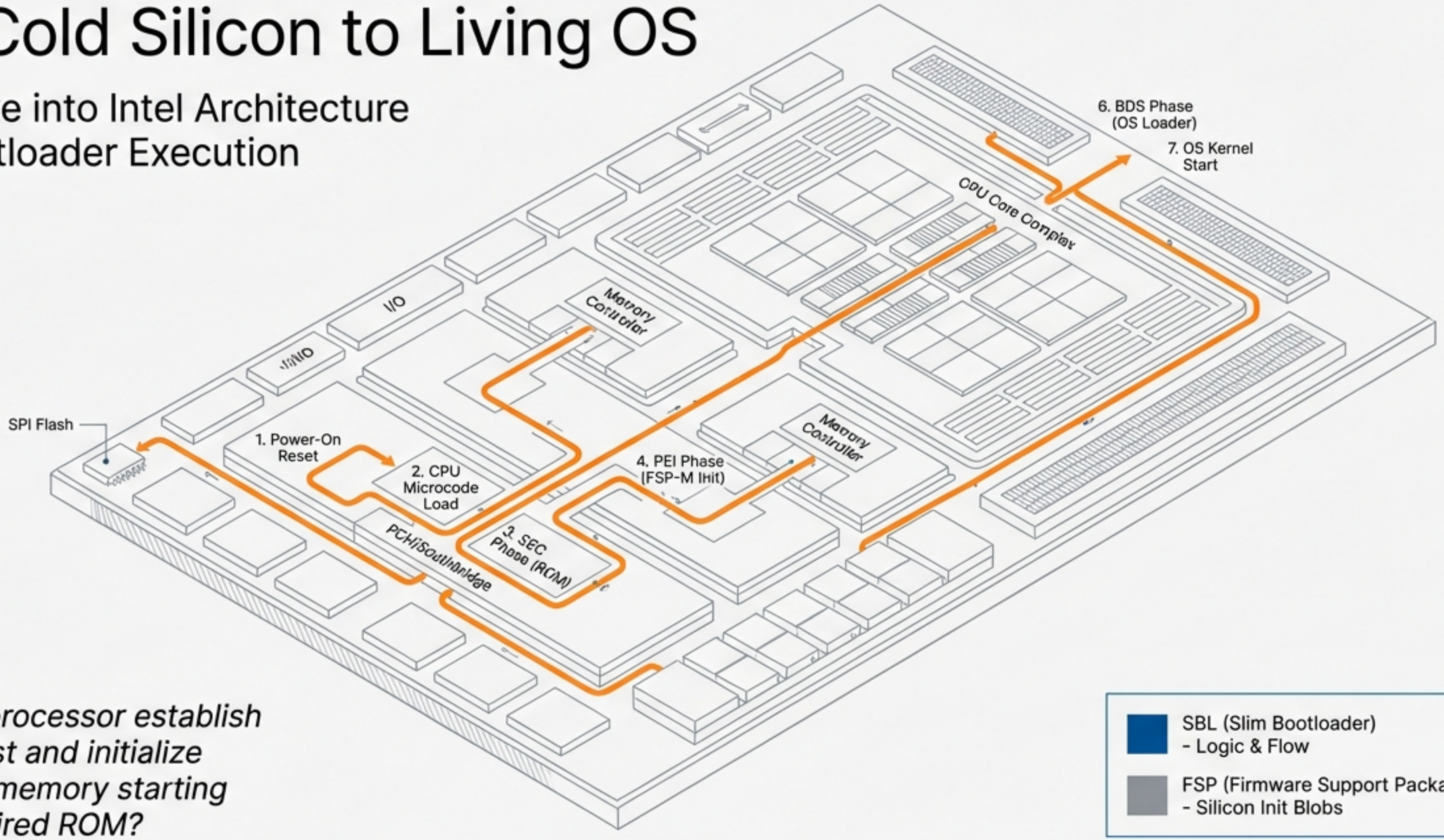
Arrow Lake Boot Flow: From Cold Silicon to Living OS

A Deep Dive into Intel Architecture & Slim Bootloader Execution

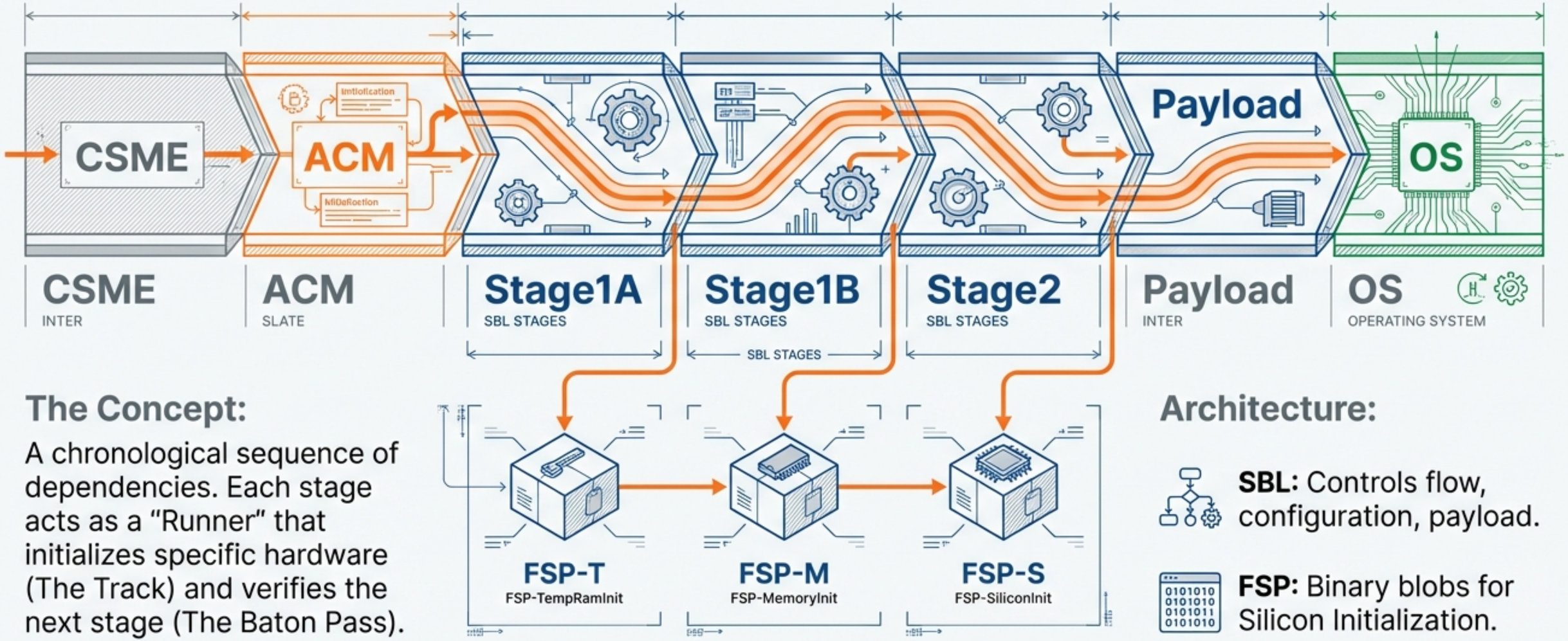


How does a processor establish a Root of Trust and initialize gigabytes of memory starting from a hardwired ROM?

SBL (Slim Bootloader)
- Logic & Flow

FSP (Firmware Support Package)
- Silicon Init Blobs

The Relay Race of Trust and Resources



The Concept:

A chronological sequence of dependencies. Each stage acts as a "Runner" that initializes specific hardware (The Track) and verifies the next stage (The Baton Pass).

Architecture:

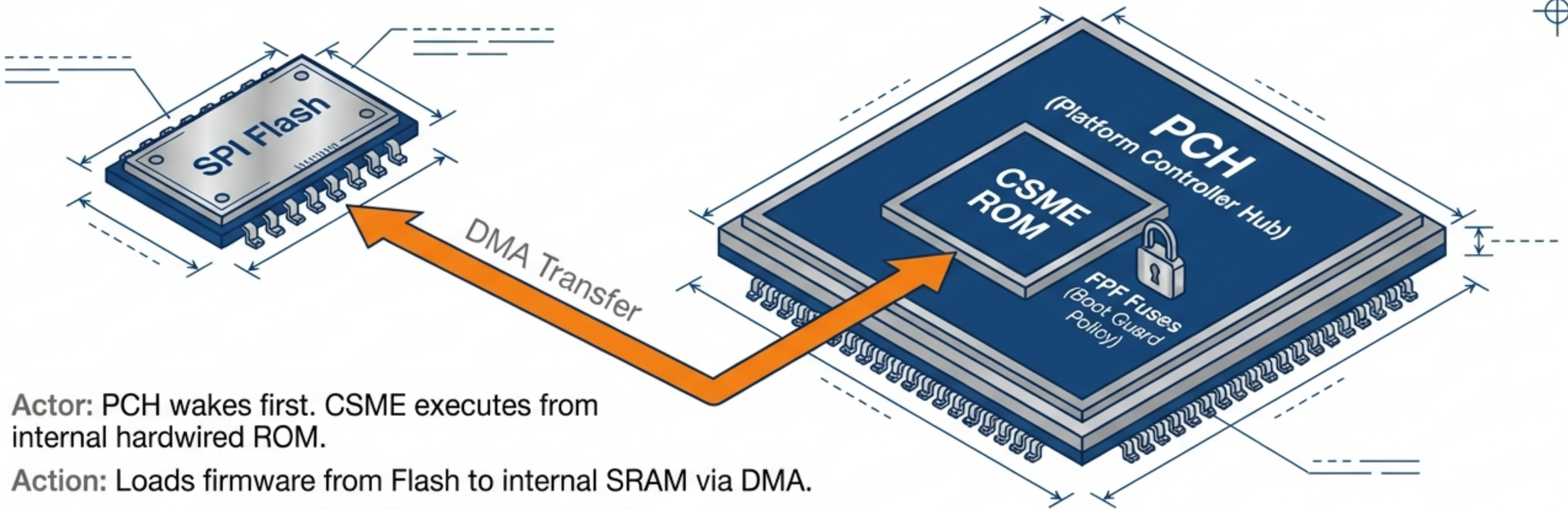
SBL: Controls flow, configuration, payload.

FSP: Binary blobs for Silicon Initialization.

The Spark: CSME and the Starter Motor

CSME > ACM > Stage1A > Stage1B > Stage2 > Payload > OS

State Box
CPU State: Reset (Asleep)
Memory: SRAM (PCH Internal)



- **Actor:** PCH wakes first. CSME executes from internal hardwired ROM.
- **Action:** Loads firmware from Flash to internal SRAM via DMA.
- **Critical Dependency:** PMC Patch. Mandatory firmware patch for Power Management Controller.
- **Role:** CSME is the gatekeeper. It prepares the environment but does NOT cryptographically validate the Key Manifest.

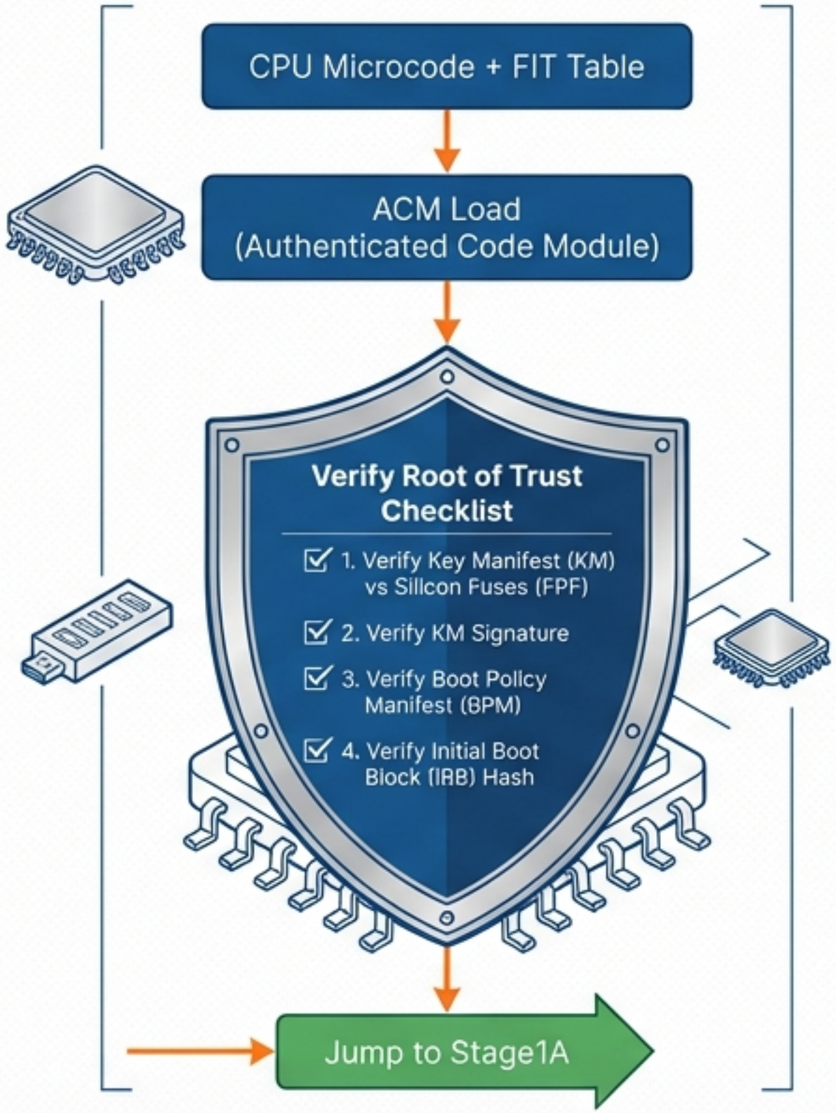
Establishing the Root of Trust

CSME > **ACM** > Stage1A > Stage1B > Stage2 > Payload > OS

State Box

CPU State: 32-bit (Microcode)
Memory: ACRAM (L3 Cache Isolated)

ACRAM is isolated.
No DMA allowed.
No external snooping.



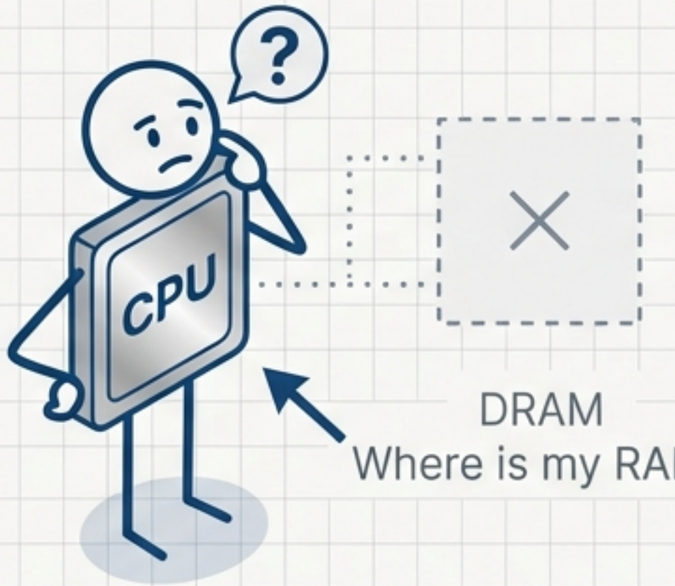
Entering Protected Mode without DRAM

CSME → ACM → **Stage1A** → Stage1B → Stage2 → Payload → OS

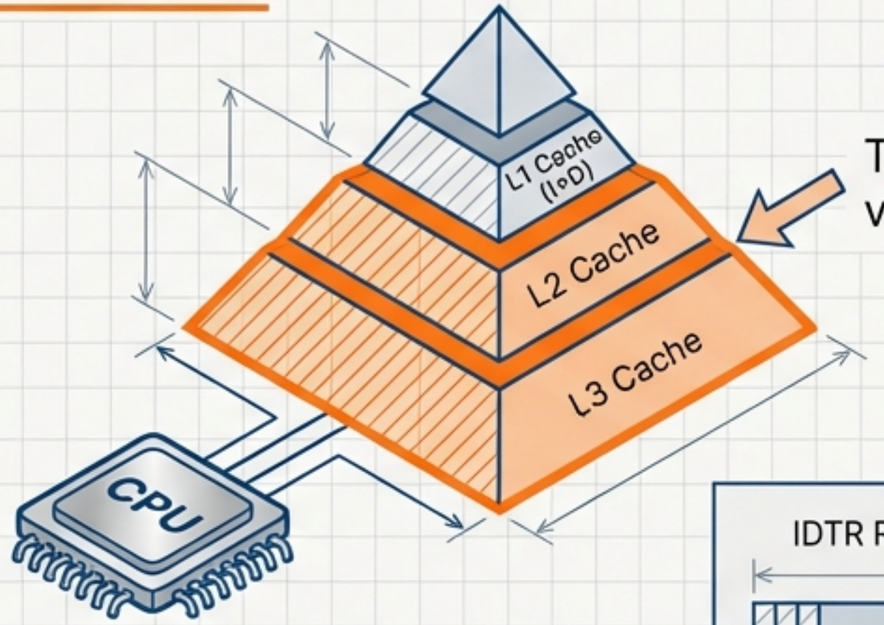
State Box

CPU State: `Real → 32-bit Protected`
Memory: `Cache-as-RAM (CAR)`

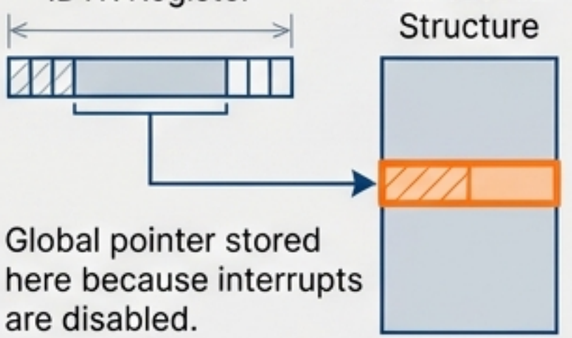
The Problem



The Solution



Temporary RAM (CAR) via `FspTempRamInit`

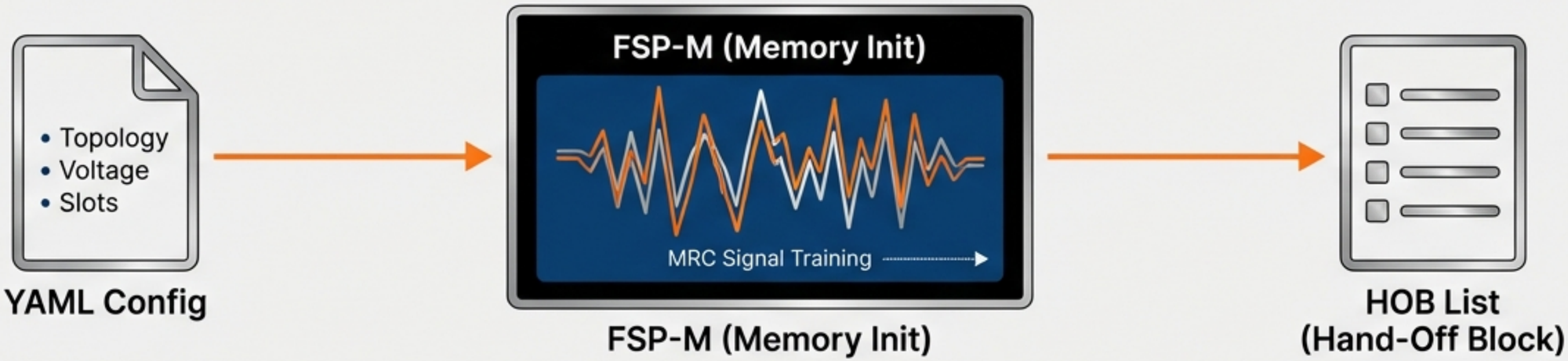


- **Transition:** Loads GDT to switch to 32-bit Protected Mode.
- **FSP-T Action:** Initializes Cache-as-RAM to provide temporary stack and heap.
- **Handoff:** Verifies Stage1B and packages `Stage1A_PARAM`.

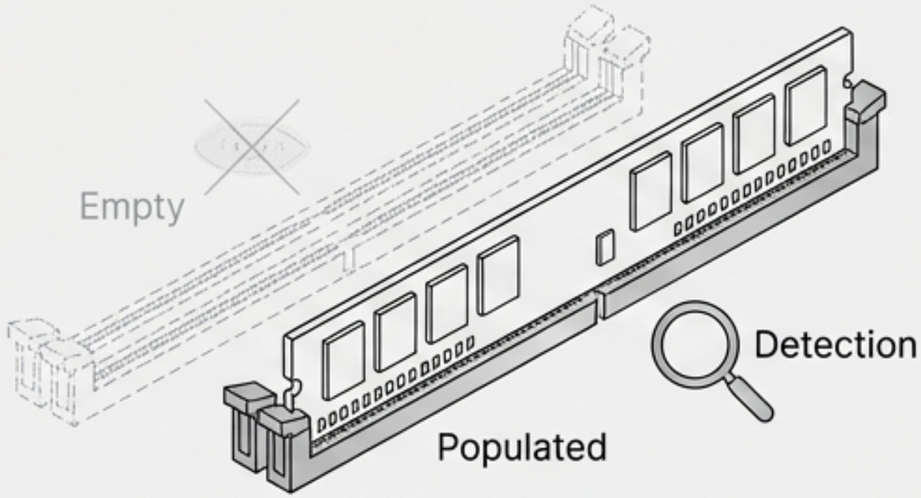
Waking the Memory: FSP-M and DDR Training

CSME > ACM > Stage1A > **Stage1B** > Stage2 > Payload > OS

State Box
CPU State: 32-bit Protected
Action: DDR Training (MRC)



- Input: Board-specific YAML populates FSP-M UPD.
- Execution: Memory Reference Code (MRC) runs silicon-validated training sequences.
- Result: Discovery of actual physical memory and creation of the HOB List map.

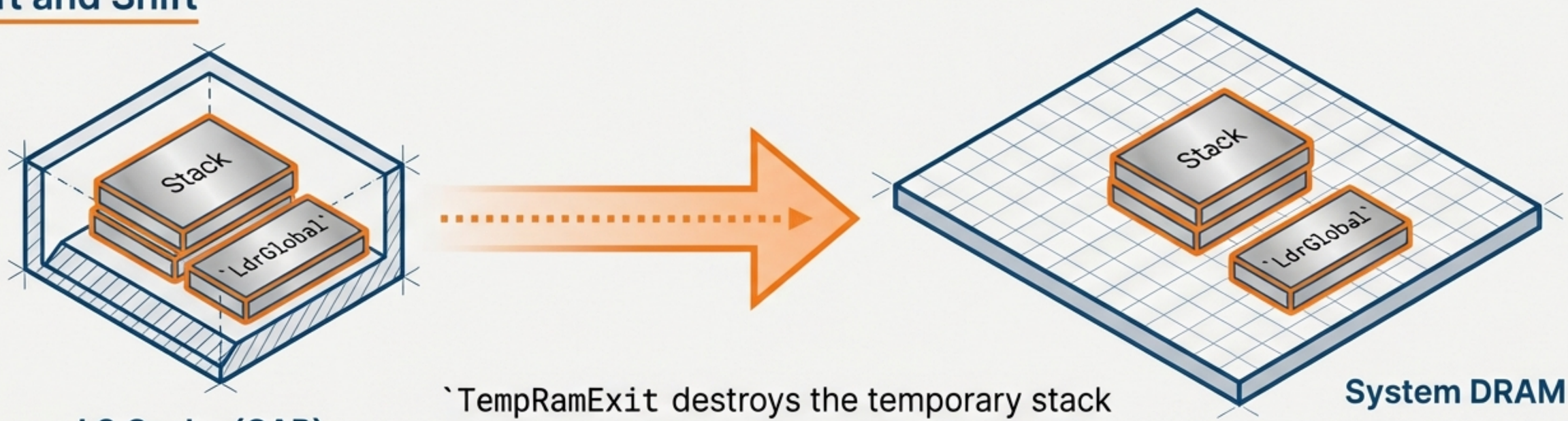


The Great Migration: Leaving Cache-as-RAM

CSME | ACM | Stage1A | **Stage1B** | Stage2 | Payload | OS

State Box
Transition: CAR → DRAM
Action: Stack Migration

Lift and Shift



L3 Cache (CAR)

`TempRamExit` destroys the temporary stack and returns the cache to normal coherency.

System DRAM

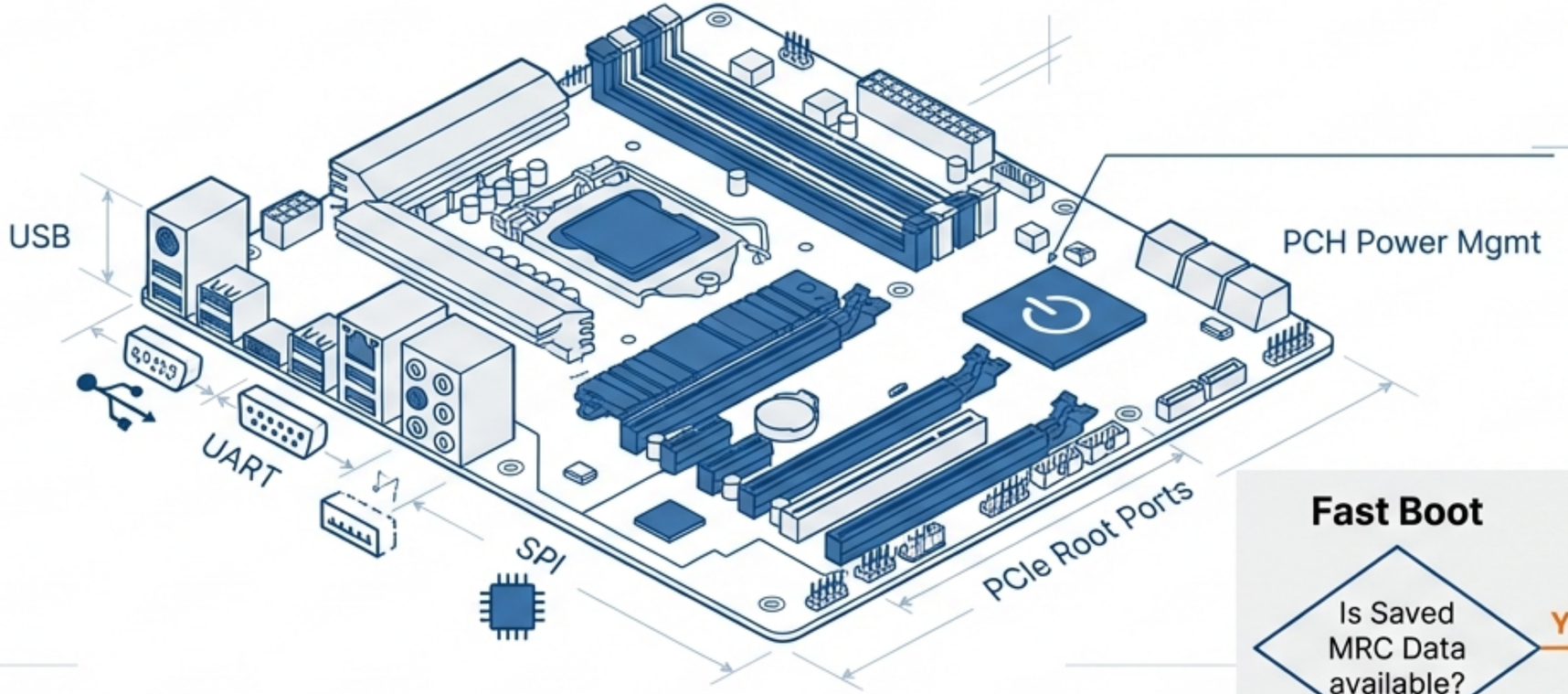
Copy Data → Update Boundaries (TOLUM/TOUUM) → Call `TempRamExit` (Clean up Cache) → Jump to Stage2

Silicon Initialization & Fast Boot

CSME > ACM > Stage1A > Stage1B > **Stage2** > Payload > OS

State Box

Memory: DRAM (Unshadowed)
Function: FSP-S (Silicon Init)



Unshadowing: Firmware runs from fast DRAM, not slow Flash.
S3 Resume: Uses saved HOB data to accelerate boot.
Action: Calls `FspSiliconInit` to configure PCH and IO.

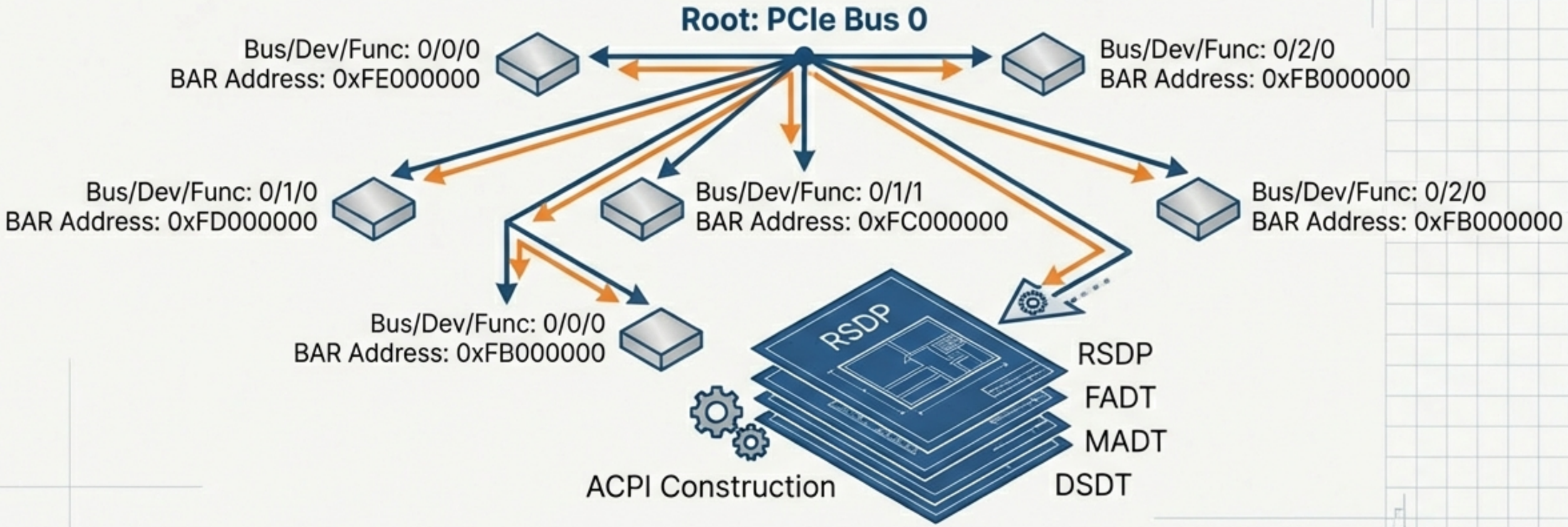
Fast Boot

Enumeration and ACPI Generation

State Box

CPU: Multi-Core Active
Task: Mapping the Platform

CSME > ACM > Stage1A > Stage1B > **Stage2** > Payload > OS



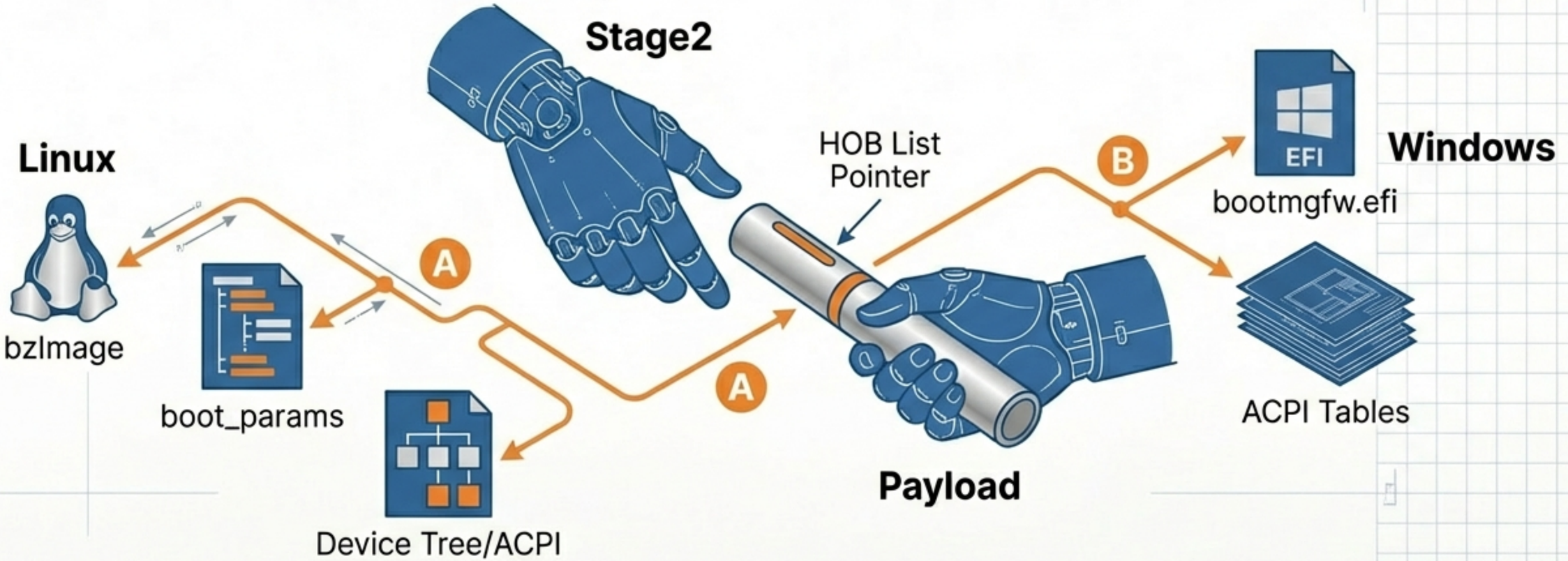
Multi-Processor Init: Waking up Application Processors (APs).
PCIe Enumeration: assigning Base Address Registers (BARs).
ACPI Construction: Building the 'Atlas' for the OS dynamically based on HOBs.
Security: Signal `EndOfFirmware` to lock TPM and clear secrets.

The Handoff: Loading the Payload

State Box

Context: Firmware -> Software
Data: `STAGE2_PARAM`

CSME > ACM > Stage1A > Stage1B > Stage2 > **Payload** > OS



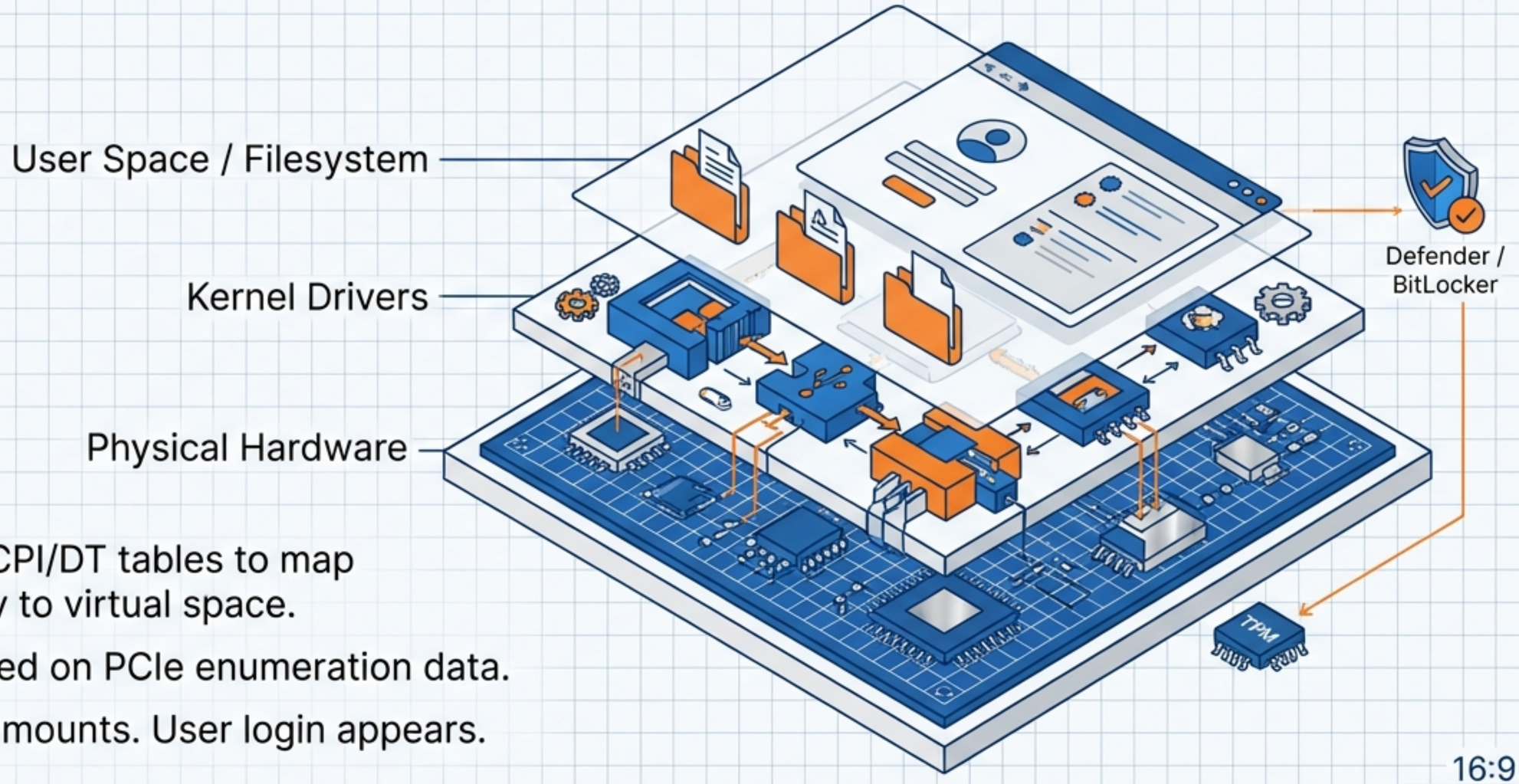
- The **Payload** acts as the bridge between firmware logic and the OS kernel.
- **Crucial Data:** The HOB List contains the hardware map the OS cannot generate itself.

Full System Control: OS Runtime

CSME > ACM > Stage1A > Stage1B > Stage2 > Payload > **OS**

State Box

`CPU:` Long Mode (64-bit)
`Memory:` Virtualized / Paged

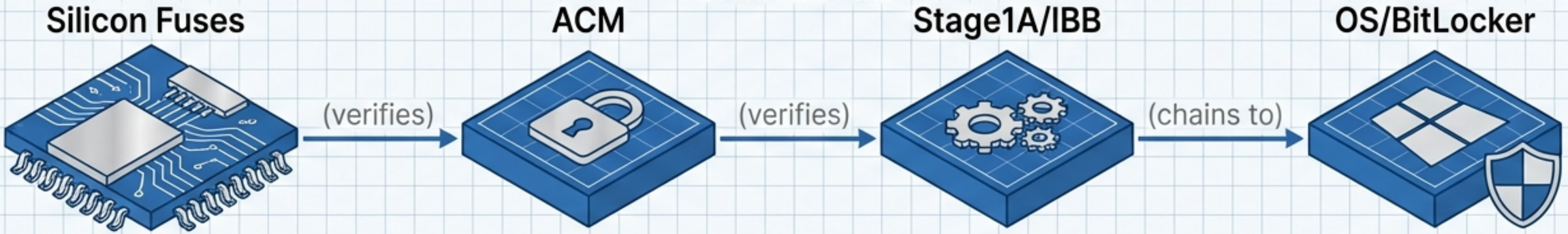


- Kernel parses ACPI/DT tables to map physical memory to virtual space.
- Drivers load based on PCIe enumeration data.
- Root Filesystem mounts. User login appears.

16:9

Summary & Reference

Trust Chain



Glossary Grid

Term	Definition	Term	Definition
CSME	Converged Security & Management Engine.	**HOB**	Hand-Off Block (Resource Descriptor).
ACM	Authenticated Code Module.	**UPD**	User Product Data (Config Input).
FSP	Firmware Support Package (Silicon Binaries).	**MRC**	Memory Reference Code (DDR Training).

Modern booting is a precise balance of rigid security (Boot Guard) and flexible configuration (FSP), ensuring the system is trustworthy before the user ever sees a logo.

16:9