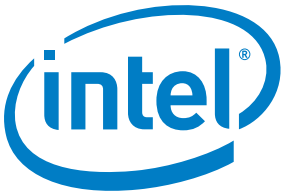


Bay Trail M/D Platform – Intel® Trusted Execution Engine (Intel® TXE) Firmware

Bring-Up Guide

Revision 1.1

September 2013

Intel Confidential

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Intel, Pentium, Celeron, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2013, Intel Corporation. All rights reserved.

Contents

Figures

Tables

Revision History

Revision Number	Description	Revision Date
0.5	• Initial release	December 2012
0.6	• Pre Alpha1 release	February 2013
0.6.1	• Pre Alpha2 release	March 2013
0.7	• Alpha release New content: - Quick Start check list - FITC Platform Selection - TXEI Installer	April 2013
0.7.1	• Alpha2 release New content: - Creating flash image using command line - Intel FWUpdate Tool - Intel TXEManuf Tool	May 2013
0.8	• Beta release New content: - Intel® System Scope Tool (Intel® SST) - FITC Soft Straps	June 2013
0.8.5	• Beta2 release - New content: Added Note in Table 9-5. SOC Strap 5 under 'Root Port Configuration' soft strap	July 2013
0.9	• Windows* 8 64-bit Beta Release New content: Added chapter 5: "Using EFI System Tools in UEFI shell with UEFI Secure Boot Enabled option"	July 2013
1.0	• PV Release	July 2013
1.1	• New content: FITC Soft Straps Update	September 2013

§

1 Introduction

This document covers the future Intel® Pentium® processor or future Intel® Celeron® processor N- & J- series based platform (formerly Bay Trail-M/D platform) firmware bring-up procedure for Intel® quad-core technology SoC (B2 silicon).

The bring-up procedure primarily involves building a FW image. Once the FW image is built, it can be programmed to the Bay Trail platform. All the paths mentioned in this guide are relative path to the root of the given kit.

1.1 Terminology

Term	Description
FITC	Flash Image Tool Creation
FPT	Flash Programming Tool
Intel® TXE	Intel® Trusted Execution Engine (Intel® TXE)
Intel® TXEI	Intel® Trusted Execution Engine Interface (Intel® TXEI)

§

2 Quick Start Check-List

2.1 First Boot of Bay Trail-M/D

To run first basic boot of the Bay Trail-M/D platform, ensure to have the following:

- Build the SPI FW image
  - Build the image using FITC tool as described in section 3.4 and flash the image components from the FW kit
- Flash the SPI FW image
  - Flash using Dediprog or FPT method as described in section 3.6
- Install Intel® Trusted Execution Engine Interface (Intel® TXEI) Driver as described in section 4
  - Once the platform boots, install the Intel TXEI driver found in the FW Kit
- Verify Intel® Trusted Execution Engine (Intel® TXE) information
  - Run TXEInfo tool found in the FW kit "\System Tools\ TXEInfo\" directory
- Verify Intel TXE status via TXEManuf tool
  - Run TXEManuf tool found in the FW kit "\System Tools\ TXEManuf\" directory
  - Use TXEManuf.cfg to enable/disable tests of interest

For more details on each of these steps, please refer to the appropriate chapter within the Intel TXE FW Bring up Guide.

§

3 Procedure

3.1 Prerequisites

- fitc.exe: can be found under \\System tools\Flash_Image_Tool folder
- DediProg SF100
- FPT can be found under \\System tools\Flash_Programming_Tool

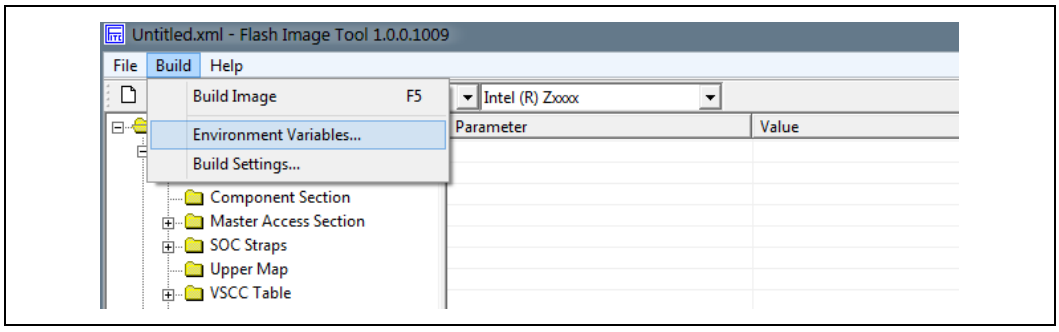
3.2 Start FITC

- Invoke Flash Image Tool by navigating to \\System tools\Flash_Image_Tool folder
- Double click fitc.exe.

3.3 Set Up Build Environment

In the main menu select Build→ Environment Variables.

Figure 3-1. Enviroment Variables



Edit your configuration as shown below.

- **$Source Dir:** The location where FITC will look for binary images during the image creation process
- **$DestDir:** The location where FITC will save the binary image
- **$WorkingDir:** The location where FITC.exe is running. Please keep it as ".”

Figure 3-2. Environment Variables

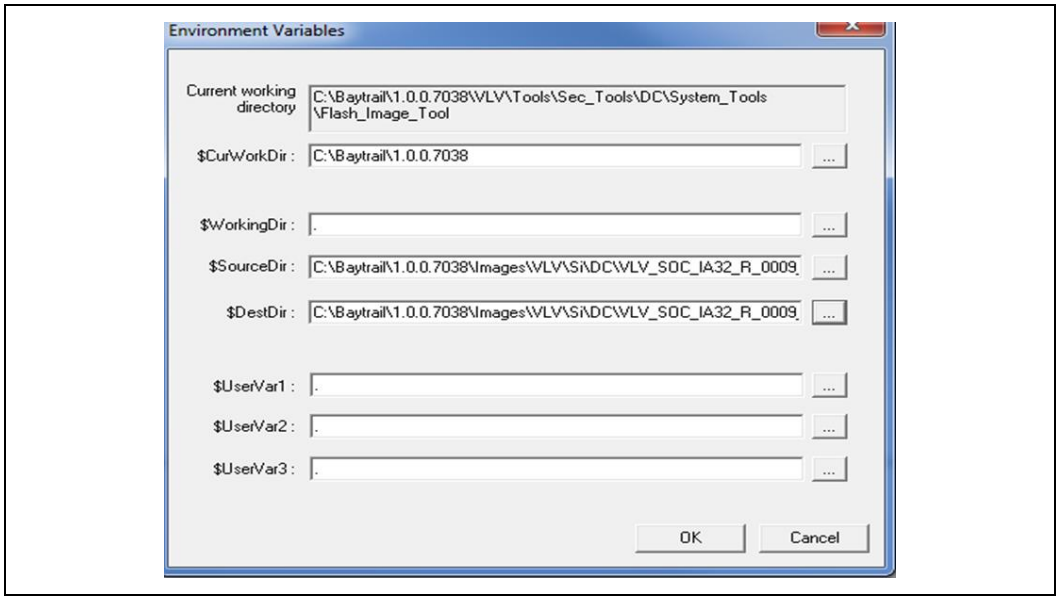
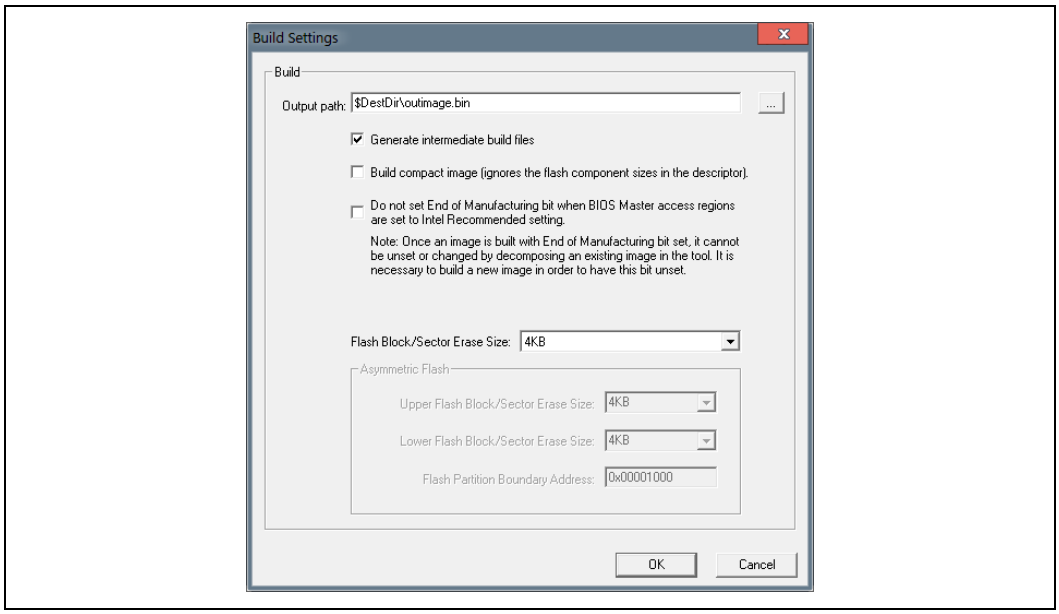


Figure 3-3. FITC Set Up



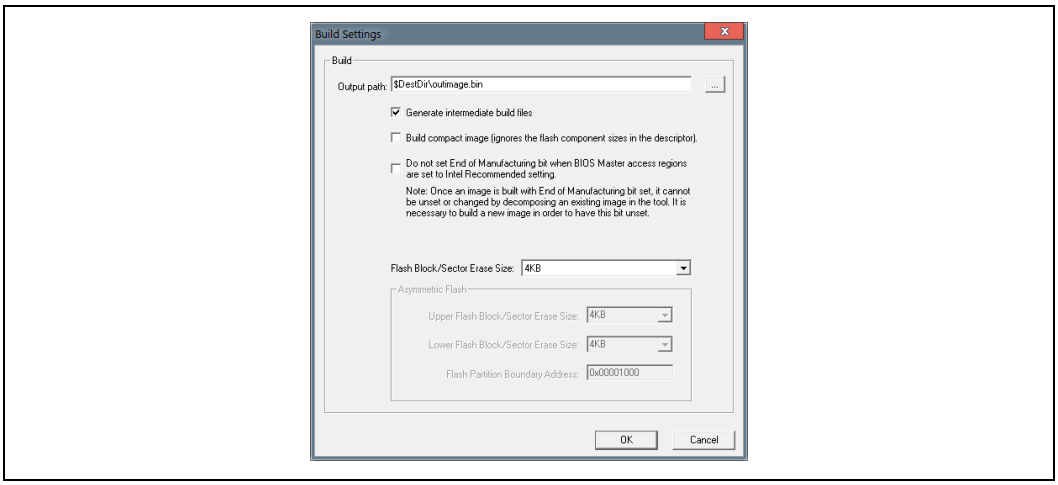
NOTE: Please use the environment variables when defining output path in Build → Build Settings, as shown

3.4 Create Flash Image

3.4.1 Using GUI

1. Run fitc.exe.
2. Define output image name and path
3. Build → Build Settings → Output path

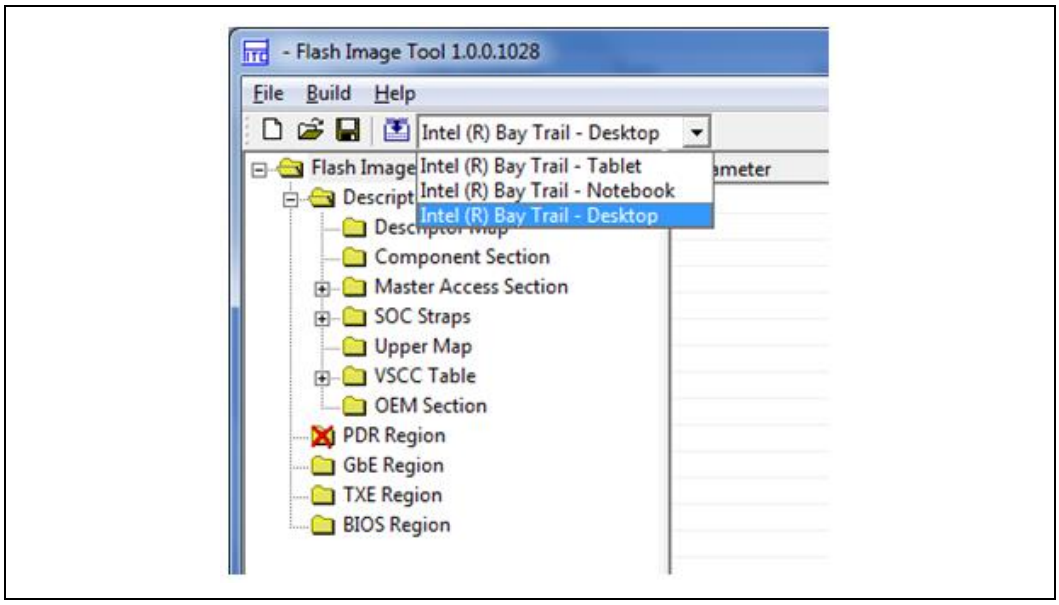
Figure 3-4. Define Output Path



4. Select platform type
    a. On the platform selection list, select Bay Trail – Notebook or Bay Trail – Desktop before modifying and building the flash image.

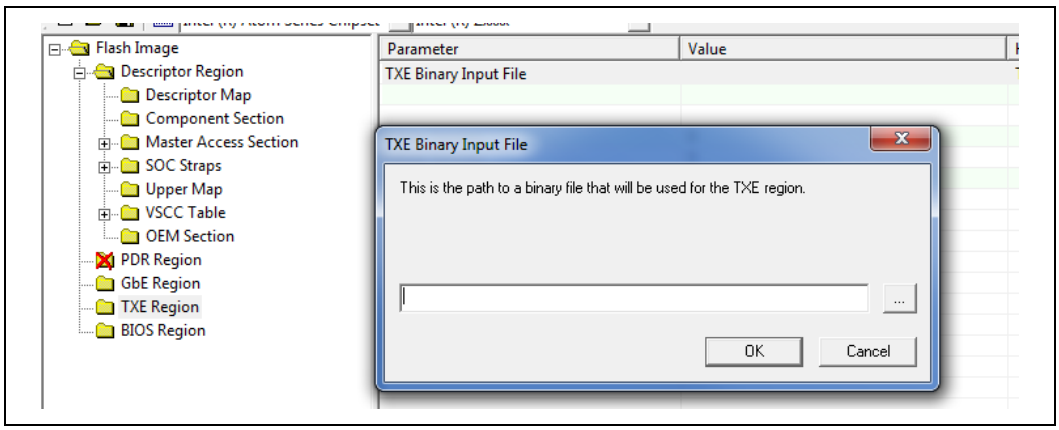
    SOC straps definition will be changed upon Platform selection.

Figure 3-5. Select Platform Type



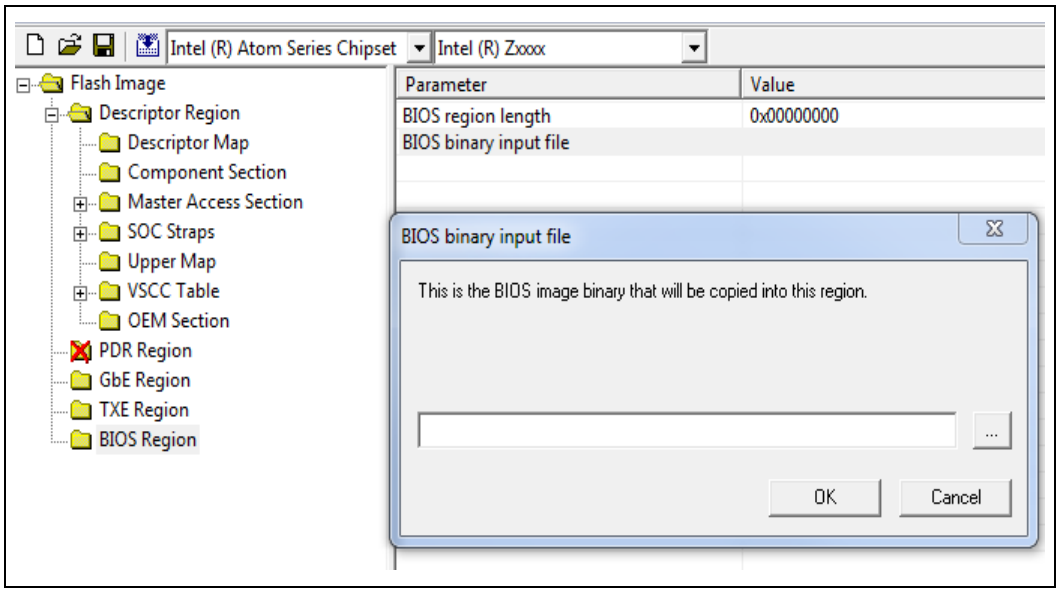
5. Fill in Intel TXE Region:
    a. Select "TXE Region" and double click "TXE Binary Input File"
    b. Select \\Image Components\TXE\TXE_REGION.bin

Figure 3-6. Intel® TXE Region



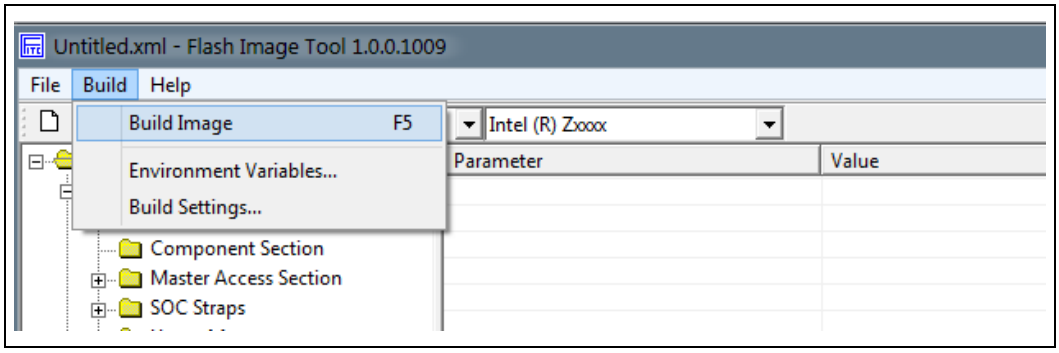
6. Fill in BIOS Region:
   a. Select "BIOS Region" and double click "BIOS binary input file"
   b. Select \\Image Components\BIOS*.ROM

Figure 3-7. BIOS Region



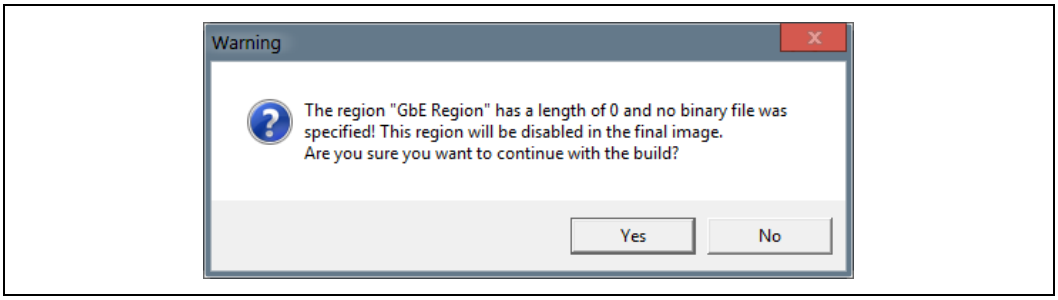
7. Build image

Figure 3-8. Build Image



Note: A warning will appear when building the image, Click "Yes".

Figure 3-9. Warning Message



The output image will be located at the path given at step 3.4.1

Figure 3-10. Image Output

3.4.2 Using Command Line

Please use the command line to create image through command line:

fitc.exe newfiletmpl.xml -b -txe PRODUCTION_TXE_Region.bin -bios BIOS_Region.ROM

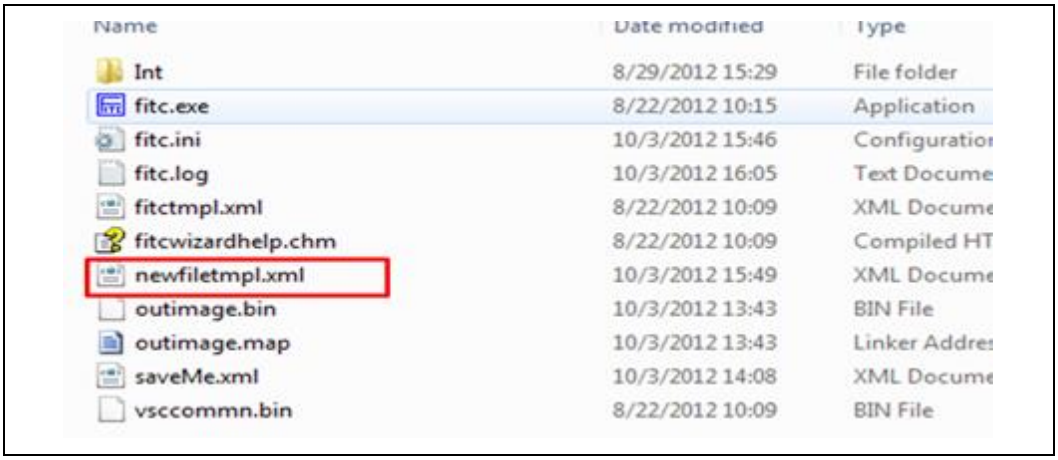
- Please note, if the Intel TXE Region or BIOS region not at the same directory as FITC tool you will need to mention the path

3.5 XML Configuration

3.5.1 Save Your Settings

1. When opening FITC.exe, it loads defaults settings defined in newfiletmpl.xml (located in the same folder as FITC.exe)

Figure 3-11. FITC Configuration



2. To save your custom settings, in the main menu select File→Save As. Select a name and location for the XML file that contains all the settings configured so far. It is recommended that you save this file in the same directory as FITC.exe is located for easy access.

Figure 3-12. Save Configuration

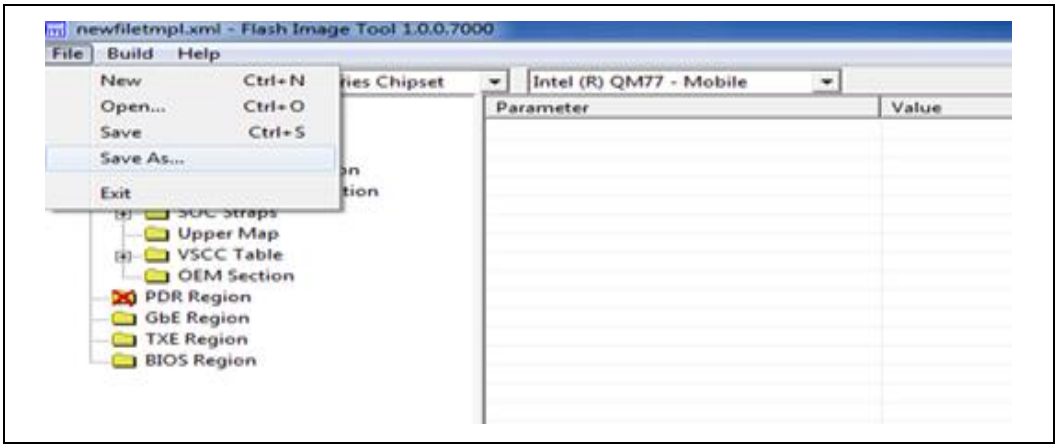
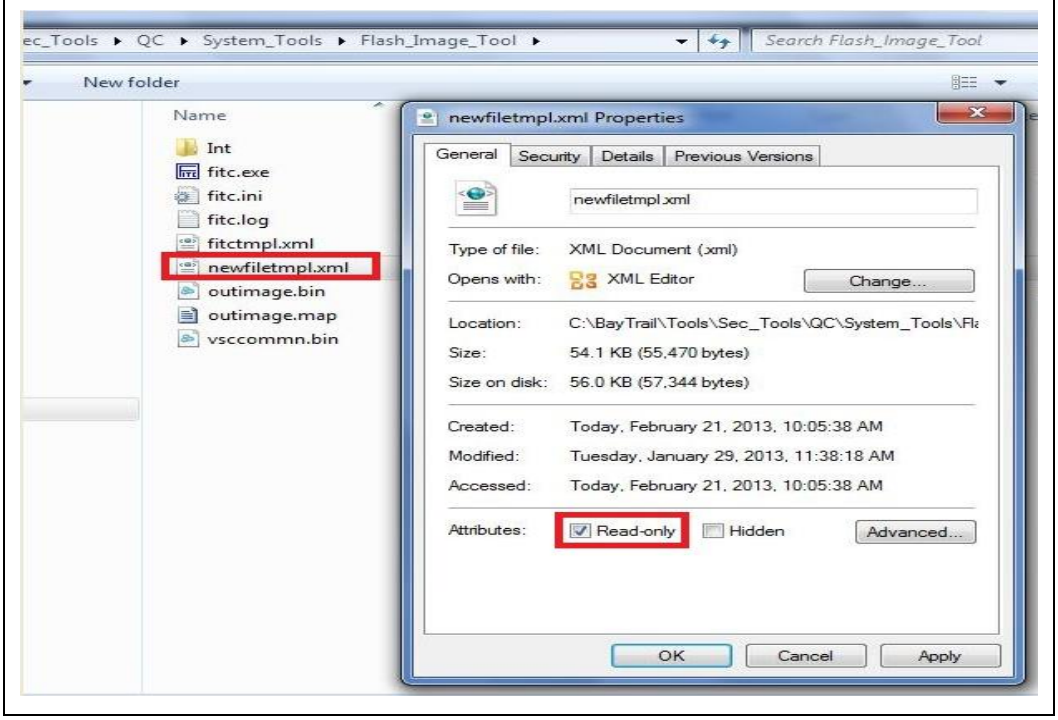


Figure 3-13. Configuration Protection

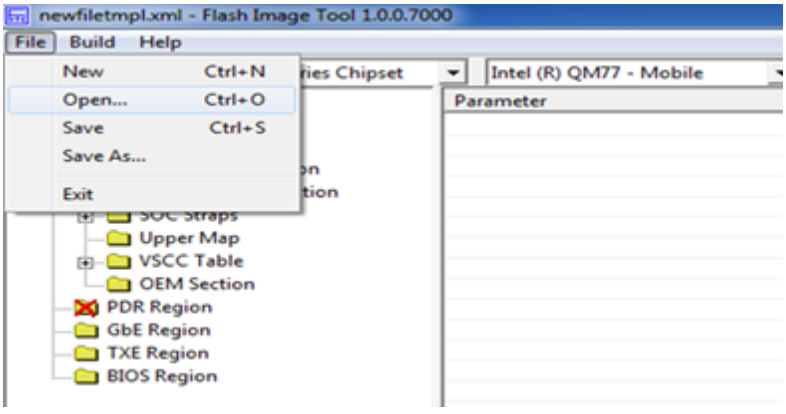


3. Protect configuration XML file from accidental changes by checking the "Read-only" attribute, as shown below.

3.5.2 Load FITC Configuration

Default or custom settings can be loaded by selecting File→Open in the main menu, and navigating to the desired xml configuration file.

Figure 3-14. Load Configuration



3.6 Flashing Target

3.6.1 Using DediProg

1. Run DediProg Software
2. Click "Detect" to verify SPI flash detection
3. Please make sure the voltage is set to 1.8v by clicking Config-> Miscellaneous settings
4. Click "File" button and select the FW image built in step 3.4.

Figure 3-15. Set Voltage

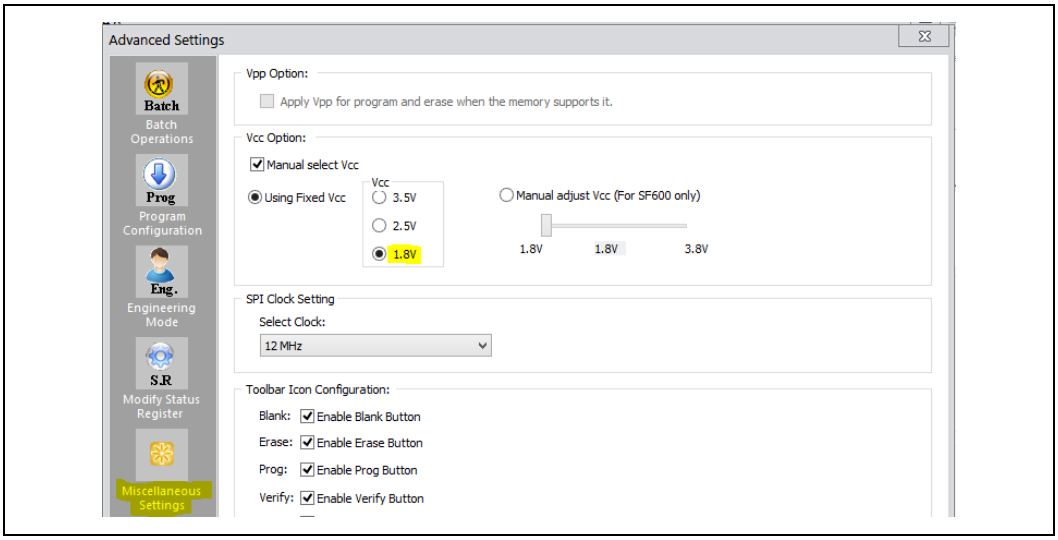
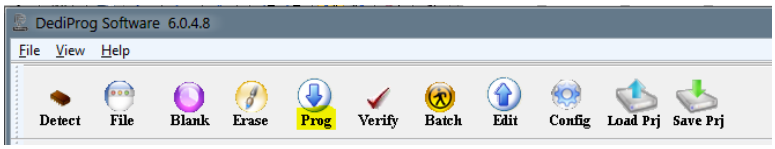


Figure 3-16. Select Image

5. Click "Prog" to flash the flash image to the target

Figure 3-17. Prog Option



6. Verify flashing was performed correctly

Figure 3-18. Result Expected

3.6.2 Using FPT

1. FPT is a Windows based tool aimed to program FW on the platform (FPT is running from the platform). Under \\System tools\Flash_Programming_Tool
2. Copy the FW image to the root folder of the FPT tool and rename it to outimage.bin. (For simplicity, we will use \\Flash_Programming_Tool\Windows when referring to FPT tool directory)
3. Open command line with administrative privileges, navigate to \\Flash_Programming_Tool\Windows or Windows64 and type:

```
Ftpt.exe -LIST
```

The system should respond with the number of SPI Flash devices available. For example:

```
--- Flash Devices Found ---

W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)

W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
```

4. Program the SPI Flash image to the Flash device(s) by issuing the following command at the prompt:

```
fptw.exe /f outimage.bin
```

5. If the programming was successful, then the following message will be shown:

```
FPT Operation Passed
```

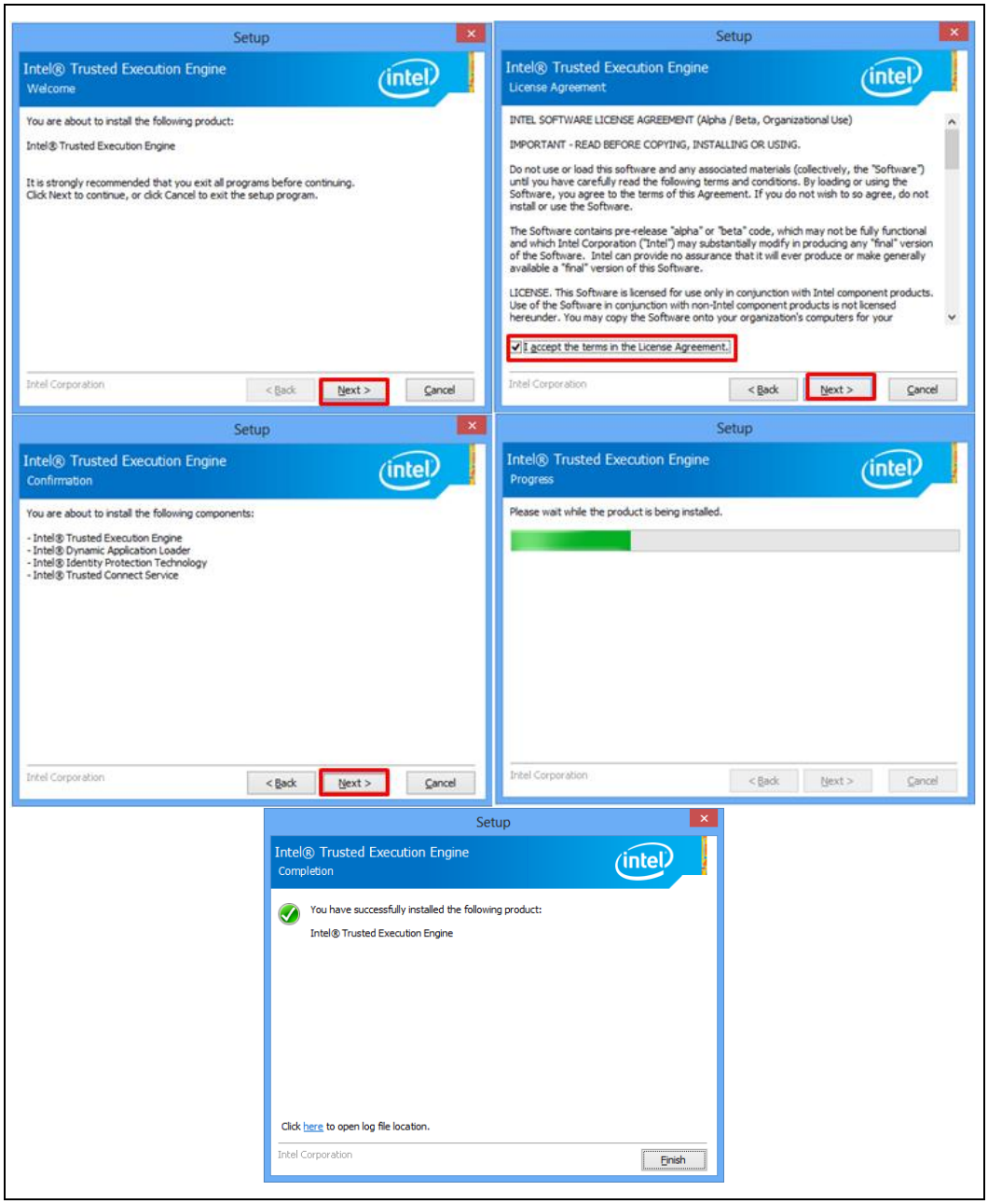
§

4 Intel® Trusted Execution Engine Interface (Intel® TXEI) Driver

4.1 Install the Intel® TXEI Driver using Installer

1. Navigate to the root folder of the Intel TXE Installer (\\Installers)
2. Double click “SetupTXE.exe”
3. Follow the installation procedure as shown in Figure 4-1. Intel® TXE Installation Steps.

Figure 4-1. Intel® TXE Installation Steps



4.2 Install the Intel® TXEI Driver using Command Line

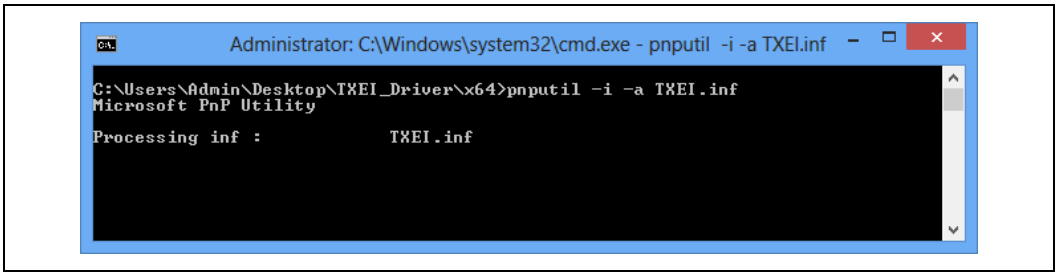
Please use this option as an alternative method. Installing the driver via Installer is the recommended method.

1. 1. Verify Intel TXEI driver is not installed on your system by:
   a. Open Device Manager (right click on My Computer -> Manage)
   b. Go to Device Manager subcategory
   c. Open System devices subcategory
   d. Look for device called "PCI Encryption/ Decryption Controller".

If "Intel® Trusted Execution Engine Interface" is already installed, uninstall it by right click->uninstall and check the "*Delete the driver software for this device*" checkbox.

2. Open command line with admin privileges and navigate to the root folder of TXEi.inf (\\TXEI_Driver\x64 or x86)
3. Type "pnputil.exe –i –a TXEI.inf

Figure 4-2. Intel® TXEI Installation



4. Select "*Install*"

Figure 4-3. Windows Security Prompt

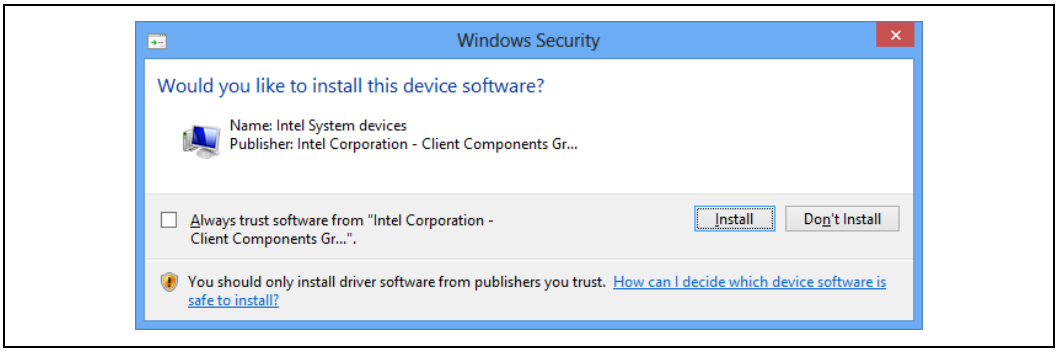
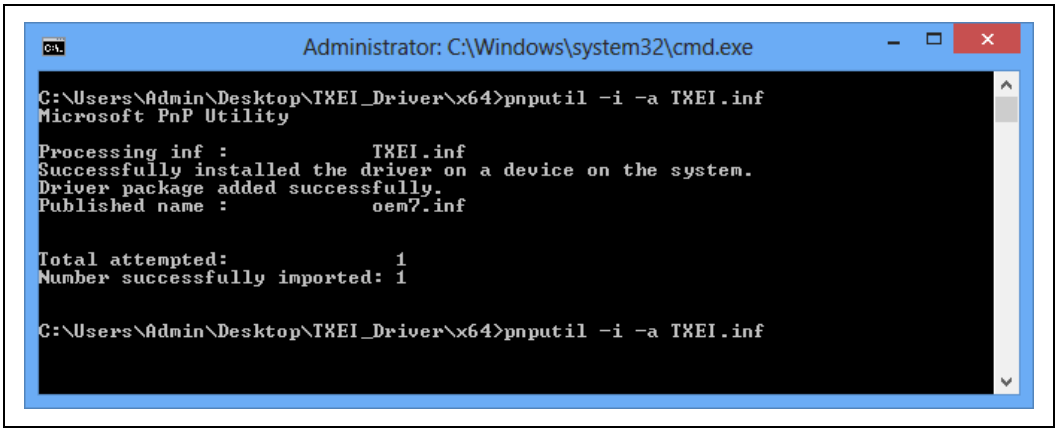
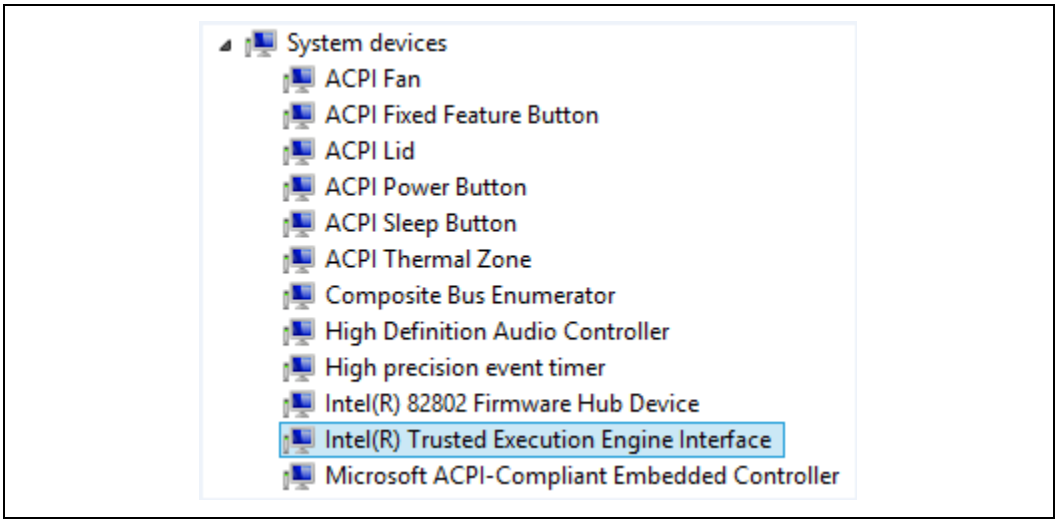


Figure 4-4. Finishing Intel® TXEI Installation



5. Verify Intel® TXEI is installed by referring to device manager→System devices:

Figure 4-5. Verify Intel® TXEI Installation in Device Manager



§

5 Using EFI System Tools in UEFI Shell with UEFI Secure Boot Enabled Option

Due to Microsoft's mandatory UEFI Shells and related applications requirement (System.Fundamentals.Firmware.UEFISecureBoot), when running Intel or customer manufacturing utilities in UEFI shell, customer is required to disable UEFI Secure boot via BIOS setup menu or UEFI variable. If OEM/ODM wants to run specific EFI tool that need to run with UEFI secure boot, OEM/ODM will sign that EFI tool with their OEM key.

6 Intel TXEManuf

Intel TXEManuf tool will auto-detect the hardware/firmware SKU, and automatically runs tests to check functionality of their related features on the manufacturing line.

6.1 Prerequisites

Intel® TXEI driver must be installed. (Please refer to section 4.1 for instructions on how to install Intel® TXEI driver).

6.2 TXEManuf Usage

For detailed instructions please refer to “Intel TXEManuf” section in “System Tools User Guide” document, located at the System Tools folder.

§

7 Intel® TXE FW Update

Intel FWUpdate tool allows an end user, such as an IT administrator, to update Intel TXE FW without having to reprogram the entire flash device. It then verifies that the update was successful.

7.1 Prerequisites

Intel® TXEI driver must be installed. (Please refer to section 4 for instructions on how to install Intel® TXEI driver).

7.2 FWUpdate Usage

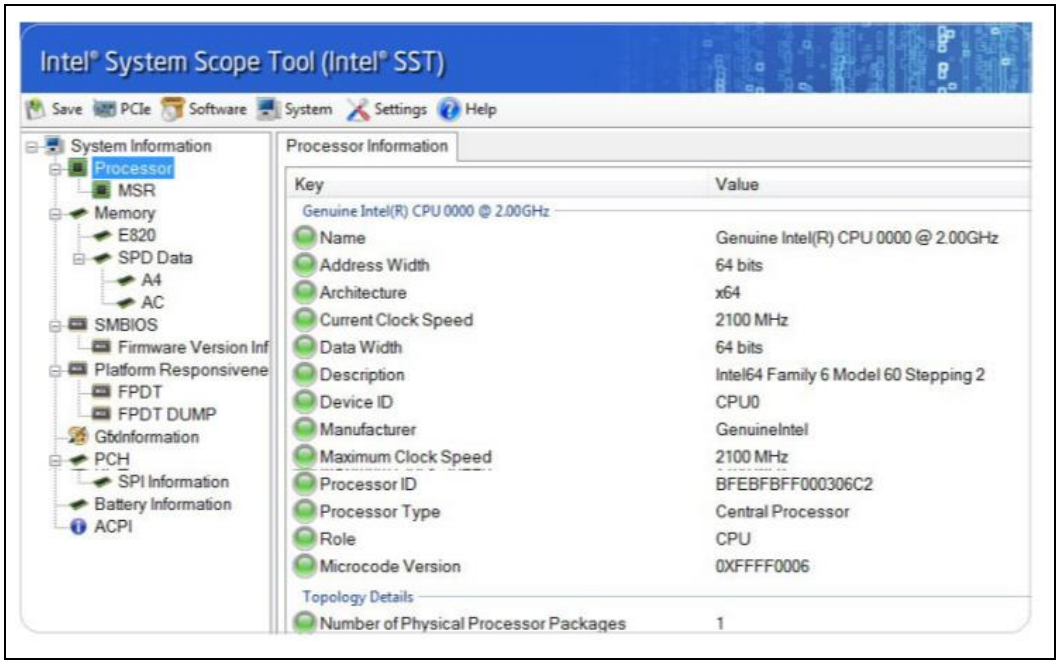
For detailed instructions please refer to “Intel TXE FW Update” section in “System Tools User Guide” document, located at the root folder.

§

8 Intel® System Scope Tool (Intel® SST)

The Intel® System Scope Tool (Intel® SST) is a tool which gives the complete snapshot of the system including both hardware and the software details.

Figure 8-1. Intel® System Scope Tool Screen Shot



- This tool is useful for providing full platform information for debugging purposes.
- An output file can be saved in .html format and attached to Bay Trail sightings
- This tool can be found on Intel® VIP inside the Bay Trail-M/D Compliance Kits (PV VIP kit # 54724).

9 FITC Soft Straps

Table 9-1. SOC Strap 0

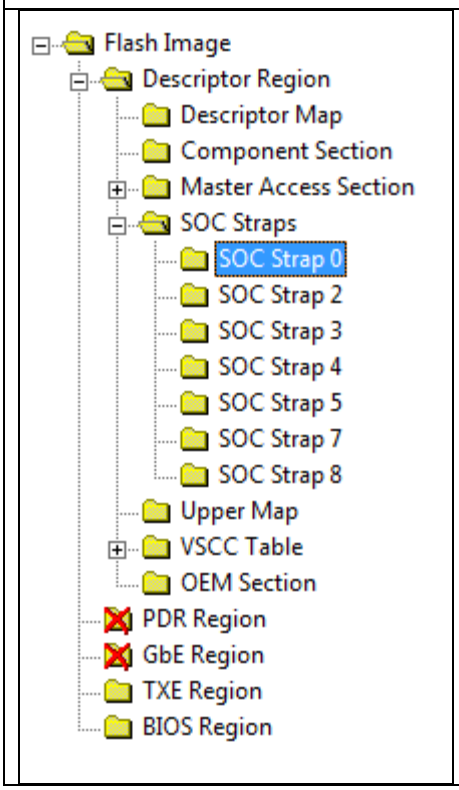
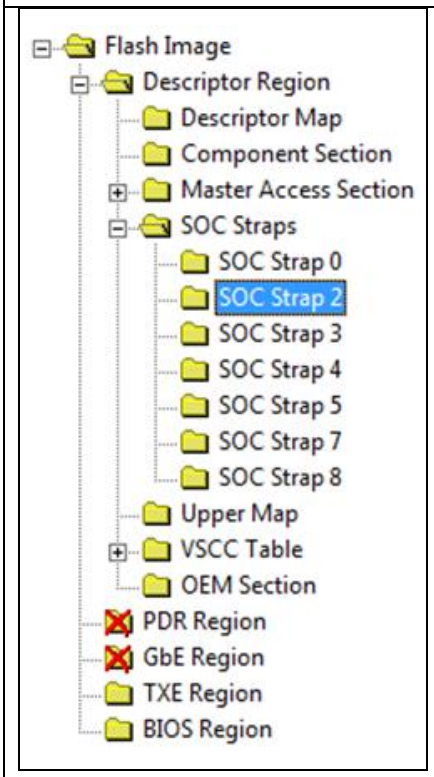
Location	Parameter	Values	Description
	BIOS Protected Range 4 Base	0x0000	Specifies the lower base of the BIOS protected range number 4. Address bits [11:0] are assumed to be 12'h000 for the base comparison. (goes to bits [12:0] at register: [Protected_Range_4] PR4 (@0x84)).
	BIOS Protected Range 4 Limit	0x0000	Specifies the upper limit of the BIOS protected range number 4. Address bits [11:0] are assumed to be 12'hFFF for the limit comparison. (Goes to bits [28:16] at register: [Protected_Range_4] PR4 (@0x84)).
	BIOS Protected Range 4 Write Protection Enable	True False (default)	When set, this bit indicates that the Base and Limit fields are valid and that writes directed to addresses between them (inclusive) must be blocked by hardware. The base and limit fields are ignored when this bit is cleared. Disabling this protected range could be done also by the security override pin strap. (this soft strap and the security override pin strap are reflected into bit 31 at register: [Protected_Range_4] PR4 (@0x84)).

Table 9-2. SOC Strap 2

Location	Parameter	Values	Description
	SPI Boot Block Size	00: 64KB (Default): Invert A16 if Top Swap is enabled. 01: 128KB: Invert A17 if Top Swap is enabled. 10: 256KB: Invert A18 if Top Swap is enabled	Sets SPI Boot Block Size
	SIO1_F0_Disable	False (default) True	Disable LPSS1 function 0 (DMA). false = enable. true = disable
	SIO1_F1_Disable	False (default) True	Disable LPSS1 function 1 (PWM#1). false = enable. true = disable
	SIO1_F2_Disable	False (default) True	Disable LPSS1 function 2 (PWM#2). false = enable. true = disable
	SIO1_F3_Disable	False (default) True	Disable LPSS1 function 3 (HSUART#1). false = enable. true = disable
	SIO1_F4_Disable	False (default) True	Disable LPSS1 function 4 (HSUART#2). false = enable. true = disable
	SIO1_F5_Disable	False (default) True	Disable LPSS1 function 5 (SPI). false = enable. true = disable
	SCC SDIO Disable	False (default) True	Disable SDIO. false = enable. true = disable
	SCC SDCARD Disable	False (default) True	Disable SDCARD. false = enable. true = disable
	HAD Disable	False (default) True	Disable HD Audio. false = enable. true = disable
	LPE Disable	False (default) True	Disable LPE. false = enable. true = disable
	XHCI Disable	False (default) True	Disable USH. false = enable. true = disable
	LAN Disable	True (default) False	Disable GbE. False = enable. true = disable
	SATA Disable	False (default) True	Disable SATA. False = enable. true = disable
	EHCI Disable	False (default) True	Disable USB: false = enable, true = disable

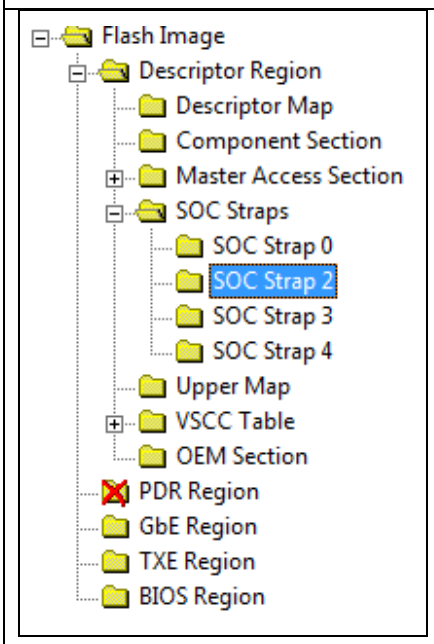
Location	Parameter	Values	Description
	PCIe 0 Disable	False (default) True	Disable PCIe port 0. False = enable. true = disable
	PCIe 1 Disable	False (default) True	Disable PCIe port 1. False = enable. true = disable
	PCIe 2 Disable	False (default) True	Disable PCIe port 2. False = enable. true = disable
	PCIe 3 Disable	False (default) True	Disable PCIe port 0. False = enable. true = disable
	SIO2 F0 Disable	False (default) True	Disable LPSS2 function 0 (I2C#0). false = enable. true = disable
	SIO2 F1 Disable	False (default) True	Disable LPSS2 function 1 (I2C#1). false = enable. true = disable
	SIO2 F2 Disable	False (default) True	Disable LPSS2 function 2 (I2C#2). false = enable. true = disable
	SIO2 F3 Disable	False (default) True	Disable LPSS2 function 3 (I2C#3). false = enable. true = disable
	SIO2 F4 Disable	False (default) True	Disable LPSS2 function 4 (I2C#4). false = enable. true = disable
	SIO2 F5 Disable	False (default) True	Disable LPSS2 function 5 (I2C#5). false = enable. true = disable

Table 9-3. SOC Strap 3

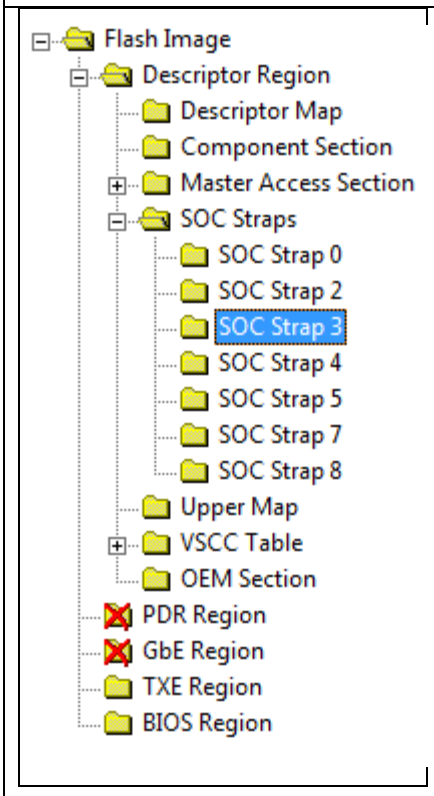
Location	Parameter	Values	Description
	SIO2 F6 Disable	False (default) True	Disable LPSS2 function 6 (I2C#6). false = enable. true = disable
	SIO2 F7 Disable	False (default) True	Disable LPSS2 function 7 (I2C#7). false = enable. true = disable
	DISBENDCLK_SSEN	False (default) True	Enable spread spectrum to DISPLAY BEND: false = disable, true = enable
	DISPSSCLK_SSEN	False (default) True	Enable spread spectrum to DISPLAY SS: false = disable, true = enable
	HFHPLLCLK_SSEN	False (default) True	Enable spread spectrum to HFHPLL: false = disable, true = enable
	PCIECLK_SSEN	False (default) True	Enable spread spectrum to PCIe: false = disable, true = enable
	SATACLK_SSEN	False (default) True	Enable spread spectrum to SATA: false = disable, true = enable
	OTG Super Speed PHY Disable	False (default) True	Disable OTG Super Speed PHY. false = enable. true = disable
	XHCI Super Speed PHY Disable	False (default) True	Disable USH Super Speed PHY. false = enable. true = disable
	Spread Percentage	0.456 (default) 0.439 0.423 0.391 and more…	Select Spread Spectrum Percentage (%). 0.456 is the Intel recommended value. Other values are for testing purposes only.

Table 9-4. SOC Strap 4

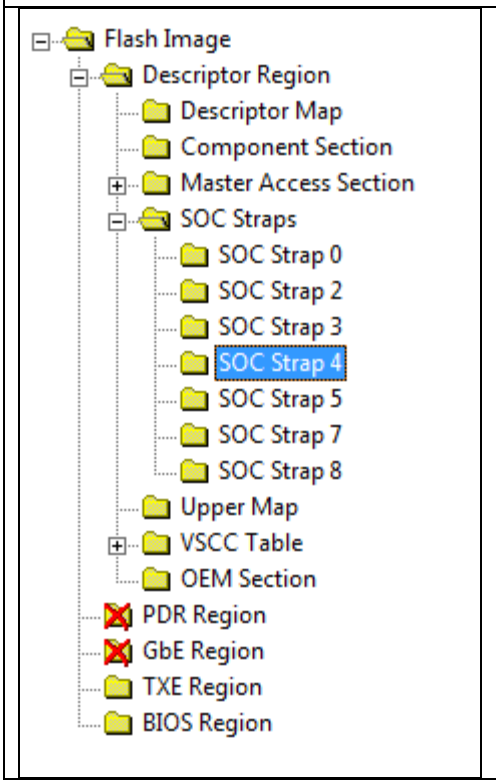
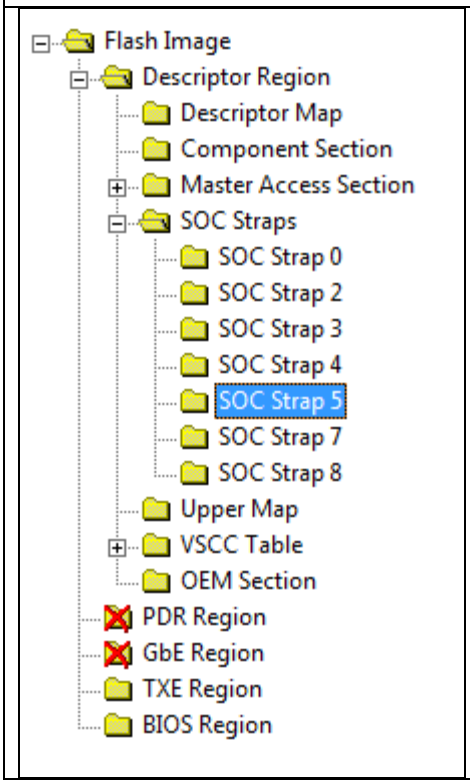
Location	Parameter	Values	Description
	LPC GPIO Select	1'b0: LPC (default) 1'b1: GPIO	Select the usage of LPC pins
	LPCCLK1_enb	True (default) False	False = disable. true = enable
	LPCCLK_SLC	1'b0 - iLPCCLK0 (default) 1'b1 - iLPCCLK1	Select LPC return clock source. This soft-strap is reflected to LPCC.LPCCLK_SLC register

Table 9-5. SOC Strap 5

Location	Parameter	Values	Description
	STGREN Register	1: Port Staggering Enabled (default) 0: No Port Staggering	Set the default for the PCI. Port Staggering Enabled: 0 = No Port Staggering, 1= Port Staggering Enabled. This strap sets the default value of the PCIe PORTSTAGEN register.
	Lane Reversal	0: No Lane Reversal (default) 1: Lane Reversal	Lane Reversal: 0 = No Lane Reversal, 1= Lane Reversal.
	Root Port Configuration	00: 4x1s Port 1 (x1), Port 2 (x1), Port 3 (x1), Port 4 (x1) (default) 01: 1x2, 2x1s Port 1 (x2), Port 3 (x1), Port 4 (x1) 10: 2x2 Port 1 (x2), Port 3 (x2) 11: 1x4 Port 1 (x4) **Note [1]**	Set the default value of root Port Configuration.

Note [1]: If the 'Root Port Configuration' default value is been changed in SOC Strap 5 the following changes need to be performed as well:

If the Value of "Root Port Configuration" been changed to "01: 1x2, 2 x1s Port 1 (x2), Port 3 (x1), Port 4 (x1)"
Require change of "PCIe 1 Disable" value in PCH Strap 2 from "false" to "true".

If the Value of "Root Port Configuration" been changed to "10: 2x2 Port 1 (x2), Port 3 (x2)",
Require change of "PCIe 1 Disable" and "PCIe 3 Disable" in PCH Strap 2 from "false" to "true".

If the Value of "Root Port Configuration" been changed to "11: 1x4 Port 1 (x4))",
Require change of "PCIe 1 Disable" and "PCIe 2 Disable" as well as "PCIe 3 Disable" in PCH Strap 2 from "false" to "true".

Table 9-6. SOC Strap 7

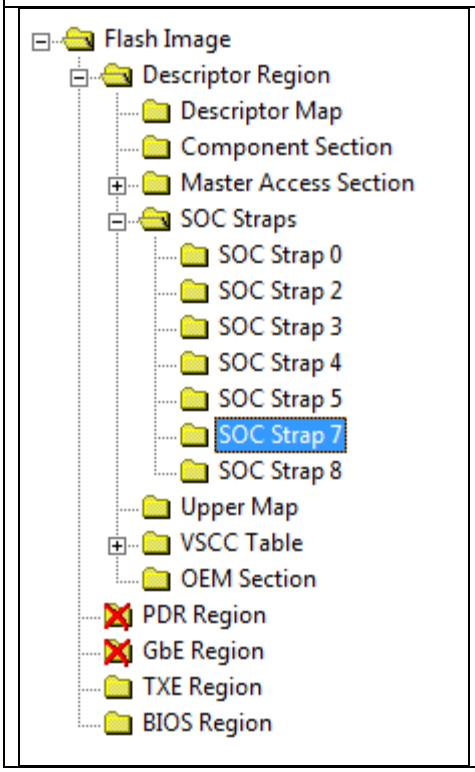
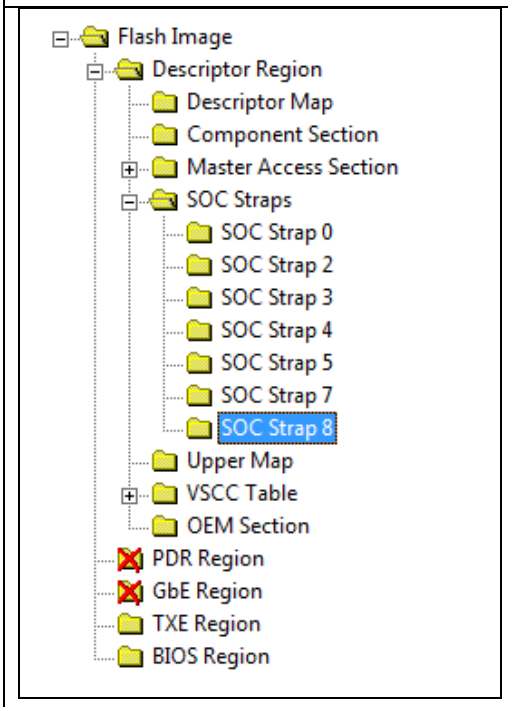
Location	Parameter	Values	Description
	PCIECMNLNPW Enable	True (default) False	False = disable, true = enable. **NOTE:** Integrated clock usage and specs must be signed off by SEG architects.
	PCIELANE0PWREN	True (default) False	PCIE Enables power for digital (synthesized) logic for the Common Lane logic and PLL1Core uPAR: false = disable, true = enable.
	PCIELANE1PWREN	True (default) False	PCIE Enables power for digital (synthesized) logic in the data lane to reduce leakage.
	PCIELANE2PWREN	True (default) False	PCIE Enables power for digital (synthesized) logic in the data lane to reduce leakage.
	PCIELANE3PWREN	True (default) False	PCIE Enables power for digital (synthesized) logic in the data lane to reduce leakage.

Table 9-7. SOC Strap 8

Location	Parameter	Values	Description
	SATACMNLNPW Enable	True (default) False	False = disable, true = enable. **NOTE:** Integrated clock usage and specs must be signed off by SEG architects.
	SATALANE0PWREN	True (default) False	SATA Enables power for digital (synthesized) logic for the Common Lane logic and PLL1Core uPAR: false = disable, true = enable.
	SATALANE1PWREN	True (default) False	SATA Enables power for digital (synthesized) logic in the data lane to reduce leakage.
	Satastatus2PMC	True (default) False	False = SATA to indicate D3 status to PMC. True = SATA to indicate DEVSLP status to PMC.

§