Trusted Firmware - M

Initialization Entry Enhancement

© 2020 Arm Limited (or its affiliates)

Summer Qin
2020.9.17
Contents

• The existing initialization flow
• The enhancement
Existing initialization entry flow - IPC

- **Reset_Handler**
  - privileged
  - thread mode
  - msp

- **SystemInit**
  - privileged
  - thread mode
  - msp

- **Swith to PSP**
  - privileged
  - thread mode
  - psp

- **toolchain:: _main / _start**
  - privileged
  - thread mode
  - psp

- **Enter to NS**
  - unprivileged
  - thread mode
  - psp

- **spm_init**
  - privileged
  - handler mode
  - msp

- **tfm::main()**
  - privileged
  - thread mode
  - psp
Existing initialization entry flow - library

Reset_Handler
- privileged
- thread mode
- msp

SystemInit
- privileged
- thread mode
- msp

Switch to PSP
- privileged
- thread mode
- psp

toolchain:: _main / _start
- privileged
- thread mode
- psp

Enter to NS
- unprivileged
- thread mode
- psp

spm_init
- privileged
- thread mode
- psp

tfm::main()
- privileged
- thread mode
- psp
Existing initialization analysis

• Booting belong to scope of SPM, while SPM should work inside a dedicated stack which should never be shared with others.
  • ARM_LIB_STACK being reused by booting code and non-secure partition

• Toolchain would set ARM_LIB_STACK into SP before launching C code
  • Toolchain regard the SPM as the ‘program’ and SPM is using MSP while booting, so ARM_LIB_STACK should represent the MSP value.

• The customized modification for switching to PSP adds un-natural modification on default platform sources for M-profile platform.
  • This switch is unnecessary during booting.
Enhanced initialization entry flow - IPC

Reset_Handler
• privileged
• thread mode
• msp

SystemInit
• privileged
• thread mode
• msp

Switch to PSP
• privileged
• thread mode
• psp

toolchain:: _main / _start
• privileged
• thread mode
• msp

Enter to NS
• unprivileged
• thread mode
• psp

spm_init
• privileged
• handler mode
• msp

tfm::main()
• privileged
• thread mode
• msp

MSP needs to be reset before scheduling
Enhanced initialization entry flow - library

- **Reset_Handler**
  - privileged
  - thread mode
  - msp

- **SystemInit**
  - privileged
  - thread mode
  - msp

- **Switch to PSP**
  - privileged
  - thread mode
  - psp

- **toolchain:: _main / _start**
  - privileged
  - thread mode
  - msp

- **spm_init**
  - privileged
  - thread mode
  - msp

- **tfm::main()**
  - privileged
  - thread mode
  - msp

- **Enter to NS**
  - unprivileged
  - thread mode
  - psp

MSP needs to be reset before working in psp
Thank You
Danke
Merci
Merci
Danke
Мерси
谢谢
謝謝
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה