Application Report

C2000™ DCSM Security Tool

Nima Eskandari

ABSTRACT

The C2000™ dual code security module (DCSM) is a security feature incorporated in C2000 devices. The C2000 DCSM Security Tool allows you to configure the DCSM module through an intuitive graphical user interface (GUI). This application report examines the features of the C2000 DCSM Security Tool.

Table of Contents

List of Figures

List of Tables

Trademarks

1 Introduction

This document guides you through the following items related to the DCSM Security Tool:

- Importing the example DCSM Security Tool (DCSM) C2000WARE project
- Exploring the DCSM Security Tool configurable options
- DCSM Security Tool generated content
- Adding DCSM Security Tool support to an existing project

2 Supplementary Online Information

For more information on the DCSM module on a specific C2000 device, see the device-specific data sheet and the corresponding Technical Reference Manual (TRM).

This application report was written using the TMS320F2837xD family of devices, but the tool also supports the TMS320F2838x, TMS320F28004x, TMS320F28002x, TMS320F2837xS and the TMS320F07x family of devices as well. The data sheet and TRM used for this application report are listed below and in Section 8.

- *TMS320F2837xD Dual-core Real-Time Microcontrollers Data Sheet*
- *TMS320F2837xD Dual-core Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F28004x Real-Time Microcontrollers Data Sheet*
- *TMS320F28004x Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F28002x Real-Time Microcontrollers Data Sheet*
- *TMS320F28002x Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F2838x Real-Time Microcontrollers Data Sheet*
- *TMS320F2838x Real-Time Microcontrollers Technical Reference Manual*

Additional support is provided by the TI E2E™ Community.

3 DCSM Security Tool Example Project

In order to use the DCSM Security Tool, you must first import the DCSM Security Tool based example projects from the C2000WARE software development kit (SDK). The DCSM Security Tool is available in C2000WARE version 3.01.00.00 and later. For multi-core devices, DCSM Security Tool enabled example projects are available for each core.

Note

For F28004x and F28002x devices, C2000WARE version 3.03.00.00 and later is required.

Note

For F2838x devices, C2000WARE version 3.04.00.00 and later is required.

Use the following instructions to import the DCSM Security Tool based example project:

1. Launch Code Composer Studio™ (CCS) version 9.2 or later and select a workspace.

   Note

   The C2000 DCSM Security Tool is a SysConfig-based tool that requires CCS version 9.2 or higher and will not work with older versions of CCS.

2. With CCS open, click **Project → Import CCS Projects...**.

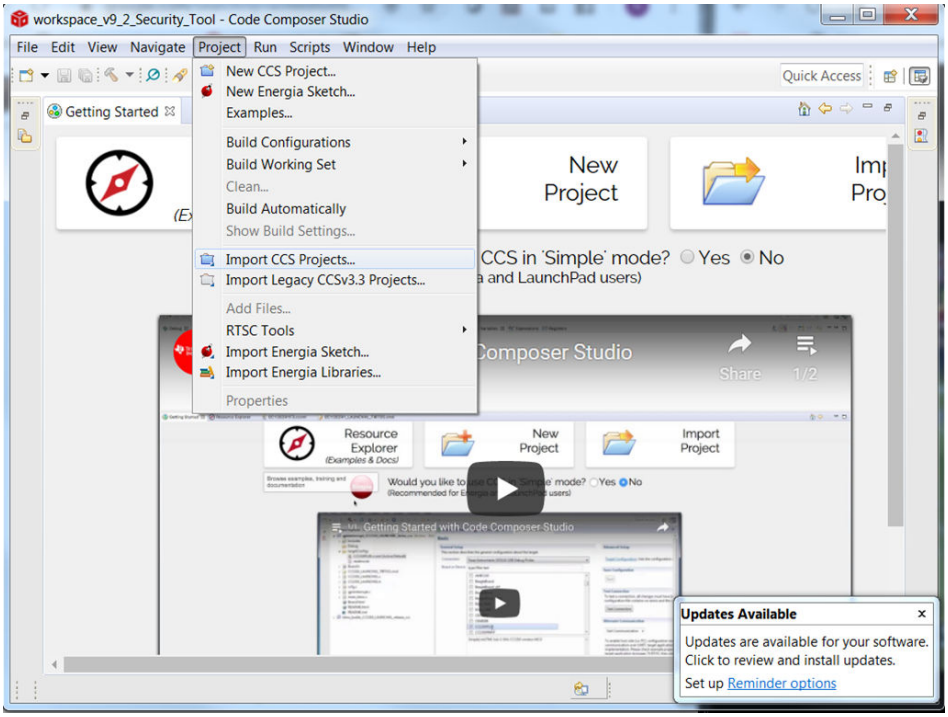

Figure 3-1. Import CCS Project

3. In the **Import CCS Projects** wizard, select **Browse...** and navigate to the folder:

   For F2837xD devices

   <C2000Ware_Install_Location>\driverlib\f2837xd\examples\cpu1\dcsm.

   Note

   Dual core example is available at:

   <C2000Ware_Install_Location>\driverlib\f2837xd\examples\dual\dcsm

   For F28004x devices

   <C2000Ware_Install_Location>\driverlib\f28004x\examples\dcsm

   For F28002x devices

   <C2000Ware_Install_Location>\driverlib\f28002x\examples\dcsm

   For F2838x devices

   <C2000Ware_Install_Location>\driverlib\f2838x\examples\c28x\dcsm

4. Select the DCSM Security Tool project and click **Finish**.

   The project should now be imported into your workspace and look similar to Figure 3-2.

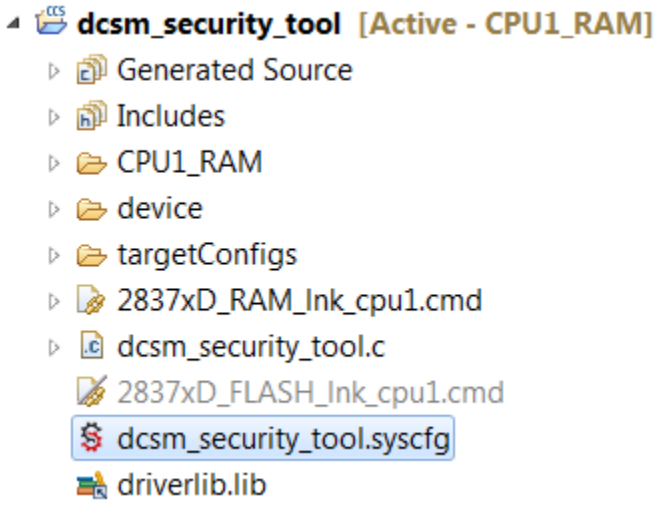

Figure 3-2. DCSM Security Tool Example Project

   The DCSM Security Tool configuration is stored inside the .syscfg file.

5. Open the **dcsm_security_tool.syscfg** file.

   The DCSM Security Tool will now open inside CCS and the DCSM Security Tool GUI is available for your to configure the DCSM module. The DCSM Security Tool looks similar to Figure 3-3.

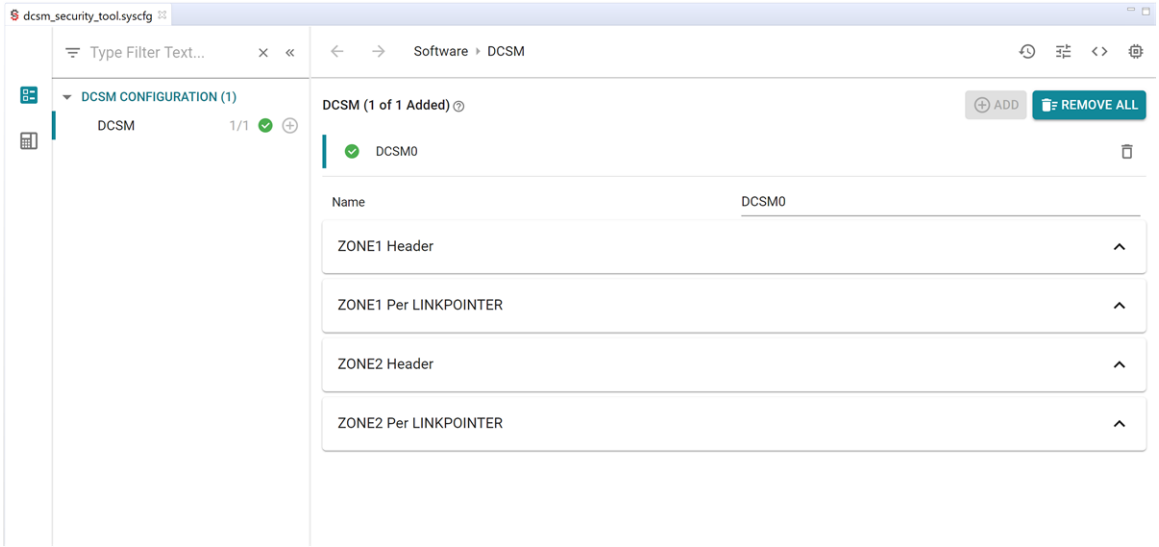

Figure 3-3. DCSM Security Tool User Interface

You can now start configuring the DCSM Security Tool. Section 4 describes all the configurable options inside the DCSM Security Tool.

4 DCSM Security Tool Configurable Options

The first step to using the DCSM Security Tool is to add an instance of the SECURITY module. This is done by clicking the ADD button at the top right corner on clicking the plus sign shown in Figure 4-1.

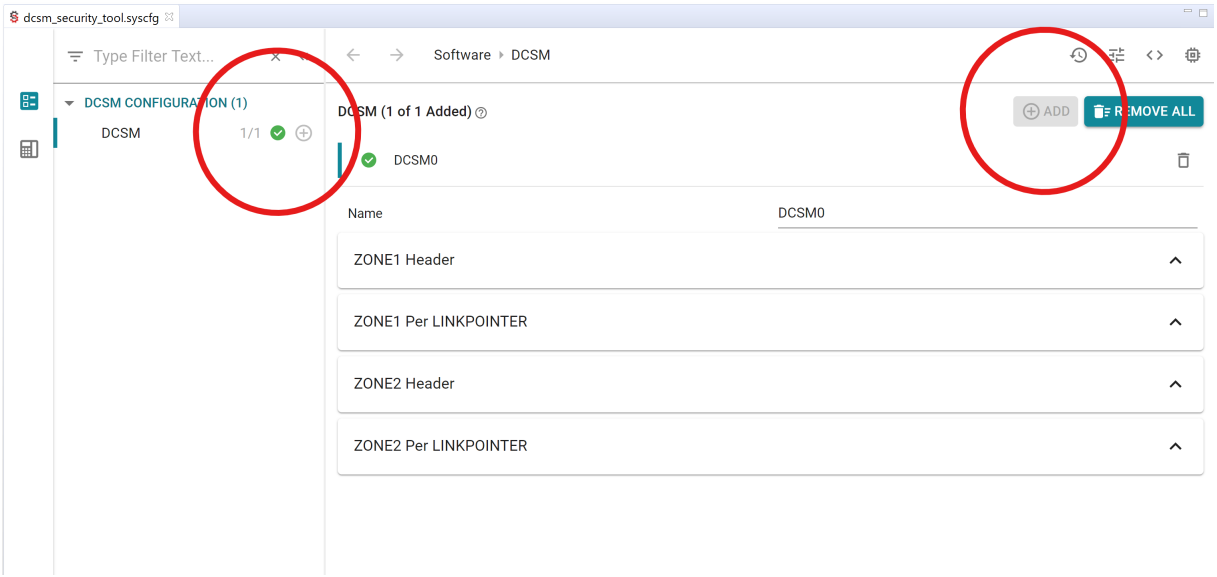

Figure 4-1. Adding a SECURITY Module to Project

The SECURITY module contains four submodules:

- ZONE1 Per LINKPOINTER: This submodule contains the configurable options for zone 1 of the DCSM peripheral that can be updated only once PER LINKPOINTER update.
- ZONE1 Header: This submodule contains the configurable options for zone 1 of the DCSM peripheral that can only be updated **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER.
- ZONE2 Per LINKPOINTER: This submodule contains the configurable options for zone 2 of the DCSM peripheral that can be updated only once PER LINKPOINTER update.
- ZONE2 Header: This submodule contains the configurable options for zone 2 of the DCSM peripheral that can only be updated **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER.

ZONE1 Per LINKPOINTER/Header and ZONE2 PER LINKPOINTER/Header submodule configurable options perform the same task for ZONE1 and ZONE2 respectively. ZONE1 options configure zone 1 of the DCSM peripheral, while ZONE2 options configure zone 2 of the DCSM peripheral. This document steps through all of the configurable options for ZONE1.

4.1 ZONE1/ZONE2 Per LINKPOINTER Submodule

The first option inside each ZONEx Per LINKPOINTER module is selecting whether that zone is configured or left unchanged. In order to configure the ZONEx Per LINKPOINTER, you must expand the ZONEx Per LINKPOINTER submodule and check the **Configure this Section** box.

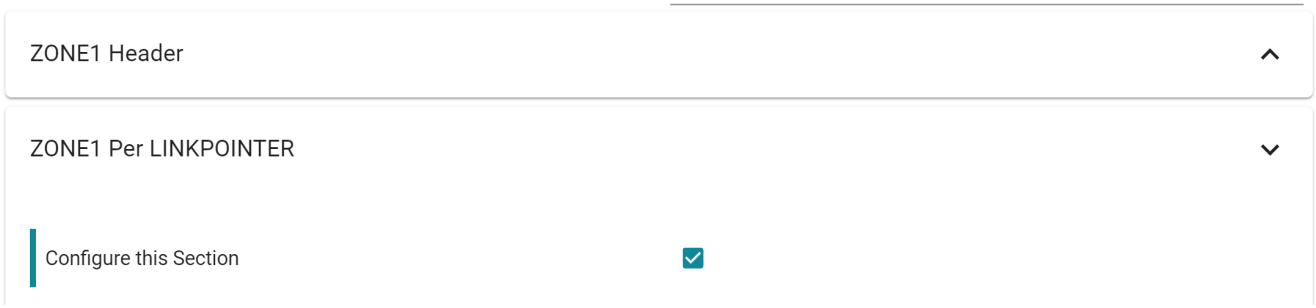

Figure 4-2. Use Zone Checkbox

The ZONE1/ZONE2 Per LINKPOINTER submodule contain the following configurable options:

- **Current LINKPOINTER**: This is the current LINKPOINTER value that is being used by the zone. The **Current LINKPOINTER** value is used to calculate the next LINKPOINTER value. You must input the **Current LINKPOINTER** value.
- **Update the LINKPOINTER**: This option is only available if the **Current LINKPOINTER** value is the default value (ex: 0x1FFFFFFF in F2837xD devices) . If you have not yet programmed the device OTP, you can use the first LINKPOINTER location by unchecking this option. If the **Current LINKPOINTER** value is default value and you have already used the first LINKPOINTER location, then the **Update the LINKPOINTER** checkbox MUST be checked. If the **Current LINKPOINTER** value is any value other than the default value, the **Update the LINKPOINTER** option is not applicable (will always pick the next LINKPOINTER location)
- **Next LINKPOINTER**: This is the value of the LINKPOINTER automatically calculated based on the **Current LINKPOINTER** and the **Update the LINKPOINTER** option. This is the value used in the generated code for the LINKPOINTER.
- **Zone Select Block (ZSB) Offset**: This is the value of the LINKPOINTER offset automatically calculated based on the **Next LINKPOINTER** address. This is the value used in the generated code for the LINKPOINTER offset.
- **Password 0-4**: The four 32-bit password values.
- **CLA, RAM, FLASH Owner Selection**: These configurable options allow you to select which zone owns each securable resource. Each securable resource can only be secured by either zone1 or zone2. The options for CLA, RAM and FLASH memory sections are different.
- **JTAGPSWDL0 and JTAGPSWDL1**: These configurable options are used along with JTAGPSWDHx to password protect JTAG access.

Note

JTAGPSWDLx is available on F2838x family of devices.

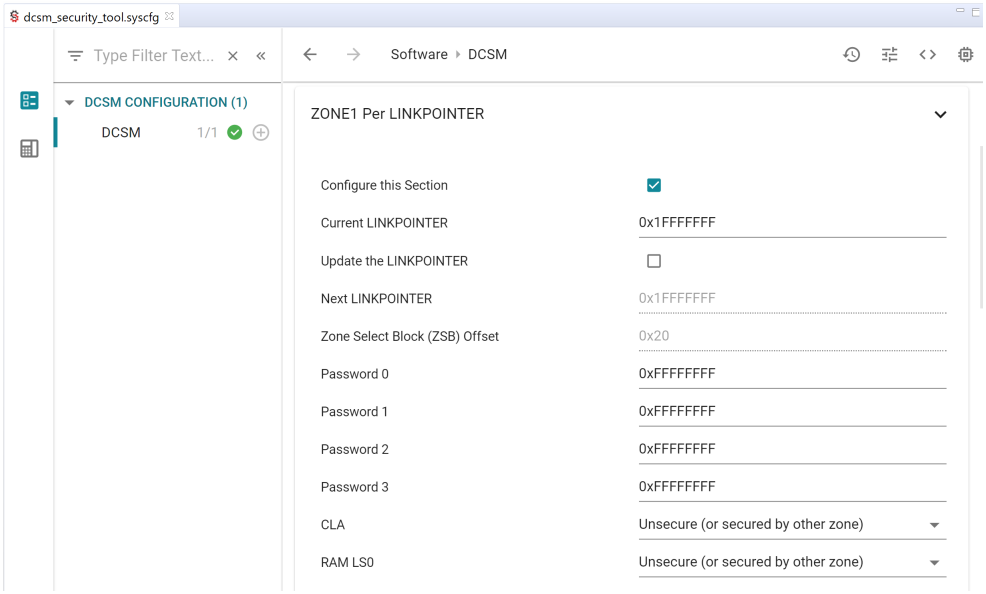

Figure 4-3. ZONE1 Per LINKPOINTER Options

Note

The ZONE1 Per LINKPOINTER options shown is for the F2837xD family of devices.

ZONE1 and ZONE2 options are similar. You can select which zone is the owner of each section of the memory by configuring the specific memory section's option in either of the ZONEx Per LINKPOINTER submodule. In the case of an error (where a memory section is assigned to be secured by both zone1 and zone2), the tool will notify you.

4.2 ZONE1/ZONE2 Header Submodule

The first option inside each ZONEx Header module is selecting whether that zone's header is configured or left unchanged. In order to configure the ZONE, you must expand the ZONEx Header submodule and check the **Configure this Section** box.

ZONEx Header submodule can only be configured **ONCE** and **ONCE ONLY**. Once these options are configured, you **CANNOT** update them even by changing the LINKPOINTER. The ZONE1/ZONE2 Header submodule contain the following configurable options:

- **Password Lock**: Disable/enable the Password Lock permanently. For more information, see the device-specific TRM.
- **CRC Lock**: Disable/enable the CRC Lock permanently. For more information, see the device-specific TRM.
- **Configure Boot Section**: This option determines whether to program the Boot Mode and Boot Pins.

For F2837xD, F2837xS and F2807x devices:

- **Boot Control PIN0/PIN1**: These options select the boot pin0/pin1 for the device.
- **Get Mode**: This is the boot mode for the device. The list of available options can be found in the device-specific TRM.
- **Boot Control Key** and **Boot Control Mode**: These values are calculated based on the **Get Mode** option.

For F2838x, F28004x and F28002x devices:

- **Number of Boot Pins**: This option will decide how many boot mode select pins (BMSP) are used, which in turn determines how many different boot modes can be defined.
- **Boot Mode Select Pins (BMSP0-2)**: These options select the boot pin0/pin1/pin2 for the device, if the BMSPx is within the usable range of **Number of Boot Pins**.

- **BOOTDEF0-7**: These options select the boot mode for the device when the BMSP2-BMSP1-BMSP0 pin values match the BOOTDEF number. For example, in 3-pin boot select mode, BOOTDEF2 determines the boot mode for the device when BMSP2 pin is pulled **LOW**, BMSP1 pin is pulled **HIGH** and BMSP0 pin is pulled **LOW**.

For F28004x and F28002x devices:

- **ERRORSTS Pin**: This options selects the ERRORSTS pin.

For F28002x and F2838x devices only:

- **Run MPOST**: Selects the Memory Power on Self-Test mode.

For F2838x devices only:

- **Enable JTAGLOCK**: Enables the JTAG lock protection on F2838x devices.
- **CMAC Key0 to Key4**: The password keys for CMAC.

Note

For F28004x devices, boot mode configuration options are only available in ZONE1.

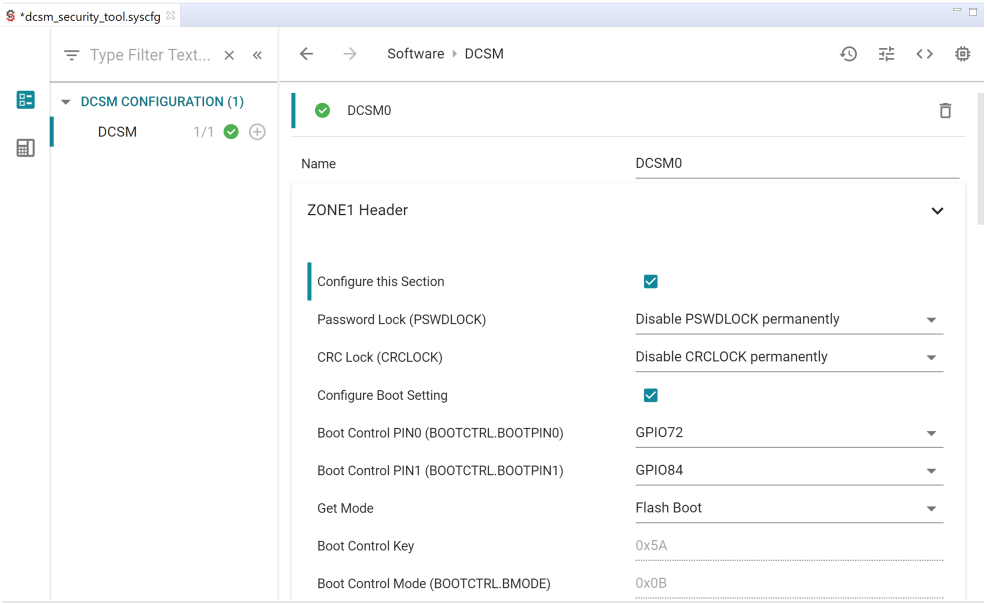

Figure 4-4. ZONE1 Header Options

Note

The example ZONE1 Header Options shown are for F2837xD device.

5 DCSM Security Tool Generated Content

The DCSM Security Tool generates the following two files:

- **dcsm.asm**: The assembly file containing your LINKPOINTER value, passwords, and other options.
- **dcsm.cmd**: The linker command file containing the MEMORY addresses and SECTIONS that references the content in **dcsm.asm** file.

The tool updates the content of the two generated files and highlights the most recent changes in the configuration in real-time. In order to view the generated files, click the item shown in Figure 5-1 and then open **dcsm.asm** file.

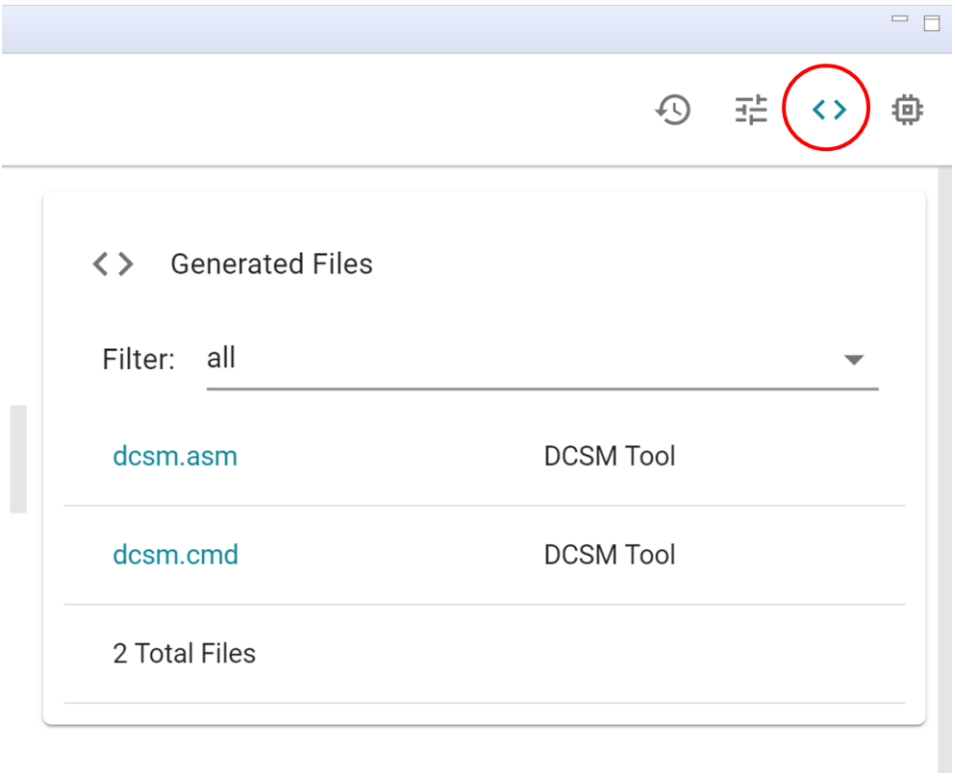

Figure 5-1. View Generated Files

In order to see the changes in the in the ASM file, change the **CRC Lock** option in the **ZONE1 Header** submodule, with the **dcsm.asm** file open. Figure 5-2 shows the latest changes in the file highlighted.

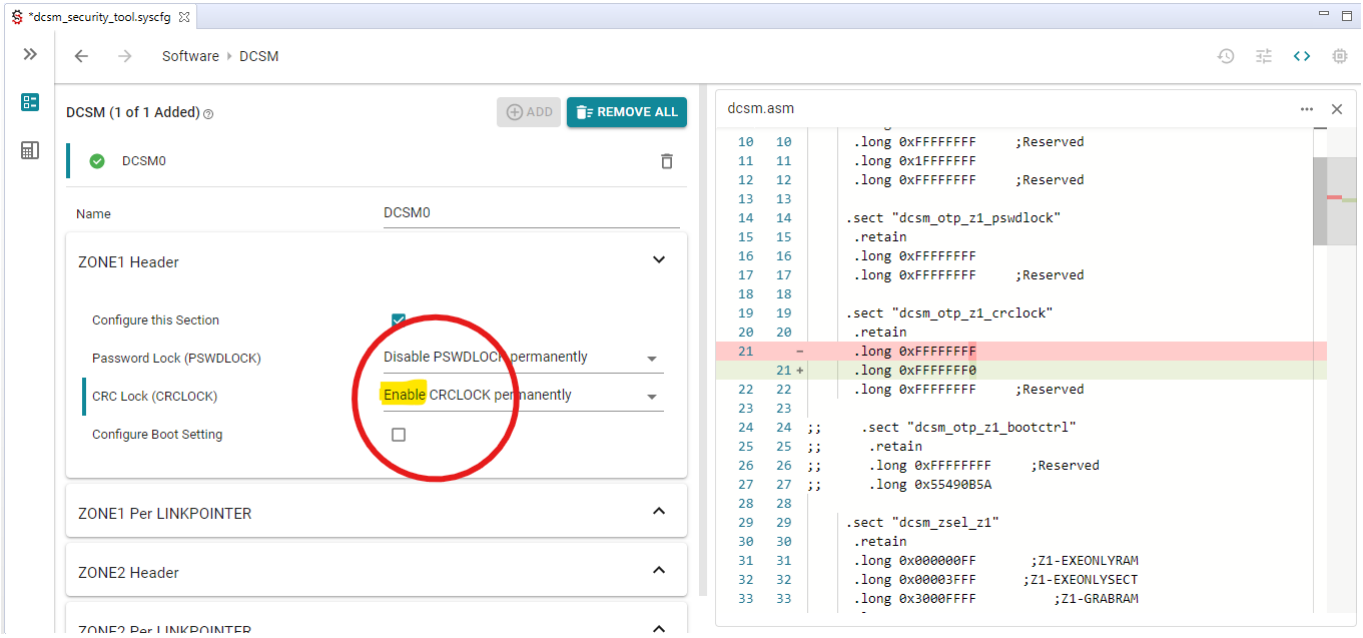

Figure 5-2. dcsm.asm Highlighting the Changes

In order to see the changes in the in the CMD file, uncheck the **Configure this Zone** option in the **ZONE1 Per LINKPOINTER** submodule, with the **dcsm.cmd** file open. Figure 5-3 shows the latest changes in the file highlighted.

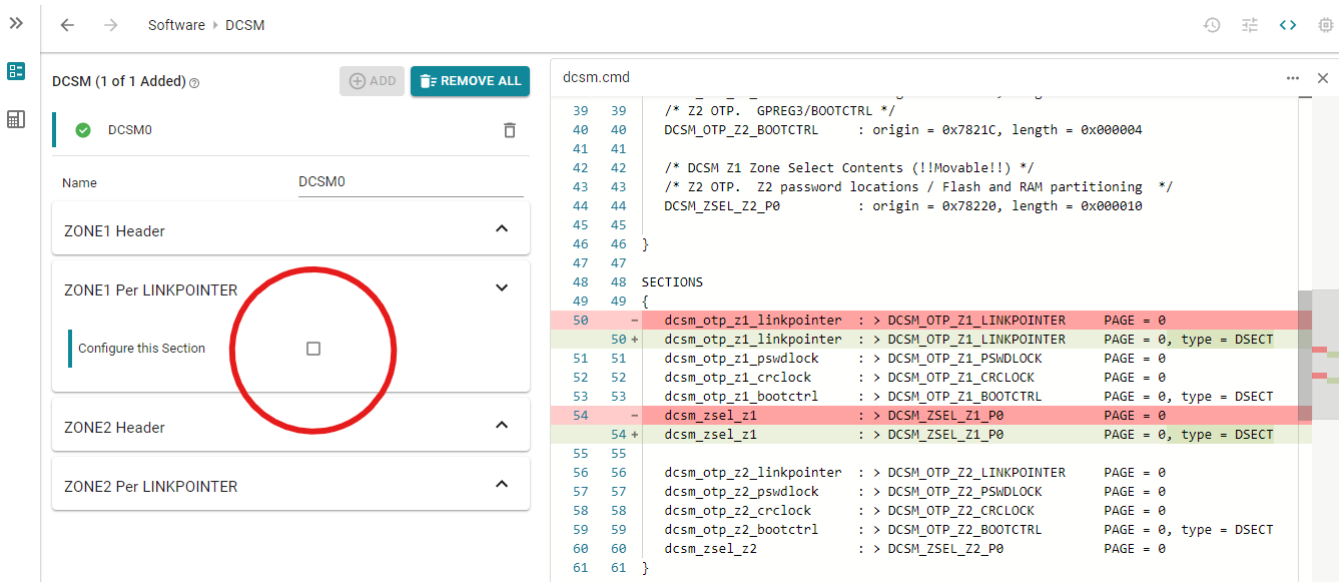

Figure 5-3. dcsm.cmd Highlighting the Changes

It is important to note that these files are auto-generated and you cannot modify them.

Save the **.syscfg** file and build the project. When the project is finished building, the generated ASM and CMD files are placed in the build directory under a folder named "syscfg". This is shown in Figure 5-4.

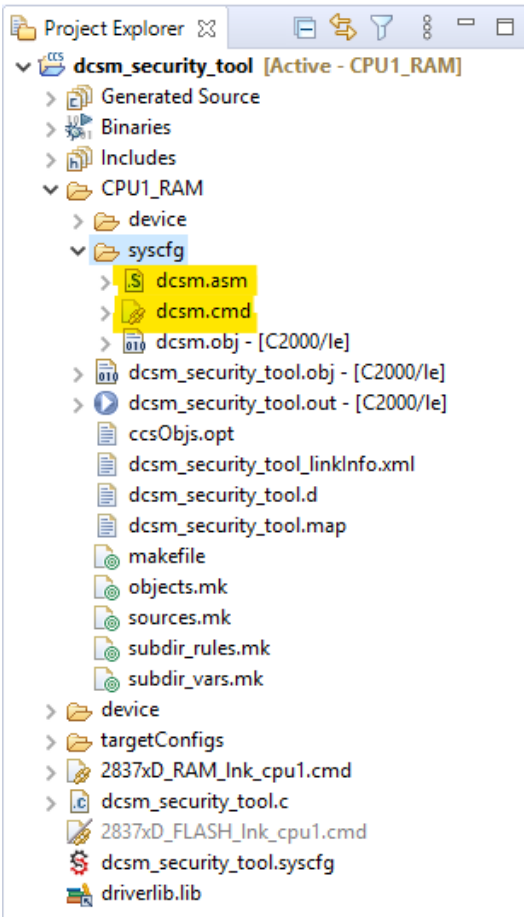

Figure 5-4. Generated Source Files in the Build Directory

When the project is built, the two generated files (security.asm and security.cmd) are automatically used to generate the .OUT binary executable file.

Note

For CCS version 9.2/9.3 users, the generated CMD file must be copied out of the "syscfg" folder and placed in the top directory of the CCS project. You must then rebuild the project for the CMD file to take effect in the build process.

You can open the .MAP file in the build directory to see the DCSM Security Tool's generated content taking effect in the build process.

```
MEMORY CONFIGURATION

         name             origin    length      used     unused   attr    fill
----------------------  --------  ---------  --------  --------  ----  --------
PAGE 0:
  BEGIN                 00000000   00000002  00000002  00000000  RWIX
  RAMM0                 00000122   000002de  00000018  000002c6  RWIX
  RAMLS0                00008000   00000800  00000000  00000800  RWIX
  RAMLS1                00008800   00000800  00000000  00000800  RWIX
  RAMLS2                00009000   00000800  00000000  00000800  RWIX
  RAMLS3                00009800   00000800  00000000  00000800  RWIX
  RAMLS4                0000a000   00000800  00000000  00000800  RWIX
  RAMD0                 0000b000   00000800  000006b9  00000147  RWIX
  DCSM_OTP_Z1_LINKPOINT 00078000   0000000c  00000000  0000000c  RWIX
  DCSM_OTP_Z1_PSWDLOCK  00078010   00000004  00000000  00000004  RWIX
  DCSM_OTP_Z1_CRCLOCK   00078014   00000004  00000000  00000004  RWIX
  DCSM_OTP_Z1_BOOTCTRL  0007801c   00000004  00000000  00000004  RWIX
  DCSM_ZSEL_Z1_P0       00078030   00000010  00000000  00000010  RWIX
  DCSM_OTP_Z2_LINKPOINT 00078200   0000000c  00000000  0000000c  RWIX
  DCSM_OTP_Z2_GPREG     0007820c   00000004  00000000  00000004  RWIX
  DCSM_OTP_Z2_PSWDLOCK  00078210   00000004  00000000  00000004  RWIX
  DCSM_OTP_Z2_CRCLOCK   00078214   00000004  00000000  00000004  RWIX
  DCSM_OTP_Z2_BOOTCTRL  0007821c   00000004  00000000  00000004  RWIX
  DCSM_ZSEL_Z2_P0       00078220   00000010  00000000  00000010  RWIX
  RESET                 003fffc0   00000002  00000000  00000002  RWIX

```

Figure 5-5. MAP File With Security Options

6 Adding DCSM Security Tool Support to an Existing Driverlib Project

Use the following steps to add DCSM Security Tool support to an existing C2000WARE DriverLib Project:

1. Add the "dcsm_security_tool.syscfg" file
   a. For F2837xD: **<C2000Ware_Install_Location>\driverlib\f2837xd\examples\cpu1\dcsm\empty.syscfg**
   b. For F2838x: **<C2000Ware_Install_Location>\driverlib\f2838x\examples\c28x\dcsm\empty.syscfg**
   c. For F28004x: **<C2000Ware_Install_Location>\driverlib\f28004x\examples\dcsm\empty.syscfg**
   d. For F28002x: **<C2000Ware_Install_Location>\driverlib\f28002x\examples\dcsm\empty.syscfg**

   from the DCSM examples folder to the project by copying the file into the project.
2. CCS will ask whether or not to enable SysConfig. Accept and select "Yes".

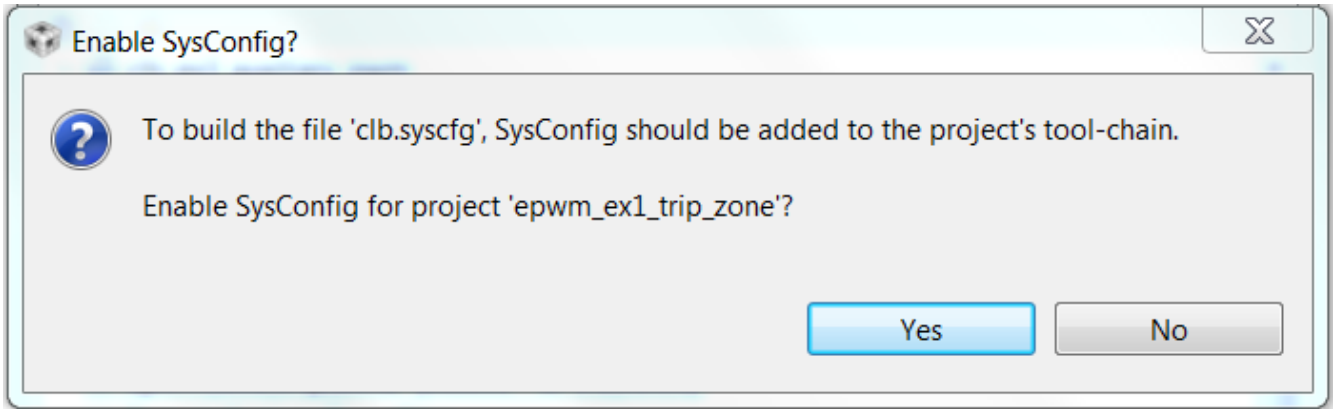

Figure 6-1. Enable SysConfig

3. Open the "Project Properties" and open the Resources → Linked Resources. Add the following Variable Paths:
   a. DCSMTOOL_SYSCFG_ROOT
      <C2000Ware_Install Location>\utilities\dcsm_tool\dcsm_syscfg
4. Open Build → SysConfig → Basic Options.
5. Add the following to the Root system config meta data list:
   a. ${DCSMTOOL_SYSCFG_ROOT}/.metadata/product.json
6. In the **Name of device (-d, --device)** option, enter your device name (**F2838x, F2837xD, F2807x, F2837xS, F28002x, F28004x**), as shown in Figure 6-2.

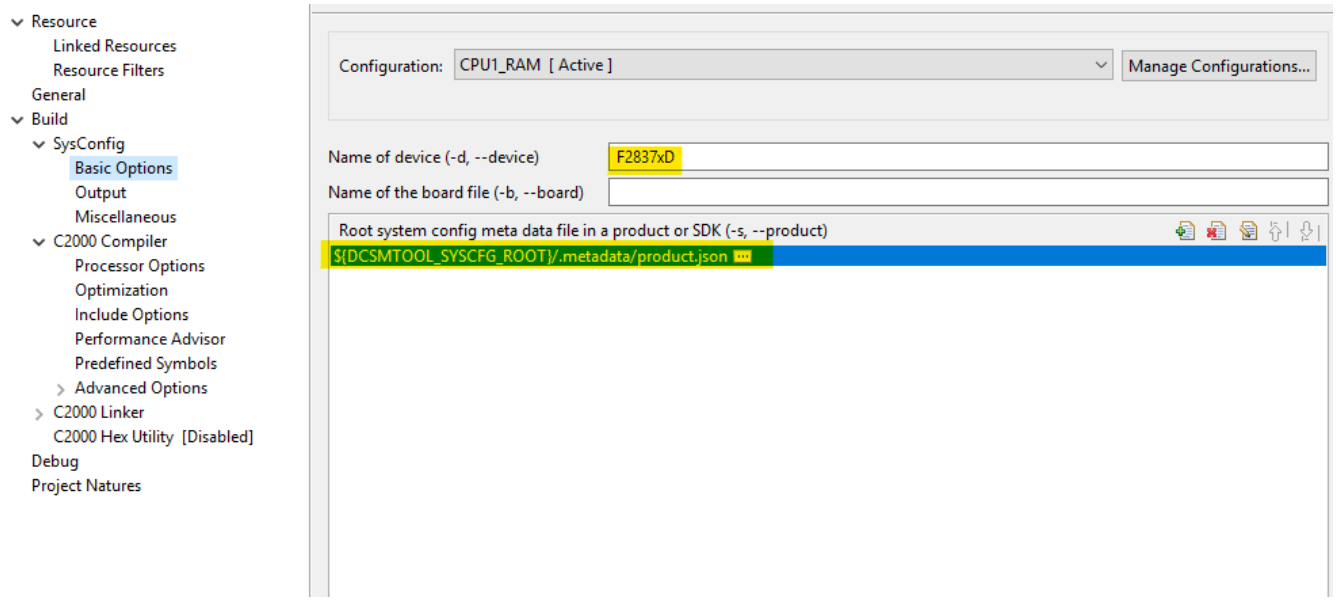

Figure 6-2. SysConfig SDK Path

7 Summary

The C2000 DCSM Security Tool allows you to configure the DCSM module by generating the source code needed to configure the peripheral. This tool is integrated within CCS. The C2000 DCSM Security Tool helps by flagging any incorrect configuration.

8 References

- *TMS320F2837xD Dual-core Real-Time Microcontrollers Data Sheet*
- *TMS320F2837xD Dual-core Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F28004x Real-Time Microcontrollers Data Sheet*
- *TMS320F28004x Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F28002x Real-Time Microcontrollers Data Sheet*
- *TMS320F28002x Real-Time Microcontrollers Technical Reference Manual*
- *TMS320F2838x Real-Time Microcontrollers Data Sheet*
- *TMS320F2838x Real-Time Microcontrollers Technical Reference Manual*

Additional support is provided by the TI E2E™ Community.

9 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from Revision * (March 2020) to Revision A (May 2021)	Page
• Updated the numbering format for tables, figures and cross-references throughout the document	2
• Added support for F28002x, F28004x and F2838x devices	2
• Update was made in Section 3	2
• Update was made in Section 4.1	6
• Update was made in Section 4.2	7
• Update was made in Section 6	13

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265