

System Firmware Training

Universal Scalable Firmware (USF): Overview

Intel Corporation



Universal Scalable Firmware (USF)

Intel's next-generation firmware initiative

 Simplify & scale firmware development from edge to cloud across all layers of the firmware stack

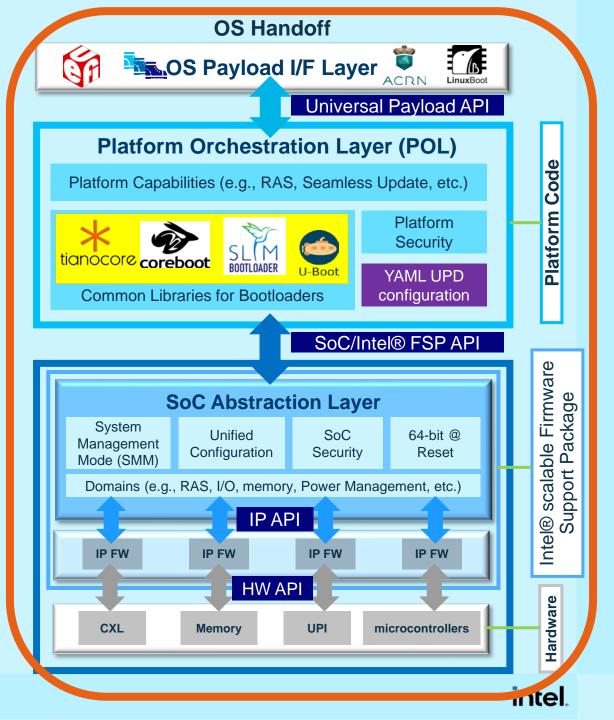
Silicon → IP Firmware → system-on-chip (SoC) Abstraction Layer → Platform Orchestration Layer → OS payloads interface

- Modular flexible architecture enables developers and technology partners to accelerate the integration of new silicon and platform technologies
- Results in efficiently deploying spectacular breakthrough products and solutions at scale.



Layers of Universal Scalable Firmware (LISE)

OS Payload Interfaces **Universal Payload API** Platform Orchestration Layer (POL) Scalable Intel® Firmware Support Package (Intel FSP) API SOC Abstraction Layer(SAL) IP API IP Firmware Interface **HW API HW** Interface





Universal Payload API

Platform Orchestration Layer (POL)

Scalable Intel® Firmware Support Package (Intel® FSP) API

SOC Abstraction Layer(SAL)

IP API

IP Firmware Interface

HW API

HW Interface









Universal Payload API

Platform Orchestration Layer (POL)

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



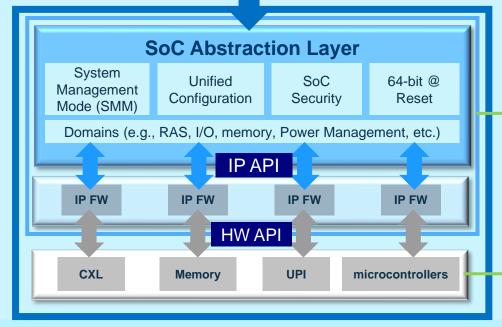
Security

Common Libraries for Bootloaders

YAML UPD configuration

Platform

SoC/Intel® FSP API



Intel® scalable Firmware Support Package

Platform Code

Hardware

Layers of Universal Scalable Firmware (USF)

OS Payload Interfaces

Universal Payload API

Platform Orchestration Layer (POL)

Scalable Intel® Firmware Support Package (Intel® FSP) API

SOC Abstraction Layer(SAL)

IP API

IP Firmware Interface

HW API

HW Interface









Universal Payload API

Platform Orchestration Layer (POL)

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

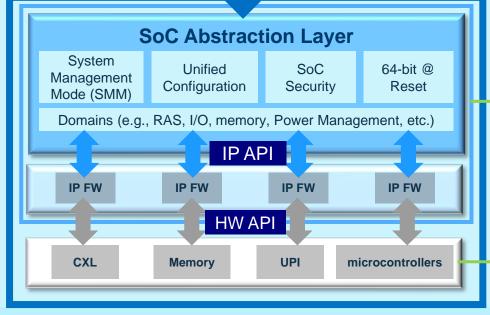


Platform Security

Common Libraries for Bootloaders

YAML UPD configuration

SoC/Intel® FSP API



Intel® scalable Firmware Support Package Hardware

Platform Code

Universal Payload API

Platform Orchestration Layer (POL)

Scalable Intel® Firmware Support Package (Intel® FSP) API

SOC Abstraction Layer(SAL)

IP API

IP Firmware Interface

HW API

HW Interface









Universal Payload API

Platform Orchestration Layer (POL)

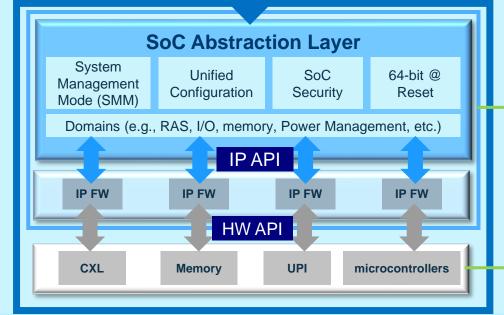
Platform Capabilities (e.g., RAS, Seamless Update, etc.)



Security

YAML UPD configuration

SoC/Inte ®FSP API



intel

Hardware

Platform Code

Intel® scalable Firmware Support Package

Universal Payload API

Platform Orchestration Layer (POL)

Scalable Intel® Firmware Support Package (Intel® FSP) API

SOC Abstraction Layer(SAL)

IP API

IP Firmware Interface

HW API

HW Interface









Universal Payload API

Platform Orchestration Layer (POL)

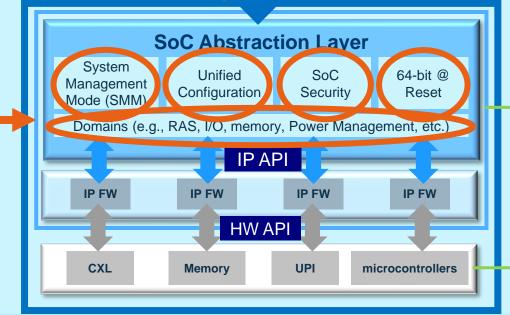
Platform Capabilities (e.g., RAS, Seamless Update, etc.)



Platform Security

YAML UPD configuration

SoC/Intel® FSP API



Intel® scalable Firmware Support Package Hardware

Platform Code

intel

Universal Payload API

Platform Orchestration Layer (POL)

Scalable Intel® Firmware Support Package (Intel® FSP) API

SOC Abstraction Layer(SAL)

IP API

IP Firmware Interface

HW API

HW Interface









Universal Payload API

Platform Orchestration Layer (POL)

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



Platform Security

YAML UPD configuration

SoC/Intel® FSP API



System Management Mode (SMM)

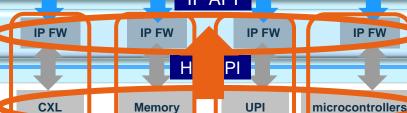
Unified Configuration

SoC Security

64-bit @ Reset

IP FW

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



Hardware

Intel® scalable Firmware Support Package

Platform Code

intel

