Open. Together.

OCP
REGIONAL
SUMMIT

Advancements to Improving Cloud System Up-Time with Runtime Firmware Upgrade

OPEN SYSTEM FIRMWARE

Murugasamy (Sammy) Nachimuthu
Sr. Principal Engineer, Intel Corporation

Mallik Bulusu
Principal Firmware Engineering Manager,
Microsoft Corporation

OPEN PLATINUM™

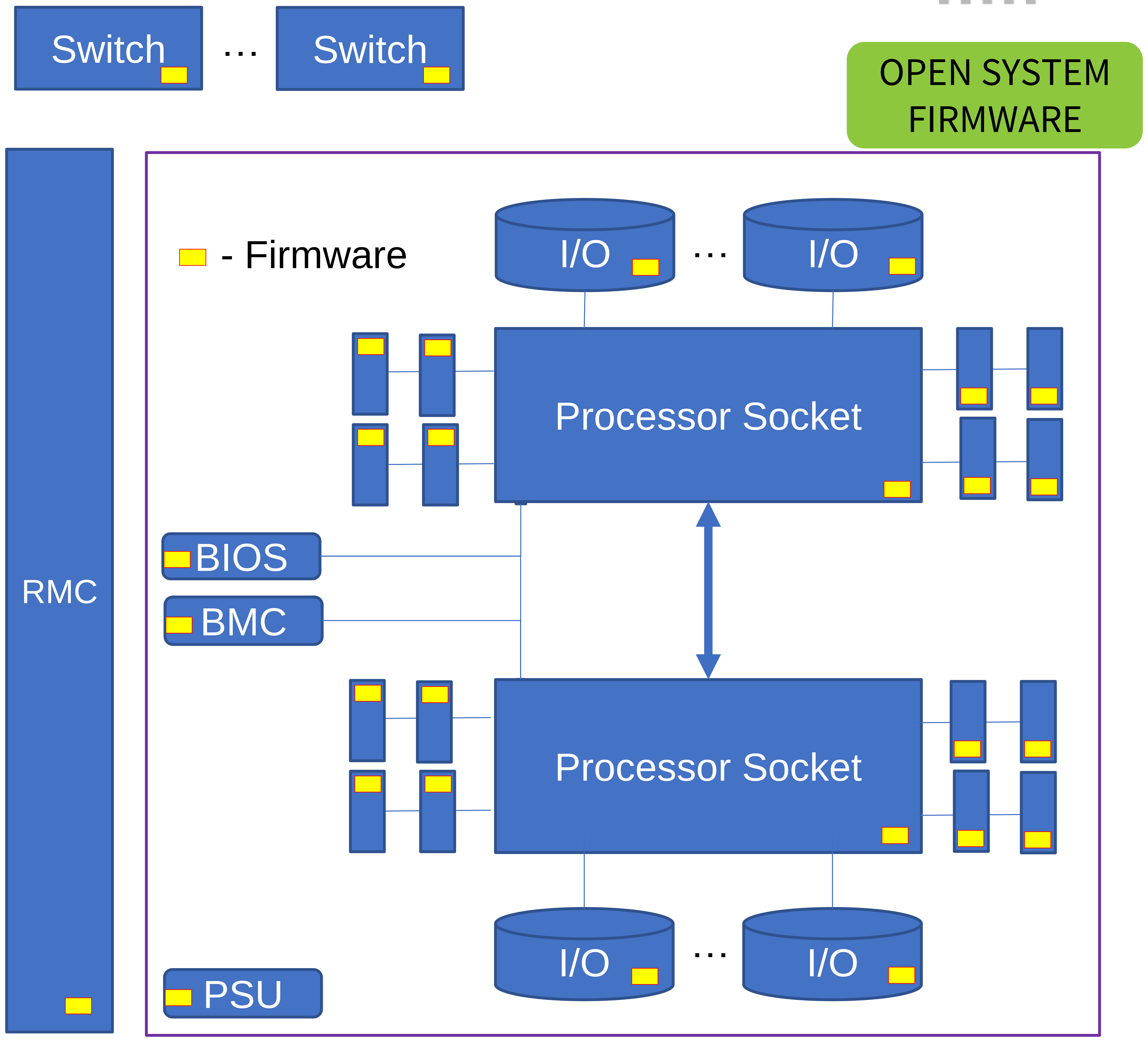
Cloud Systems Demands High Up-time

- Secure
- Reliable
- Predictable performance
- Highly available
- No perceived service interruption
- No data loss
- Etc.

Cloud Firmware Update Challenges

OPEN SYSTEM FIRMWARE

- Today's OCP system contains many hardware components with firmware
  - System Firmware – BIOS, BMC, etc.
  - Device Firmware – Microcode, Network, Storage, PSU, etc.
- Over life time of the system, the firmware components are upgraded to address:
  - Security, power, performance, bug fixes, debug/telemetry, etc.
- In most cases, system is rebooted to activate new firmware



Key Aspects to Cloud Firmware Updates

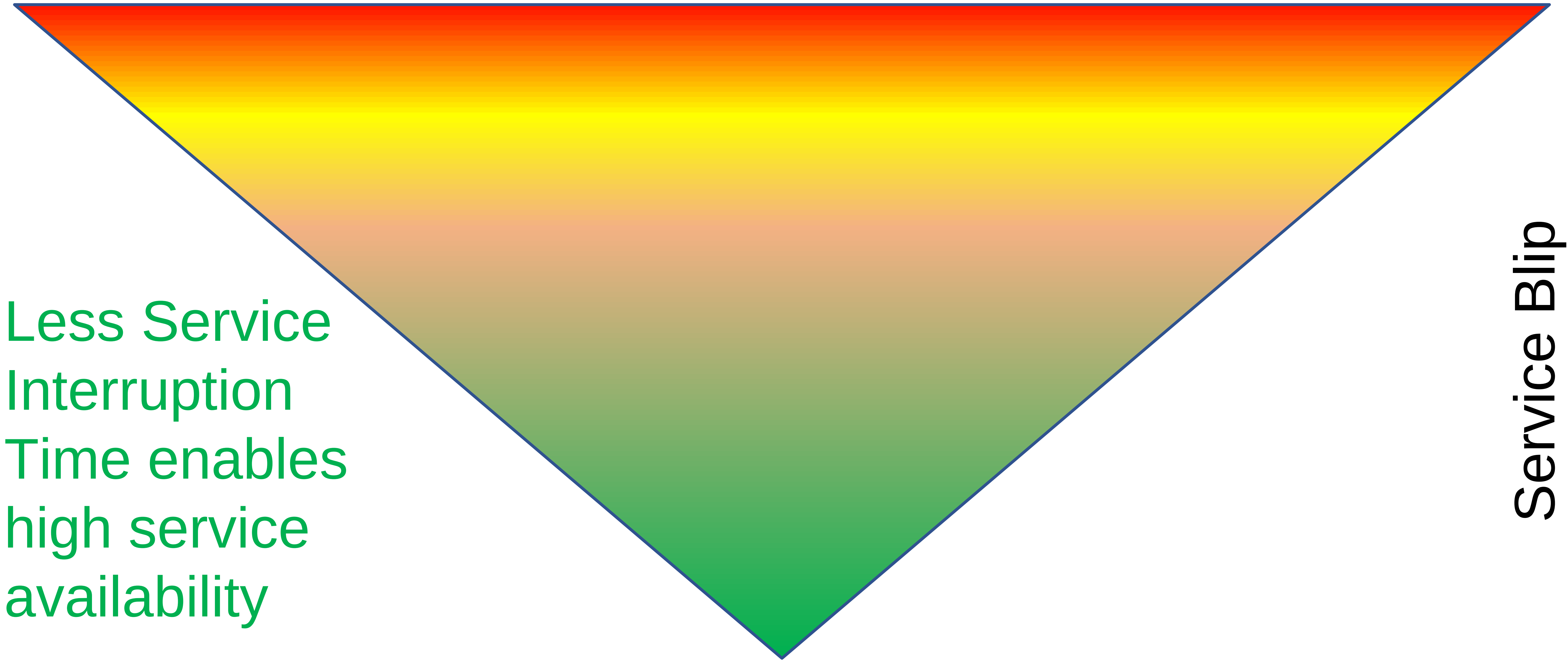
- Supply chain integrity
- Ease of deployment at scale
- Impact less updates
- Automatic Recovery / Rollback
- Audit trails
- Root of trust
- Low boot time
- Configuration / Policy management

Cloud Demands High Service Availability

OPEN SYSTEM FIRMWARE

Stop All VM and Services → Shutdown OS/VMM → Reboot System with new firmware → Boot OS/VMM → Restart VMs and Services

Service Interruption Time



Less Service Interruption Time enables high service availability

Update FW Module (s)

Service Blip:

- Pause/Preserve VMs
- Trigger FW Activation
- FW Activation occurs in associated HW
- OS is Reloaded

Services Resume

- OS Constructs for Runtime Updates
  - Unix/Linux – kexec
  - Windows – Memory Preserving Maintenance

Intel® is working with partners in OCP on improving FW upgrades

Runtime FW Upgrade Solution Requires

OPEN SYSTEM FIRMWARE

- Security mechanism for runtime FW upgrade
- FW module dependency
- Low FW activation time
- FW/OS interfaces
- OS support

Specifications

Runtime Firmware Activation Security

OPEN SYSTEM FIRMWARE

- Boot time FW attestation is not sufficient to handle runtime FW changes
- OCP Security Project includes mechanism for Runtime attestation
    - Cerberus provides RoT and attestation
    - New firmware additions are added to the Platform Firmware Manifest (PFM) and reported as Platform Active RoT (PA-ROT)

Specifications

FW Module Dependency

OPEN SYSTEM FIRMWARE

- Similar to boot time FW module compatibility, the runtime FW module compatibility need to be verified before activation
- If runtime FW activation fails, proper roll back need to be followed, otherwise may end-up with non-compatible state

Specifications

FW/OS Interface Support

OPEN SYSTEM FIRMWARE

- Host OS understanding of FW capabilities
- Host OS preparing the OS subsystem for FW activation
- BIOS/BMC/End-point Devices/OS interactions for enabling new FW

Specifications

Summary and Call to Action

- OCP systems are used in cloud that require high service availability.
- High availability needs modular firmware updates and activation
- Get involved into Open System Firmware
  - https://www.opencompute.org/projects/open-system-firmware

OCP
REGIONAL
SUMMIT

Open. Together.

OCP Regional Summit

26–27, September, 2019