Introduction:

The PEI foundation is unaware the system boot pat. Only PEIMs know the boot mode and takes appropriate actions based on the boot mode.

To implement this each PEIM has the ability to change the boot mode using PeiService SetBootMode().

Change in boot mode doesn’t influence the order of PEIMs dispatched.

Code Flow:

The normal code flow in platform initialization is in the following order

1. SEC
2. PEI
3. DXE
4. BDS
5. Runtime
6. Afterlife

Defined Boot modes:

The list of possible boot modes is defined in GetBootMode() function.

Priority of Boot Paths:

Within a given PEIM, the priority of the boot mode is from highest to lowest.

1. BOOT\_IN\_RECOVERY\_MODE
2. BOOT\_ON\_FLASH\_UPDATE
3. BOOT\_ON\_S3\_RESUME
4. BOOT\_WITH\_MINIMAL\_CONFIGURATION
5. BOOT\_WITH\_FULL\_CONFIGURATION
6. BOOT\_ASSUMING\_NO\_CONFIGURATION\_CHANGES
7. BOOT\_WITH\_FULL\_CONFIGURATION\_PLUS\_DIAGNOSTICS
8. BOOT\_WITH\_DEFAULT\_SETTINGS
9. BOOT\_ON\_S4\_RESUME
10. BOOT\_ON\_S5\_RESUME
11. BOOT\_ON\_S2\_RESUME

The boot modes listed above are defined in PEI services SetBootMode().

Reset Boot Paths:

1. Intel Itanium Processor Reset:

The internal microcode on the processor silicon, which starts up at PowerGood reset, finds the first layer of processor abstraction code (called PAL-A) located in the BFV. If the authentication of PAL-A passes, then invokes next layer PAL-B.

1. Non-Power-On Reset:

Non-power-on reset can occur for many reasons. Some PEI and DXE services reset and reboot the entire platform. This can occur due to following reasons.

1. Resetting processor to change frequency settings
2. Resetting hardware to complete chipset initialization
3. Responding to catastrophic failure

Normal Boot Path:

1. Basic G0 to S0 and S0 variation boot paths:

S0 boot path is *boot with full configuration.* This setting informs all PEIMs to do full configuration.

Other supported booth paths:

1. Boot with minimal configuration
2. Boot assuming no configuration changes
3. Boot with full configuration plus diagnostics
4. Boot with default settings
5. S-State boot paths:
   1. S3 (Suspend to RAM):

Must take extra care to preserve/restore system RAM and critical hardware, assumes previous settings are valid.

* 1. S4 (Suspend to Disk)

It is similar to S5, platform completely initializes, assumes previous settings are valid.

* 1. S5 (Soft off)

Platform initializes completely, can’t assume previous settings are valid.

Recovery Paths:

All the previously described boot paths can be modified or aborted if the system detects the recovery is needed. Recovery is the process of reconstituting a system’s firmware that have been corrupted. Generally, firmware is present in non-volatile memory as blocks. The reasons for firmware corruption could be a errant hardware or software.