OCP/OSF (Open System Firmware)

Workstream: OSF Requirements for OCP compliant Board and CPU Silicon Designs

Author(s): Gundrala Devender Goud (Microsoft)
Trammell Hudson (Two Sigma)
Date: Aug 8th, 2018 Version: V0.3

Revision History:

Revision	Key updates	Updates by		
V0.1	Initial Draft	Trammell		
V0.2	Updates on HW board requirements	Devender		
V0.3	Aug 08th OSF call review feedback	Devender		

System owners must be able to build and flash their own firmware

- "GPL compliance" tar files are not sufficient
  - Since OSF development strategy is continuous integration model, Code to build OSF based FW for a given HW must be available in the GitHub repo.

System owners must be able to resell their hardware

- either a clean vendor firmware
- Or their own modified firmware
- HW vendors must document all stateful components and procedure to returning to initial manufacturing state and audit the state machines (comply with NIST platform FW resiliency guidelines: #800-193)
  - Fuses, CPLD, PSUs, etc

Firmware must be updatable by system owner

- Via software with an owner (not vendor) provided key
- Via out-of-band channel like the BMC OR Via in-system-programming header
- Via replacing the flash chip

Trammel and David: will explore some kind of a ref design to support above Firmware Flashing mechanism.

If manufacturing-time CPU lockdown facilities are available (such as bootguard), they must be configured in measured mode to allow owners to flash their own firmware.

For OSF development, board manufacturer is expected to ship HW in unsecure mode to enable OSF development and later ON HW solution provider can choose to lock down with some kind of a fusing mechanism. All the tooling associated with this requirement should be well documented.

If the vendor components modify the PCRs or other measured state, the parameters for what goes into the measurements must be documented and reproducibly built.

For Silicon vendor provided modules When the vendor binary blobs hand over control the system must be left unlocked

- SMM
- BIOS CNTL
- FLOCKDN
- Etc

Document the following as part of HW board collateral:

(1) Clearly identify board level topology/connectivity diagram: This is required for OSF FW development teams to help them to configure various OSF modules and platform specific hooks to HW. Additionally, for ACPI aware Operating Systems boot, this information is a requirement to configure ACPI tables, develop runtime ASL hooks, board specific configurations run-time hooks, etc.

(2) I2C topology, SMBUS addresses, master/slave schema: This is required to configure PEI (FSP modules, HW devices detection and side band comms, etc.)

(3) PCIe topology (bifurcation, hot-plug, etc.): this is a general requirement to detect PCI bus topology of the board HW, configure PCI devices, allocate resources, etc.

(4) GPIOs with purpose: This is self-explanatory and must have for OSF developers to configure their modules or runtime handling of various events.

(5) All Error routing pins: This is required for OSF developers to configure error handling schema and routing. (especially handling of IERRs, CATERRs, Thermtrip, etc.)

(6) Interrupt routing: This has two fold requirements, one for OSF developers to configure and help OS runtime drivers to handle interrupts from endpoint devices and secondly, to configure routing of SMI/SCIs for runtime OSF error handling services.

(7) BMC communication hooks: This is specific to server usage models and it is paramount important for OSF to communicate to BMC and platform/DC node/rack level diags and telemetry from Data planes.

(8) Ability to tune industry standard (DDRx, PCIe, etc.) HS buses: These days HS links speeds are increasing gen to gen and FW is the saving grace to

accomplish HS margins. Therefore OSF needs to know the HW hooks/ process to optimize HS links for margins.

(9) All jumpers and special non-standard connector details must be documented.