Hacking Hardware and Software

- DIAGNOSTICS PERSPECTIVE

-VADIVEL

Objectives of Diagnostics

➢Reduce Board "RMA" Rate.

➢In Service RCA Analysis.

➢Support hardware failure Characterization.

➢Generate Failure Event Reports.

Diagnostics Paradigm

- **Bootstrap:**
  - Hardware bootstrap
  - Hardware Tuning and interface Map.
  - Programmable
  - Secure boot

- **Debug:**
  - RCA, Hardware Characterization and Persistent Event logs.

- **Infrastructure:**
  - Dynamic and Static Diagnostics framework

- **Correlation:**
  - Process, Symptoms, Failures.

- **Correction:**
  - Redundancy, Recover from Transient Errors, Hardware Errata's.

- **Security:**
  - Security Validation of programmable - Firmware, Microcode, FPGA.
  - Secure Upgradable.
  - Signature and License verification

Abstract Hardware Block
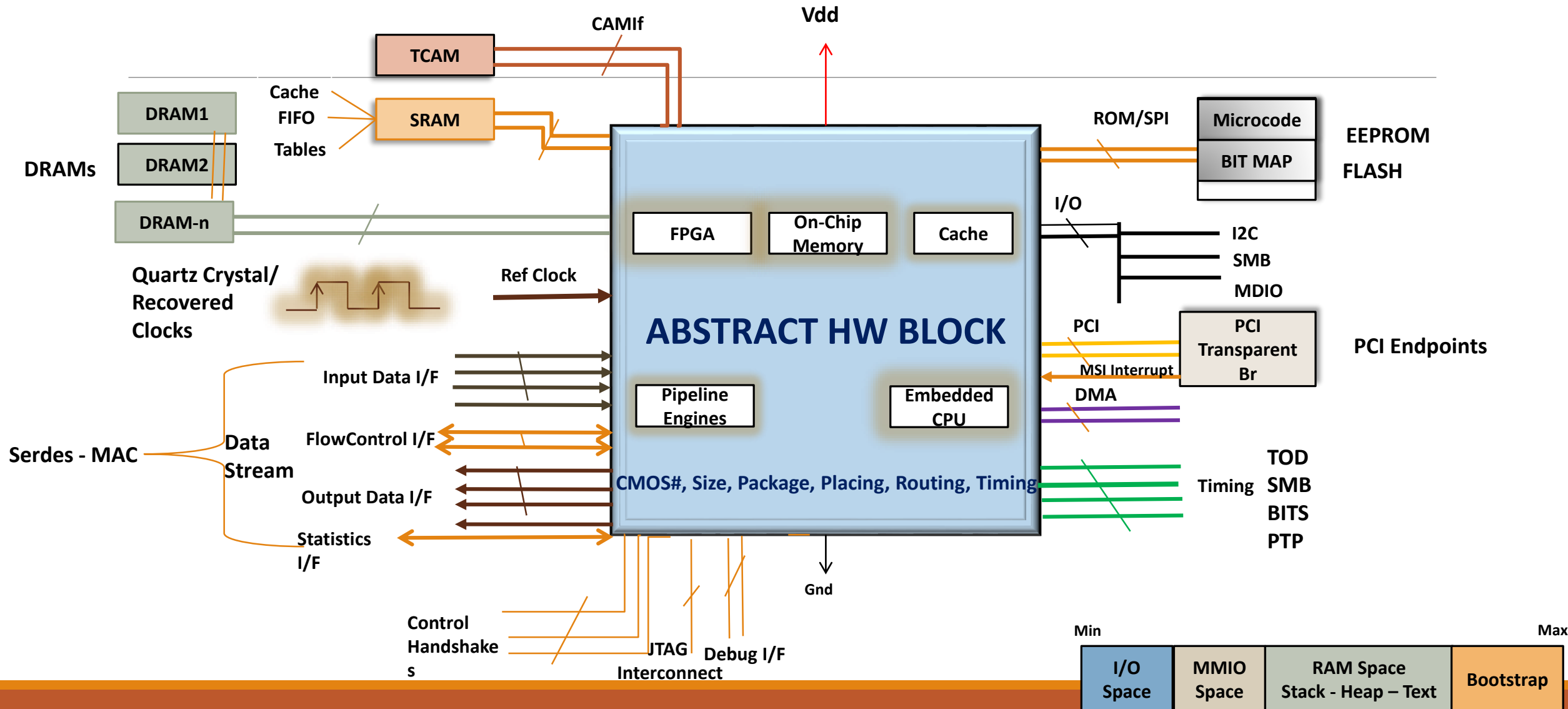
Diagnostics for Router platform

Data Plane Diagnostics

◦ Traffic Internal/External Generation

◦ Traffic Error Injection with DPI and IFP/EFP rules

◦ Forwarding Routing rules

◦ Traffic oversubscription, underrun, multicast

◦ PRBS Polynomial Patterns.

◦ Serdes Eyescan

◦ TCAM Memory

◦ Ingress and Egress Pipeline state machines

◦ Statistics

◦ Packet memory Interfaces - DDR/RLD

Control Plane Diagnostics

• Memory Banks, SPD, Cell walkthrough, CAS, latency

• Programmable

• PCI enumeration

• IO Interfaces - I2c, SMB, GPIO, SFI

• Custom specific components

Bootstrap

◦ **Hardware Tuning**

◦ SFI/XFI/CFI serdes Tuning
  ◦ Signal pins to Serdes lanes
  ◦ Serdes Tx Pre/post emphasis, Equalization - amp, main
  ◦ CL72 Training, CL73 Auto-negotiation.
◦ DDR/RLD Serdes Tuning
◦ PCI Serdes Tuning
◦ Memory "Shmooing"
◦ Programmable Validation.

- **Interface Maps**

  - System Memory Map
    - TLB, LAW, IO, MMIO
    - Device Controller memory translation
  - PCI Transparent and Non-Transparent Bridge Mapping

Diagnostics Framework

Framework

- Device Objects
- Device Maps
- Device Interface encapsulation
- Parametric Configuration

- **Levels of Diagnostics**

  - Pre-boot Diagnostics
    - Firmware, bios

  - Non-Intrusive Diagnostics
    - In service and online diagnostics

  - Intrusive Diagnostics
    - Out of Service Diagnostics
    - Design Validation

  - Software Diagnostics
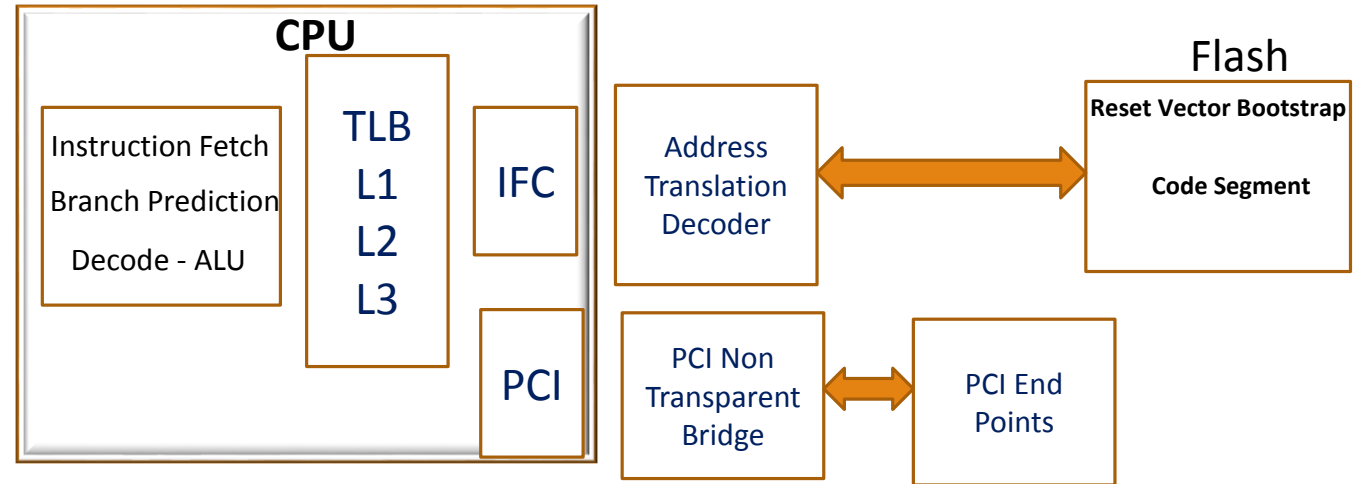   - System Tap, Exception handler hacks.

Correlation of Symptoms - Cause

Process - Production and Manufacturing

- ◦ Design Validation (DVT)
- ◦ SMT, REFLOW, ICT
- ◦ Process Variations
  - ◦ Burnin, ESS, Functional
- ◦ Yields

Hardware Software Isolation

Issue 1: Machine Check NMI exception

CPU

Instruction Fetch

Branch Prediction

Decode - ALU

TLB
L1
L2
L3

IFC

PCI

Address
Translation
Decoder

PCI Non
Transparent
Bridge

PCI End
Points

Flash

Reset Vector Bootstrap

Code Segment

➢Hardware error exception

➢Enable and Read Cycle Synchronization

➢Kernel Panic

➢Unmapped PCI BAR device addresses

➢Watchdog NMI exception

Issue 2: Packet Drops
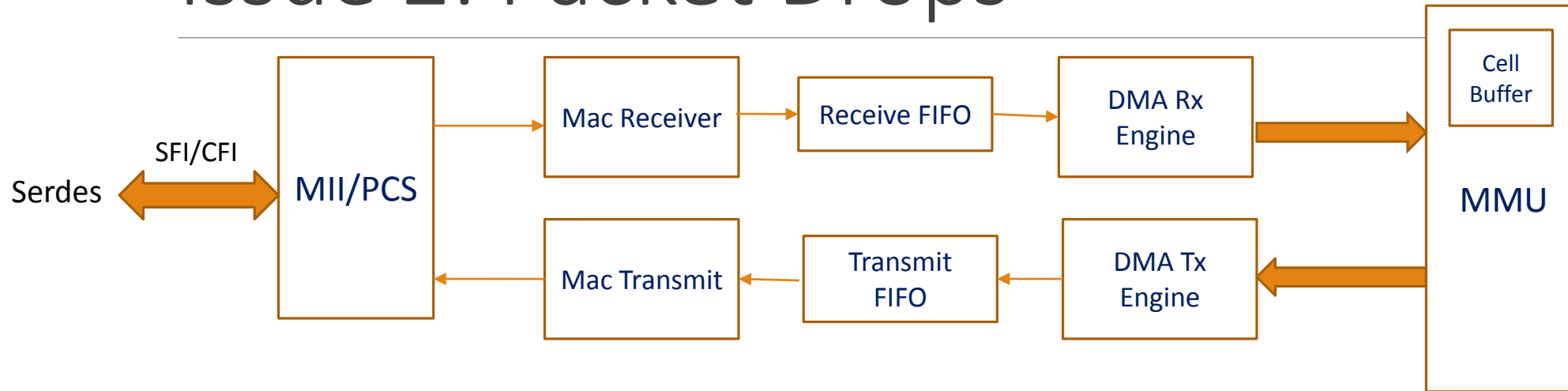
Links
- Serdes Links
- Link serdes Tx Param tuning.

Memory Interfaces
- DDR
- RLD
- Internal SOC memories.

- **RED Drops**
  - Cell size mismatch
  - MMU credits for queue scheduler
  - VOQ allocation

- **Forwarding Rules**
  - Multicast
  - VLAN ID
  - Destination mac lookup

Challenges

➢ Diagnostics of virtual functions (VF) and resource pools in virtualized infrastructure.

➢ Real-time diagnostics

➢ Software diagnostics

➢ Diag Services in the cloud

Questions? Your Turn!