial port.
6. Select the *Program* action.

7. Click the *Browse* button for the *File to download*, and select the appropriate *.hex* file for the connected EZ-KIT from the *examples* directory of the CCSFP install.
8. Click *Start*.
    a. If the autobaud fails when trying to send the second stage kernel, retry steps 1 to 3.
    b. If the autobaud fails when trying to program the flash, the part is probably locked. See the Recovering a locked part section below.
9. Once the operation completes, select boot mode 1 on the board and reset.
10. The example application should now be running. Pressing the *PB1* or *PB2* buttons should toggle the LEDs adjacent to them.

5.1.2 Security

ADSP-CM40x parts implement a security scheme intended to prevent unauthorized reading of the flash content. This uses a 128-bit key that is part of a security header at the start of flash at address 0x1800_0000.

In the ESP example projects, the key is defined in header *inc\adi_ecc.h*. That header and the ESP release notes have further details on this. Initially, the header contains the so-called default debug key, which enables debugging and disables security:

```
#define ADI_SECURITY_USER_KEY0      0xa4b8e4a5
#define ADI_SECURITY_USER_KEY1      0xd2041dd7
#define ADI_SECURITY_USER_KEY2      0x18839df8
#define ADI_SECURITY_USER_KEY3      0x8392c1fe
```

However, if an application image with a valid secure header containing a key other than the default debug key has been written to flash, then that key needs to be provided to allow programming through CCSFP. (Note that changing the key in *inc\adi_ecc.h* header requires a utility called *EccGen.exe* to be run on it to update the checksum fields in the header. Otherwise the security header becomes invalid. Further details are in the header.)

The key has to be entered as a 32-digit hexadecimal number into CCSFP's *Key* field, in the same order as the definitions in the header, and without a *0x* or other prefix. For example, a key defined as follows would need to be entered as *00112233445566778899aabbccddeeff*:

```
#define ADI_SECURITY_USER_KEY0      0x00112233
#define ADI_SECURITY_USER_KEY1      0x44556677
#define ADI_SECURITY_USER_KEY2      0x8899aabb
#define ADI_SECURITY_USER_KEY3      0xccddeeff
```

(Due to little-endian byte order within words, in flash that key would be stored in order *33 22 11 00 77 66 55 44 bb aa 99 88 ff ee dd cc*.)

5.1.3 Recovering a locked part

If a part is locked due to an invalid security header or a valid security header with a non-default key, it can be recovered by using the *Erase locked flash* action after resetting in boot mode 3. This sends a command for erasing the entire flash. The command is ignored if the flash is not locked.

The erase operation may take up to 4 minutes, although on EZ-KITs it typically takes less than 30 seconds. Completion is not reported back to the host, but is indicated by the SYS_FAULT pin connected to a red LED on EZ-KITs. Following the erase, the part has to be reset again to enable programming.

5.2 ADSP-CM41x

The ADSP-CM41x boot ROM directly supports flash programming, so a second stage kernel is not required. This requires the UART boot mode to be enabled by pulling the SYS_BMODE pin high. On ADSP-CM419F EZ-Boards, this can be done by closing jumper JP1.

The boot ROM receives commands via UART3. On ADSP-CM419F EZ-Boards, this is connected to an on-board USB-to-serial converter, so the host needs to be connected with a USB cable plugged into the mini-USB socket labelled P3. Connecting an actual serial cable to one of the RS232 sockets will not work.

CCSFP supports the following actions for ADSP-CM41x parts:

- Program: Program an image to the flash user area, after erasing it up to the last page touched by the image.
- Write key: Write 128-bit key to the key field of the flash info area.
- Erase user area: Mass erase the flash user area.
- Erase and initialize: Mass erase both the info and user areas of flash and write the info area "contrast" field to mark it as initialized, so that the other actions are permitted. This also clears any key that might have been written.

Programming of info space outside the contrast and key fields is not currently supported.

5.2.1 Example

The *examples* directory of the CCSFP install contains an example flash application image for ADSP-CM419F EZ-KIT boards: *ADSP-CM41x-Button.hex*. This is a build of the Button_LED_polled/M4 example from the *ADSP-CM41x Board Support Package* (BSP) version 1.0.0 Alpha.

Instructions for ADSP-CM419F EZ-BOARD BOM 1.1:

1. Connect the host to the mini-USB socket labelled P3.

2. Ensure jumper JP1 is closed (to pull the SYS_BMODE pin high).
3. Reset.
4. Open CrossCore Serial Flash Programmer.
5. Select *ADSP-CM41x* as the target.
6. Select the appropriate "COMx (USB Serial Port)" from the serial port dropdown.
7. Select the *Program* action.
8. Click the *Browse* button for the *File to download*, and select the *ADSP-CM41x-Button.hex* file from the *examples* directory of the CCSFP install.
9. Click *Start*.
    a. If the autobaud fails when trying to send the second stage kernel, retry steps 1 to 3.
    b. If programming fails with "Permission denied", the part has been protected with a key. Either the correct key needs to be provided, or the key and all content of the flash have to be erased using the "Erase and initialize" action.
10. Once the operation completes, open jumper JP1 and reset.
11. The example application should now be running. Pressing the *SW4* button should light up *LED3* nearby.

5.2.2 Security

ADSP-CM41x parts implement a security scheme intended to prevent unauthorized reading of the flash content. This uses a 128-bit key located in the the info space part of the flash.

A key can be written using the *Write Key* action. The key has to be entered as a 32-digit hexadecimal number, without a *0x* or other prefix. It is written to flash with little-endian byte order within each 32-bit word. For example, a key entered as *00112233445566778899aabbccddeeff* would be written in byte order *33 22 11 00 77 66 55 44 bb aa 99 88 ff ee dd cc*. Writing an all-F key is equivalent to not writing a key at all. Writing an all-zero key also leaves the part unlocked.

When a key has been written, the same key has to be provided for the *Program* and *Erase user area* actions to be permitted. In this case, before programming an image, CCSFP downloads and runs a small application that confirms that the security features have been enabled during manufacture of the target part, so that protected code is not accidentally written to an unsecured part.

If the key has been lost, the part can be recovered using the *Erase and Initialize* action, which erases both the info and user areas of the flash, including the key. Similarly, changing a known key requires *Erase and Initialize* before writing a new key.

5.3 ADuCM302x

The default ADuCM302x boot kernel in the flash info space does not directly support flash programming. Therefore, CCSFP works by first downloading a second stage kernel to RAM, which then receives and programs the actual flash image.

This requires the UART boot mode to be enabled by pulling pin GPIO01 high during reset. On ADuCM302x EZ-KIT boards, this can be done by holding the button labelled *BOOT* while pressing the *RESET* button.

In UART boot mode, the boot kernel receives commands via UART0. On EZ-KIT boards, this is connected to an on-board USB-to-serial converter, so the host needs to be connected with a USB cable plugged into the mini-USB socket labelled *USB TO UART*. In the CCSFP serial port selection, this will appear as "COMx (USB Serial Port)", whereby the 'x' is a number automatically assigned by the system.

The *ADuCM302x-FlashProgrammer.hex* file in the CCSFP install contains the second stage kernel. Its source code can be found in the *src\ADuCM302x* directory.

CCSFP supports the following actions for ADuCM302x parts:

- Erase: Erase the entire user flash.
- Program: Program a flash image, erasing the entire user flash first.
- Load & Run: Load and run an application that has been linked to run from SRAM.

Programming the ADuCM302x flash info space is not supported.

5.3.1 Examples

Programming flash

The *examples* directory of the CCSFP install contains an example flash application image for ADuCM302x EZ-KIT boards: *ADuCM302x-Button.hex*. This is a build of the LED_button_polled example from the *ADuCM302x Board Software Package* (BSP) version 1.0.1.

Instructions:

1. Connect the host to the EZ-KIT's USB TO UART mini-USB socket.
2. Hold down the BOOT button while pressing RESET.
3. Open CrossCore Serial Flash Programmer.
4. Select *ADuCM302x* as the target.
5. Select the appropriate "COMx (USB Serial Port)" from the serial port dropdown.

6. Select the *Program* action.
7. Click the *Browse* button for the *File to download*, and select the *ADuCM302x-Button.hex* file from the *examples* directory of the CCSFP install.
8. Click *Start*.
    a. If the autobaud fails when trying to send the second stage kernel, retry steps 1, 2 and 5.
    b. If the autobaud fails when trying to program the flash, the part might be write-protected. The correct key will be needed to program it.
9. Once the operation completes, press RESET again, without holding the BOOT button.
10. The example application should now be running. Pressing the *PB0* or *PB1* buttons should light up *LED4* or *LED5* adjacent to them.

Running from RAM

The examples directory also contains an example SRAM application image: *ADuCM302x-Button-RAM.hex*. This is a build of the LED_button_polled example that has been modified to place its code in RAM rather than flash.

Instructions:

1. Connect the host to the EZ-KIT's USB TO UART mini-USB socket.
2. Hold down the BOOT button while pressing RESET.
3. Open CrossCore Serial Flash Programmer.
4. Select *ADuCM302x* as the target.
5. Select the appropriate "COMx (USB Serial Port)" from the serial port dropdown.
6. Select the *Load & Run* action.
7. Click the *Browse* button for the *File to download*, and select the *ADuCM302x-Button-RAM.hex* file from the *examples* directory of the CCSFP install.
8. Click *Start*. If the autobaud fails, retry steps 1, 2 and 5.
9. Once the operation completes, the example application should be running. Pressing the *PB0* or *PB1* buttons should light up *LED4* or *LED5* adjacent to them.

5.3.2 Security

The default ADuCM302x boot kernel in flash info space implements a security scheme intended to prevent unauthorized reading or writing of the user flash content, which involves a security header at flash address 0x0000_0180. The scheme uses a 128-bit key. The security header in flash only stores a 128-bit hash of the key, which is calculated using the SHA256 algorithm.

If write protection has been enabled by programming 0x4E6F5772 ("NoWr") at flash address 0x0000_0198, the boot kernel will only start the second stage or other program downloaded via UART if the key matching the hash has been provided at SRAM address 0x2000_0180. If a key is entered in the CCSFP user interface, it will be placed at that address before attempting to start the downloaded program.

The key is not needed for programming when read protection but not write protection has been enabled. However, it would be needed when attempting to Load & Run a program that needs to read the flash content. Without the key, the program would be allowed to run, but attempts to read the flash would fail.

In CCSFP, the 128-bit key has to be entered as a 32-digit hexadecimal number, without a *0x* or other prefix. It is written to SRAM with little-endian byte order within each 32-bit word. For example, a key entered as *00112233445566778899aabbccddeeff* would be written in byte order *33 22 11 00 77 66 55 44 bb aa 99 88 ff ee dd cc*.

6 Command line invocation

CCSFP can also be invoked from a command line, as follows:

```
Usage: ccsfp [options] [file]

Options:
-a|-auto
        Enable unattended mode.
-b|-baud <number>
        Select baud rate.
-k|-key <key>
        Provide 32-digit hexadecimal unlock key.
-p|-port <name>
        Select serial (e.g. COM1).
-t|-target <name>
        Select target (as defined in ADIChip.ini).
-x|-action program|erase|load
        Select action. Defaults to 'program'.
-v|-version
        Print version information.
-h|-help
        Print this help message.
```

In unattended mode, the file argument has to be provided. The download starts automatically and the application exits as soon as the download finishes or fails. Settings not provided on the command line are read from the settings file. The exit code is 0 in case of a successful download, 1 in case of failure, and 2 if invalid command line arguments are supplied.

For example:

```
> ccsfp -a -p COM0 -b 115200 ADSP-CM403F-Button.hex
```

Note that since ccsfp.exe is a Windows subsystem program rather than a Console one, the Windows Command Prompt (cmd.exe) will automatically launch it as a background process, which means that the process cannot print to the console and that cmd.exe does not wait for it to finish. This can be worked around by piping output to the *more* command:

```
> ccsfp -a -p COM0 -b 115200 ADSP-CM403F-Button.hex | more
```

No such workaround is needed when running from a Cygwin terminal.