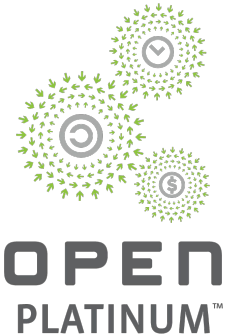
OPEN POSSIBILITIES.

OCP Server Delta Lake
OSF RAS Features

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

OCP Server Delta Lake OSF RAS Features

Jonathan Zhang, Software Engineer, Facebook



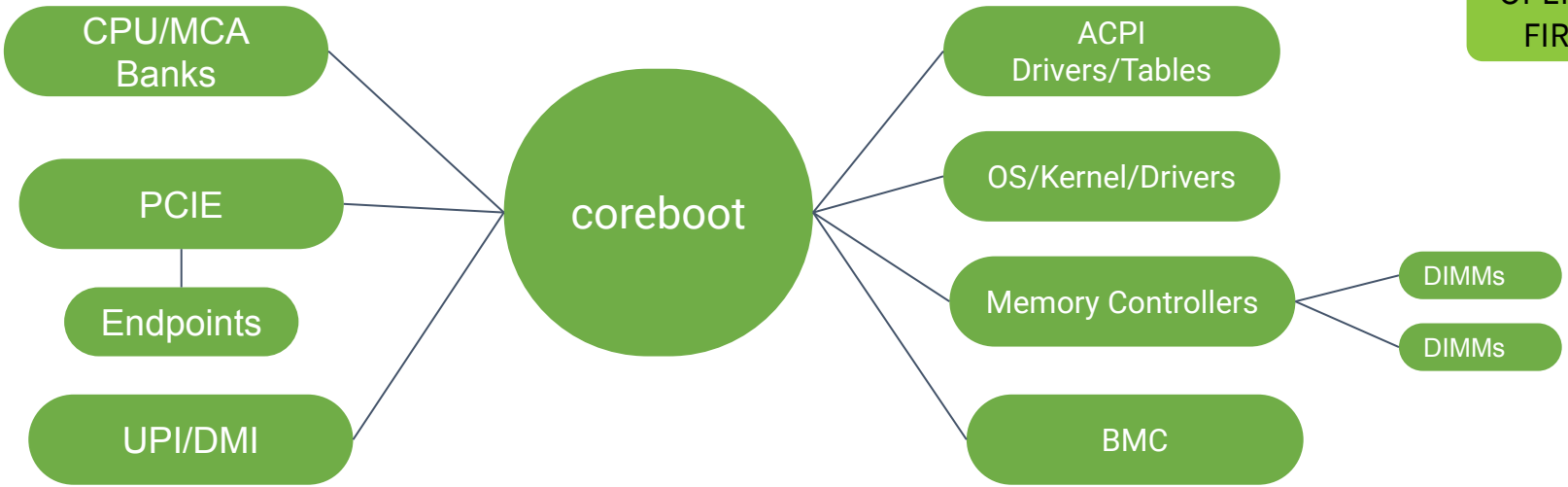
OPEN POSSIBILITIES.

OSF RAS Overview

OPEN SYSTEM FIRMWARE

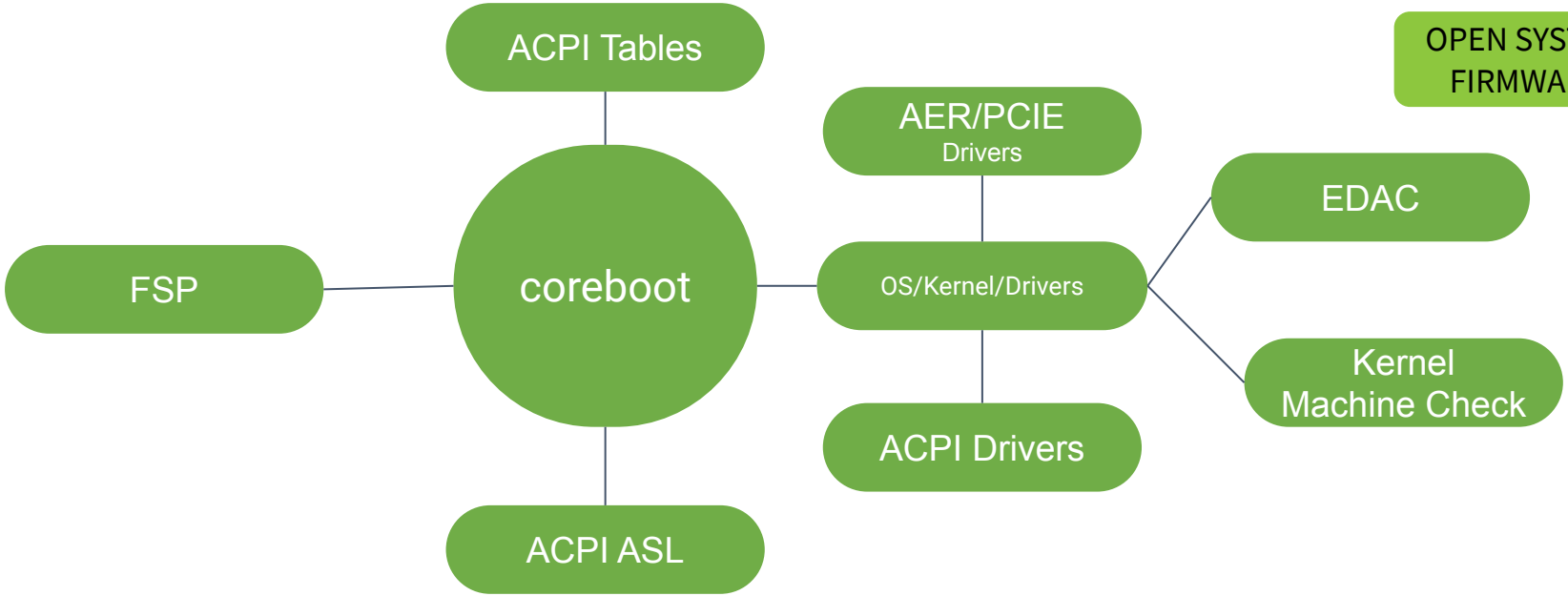
- RAS - Reliability, Availability, Serviceability
  - Reliability - the ability of a system to protect data integrity and self correct
  - Availability - the resiliency of a computer system to stay operational
  - Serviceability - speedy recovery, repair and maintenance
- RAS consists of both hardware and software components
  - Dispersed across multiple areas of HW and SW
    - CPU, PCIE, DMI, memory
    - Firmware, ACPI tables, ACPI ASL, OS kernel, OS drivers
- RAS helps identify failures early
- RAS provides a structured mechanism of reporting errors to higher level SW

SW & HW Building Blocks



OPEN SYSTEM FIRMWARE

SW Dependencies



OPEN SYSTEM FIRMWARE

OSF RAS Feature Support

OPEN SYSTEM FIRMWARE

Memory
- Correctable, uncorrectable, patrol scrub, parity error
- No support for features that reduce memory capacity or system performance

CPU - IERR, MCERR
- No UPI support or multi-socket support (yet)

AER/PCIE/, DMI

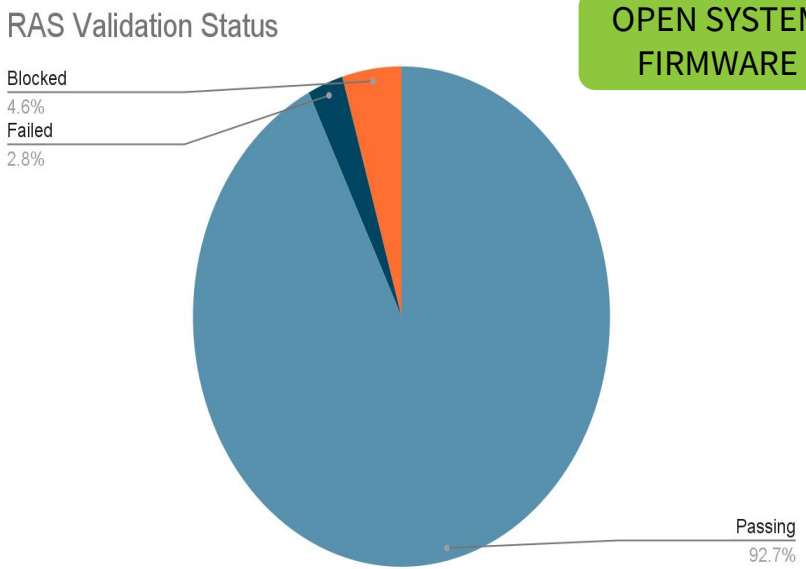
ACPI/APEI - EINJ, HEST, & GHES (APEI)

Kconfig options
- Manage Firmware First or OS-1st error handling and reporting
- Error thresholds, error propagation, & corrupt data containment
- Error reporting to BMC and OS via UEFI CPER (common platform error record)

Many debug config options

OSF RAS Validation Status

- Test status: > 92% passing
- Passed Tests
  - All memory controllers and channels
    - Memory correctable
    - Memory uncorrectable non-fatal
    - Memory uncorrectable fatal
    - Patrol Scrub & parity errors



OPEN SYSTEM FIRMWARE

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

OSF Validation Status (con't)

OPEN SYSTEM FIRMWARE

- Passed Tests
  - PCIE
    - Correctable, uncorrectable
    - All IIO stacks and endpoints
    - LER (link error recovery)
    - DMI
  - BMC
    - Logging of errors to BMC via SEL
- **GAPS/Failures**
  - BERT (Boot error record table), FSP error handling
  - IERR/MCERR - error injection is not functional
  - PCIE error issue during bootup with LER (deferred)
  - UPI support

OSF RAS Code Status

OPEN SYSTEM FIRMWARE

- Code base located mostly in src/soc/intel/xeon_sp folder

  https://github.com/coreboot/coreboot

- Support for Deltalake Mainboard
- Intel Xeon Processor CPX-6: 3rd Gen Intel Xeon Scalable
- Non-NDA code is already part of public repo

Call to Action

OPEN SYSTEM FIRMWARE

- Contribute to coreboot and LinuxBoot open source projects
- Please contact Wiwynn for purchasing Delta Lake
- Please contact 9elements Cyber Security for Delta Lake OSF feature development and professional support

OCP OSF Delta Lake: https://github.com/opencomputeproject/OpenSystemFirmware/tree/master/Wiwynn/deltalake

Where to buy: https://www.wiwynn.com/contact-wiwynn/

9elements Cyber Security: https://9esec.io/contact

coreboot: https://coreboot.org/

LinuxBoot: https://www.linuxboot.org/

Converged Security Suite: https://github.com/9elements/converged-security-suite

OPEN POSSIBILITIES.

Thank you!

NOVEMBER 9-10, 2021

BACKUP

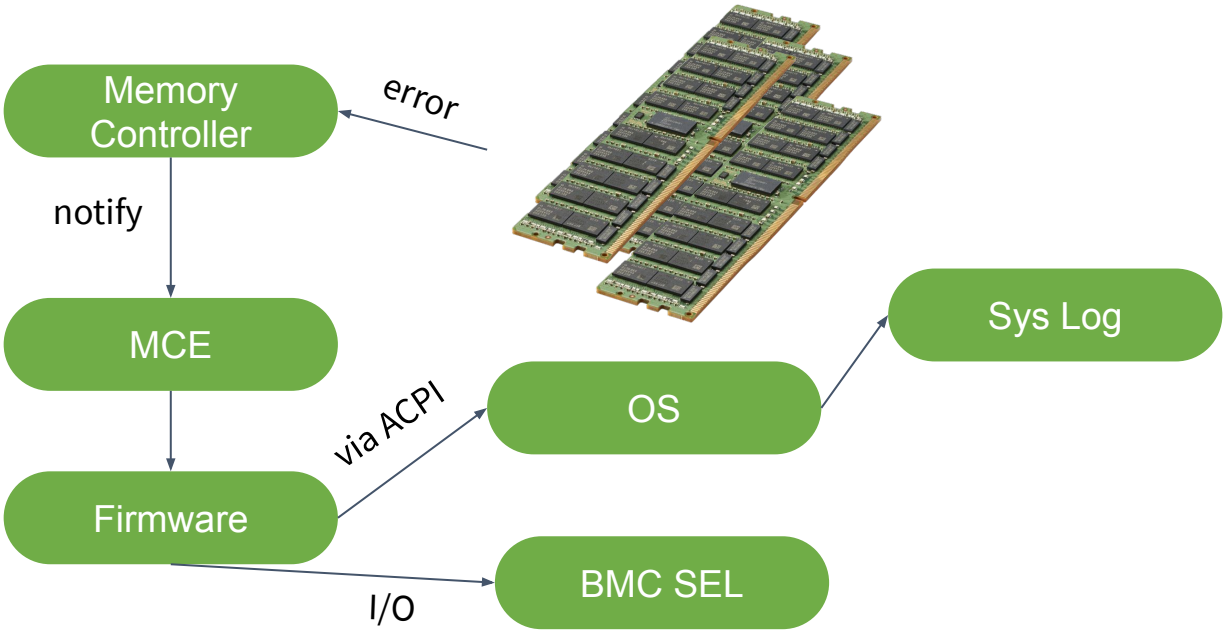
RAS Code Layout

OPEN SYSTEM FIRMWARE

RAS Folder, ~14 C files, 4 header files, many hooks into other components

MCA setup and init	SMM specific init	MCE handler
Uncore handler	Core handler	IIO/pcie handler
Access routines	Kconfig/Makefiles	IEH (integrated error hub)
Hest, GHES (acpi tables)	Elog (enhanced log)	EINJ
DMI	AER init	AER SMM
ACPI SCI	BMC error logging	UEFI/CPER

Memory CE/UCE Flow



OPEN SYSTEM FIRMWARE