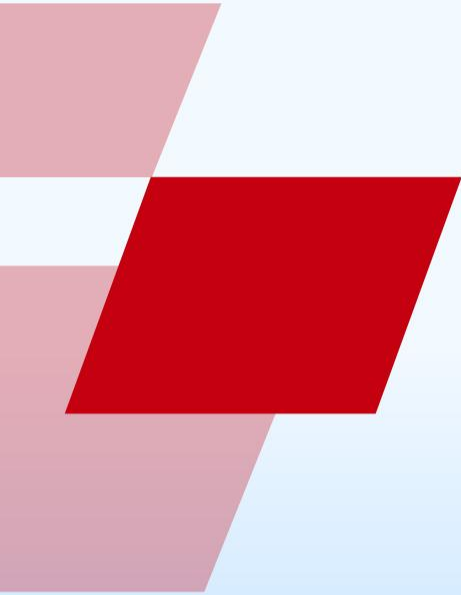




ASPEED Caliptra 2.1 Subsystem Integration on AST1040

End-to-end I3C streaming boot, proven on real silicon | AST1040 target + AST2700 BMC host |
Caliptra Workshop · Aug 10, 2026

ASPEED integration, proven on real silicon

01

Real silicon

Caliptra 2.1 SS runs on the actual
AST1040 chip — not a model or
FPGA.
Proven live today

02

End-to-end boot

AST2700 BMC streams the full boot
path to AST1040 over I3C — host to
Zephyr shell.
One continuous demo

03

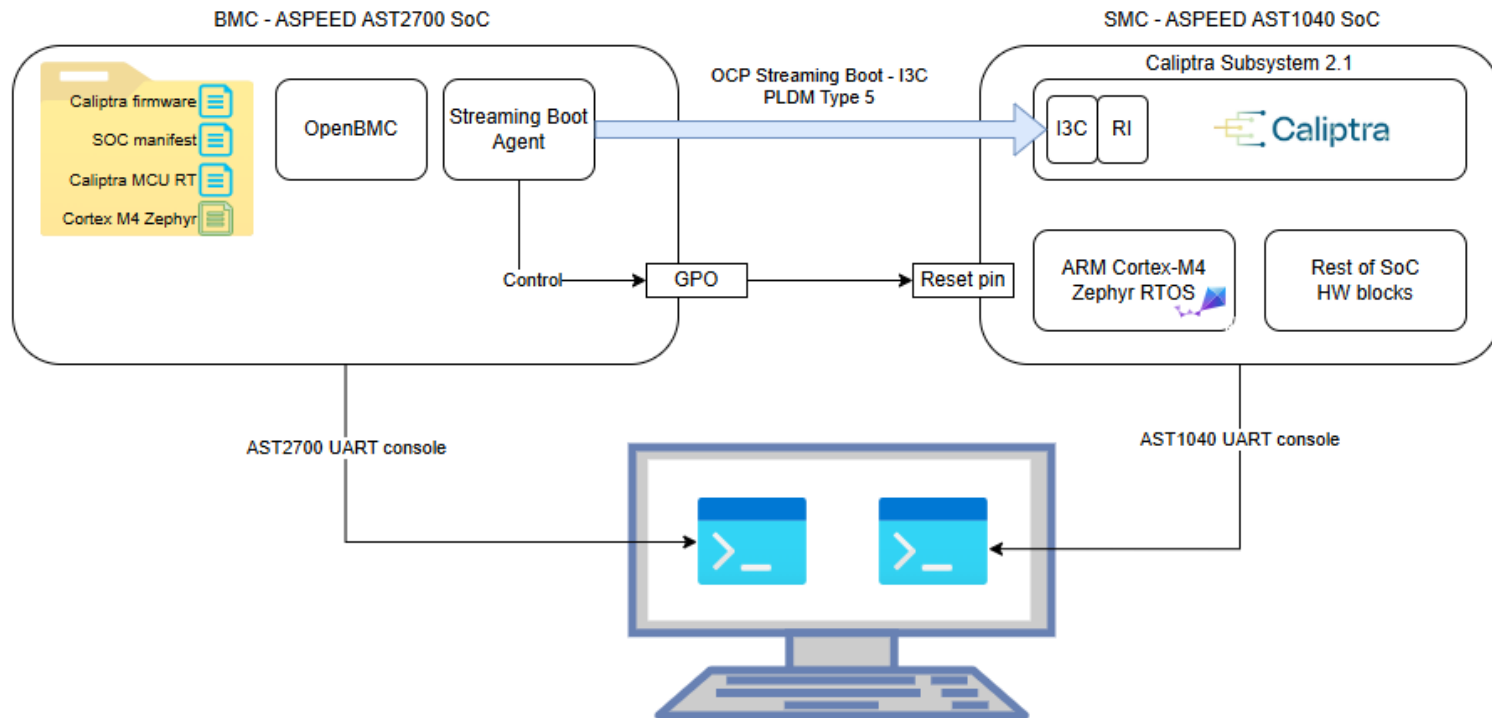
ASPEED integration

I3C recovery target, runtime PLDM
transport, and SoC boot handoff
around Caliptra.
Focus of this talk

Generic Caliptra SS boot & RT FW stack were covered in the earlier session — here we focus on the ASPEED integration and its live proof.

Top-level view: what ASPEED built, and the on-hardware evidence that it works end to end.

Demo setup connects AST2700 host to AST1040 target



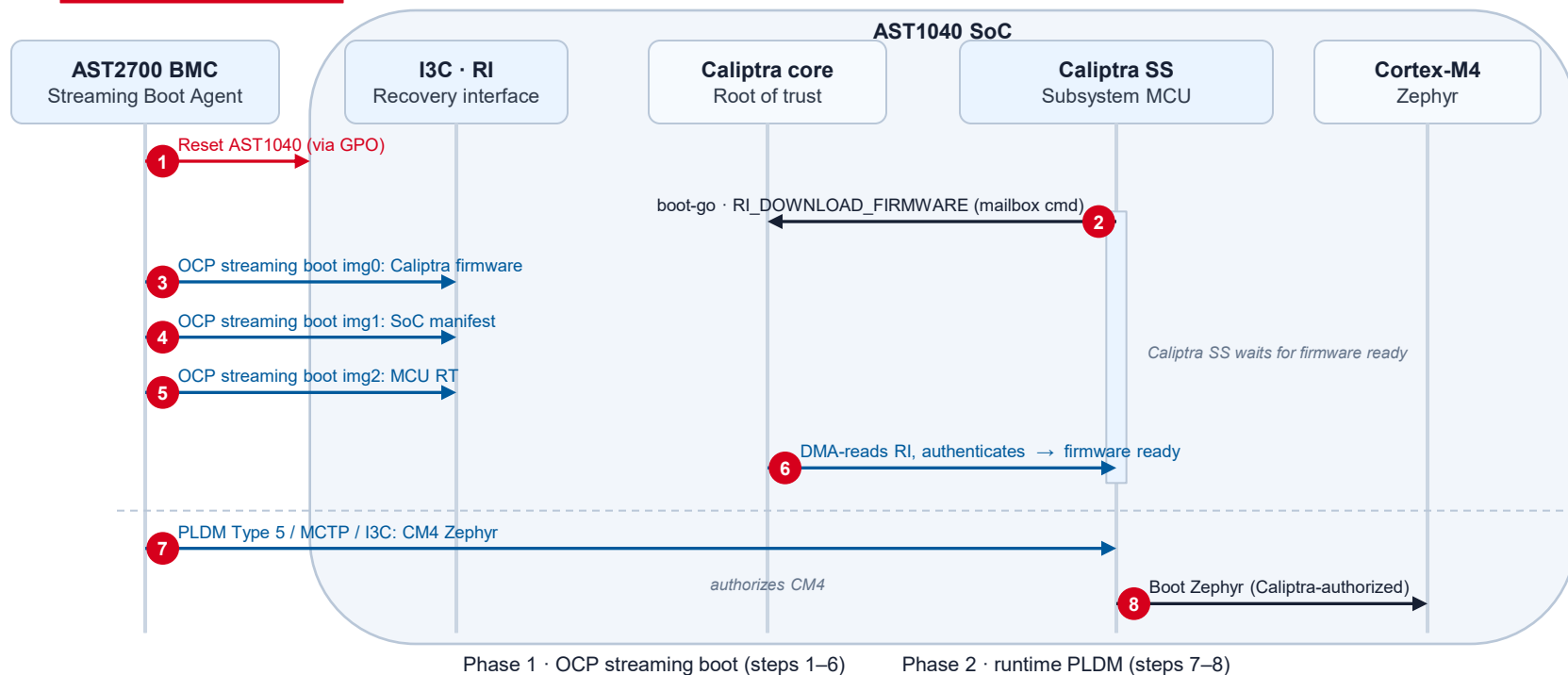
AST1040 proves four boot-critical integration points

Integration point	Path exercised in the demo	Observable evidence
1 Native I3C recovery endpoint	AST2700 streams Caliptra FW, SoC manifest, and MCU RT over OCP streaming boot / I3C.	Host log: 3 FIFO transfers (182 / 34 / 248 KB)
2 ROM to runtime chain	MCU ROM initializes I3C, reaches mailbox readiness, downloads firmware, then jumps to MCU RT.	Target log: ROM -> MCU RT
3 Mailbox and authorization	Caliptra accepts mailbox commands and authorizes the Cortex-M4 image before boot.	Target log: authorization complete
4 Runtime SoC handoff	PLDM Type 5 over MCTP / I3C delivers the Cortex-M4 Zephyr image and starts the CM4 boot path.	UART: zephyr~\$

Topology, boot sequence, and live evidence for each checkpoint follow.

BOOT SEQUENCE

Streaming boot flows through the I3C recovery interface



Two-phase delivery: OCP streaming boot, then runtime PLDM

PHASE 1 — OCP STREAMING BOOT · three boot images streamed over I3C

0x0

Caliptra firmware

Initial Caliptra FW payload streamed
by AST2700.

182 KB · firmware ready

0x1

SoC manifest

Image metadata and trust inputs for
authorization.

34 KB · manifest accepted

0x2

Caliptra MCU RT

Runtime that starts the post-boot
service path.

248 KB · MCU RT running

PHASE 2 — RUNTIME PLDM

Phase 2 — PLDM Type 5 / MCTP over I3C: the BMC delivers the Cortex-M4 Zephyr image (~880 KB); Caliptra authorizes it before CM4 boot.

Streaming boot stages the trust base; PLDM then delivers and authorizes the application image — over the same I3C link.

See the streaming boot run end to end

```

date      : Date commands
demo      : Demo commands
device    : Device commands
devmem    : Read/write physical memory
           Usage:
             Read memory at address with optional width:
             devmem <address> [<width>]
             Write memory at address with mandatory width and value:
             devmem <address> <width> <value>
dynamic   : Demonstrate dynamic command usage.
flash     : Flash shell commands
gpio      : GPIO commands
help      : Prints the help message.
history   : Command history.
iic       : ASPEED IIC commands
kernel    : Kernel commands
log       : Commands for controlling logger
log_test  : Log test
md        : Mem Display command
mw        : Mem Write command
pect      : PECTI shell commands
pwm       : PWM shell commands
rem       : Ignore lines beginning with 'rem '
resize    : Console gets terminal screen size or assumes default in
           case the readout fails. It must be executed after each
           terminal width change to ensure correct text display.
retval    : Print return value of most recent command
section_cmd : Demo command using section for subcommand registration
sensor    : Sensor commands
shell     : Useful, not Unix-like shell commands.
shell_uart_release : Uninitialize shell instance and release uart, start
           loopback on uart. Shell instance is reinitialized when
           'x' is pressed
stats     : Stats commands
version   : Show kernel version
zephyr~$
ATL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Offline | ttyS13

2026-08-04T07:33:22.685Z INFO [pldm_ua:update_sm] Apply success
2026-08-04T07:33:22.737Z INFO [pldm_ua:update_sm] FD confirmed ReadyXfer after 52.344139ms (1 poll(s)), sending ActivateFirmware
2026-08-04T07:33:22.737Z INFO [pldm_ua:update_sm] Num components downloaded: 1
2026-08-04T07:33:22.737Z INFO [pldm_ua:update_sm] No activation needed
2026-08-04T07:33:22.738Z INFO [pldm_ua:update_sm] ActivateFirmware response success
2026-08-04T07:33:22.738Z INFO [pldm_ua:update_sm] ActivateFirmware response success, no activation needed
2026-08-04T07:33:22.738Z INFO [pldm_ua:update_sm] Stopping update
PLDM update completed
AST1040 firmware is loaded
root@ast2700-default:~#
[0] ~Minicom~ "minicom -c on -D /dev" 15:33 04-Aug-26

```

AST2700 host (bottom) drives AST1040 (top): reset → OCP streaming boot → PLDM → Zephyr, ~26 s at 8 MHz.

AST2700 host: recovery and PLDM delivery

AST2700-I3C_boot.txt — BMC host console (OpenBMC)

```
$ /bin/run_demo.sh
```

Reset AST1040

Send AST1040 firmware via I3C recovery interface

[INFO] Device /dev/i3c-mctp-7 is opened

[INFO] Sending via FIFO: caliptra-fw_align_256.bin (186112 bytes)

[INFO] Sending via FIFO: ast1040-...-auth-manifest.bin (34560 bytes)

[INFO] Sending via FIFO: ssmcu-runtime_align_256.bin (253952 bytes)

[INFO] set-eid --dest-eid 0 0x08 -> Target endpoint is now EID 0x08

Starting PLDM update: src EID=0x09, FD EID=0x08

[pldm_ua::update_sm] Transferred 1024 / 901496 bytes ...

[pldm_ua::update_sm] ... streaming ~880 KB over I3C ...

[pldm_ua::update_sm] Transfer complete success

[pldm_ua::update_sm] Verify success

[pldm_ua::update_sm] Apply success

PLDM update completed

AST1040 firmware is loaded

I3C SCL at 8 MHz (max 12.5) on purpose — each phase transition stays visible.

AST1040 target: ROM to Zephyr shell

```
AST1040-I3C_boot.txt — Caliptra subsystem UART

[mcu-rom] Hello from ROM
[mcu-rom] Cold boot detected
[mcu-rom] Initializing I3C
[mcu-rom] Caliptra is ready for mailbox commands
[mcu-rom] Sending RI_DOWNLOAD_FIRMWARE command
[mcu-rom] Firmware is ready
[mcu-rom] Jumping to firmware
[mcu-runtime-i3c] Enabling I3C interrupts
MUX MCTP enable
MCU initialization complete.
[ast1040-pldm] booting CM4 image 0x100e via PLDM
[pldm-client] image download complete
[pldm-loader] Caliptra authorization complete
[bootdev] IMAGE_INITIAL(image_id=0x100e)
<inf> app: Welcome to ASPEED
zephyr~$
```

Target reaches the Zephyr shell — the Caliptra-authorized CM4 image booted.



**AST1040 is ready for Caliptra 2.1 integration —
the end-to-end I3C streaming boot path is proven on real silicon.**

Next: align on customer integration requirements and production boot-flow.
OBMF firmware-stack architecture follows after the break.