arm

Trusted Firmware - M

Initialization Entry Enhancement

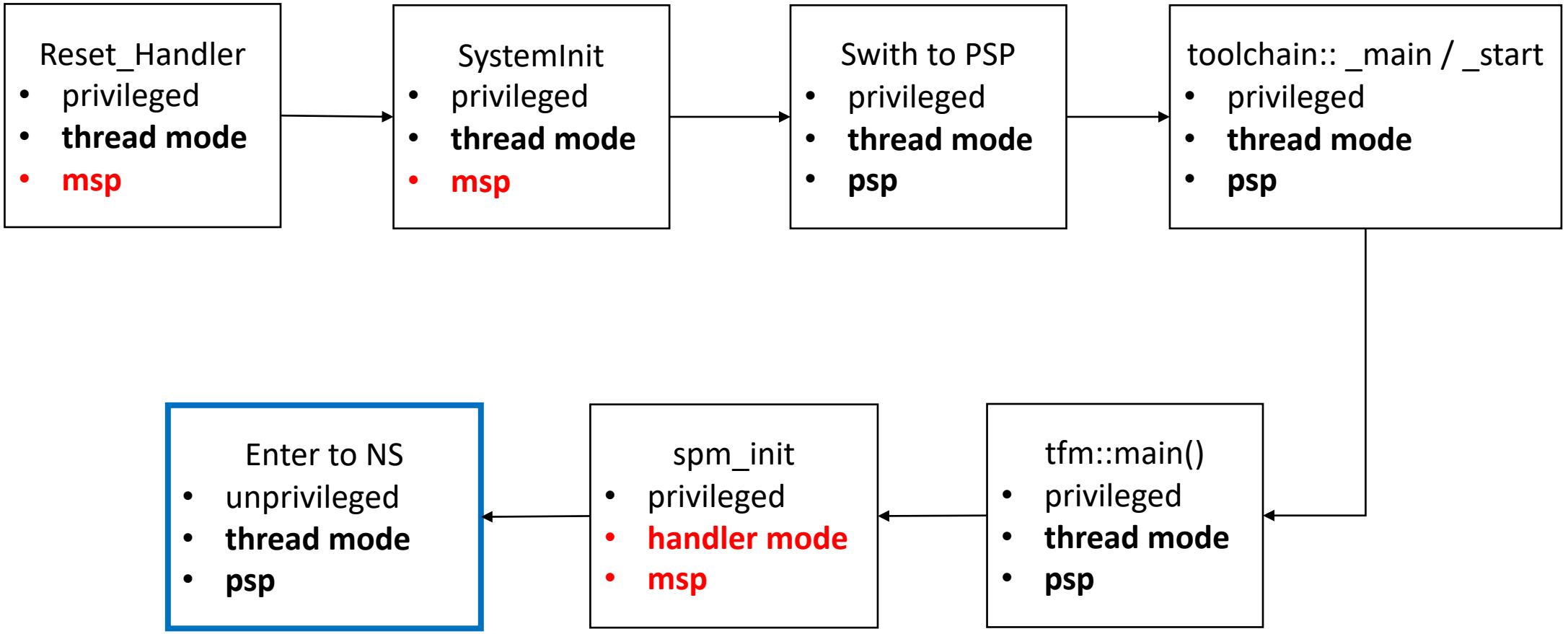
Summer Qin

2020.9.17

Contents

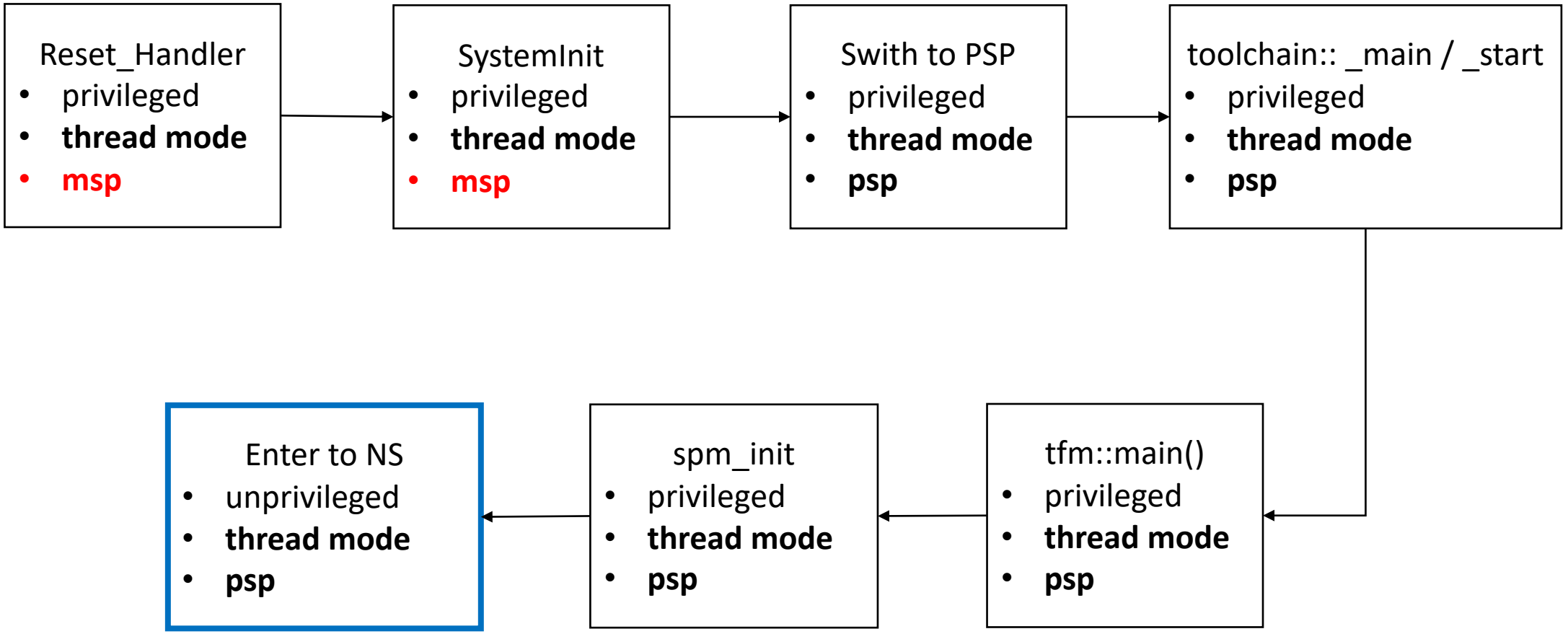
- The existing initialization flow
- The enhancement

Existing initialization entry flow - IPC



arm

Existing initialization entry flow - library



arm

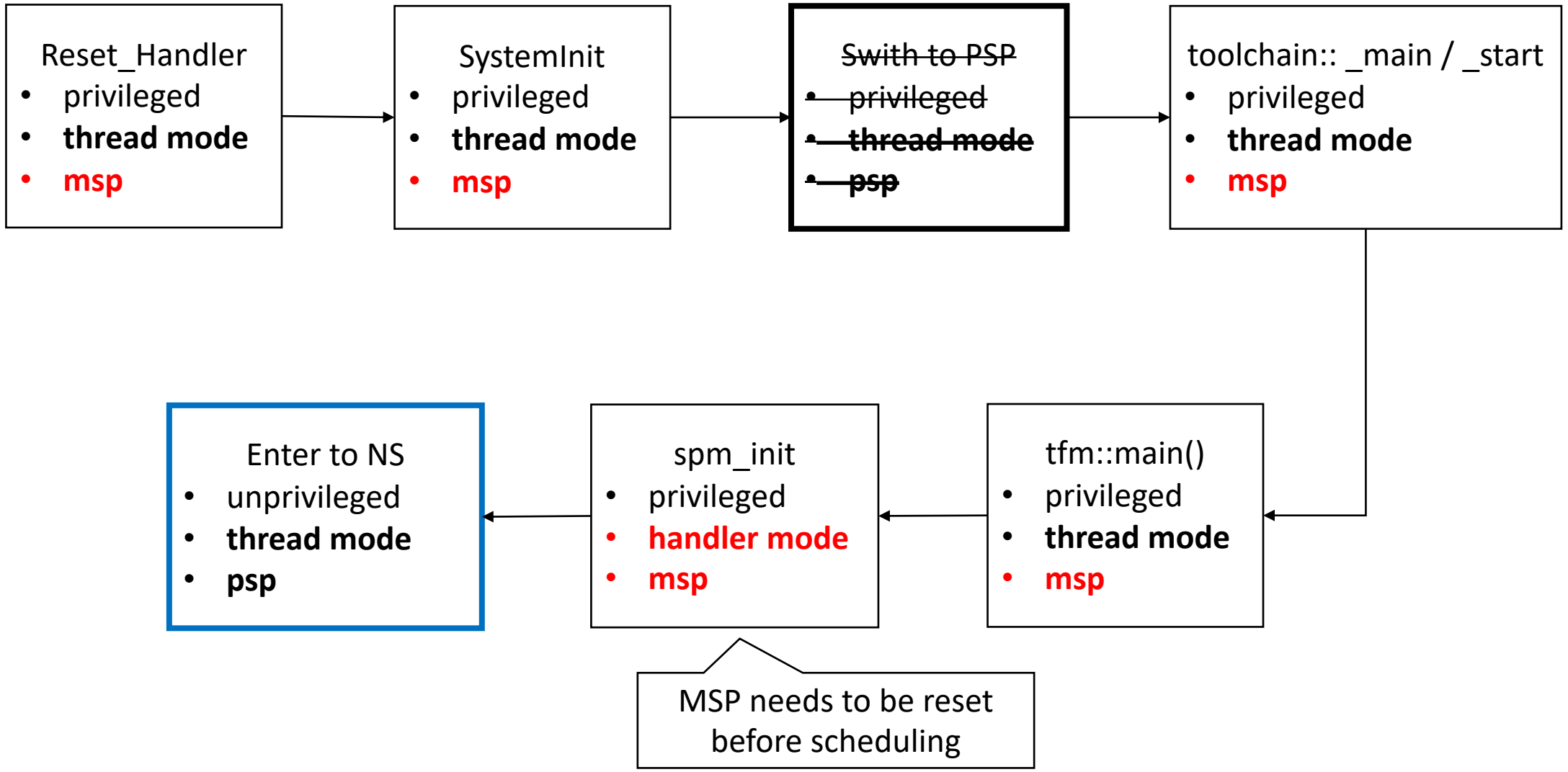
Existing initialization analysis

- 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.

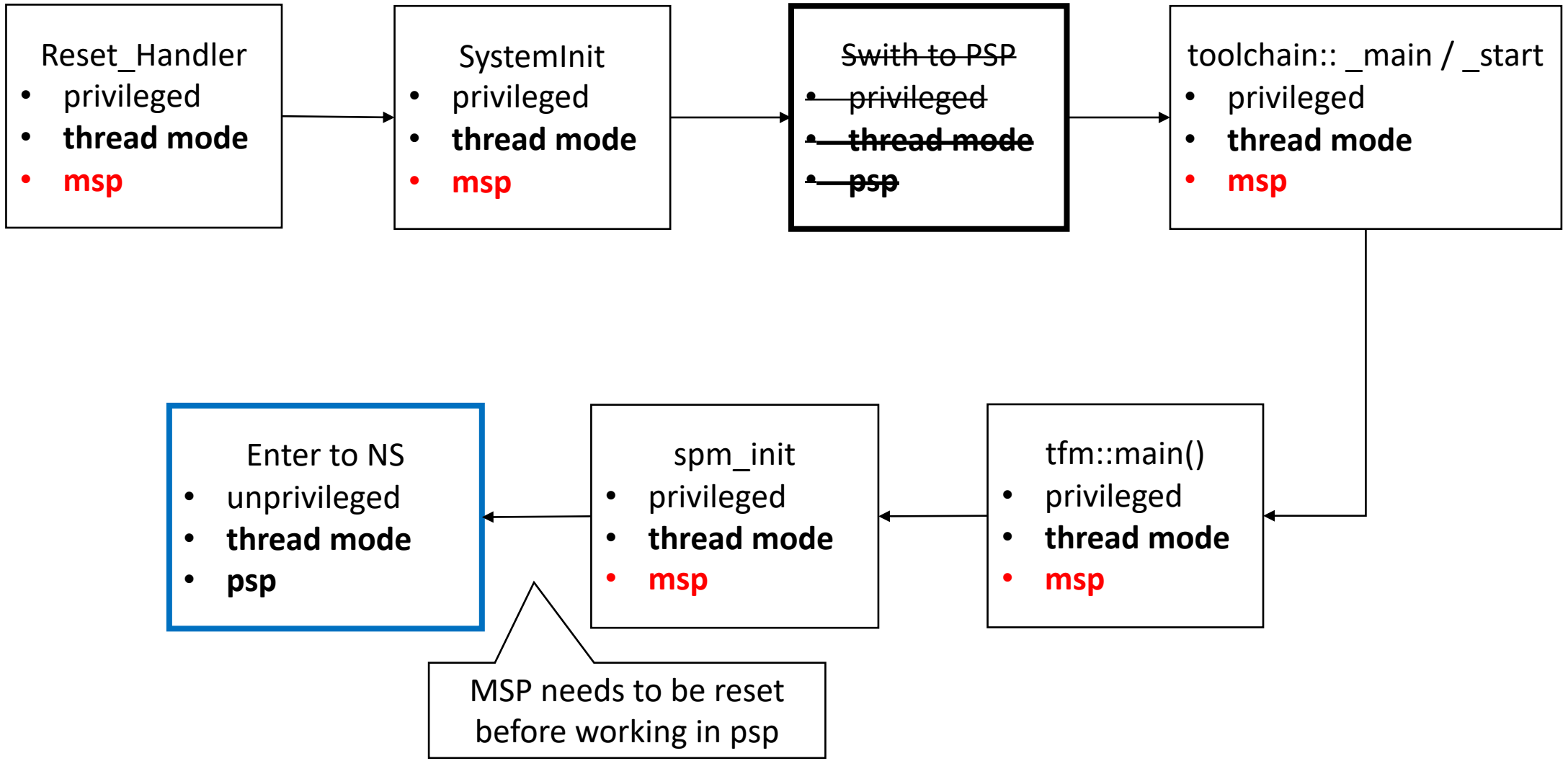
- The customized modification for switching to PSP adds un-natural modification on default platform sources for M-profile platform.
  - This switch is unnecessary during booting.

Enhanced initialization entry flow - IPC



arm

Enhanced initialization entry flow - library



arm

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה