SSE-300 MPS3

TFM-PF Pack User Guide

Version:	1.0
Date of Issue:	19/03/2021

Contents

Introduction

This document is a general guide to use the SSE-300 MPS3 TFM-PF CMSIS pack. The CMSIS pack is to be used with the Corstone-300 platform MPS3 FVP model or AN547 FPGA (AN547: Arm Corstone™ SSE-300 with Ethos™-U55 Example Subsystem for MPS3). The pack includes support for TF-M (Trusted Firmware-M), including two example TF-M test projects with and without bootloader.

This document specifies system prerequisites and explains how to build and run the reference Blinky example on the SSE-300 MPS3 FVP model and on the AN547 FPGA.

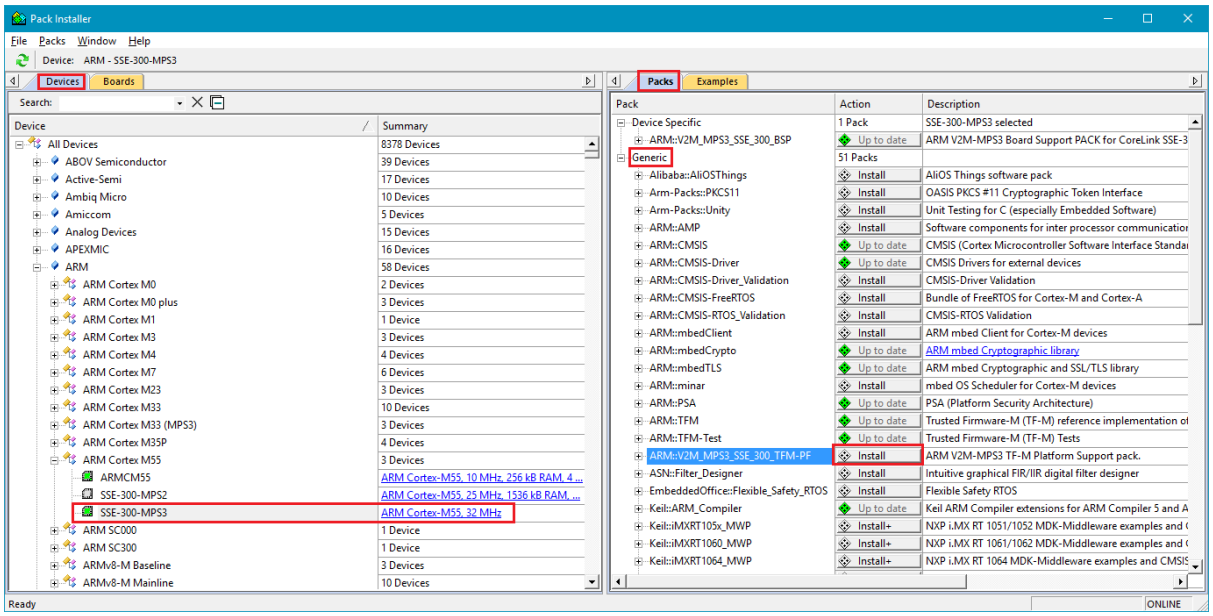
Prerequisites

Note: At time of creating this document, the FVP model is only available for Linux, but expected to be available for Windows soon. About using the pack with Linux, please refer to the SSE-300 MPS3 BSP Pack User Guide.

- ARM.V2M_MPS3_SSE_300_TFM-PF.1.0.0.pack Download from Keil or Install from Pack Installer
- Minimum Keil MDK v5.30
- (FVP) Download and install Corstone SSE-300 MPS3 FVP model.
- (FPGA) Download and install AN547: Arm Corstone™ SSE-300 with Ethos™-U55 Example Subsystem for MPS3 FPGA files.
- (TFM Bootloader example) Python and imgtool (>=1.7.0) for signing binaries

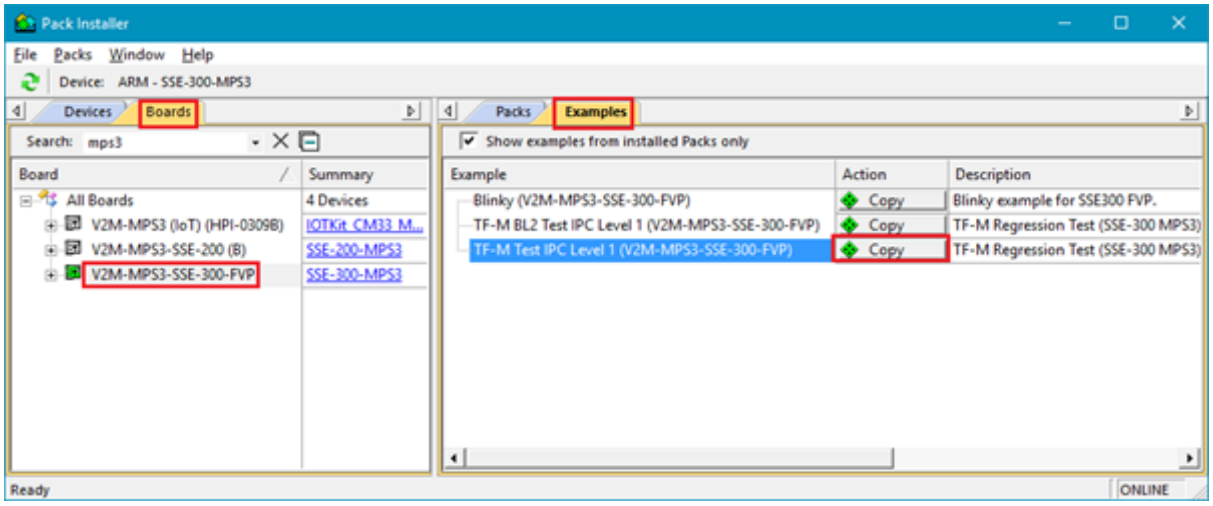
Pack Installation – Keil MDK

Install ARM::V2M_MPS3_SSE_300_TFM-PF using the Pack Installer. The pack can be browsed by selecting SSE-300-MPS3 device under ARM Cortex M55 Devices.

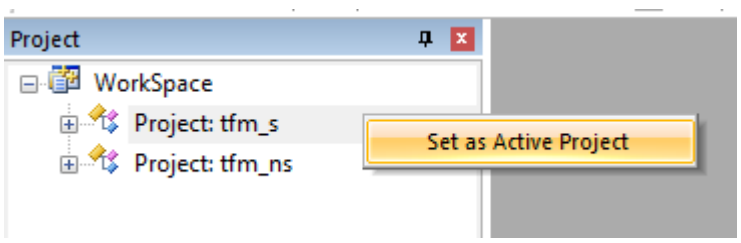


Import and build TF-M Test IPC Level 1 project – Keil MDK

Copy the TF-M Test IPC Level 1 project using the Pack Installer. The example project can be found by searching and selecting V2M-MPS3-SSE-300-FVP Board under the Boards section.



Once copied, open the project using the uVision, and set Project: tfm_s as active: right click on project name, then click Set as Active Project.



Build the project, then select Project: tfm_ns as active, and build that too.

Run TF-M Test IPC Level 1 project – FVP

After the import and build steps, the following output files will be needed:

- `tfm_s/tfm_s.axf`
- `tfm_ns/tfm_ns.axf`

The FVP can be run with the following parameters:

```
<path_to_fvp>/FVP_Corstone_SSE-300_Ethos-U55 -a tfm_ns.axf -a
tfm_s.axf
```

Run and debug TF-M Test IPC Level 1 (FPGA) – Keil MDK

After the import and build steps. Create the binaries from the axf file using fromelf:

```
fromelf.exe --bincombined --output tfm_s.bin tfm_s.axf
fromelf.exe --bincombined --output tfm_ns.bin tfm_ns.axf
```

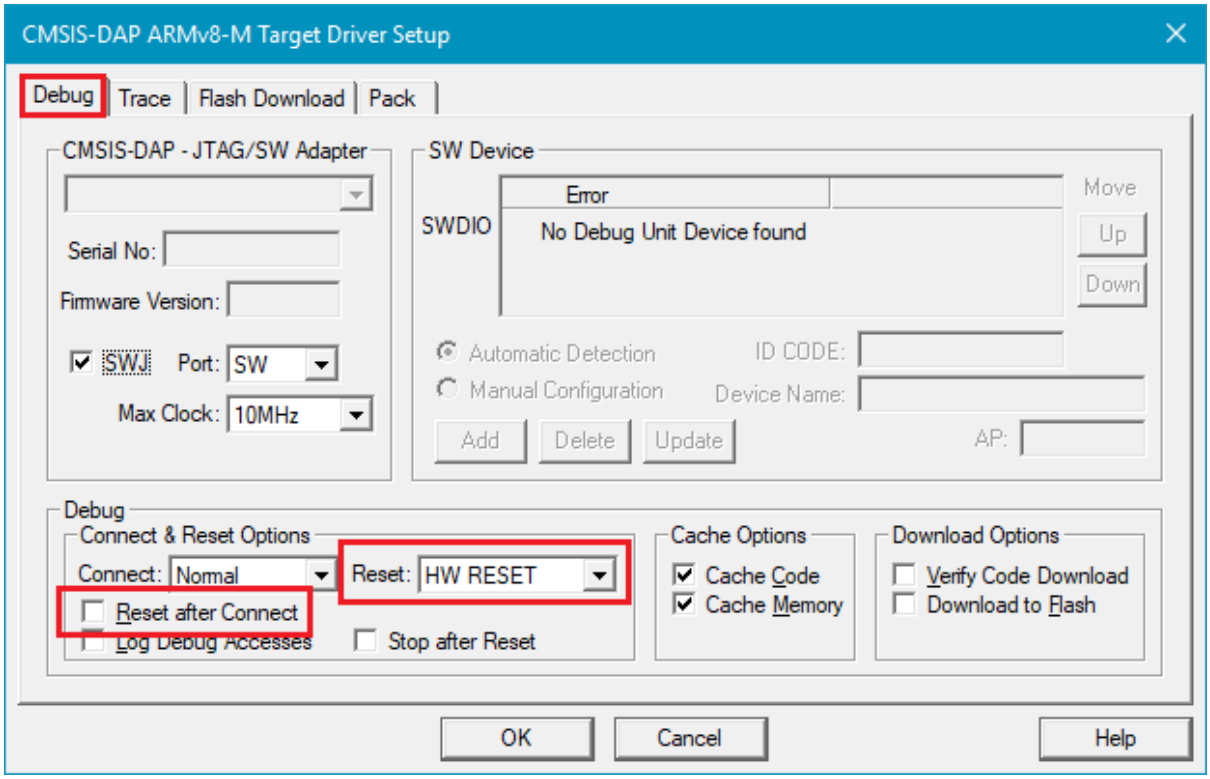
Copy the binaries to the SD card and use the following addresses in images.txt:

```
IMAGE0ADDRESS: 0x00000000          ;
IMAGE0UPDATE: AUTO                 ;
IMAGE0FILE: \SOFTWARE\tfm_s.bin    ;
IMAGE1ADDRESS: 0x02060000          ;
IMAGE1UPDATE: AUTO                 ;
IMAGE1FILE: \SOFTWARE\tfm_ns.bin   ;
```

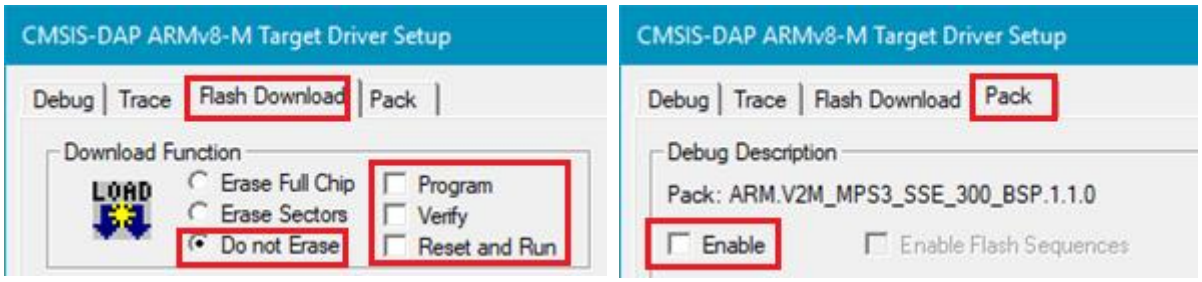
Restart the FPGA.

Select tfm_s as Active Project. In “Options for Target …”, in the Debug tab, Use: “CMSIS-DAP ARMv8-M Debugger” is selected. Depending on your setup, you can also use “ULINK Pro ARMv8-M Debugger”.

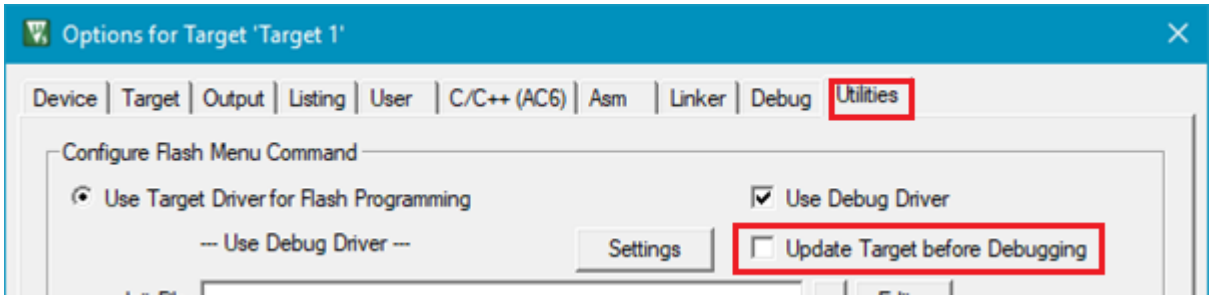
Click Settings. Make sure that on Debug tab, at Debug section, Reset after Connect is unchecked and Reset is set to HW RESET.



In Flash Download tab, Do not Erase is selected and none of the checkboxes are checked and on Pack tab, Enable is unchecked.



Click OK. At Utilities tab, make sure that Update Target before Debugging is unchecked.



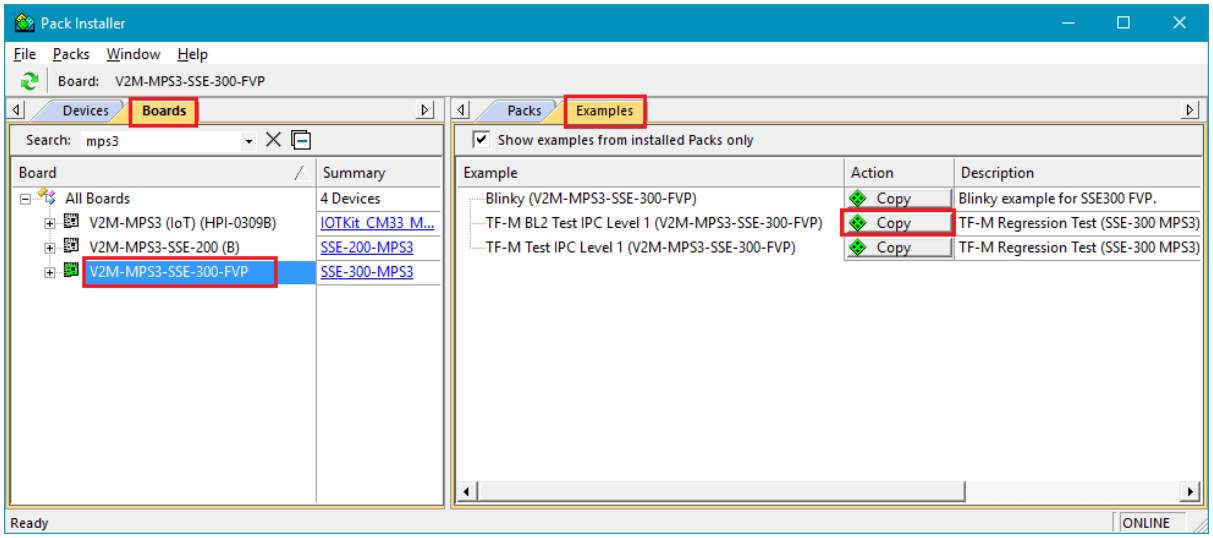
Click the debug button at top to start a debug session.

After connection, Reset is only possible when the target is running. If you wish to Reset the target, make sure to Run the target before pressing Reset.

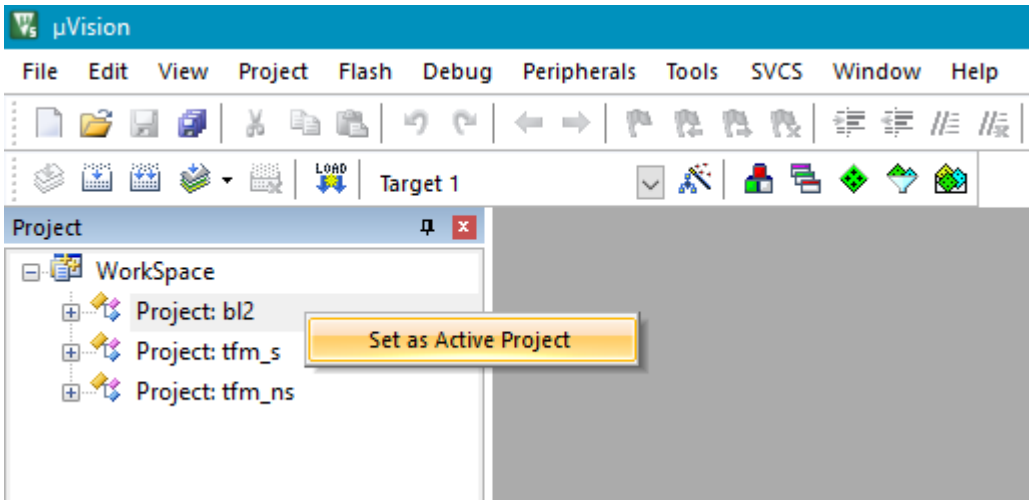
Import and build TF-M BL2 Test IPC Level 1 project – Keil MDK

Note: Secure side image (tfm_s) and non-secure side image (tfm_ns) are signed and encapsulated with header and trailer during post build process. The following external tools are required:
- python + imgtool (>=1.7.0)
The above executables need to be in the command line path.

Copy the TF-M BL2 Test IPC Level 1 project using the Pack Installer. The example project can be found by searching and selecting V2M-MPS3-SSE-300-FVP Board under the Boards section.



Once copied, open the project using the uVision, and set Project: bl2 as active: right click on project name, then click Set as Active Project.



Build the project, then select Project: tfm_s as active, build it, then finally do the same for Project: tfm_ns.

Run TF-M BL2 Test IPC Level 1 project – FVP

After the import and build steps, the following output files will be needed:

- bl2/bl2.axf
- tfm_s/tfm_s_signed.bin
- tfm_ns/tfm_ns_signed.bin

The FVP can be run with the following parameters:

```
<path_to_fvp>/FVP_Corstone_SSE-300_Ethos-U55 --data
tfm_s_signed.bin@0x11000000 --data tfm_ns_signed.bin@0x01060000 -a
bl2.axf
```

Run and debug TF-M BL2 Test IPC Level 1 (FPGA) – Keil MDK

After the import and build steps. Create the binary from the axf file using fromelf:

```
fromelf.exe --bincombined --output bl2.bin bl2.axf
```

Rename the signed binaries as tfm_s_signed.bin → tfm_s.bin and tfm_ns_signed.bin → tfm_ns.bin. Copy the files to the SD card and use the following addresses in images.txt:

```
IMAGE0ADDRESS: 0x00000000          ;
IMAGE0UPDATE: AUTO                 ;
IMAGE0FILE: \SOFTWARE\bl2.bin      ;
IMAGE1ADDRESS: 0x02000000;
IMAGE1UPDATE: AUTO                 ;
IMAGE1FILE: \SOFTWARE\tfm_s.bin    ;
IMAGE2ADDRESS: 0x02060000;
IMAGE2UPDATE: AUTO                 ;
IMAGE2FILE: \SOFTWARE\tfm_ns.bin   ;
```

Restart the FPGA.

Before starting the debug session, select bl2 as Active Project and check the options described in “Run and debug TF-M Test IPC Level 1 (FPGA)”.