2.0 Hardware HA

The hardware HA can be solved by several legacy HA schemes. However, when considering the NFV scenarios, a hardware failure will cause collateral damage to not only to the services but also virtual infrastructure running on it.

A redundant architecture and automatic failover for the hardware are required for the NFV scenario. At the same time, the fault detection and report of HW failure from the hardware to VIM, VNFM and if necessary the Orchestrator to achieve HA in OPNFV. A sample fault table can be found in the Doctor project. (https://wiki.opnfv.org/doctor/faults) All the critical hardware failures should be reported to the VIM within 1s.

Other warnings for the hardware should also be reported to the VIM in a timely manner.

General Requirements:

- Hardware Failures should be reported to the hypervisor and the VIM.
- Hardware Failures should not be directly reported to the VNF as in the traditional ATCA architecture.
- Hardware failure detection message should be sent to the VIM within a specified period of time, based on the SAL as defined in Section 1.
- Alarm thresholds should be detected and the alarm delivered to the VIM within 1min. A certain threshold can be set for such notification.
- Direct notification from the hardware to some specific VNF should be possible. Such notification should be within 1s.
- Periodical update of hardware running conditions (operational state?) to the NFVI and VIM is required for further operation, which may include fault prediction, failure analysis, and etc.. Such info should be updated every 60s
- Transparent failover is required once the failure of storage and network hardware happens.
- Hardware should support SNMP and IPMI for centralized management, monitoring and control.

Network plane Requirements:

- The hardware should provide a redundant architecture for the network plane.
- Failures of the network plane should be reported to the VIM within 1s.
- QoS should be used to protect against link congestion.

Power supply system:

- The power supply architecture should be redundant at the server and site level.
- Fault of the power supply system should be reported to the VIM within 1s.
- Failure of a power supply will trigure automatic failover to the redundant supply.

Cooling system:

- The architecture of the cooling system should be redundant.
- Fault of the cooling system should be reported to the VIM within 1s
- Failure of the cooling systme will trigger automatic failover of the system

Disk Array:

- The architecture for the disk array should be redundant.
- Fault of the disk array should be reported to the VIM within 1s
- Failure of the the disk array will trigger automatic failover of the system support for protected cache after an unexpected power loss.
- **Data shall be stored redundantly in the storage backend**

  (e.g., by means of RAID across disks.)
- Upon failures of storage hardware components (e.g., disks services, storage nodes) automatic repair mechanisms (re-build/re-balance of data) shall be triggered automatically.
- Centralized storage arrays shall consist of redundant hardware

Servers:

- Support precise timming with accuracy higher than 4.6ppm