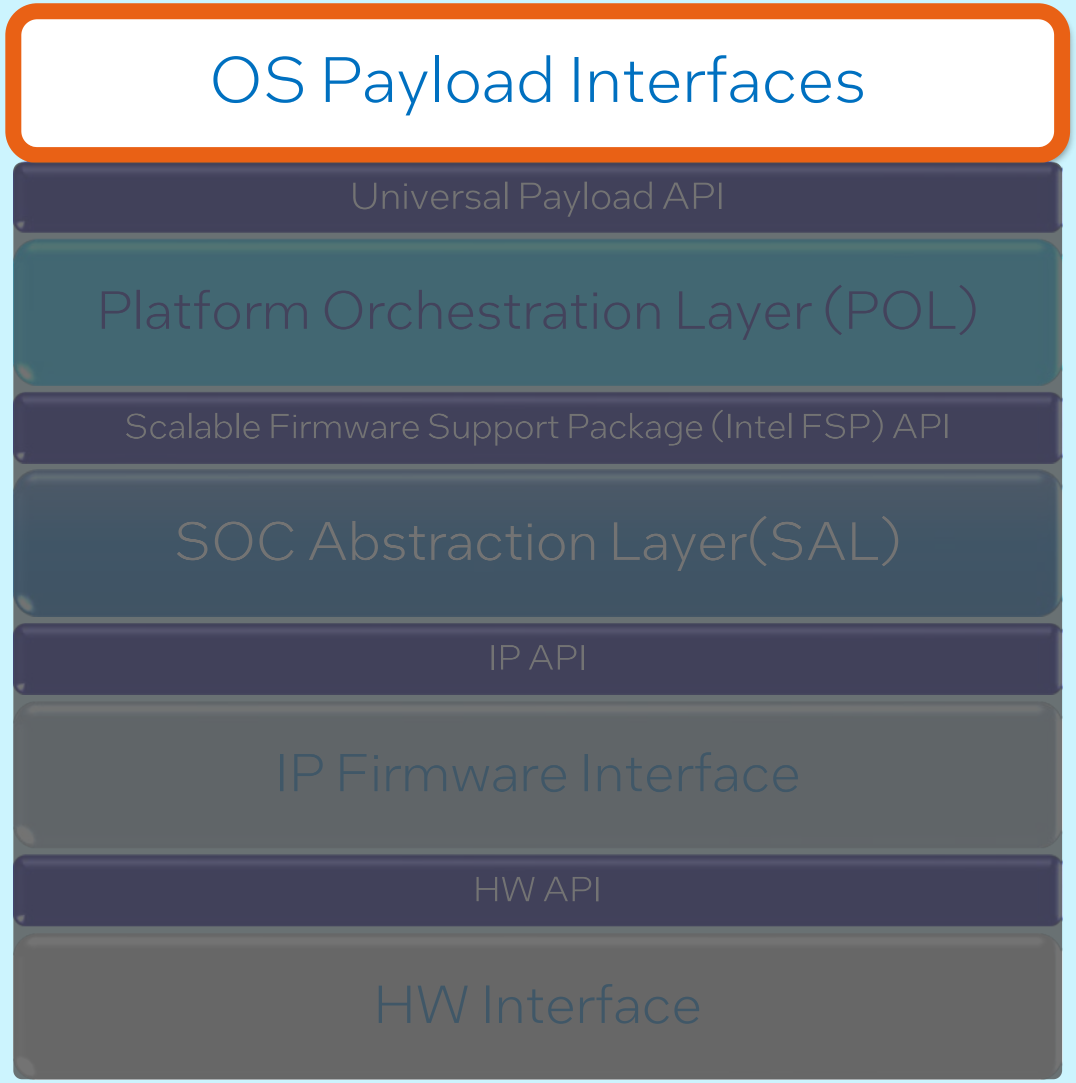
System Firmware Training

Universal Scalable Firmware (USF) :

Operating System Interfaces

Intel Corporation



OS Payload Interfaces

Universal Payload API

Platform Orchestration Layer (POL)

Scalable Firmware Support Package (Intel FSP) API

SOC Abstraction Layer(SAL)

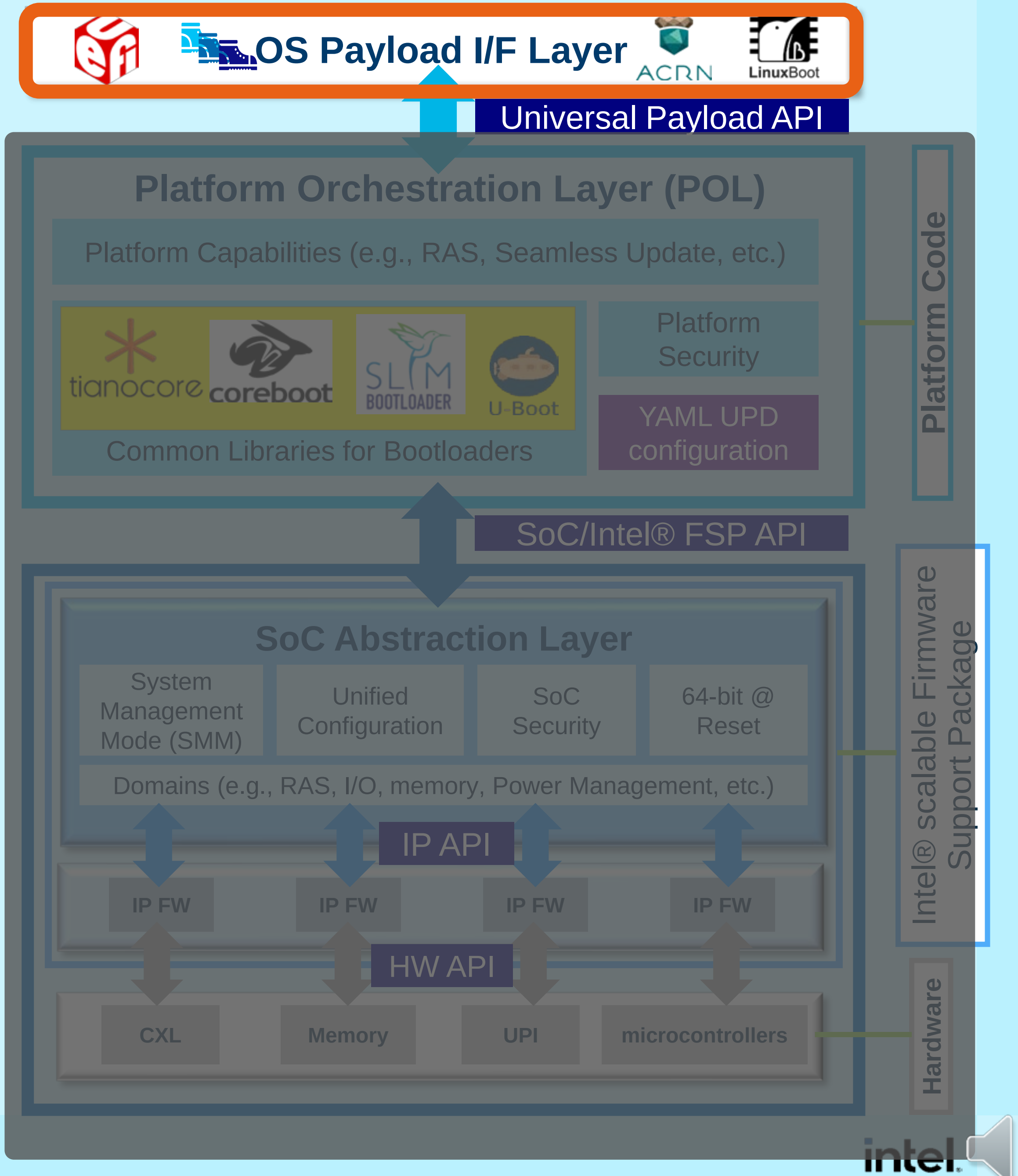
IP API

IP Firmware Interface

HW API

HW Interface

OS Handoff



OS Payload I/F Layer

Universal Payload API

Platform Orchestration Layer (POL)

Platform Capabilities (e.g., RAS, Seamless Update, etc.)

Common Libraries for Bootloaders

Platform Security

YAML UPD configuration

Platform Code

SoC/Intel® FSP API

SoC Abstraction Layer

System Management Mode (SMM)

Unified Configuration

SoC Security

64-bit @ Reset

Domains (e.g., RAS, I/O, memory, Power Management, etc.)

IP API

IP FW

IP FW

IP FW

IP FW

HW API

CXL

Memory

UPI

microcontrollers

Intel® scalable Firmware Support Package

Hardware

OS Interfaces – OS Boot Protocols

Unified Extensible Firmware Interface (UEFI)

- Runtime services to interface with the Platform firmware
- Includes data tables, configuration data, and variable services

Multiboot Protocol

- Open standard describing how a boot loader can load an Intel® Architecture operating system kernel.
- Allows different OS and Boot loaders working together without needing a specific boot loader

Linux Boot Protocol

- Linux kernel can itself be a bootable image without needing a separate OS loader
- Defines requirements to launch Linux kernel as a boot target

ACRN

- Flexible, lightweight reference hypervisor, built with real-time and safety criticality in mind
- Optimized to streamline embedded development through an open-source platform

OS Data Interfaces

Advanced Configuration and Power Interface (ACPI)

- Open standard that operating systems can use to discover and configure computer hardware components, to perform power management
  - Example, putting unused components to sleep, and to perform status monitoring.

System Management BIOS (SMBIOS)

https://www.dmtf.org/standards/smbios

Device Tree

- Data structure for describing hardware.
- Data structure with nodes that describe the devices in a system.
- Each node has property/value pairs that describe the characteristics of the device being represented.

https://www.devicetree.org

intel®