Technical Note

Infineon AURIX TC3xx: HSM programming

May 2023

This Technical Note describes a procedure of programming an HSM application through winIDEA on Infineon AURIX TC3xx devices.

Tool requirements:
- ✓ winIDEA 9.21.0 or newer
- ✓ BlueBox iC5700, iC5000
- ✓ Infineon AGBT Active Probe or Infineon DAP/DAPE Active Probe or 10-pin 1.27 mm Infineon DAP2 Wide Debug Adapter or 22-pin ERF8 DAP2 Debug Adapter

The HSM (Hardware Security Module) is a module available on all AURIX TC3xx devices. Through winIDEA you can program an HSM application and configure the UCB (User Configuration Block) which is required to enable the HSM on your AURIX device.

HSM application programming and UCB configuration requires caution because a misconfiguration can potentially lock your chip.

It is recommended to use Image checker during UCB or HSM code programming. Please note that a separate license is needed for Image checking.

winIDEA Configuration

The proper procedure to program your HSM application can be summarized in two steps:
1. Program the TriCore application and the HSM code.
2. Enable the HSM in the UCB.

Program the TriCore application and the HSM code

1. Prevent chip locking by misconfiguration via *Hardware / CPU Options / Debugging / Image checker / Reject programming*.

2. Verify that you have selected the program files for the regular TriCore application(s) as well as the program file for the HSM via *Debug / Configure session / SoC / Program Files*.

Proceed to the next step only when you are sure that the HSM code has been downloaded. The chip will be locked after the next power-on reset if the HSM is enabled while no valid HSM code is present.

Enable the HSM in the UCB

1. Enable writing to the UCB via *Hardware / Options / Programming* by checking *Infineon TC3xx_UCB_24kB*.

The amount of writes to the UCB is limited. For the exact number of writes, refer to your AURIX device reference manual. Uncheck the UCB memory device once the UCB is programmed.

2. Establish a new session via *Debug / Load Symbols Only*.

3. Open the *UCB plugin window* by selecting *View / [TC3xx] Aurix / UCB*.
To configure the boot mode headers open *Extra Commands / Set Startup Address*. In the *Configuration* section, specify the *Address* of your primary application and select the *Startup mode*. In the *UCBs to program* section, choose a UCB you would like to program. At least one valid boot mode header needs to be programmed before enabling the HSM.

4. Before proceeding, check the validity of the programmed boot mode header by making sure that the CPU0 boots correctly.
   a. Disable presenting the CPU0 program counter by setting *Hardware / CPU Options / Cores / CPU0 / Preset PC after stopped in init* to *Do not preset*.
   b. Reset the CPU via *Debug / Reset* and observe its reset vector.

Enabling the HSM without having a valid boot mode header programmed can permanently lock your chip!

5. In the *UCB plugin window*, select *Extra Commands / Configure HSM*. In the *Configuration section*, tick *HSM Boot Enable* and specify *HSM Boot Logical Sector Indexes* according to the location of your HSM boot code. In the *UCBs to program section*, choose those UCBs you want to program.

In case of any security violation, programming is rejected. This completes the configuration. After the power-on reset, the newly entered UCBs are read by the CPU and the HSM is started accordingly.

More resources in winIDEA Help

- UCB plugin
- Image checker
- HSM Configuration
- Demo mode
- Load Map
- UCB programming