OPEN Compute Project | inspur | intel

OCP CHINA DAY | June 25th 2019 Beijing

Firmware Innovations Towards Cloud

Intel's Implementation for Open System Firmware

Song, Edmund | Software Architect

25th June, 2019

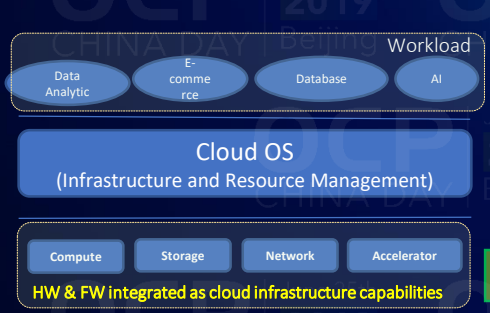
OCP CHINA DAY June 25th 2019 Beijing

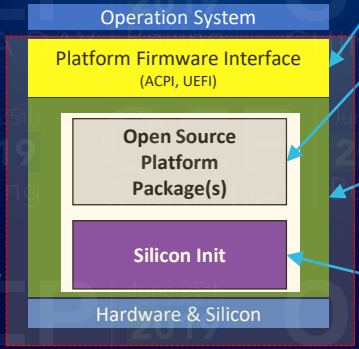
intel

CONTENTS

OCP CHINA DAY June 25th 2019 Beijing

UEFI Based Open System Firmware





Interfaces: Platform interface tables to support OS boot https://uefi.org

MinPlatform: Platform (board) Specific Code at https://github.com/tianocore/edk2-platforms

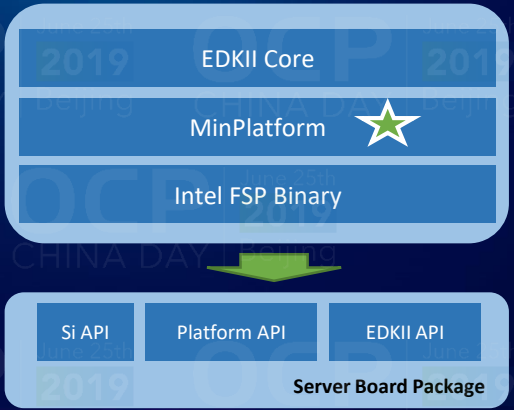
EDKII: Existing upstream/open source core at https://github.com/tianocore/edk2

Firmware Support Package: Intel binaries for board invariant Si code at https://github.com/intelfsp

Agile, Open and Standard Firmware Design Model to Support Cloud Requirements

MinPlatform

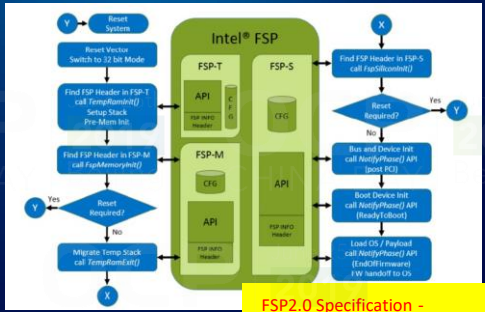
- Open source package with minimum set of platform code needed to realize server with white box configuration
- Offer buildable and bootable “white box” configuration using Intel® FSP
- Reduce volume of “closed source” needed to support Server products



OCP CHINA DAY June 25th 2019 Beijing

FSP (Firmware Support Package)

- Binary package to provide processor and chipset initialization easily be incorporated into industry boot loader framework (e.g. core boot, Tiano Core etc.)
- To abstract the complexity of silicon initialization and publicly distribute binaries of silicon code

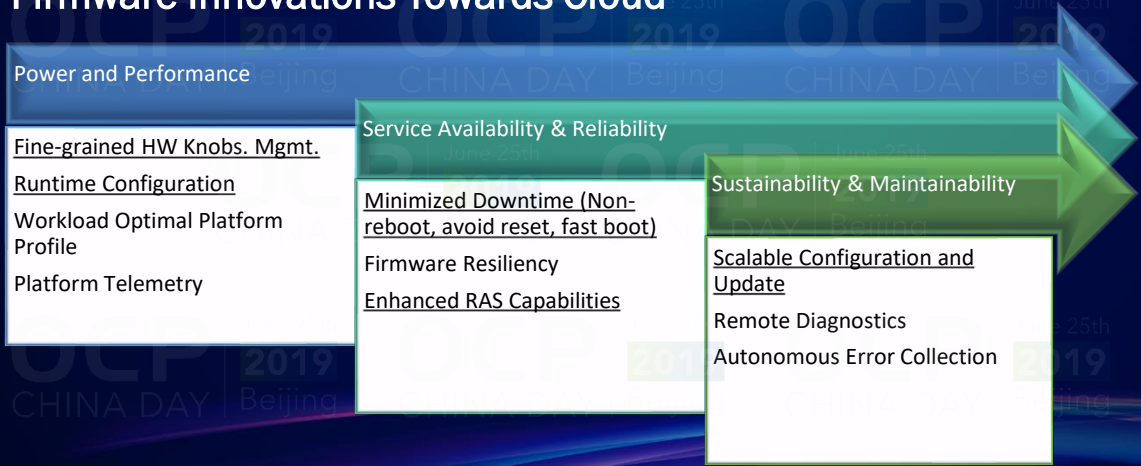


FSP2.0 Specification - https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp-architecture-spec-v2.pdf

Native Integration w/ UEFI

Coreboot integration scenario

Firmware Innovations Towards Cloud



OCP CHINA DAY June 25th 2019 Beijing

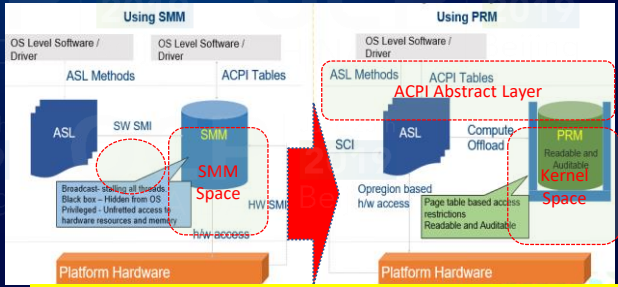
Platform Runtime Mechanism (PRM)

SMM (System Management Mode)

- Operating mode all threads/cores execution suspended
- SMM latency increase with more core count - implicated performance degradation
- Security concerns due to higher SMM privilege

PRM

- Enable firmware runtime functions in kernel space instead of SMM
- ACPI abstract layer to allow OS to invoke runtime code w/o awareness of platform specific details



PRM moving SW SMI (w/o SMM privilege) to kernel space

Sample PRM handler and ACPI Bridge Driver available in GitHub: https://github.com/tianocore/edk2-staging/tree/PRMCaseStudy

OCP CHINA DAY June 25th 2019 Beijing

intel

Boot Time Optimization

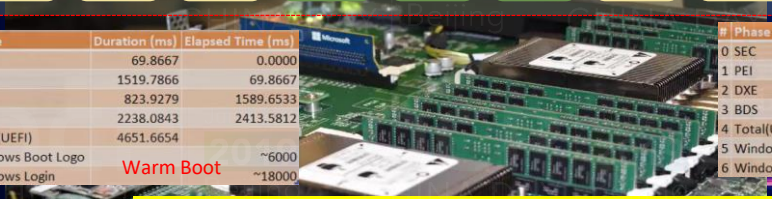
Boot Flow

Boot Time Optimization

ACM	SEC uCode Load CPU Init	UPI Discovery Setup	MRC Discovery Training ECC Init Memory Test Address Map	MP Init	Platform Init	PCIe Device Enum.	Publish Memory Map, ACPI SMBIOS	Option ROM	Boot Device Selection	OS Handoff

#	Phase	Duration (ms)	Elapsed Time (ms)
0	SEC	69.8667	0.0000
1	PEI	1519.7866	69.8667
2	DXE	823.9279	1589.6533
3	BDS	2238.0843	2413.5812
4	Total(UEFI)	4651.6654	
5	Windows Boot Logo		~6000
6	Windows Login		~18000

Warm Boot



#	Phase	Duration (ms)	Elapsed Time(ms)
0	SEC	2449.9778	0.0000
1	PEI	3552.6876	2449.9778
2	DXE	820.3926	6002.6654
3	BDS	2989.2274	6823.0580
4	Total(UEFI)	9812.2854	
5	Windows Boot Logo		~11000
6	Windows Login		~25000

Cold Boot

Optimized Boot Time with MinPlatform Package on Mt. Olympus (OCP Board)

OCP CHINA DAY June 25th 2019 Beijing

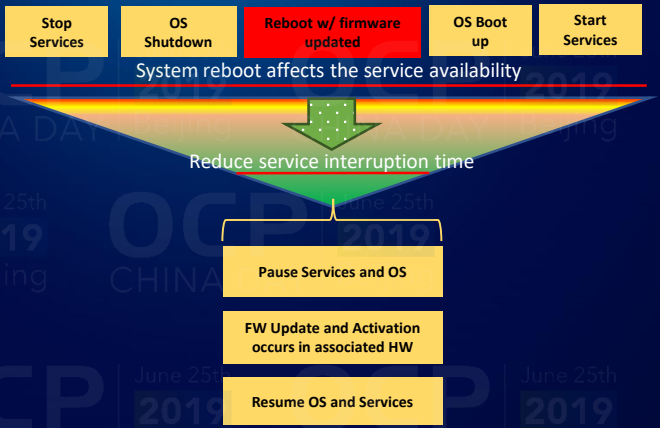
Firmware Activation

OS Constructs for Runtime Update

- Unix/Linux – kexec
- Windows – Memory Preserving Maintenance

Firmware Activation Mechanisms

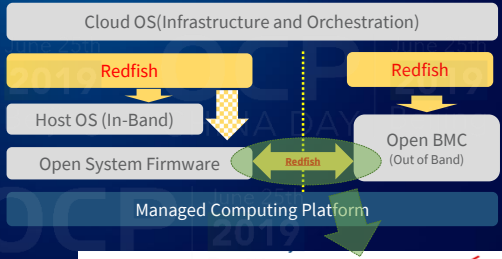
- Pause/Preserve Services (VM, Containers etc.) and OS
- Invoke Modified Reset Flow
- Update and Activate New FW modules
- Activate new FW modules
- Resume OS and Services



Intel working with partners in OCP to improve FW Update

Web-scale Configuration

- Need consistent HW Management API model across In band interface and Out of band interface
- Extend Redfish Model for Firmware Configuration Interface, including boot, power, performance, update etc.
- DMTF Redfish Host Interface between Host CPU and Out of Band Management Controller



EDKII Redfish Host Interface support available in GitHub: https://github.com/tianocore/edk2-staging/tree/UEFI_Redfish

OCP CHINA DAY June 25th 2019 Beijing

intel

Call To Action

- Get involved into Open System Firmware Project:
  OCP-OSF: https://www.opencompute.org/projects/open-system-firmware

- Engage with Intel on MinPlatform and FSP:
  MinPlatform: https://github.com/tianocore/edk2-platforms
  Intel FSP: https://www.intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html

- Accelerate innovations through industry collaboration (OCP, UEFI, Redfish etc.)

OCP CHINA DAY June 25th 2019 Beijing

intel

Thank you