TF-A Tech Forum

Firmware update design

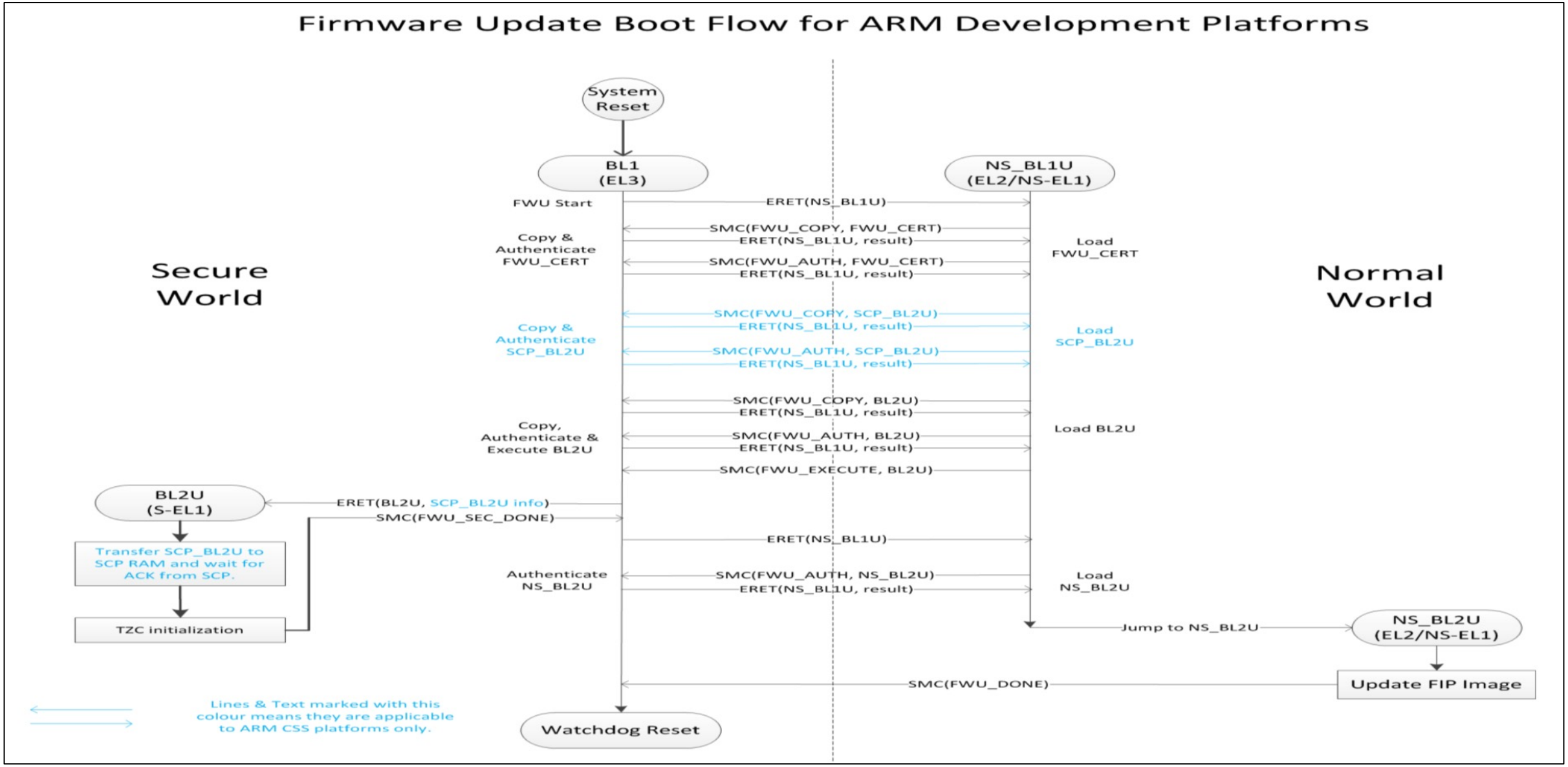
Manish Badarkhe

29-Jul-2021

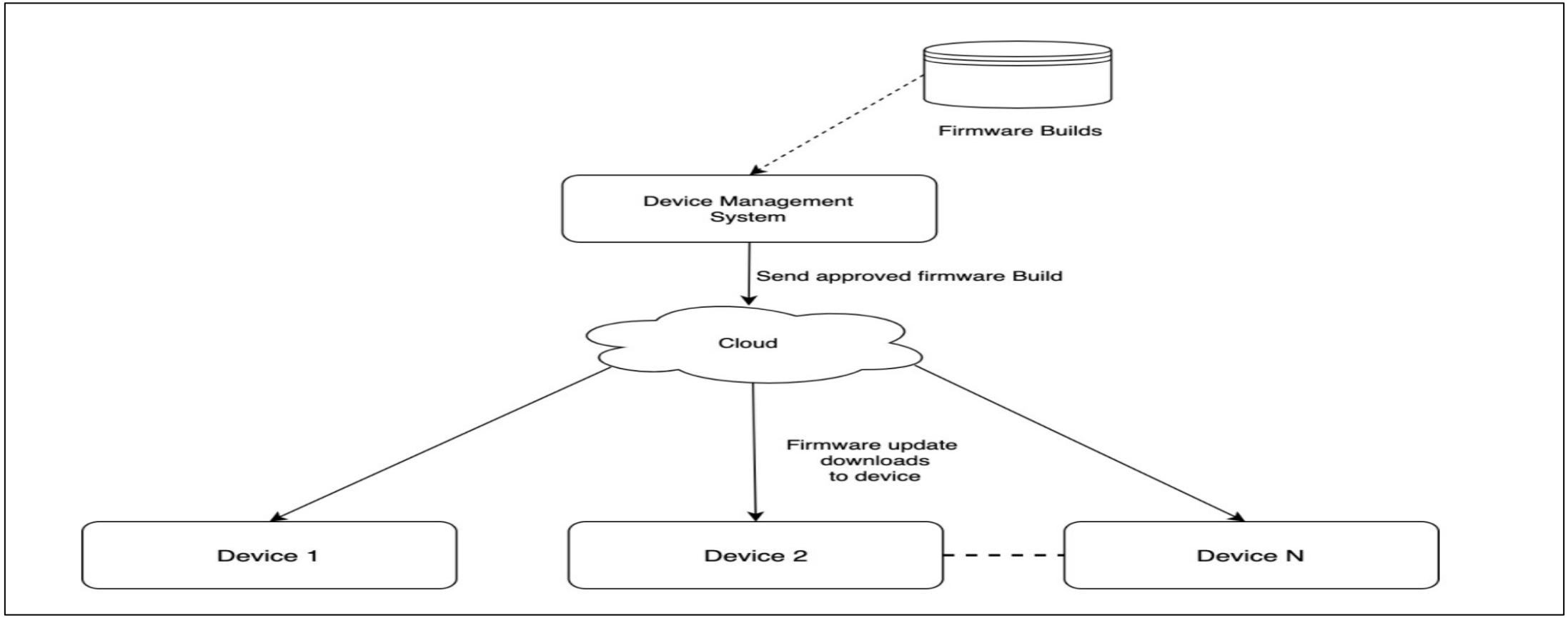
Agenda

- Firmware update current scenario in Arm platforms
- Overview of firmware update flow
  - Flash controlled by Secure world
  - Flash controlled by Non-secure world
- Firmware update - metadata
- Firmware update - ABIs and state machine
- Firmware update tasks in TF-A
- Unit/Integration tests executed

Firmware update current scenario – Recovery mechanism

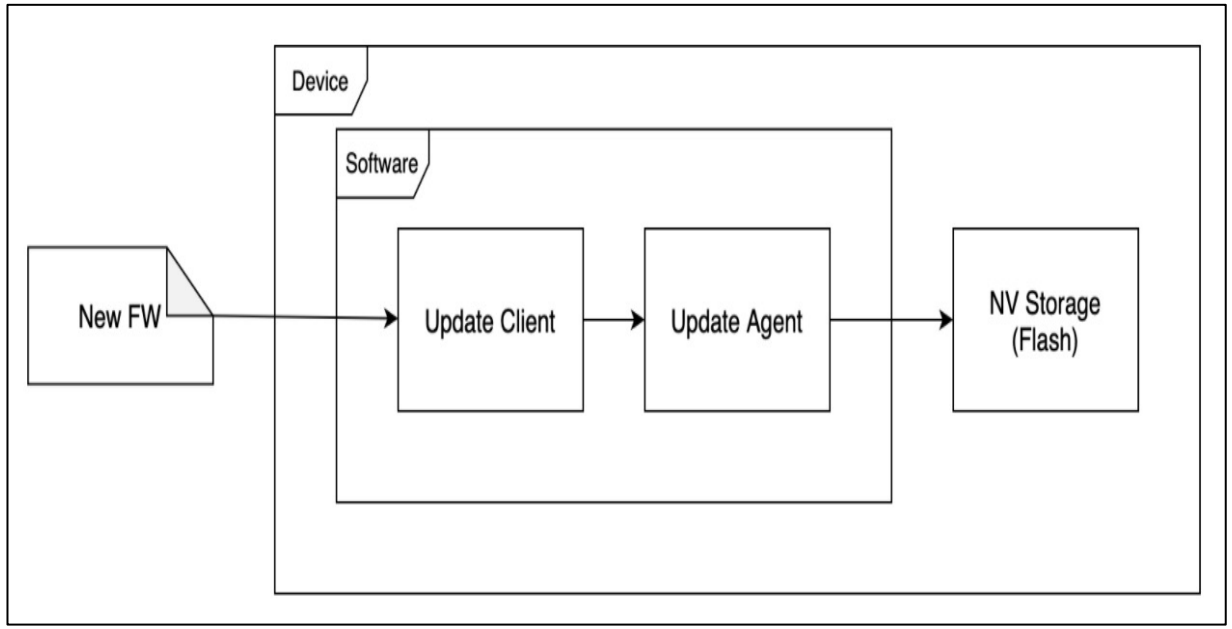


Firmware update – Basic Flow



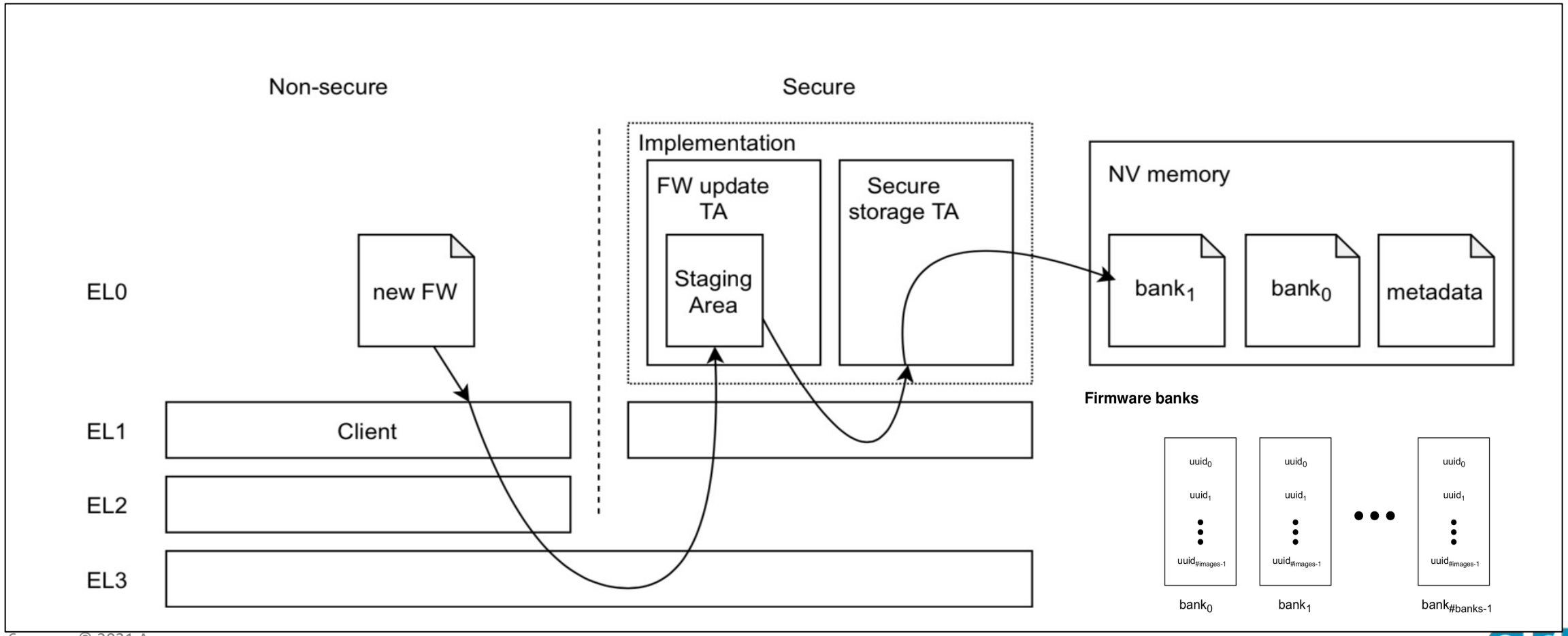
Firmware update components

- Update Client
  - Receives new firmware images and initiate the FW update operation
- Update Agent
  - Receives FW images from client and write them to NV storage (Flash)

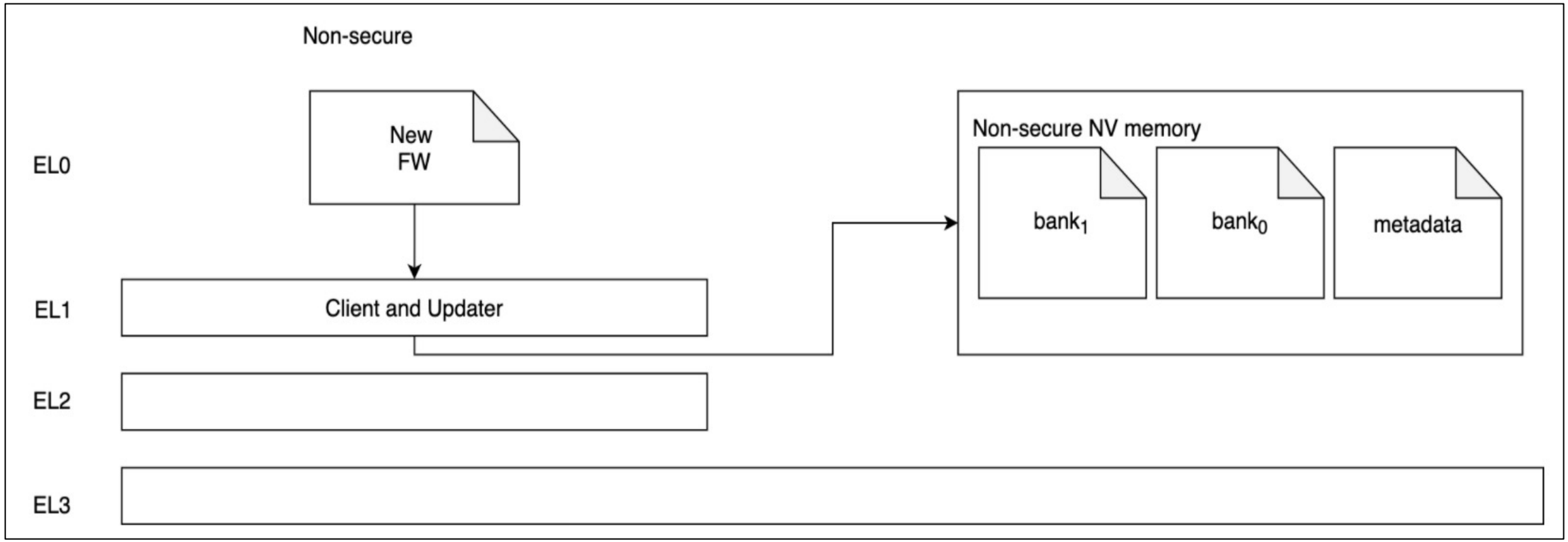


Firmware Update - Secure world control

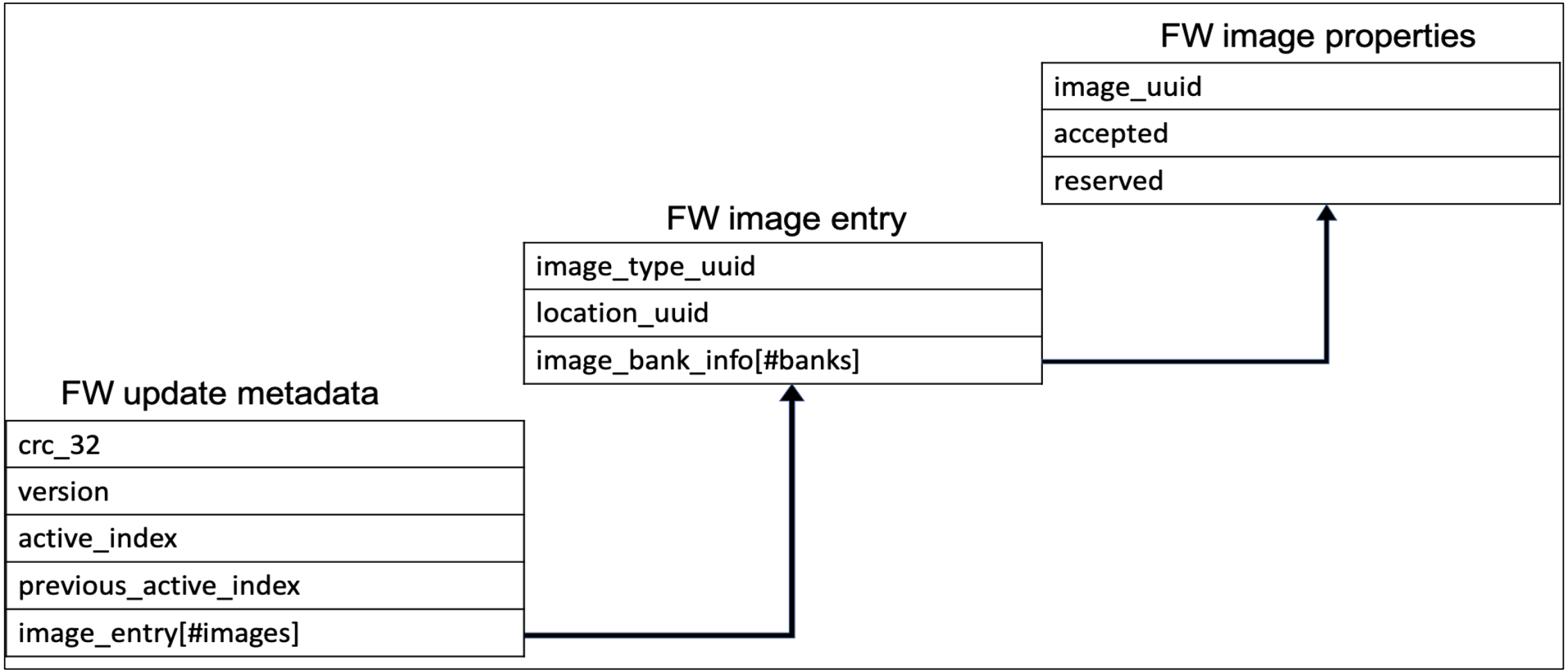
- Update Agent in the Secure World
- Client executes in the Non-secure World



Firmware Update – Non-Secure world control



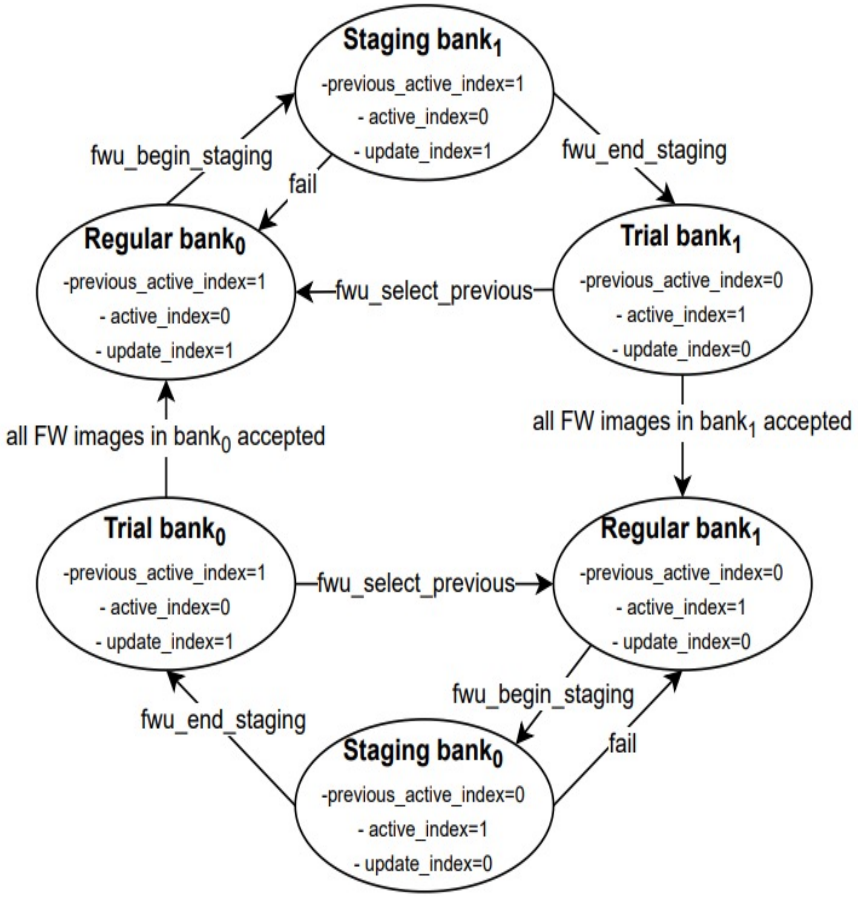
Firmware update metadata



ABIs and State machine

These ABIs are a contract between caller (Client) and and the callee (Update Agent)

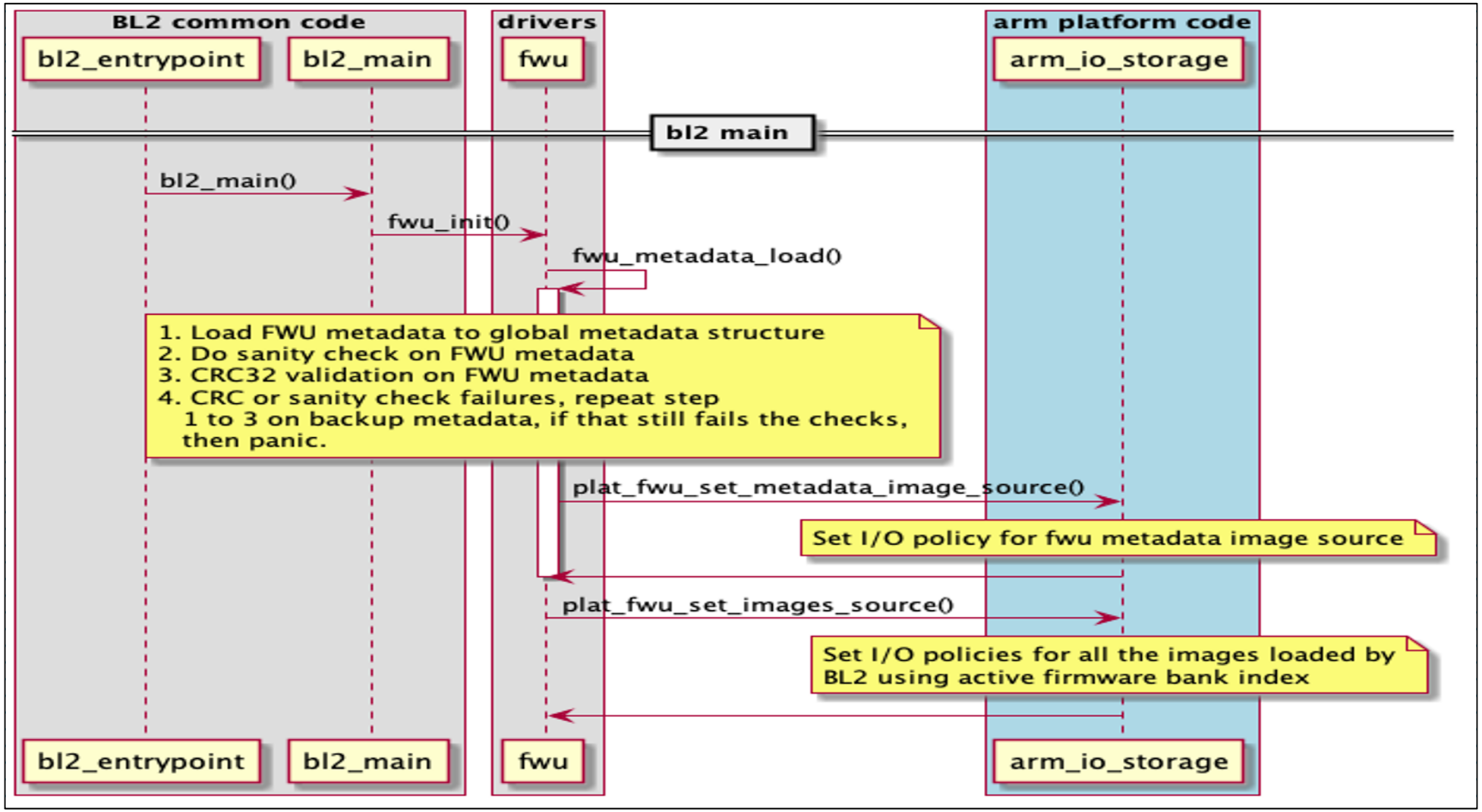
- fwu_discover
- fwu_begin_staging
- fwu_end_staging
- fwu_cancel_staging
- fwu_open
- fwu_write_stream
- fwu_read_stream
- fwu_commit
- fwu_accept_image
- fwu_select_previous



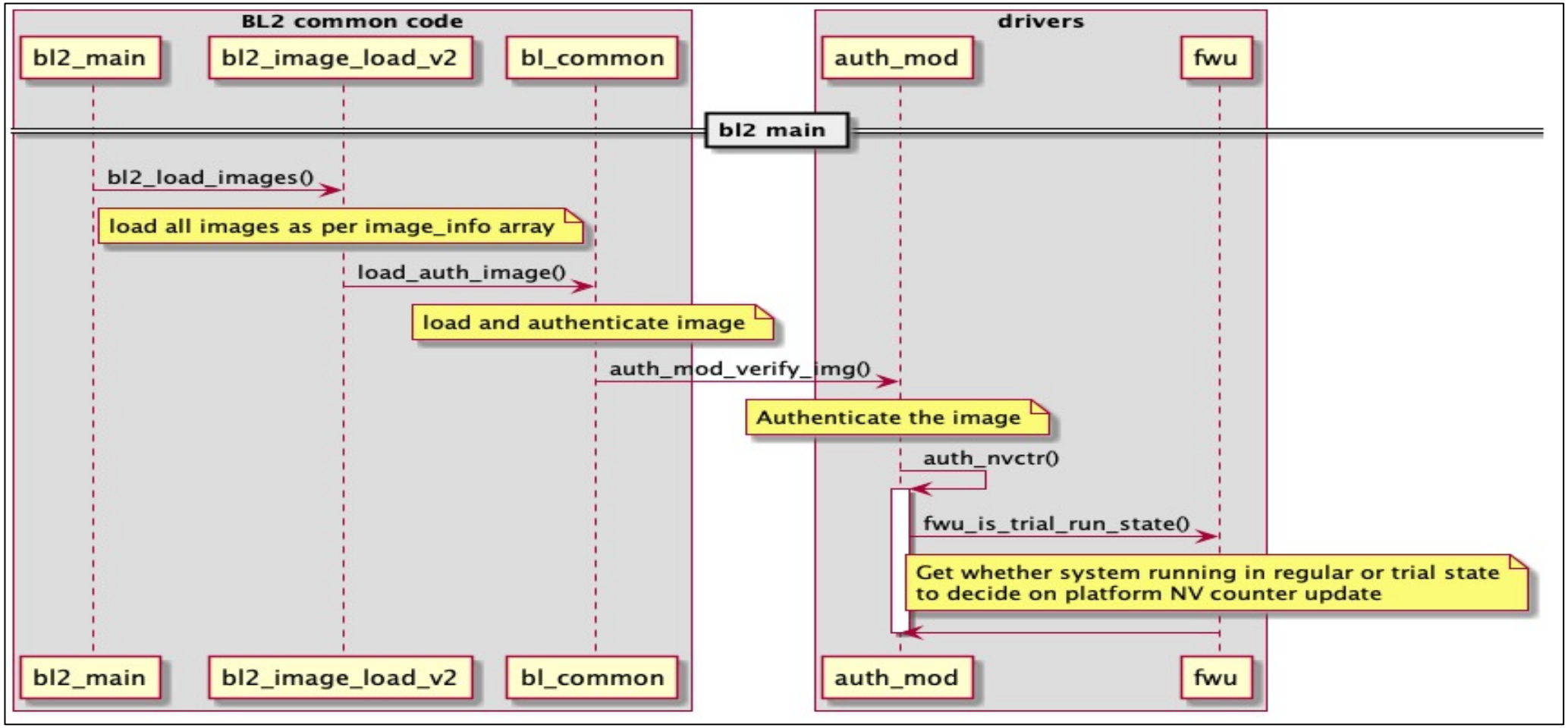
TF-A BL2 involvement in Firmware update

- GPT parser support enablement
- Hardware and Software CRC32 support
- Loading and parsing of Firmware update metadata
- Select the updatable images in non-volatile storage by reading active index (as a part of metadata)
- Avoid NV-counter update in trial run state

Boot Flow 1/2 - BL2 Execution



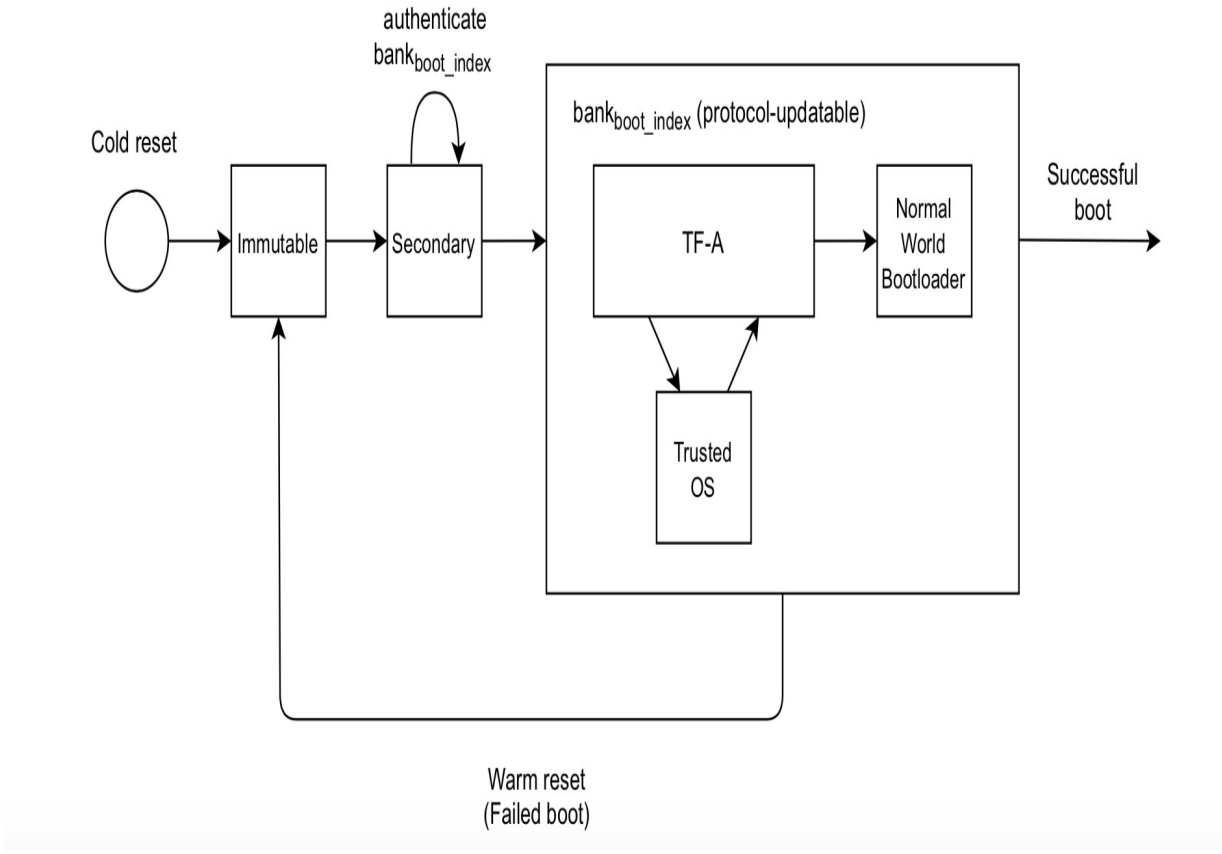
Boot Flow 2/2 – Trial run detection



Firmware bank boot index decision

Each boot_index assignment tried with max_failed_boots

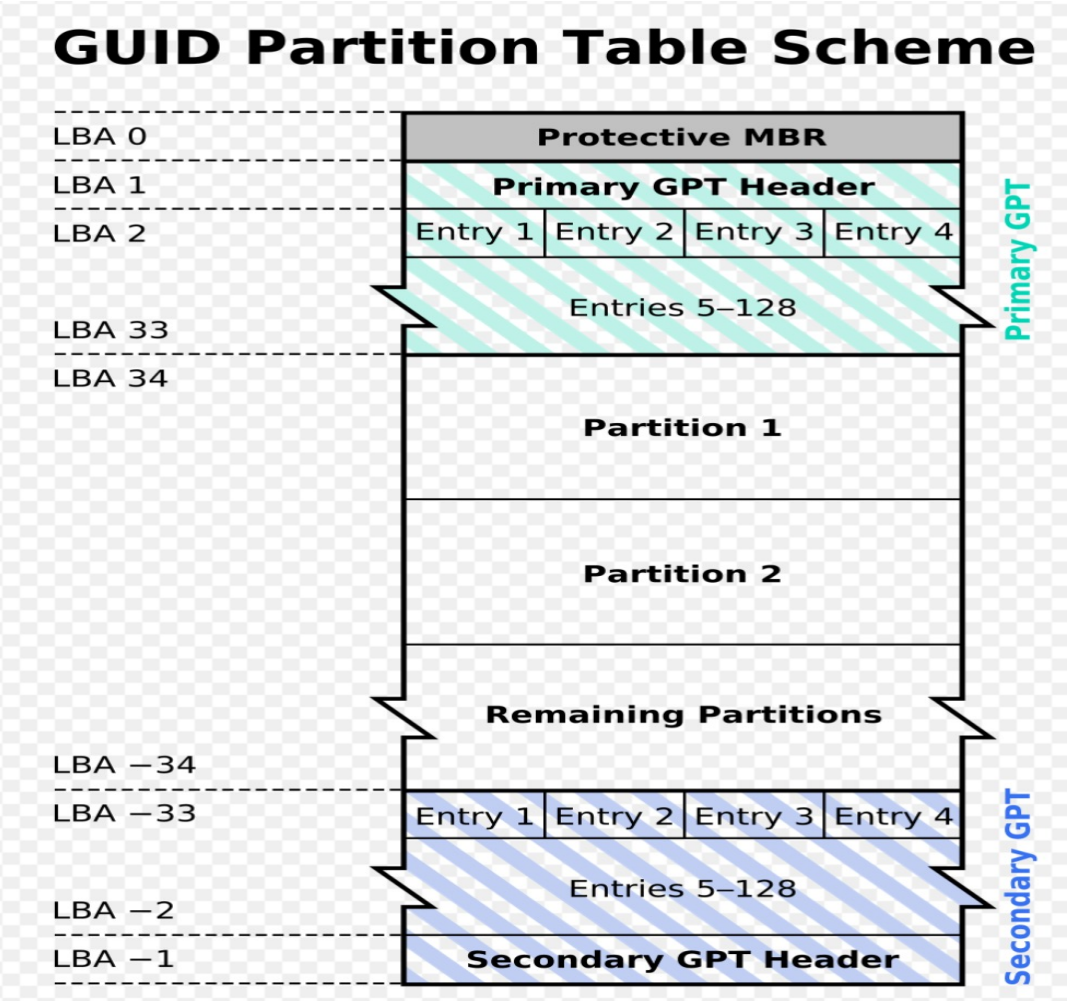
1. boot_index = active_index
2. boot_index = previous_active_index
   if,
   active_index != previous_active_index,
   otherwise step 3
3. boot_index = <recovery bank index>
   [IMP defined]
4. Propogate boot index to update agent using platform defined way



Verification

- Manually created GPT image with two FIP and two FWU metadata images
- Created sample FWU metadata binary to check various flow in the code using FVP model
  - loading of partition table
  - loading of metadata in SRAM
  - CRC32 calculation and verification of metadata
  - regular state vs trial state
  - select FIP A vs FIP B
  - avoid NV counter update in trial run state
- Patches are posted externally for review:
  - https://review.trustedfirmware.org/q/topic:%22fw-update-2%22+(status:open%20OR%20status:merged)

GPT format image




```
manishbadarkhe@manishbadarkhe-VirtualBox:~/.../trusted-firmware-a$ gdisk -l sample-fwu-gpt.img
GPT fdisk (gdisk) version 1.0.4

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
Disk sample-fwu-gpt.img: 2048 sectors, 1024.0 KiB
Sector size (logical): 512 bytes
Disk identifier (GUID): 85A7AAE8-DF95-44A8-AA89-F8DB67842AC2
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 2014
Partitions will be aligned on 2-sector boundaries
Total free space is 361 sectors (180.5 KiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1              34             833   400.0 KiB   8300  FIP_A
   2             834            1633   400.0 KiB   8300  FIP_B
   3            1634            1643   5.0 KiB     8300  FWU-Metadata
   4            1644            1653   5.0 KiB     8300  Bkup-FWU-Metadata
```

Prototype – Flash in secure side

- This is currently tested on QEMU platform, with u-boot and running StMM on top of OPTEE
- Driver is implemented in StMM to flash the images in secure flash

Ongoing tasks

- Boot index decision - Max boot retry with active FIP, switch back to previous active FIP
- Arm platform – Recovery flow implementation
- Integrate TF-A patch work with a total compute platform stack to exercise full firmware update flow

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