Intel(R) Firmware Support Package (FSP) Integration Guide

Thu Jan 21 2021 23:24:12

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: `http://www.intel.com/design/literature.htm`

Any software source code reprinted in this document is furnished for informational purposes only and may only be used or copied and no license, express or implied, by estoppel or otherwise, to any of the reprinted source code is granted by this document.

[When the doc contains software source code for a special or limited purpose (such as informational purposes only), use the conditionalized Software Disclaimer tag. Otherwise, use the generic software source code disclaimer from the Legal page and include a copy of the software license or a hyperlink to its permanent location.]

This document contains information on products in the design phase of development. Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: `http://www.intel.com/products/processor_number/`

Code Names are only for use by Intel to identify products, platforms, programs, services, etc. ("products") in development by Intel that have not been made commercially available to the public, i.e., announced, launched or shipped. They are never to be used as "commercial" names for products. Also, they are not intended to function as trademarks.

Intel, Intel Atom, [include any Intel trademarks which are used in this document] and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Chapter 1

INTRODUCTION

1.1 1 Introduction

1.1.1 1.1 Purpose

The purpose of this document is to describe the steps required to integrate the Intel® Firmware Support Package (FSP) into a boot loader solution. It supports CometLake platforms.

1.1.2 1.2 Intended Audience

This document is targeted at all platform and system developers who need to consume FSP binaries in their boot loader solutions. This includes, but is not limited to: system BIOS developers, boot loader developers, system integrators, as well as end users.

1.1.3 1.3 Related Documents

- *Platform Initialization (PI) Specification v1.4* located at `http://www.uefi.org/specifications`
- *Intel® Firmware Support Package: External Architecture Specification (EAS) v2.0* located at `http://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp` `pdf`
- *Boot Setting File Specification (BSF) v1.0* `https://firmware.intel.com/sites/default/files/BSF_1_0.pdf`
- *Binary Configuration Tool for Intel® Firmware Support Package* available at `http://www.intel.com/fsp`

Acronym	Definition

1.1.4 1.4 Acronyms and Terminology

Acronym	Definition
BCT	Binary Configuration Tool
BSF	Boot Setting File
BSP	Boot Strap Processor
BWG	BIOS Writer's Guide
CAR	Cache As Ram
CRB	Customer Reference Board
FIT	Firmware Interface Table
FSP	Firmware Support Package
FSP API	Firmware Support Package Interface
FW	Firmware
PCH	Platform Controller Hub
PMC	Power Management Controller
SBSP	System BSP
SMI	System Management Interrupt
SMM	System Management Mode
SPI	Serial Peripheral Interface
TSEG	Memory Reserved at the Top of Memory to be used as SMRAM
UPD	Updatable Product Data
IED	Intel Enhanced Debug
GTT	Graphics Translation Table
BDSM	Base Data Of Stolen Memory
PMRR	Protected Memory Range Reporting
IOT	Internal Observation Trace
MOT	Memory Observation Trace
DPR	DMA Protected Range
REMAP	Remapped Memory Area
TOLUD	Top of Low Usable Memory
TOUUD	Top of Upper Usable Memory

Chapter 2

FSP OVERVIEW

2.1 FSP Overview

2.1.1 2.1 Technical Overview

The *Intel® Firmware Support Package (FSP)* provides chipset and processor initialization in a format that can easily be incorporated into many existing boot loaders.

The FSP will perform the necessary initialization steps as documented in the BWG including initialization of the CPU, memory controller, chipset and certain bus interfaces, if necessary.

FSP is not a stand-alone boot loader; therefore it needs to be integrated into a host boot loader to carry out other boot loader functions, such as: initializing non-Intel components, conducting bus enumeration, and discovering devices in the system and all industry standard initialization.

The FSP binary can be integrated easily into many different boot loaders, such as Coreboot, EDKII etc. and also into the embedded OS directly.

Below are some required steps for the integration:

- **Customizing** The static FSP configuration parameters are part of the FSP binary and can be customized by external tools that will be provided by Intel.
- **Rebasing** The FSP is not Position Independent Code (PIC) and the whole FSP has to be rebased if it is placed at a location which is different from the preferred address during build process.
- **Placing** Once the FSP binary is ready for integration, the boot loader build process needs to be modified to place this FSP binary at the specific rebasing location identified above.
- **Interfacing** The boot loader needs to add code to setup the operating environment for the FSP, call the FSP with correct parameters and parse the FSP output to retrieve the necessary information returned by the FSP.

2.1.2 2.2 FSP Distribution Package

- The FSP distribution package contains the following:
  - FSP Binary
  - FSP Integration Guide
  - BSF Configuration File
  - Data Structure Header File
- The FSP configuration utility called BCT is available as a separate package. It can be downloaded from link mentioned in Section 1.3.

2.1.2.1 2.2.1 Package Layout

- **Docs (Auto generated)**
  - FSP_Integration_Guide.pdf
  - FSP_Integration_Guide.chm
- **Include**
  - FsptUpd.h, FspmUpd.h and FspsUpd.h (FSP UPD structure and related definitions)
  - GpioSampleDef.h (Sample enum definitions for Gpio table)
- ∗FspBinPkg.dec (EDKII declaration file for package)
- Fsp.bsf (BSF file for configuring the data using BCT tool)
- Fsp.fd (FSP Binary)

Chapter 3

FSP INTEGRATION

3.1 3 FSP Integration

3.1.1 3.1 Assumptions Used in this Document

The FSP for this platform is built with a preferred base address given by PcdFspAreaBaseAddress and so the reference code provided in the document assumes that the FSP is placed at this base address during the final boot loader build. Users may rebase the FSP binary at a different location with Intel's Binary Configuration Tool (BCT) before integrating to the boot loader.

For other assumptions and conventions, please refer section 8 in the FSP External Architecture Specification version 2.0.

3.1.2 3.2 Boot Flow

Please refer Chapter 7 in the FSP External Architecture Specification version 2.0 for Boot flow chart.

3.1.3 3.3 FSP INFO Header

The FSP has an Information Header that provides critical information that is required by the bootloader to successfully interface with the FSP. The structure of the FSP Information Header is documented in the FSP External Architecture Specification version 2.0 with a HeaderRevision of 3.

3.1.4 3.4 FSP Image ID and Revision

FSP information header contains an Image ID field and an Image Revision field that provide the identification and revision information of the FSP binary. It is important to verify these fields while integrating the FSP as API parameters could change over different FSP IDs and revisions. All the FSP FV segments(FSP-T, FSP-M and FS↩
P-S) must have same FSP Image ID and revision number, using FV segments with different revision numbers in a single FSP image is not valid. The FSP API parameters documented in this integration guide are applicable for the Image ID and Revision specified as below.

The FSP ImageId string in the FSP information header is given by **PcdFspImageIdString** and the ImageRevision field is given by SiliconInitVersionMajor|Minor|FspVersionRevision|FspVersionBuild (Ex:0x07020110).

3.1.5 3.5 FSP Global Data

FSP uses some amount of TempRam area to store FSP global data which contains some critical data like pointers to FSP information headers and UPD configuration regions, FSP/Bootloader stack pointers required for stack switching etc. HPET Timer register(2) PcdGlobalDataPointerAddress is reserved to store address of this global data, and hence boot loader should not use this register for any other purpose. If TempRAM initialization is done by boot loader, then HPET has to be initialized to the base so that access to the register will work fine.

3.1.6 3.6 FSP APIs

This release of the FSP supports the all APIs required by the FSP External Architecture Specification version 2.0. The FSP information header contains the address offset for these APIs. Register usage is described in the FSP External Architecture Specification version 2.0. Any usage not described by the specification is described in the individual sections below.

The below sections will highlight any changes that are specific to this FSP release.

3.1.6.1 3.6.1 TempRamInit API

Please refer Chapter 8.5 in the FSP External Architecture Specification version 2.0 for complete details including the prototype, parameters and return value details for this API.

TempRamInit does basic early initialization primarily setting up temporary RAM using cache. It returns ECX pointing to beginning of temporary memory and EDX pointing to end of temporary memory + 1. The total temporary ram currently available is given by PcdTemporaryRamSize starting from the base address of PcdTemporaryRamBase. Out of total temporary memory avaiable, last PcdFspReservedBufferSize bytes of space reserved by FSP for Temp↩ RamInit if temporary RAM initialization is done by FSP and remaining space from **TemporaryRamBase**(ECX) to **TemporaryRamBase+TemporaryRamSize-FspReservedBufferSize** (EDX) is avaiable for both bootloader and FSP binary.

TempRamInit∗∗ also sets up the code caching of the region passed CodeCacheBase and CodeCacheLength, which are input parameters to TempRamInitApi. if 0 is passed in for CodeCacheBase, the base used will be 4 GB - 1 - length to be code cached instead of starting from CodeCacheBase.

Note

: when programming MTRR CodeCacheLength will be reduced, if SKU LLC size is smaller than the requested.

It is a requirement for Firmware to have Firmware Interface Table (FIT), which contains pointers to each microcode update. The microcode update is loaded for all logical processors before reset vector. If more than microcode update for the CPU is present, the microcode update with the latest revision is loaded.

FSPT_UPD.MicrocodeRegionBase∗∗ and **FSPT_UPD.MicrocodeRegionLength** are input parameters to Temp↩ RamInit API. If these values are 0, FSP will not attempt to update microcode. If a region is passed, then if a newer microcode update revision is in the region, it will be loaded by the FSP.

MTRRs are programmed to the default values to have the following memory map:

Memory range	Cache Attribute
0xFEF00000 - 0x00040000	Write back
CodeCacheBase - CodeCacheLength	Write protect

3.1.6.2 3.6.2 FspMemoryInit API

Please refer to Chapter 8.6 in the FSP external Architecture Specification version 2.0 for the prototype, parameters and return value details for this API.

The **FspmUpdPtr** is pointer to **FSPM_UPD** structure which is described in header file FspmUpd.h.

Boot Loader must pass valid CAR region for FSP through **FSPM_UPD.FspmArchUpd.StackBase** and **FSPM_U↩ PD.FspmArchUpd.StackSize** UPDs.

Starting with v2.1 specification FSP will run on top of the stack provided by the bootloader instead of establishing a separate stack.

Below are the heap and stack requirement for FSP v2.1:

HOB Heap requirement:

HOB Heap	UPD	Setting ------—
Base	FSPM_UPD.FspmArchUpd.StackBase	Any non-conflict CAR region (0xFEF17F00 as default)
Size	FSPM_UPD.FspmArchUpd.StackSize	at least 64KB

Stack requirement: FSP would start stack usage from current stack pointer. The minimum stack size requirement for FSP-M is 128kb. Bootloader needs to ensure the stack size allocated meets its requirement and also accomodate FSP-M minimum stack size requirement.

The base address of HECI device (Bus 0, Device 22, Function 0) is required to be initialized prior to perform Fsp↩ MemoryInit flow. The default address is programmed to 0xFED1A000.

Calculate memory map determining memory regions TSEG, IED, GTT, BDSM, ME stolen, Uncore PMRR, IOT, MOT, DPR, REMAP, TOLUD, TOUUD. Programming will be done at a different time.

3.1.6.3 3.6.3 TempRamExit API

Please refer to Chapter 8.7 in the FSP external Architecture Specification version 2.0 for the prototype, parameters and return value details for this API.

If Boot Loader initializes the Temporary RAM (CAR) and skip calling **TempRamInit API**, it is expected that bootloader must skip calling this API and bootloader will tear down the temporary memory area setup in the cache and bring the cache to normal mode of operation.

This revision of FSP doesn't have any fields/structure to pass as parameter for this API. Pass Null for *TempRam↩ ExitParamPtr*.

At the end of *TempRamExit* the original code and data caching are disabled. FSP will reconfigure all MTRRs as described in the table below for performance optimization. If the boot loader wish to reconfigure the MTRRs differently, it can be overridden immediately after this API call.

Memory range	Cache Attribute
0xFF000000 - 0xFFFFFFFF (Flash region)	Write protect
0x00000000 - 0x0009FFFF	Write back
0x000C0000 - Top of Low Memory	Write back
xxxx - xxxx	x ∗Note1
0x100000000 - Top of High Memory	Write back ∗Note2

Note1: Certain silicon feature required specific cache type of its own memory and will be configured by FSP accordingly when feature enabled.

Note2: In some cases MTRR might not be enough to cover all desired regions, in this case memory regions need to be adjusted for better alignment (e.g., adjust MmioSize or MmioSizeAdjustment UPD) Covering flash region and above 4GB memory is another case which may consume more MTRRs, when there is no enough MTRR available FSP will only cover above 4GB memory partially. In this case boot loader should optimize MTRR in late phase without flash coverage before booting OS.

3.1.6.4 3.6.4 FspSiliconInit API

Please refer to Chapter 8.8 in the FSP external Architecture Specification version 2.0 for the prototype, parameters and return value details for this API.

The *FspsUpdPtr* is pointer to **FSPS_UPD** structure which is described in header file FspsUpd.h.

It is expected that boot loader will program MTRRs for SBSP as needed after **TempRamExit** but before entering **FspSiliconInit**. If MTRRs are not programmed properly, the boot performance might be impacted.

The region of 0x5_8000 - 0x5_8FFF is used by FspSilicionInit for starting APs. If this data is important to bootloader, then bootloader needs to preserve it before calling FspSilicionInit.

It is a requirement for bootloader to have Firmware Interface Table (FIT), which contains pointers to each microcode. The microcode is loaded for all cores before reset vector. If more than one microcode update for the CPU is present, the latest revision is loaded.

MicrocodeRegionBase and MicrocodeRegionLength are both input parameters to TempRamInit and UPD for SiliconInit API. UPD has priority and will be searched for a later revision than TempRamInit. If MicrocodeRegion↩ Base and MicrocodeRegionLength values are 0, FSP will not attempt to update the microcode. If a microcode region is passed, and if a later revision of microcode is present in this region, FSP will load it.

FSP initializes PCH audio including selecting HD Audio verb table and initializes Codec.

PCH required initialization is done for the following HECI, USB, HSIO, Integrated Sensor Hub, Camera, PCI Express, Vt-d.

FSP initializes CPU features: XD, VMX, AES, IED, HDC, x(2)Apic, Intel® Processor Trace, Three strike counter, Machine check, Cache pre-fetchers, Core PMRR, Power management.

Initializes HECI, DMI, Internal Graphics. Publish EFI_PEI_GRAPHICS_INFO_HOB during normal boot but this HOB will not be published during S3 resume as FSP will not launch the PEI Graphics PEIM during S3 resume.

Programs SA Bars: MchBar, DmiBar, EpBar, GdxcBar, EDRAM (if supported). Please refer to section 2.↩ 8 (MemoryMap) for the corresponding Bar values. GttMmadr (0xDF000000) and GmAdr(0xC0000000) are temporarily programmed and cleared after use in FSP.

3.1.6.5 3.6.5 NotifyPhase API

Please refer Chapter 8.9 in the FSP External Architecture Specification version 2.0 for the prototype, parameters and return value details for this API.

3.1.6.5.1 3.6.5.1 PostPciEnumeration Notification

This phase *EnumInitPhaseAfterPciEnumeration* is to be called after PCI enumeration but before execution of third party code such as option ROMs. Currently, nothing is done in this phase, but in the future updates, programming may be done in this phase.

3.1.6.5.2 3.6.5.2 ReadyToBoot Notification

This phase *EnumInitPhaseReadyToBoot* is to be called before giving control to boot. It includes some final initialization steps recommended by the BWG, including power management settings, Send ME Message EOP (End of Post).

3.1.6.5.3 3.6.5.3 EndOfFirmware Notification

This phase *EnumInitEndOfFirmware* is to be called before the firmware/preboot environment transfers management of all system resources to the OS or next level execution environment. It includes final locking of chipset registers

3.1.7 3.7 Memory Map

Below diagram represents the memory map allocated by FSP including the FSP specific regions.

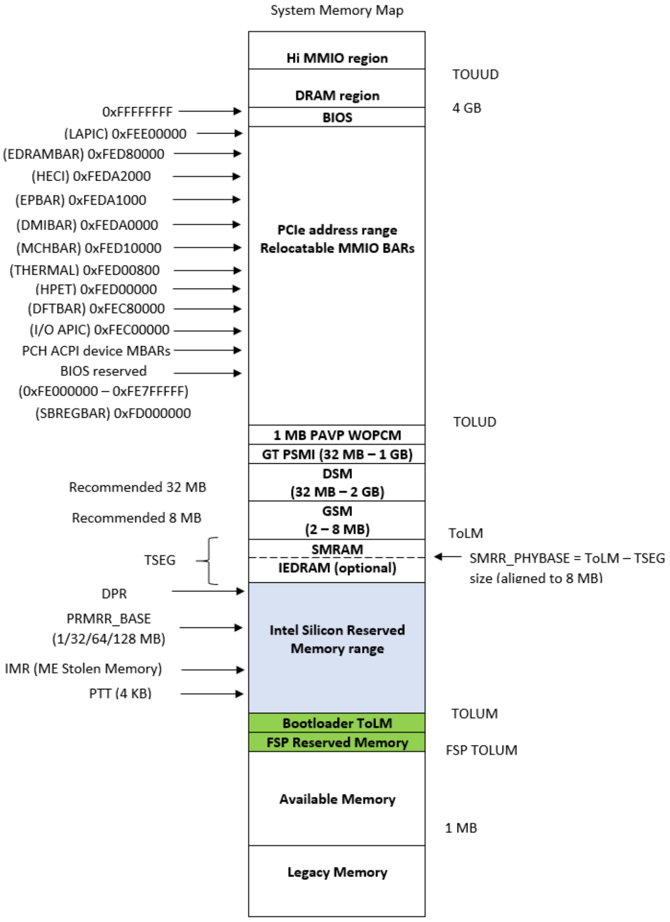


Figure 3.1 System Memory Map

/**

Chapter 4

FSP PORTING RECOMMENDATION

4.1 4 FSP Porting Recommendation

Here listed some notes or recommendation when porting with FSP.

4.1.1 4.1 Locking PAM register

FSP 2.0 introduced EndOfFirmware Notify phase callback which is a recommended place for locking PAM registers so FSP by default implemented this way. If it is still too early to lock PAM registers then the PAM locking code inside FSP can be disabled by UPD -> FSP_S_TEST_CONFIG -> SkipPamLock or SA policy -> _SI_PREMEM_POLICY_STRUCT -> SA_MISC_PEI_CONFIG -> SkipPamLock, and platform or wrapper code should do the PAM locking right before booting OS (so do it outside FSP instead) by programming one PCI config space register as below.

This PAM locking step has to been applied in all boot paths including S3 resume. To lock PAM regsiter:

```
MmioOr32 (B0: D0: F0: Register 0x80, BIT0)
```

4.1.2 4.2 Locking SMRAM register

Since SMRAM locking is recommended to be locked before any 3rd party OpROM execution and highly depending on platform code implementation, the FSP code by default will not lock it. The platform or FSP Wrapper code should lock SMRAM by below programming step before any 3rd partiy OpRom execution (and should be locked in S3 resume right before OS waking vector).

```
PciOr8 (B0: D0: F0: Register 0x88, BIT4); Note: it must be programmed by CF8/CFC Standard PCI access
      mechanism. (MMIO access will not work)
```

4.1.3 4.3 Locking SMI register

Global SMI bit is recommended to be locked before any 3rd party OpROM execution and highly depending on platform code implementation after SMM configuration. FSP by default will not lock it. Boot loader is responsible for locking below regsiters after SMM configuration. Set AcpiBase + 0x30[0] to 1b to enable global SMI. Set PMC PCI offset A0h[4] = 1b to lock SMI.

4.1.4 4.4 Verify below settings are correct for your platforms

PMC PciCfgSpace is not PCI compliant.FSP will hide the PMC controller to avoid external software or OS from corrupting the BAR addresses. FSP will program the PMC controller IO and MMIO BAR's with below addresses. Please use this addrerss in the wrapper code instead of reading from PMC controller.

Register	Values ----—
ABASE	0x1800
PWRMBASE	0xFE000000
PCIEXBAR_BASE_ADDRESS	0xE0000000

Note

:

- Boot Loader can use different value for PCIEXBAR_BASE_ADDRESS either by modifying the UPD (under FSP-T) or by overriding the PCIEXBAR (B0:D0:F0:R60h) before calling FspMemoryInit Api.
- Boot Loader should avoid using conflicting address when reprogramming PCIEXBAR_BASE_ADDRESS than the recommended one.

4.1.5 4.5 FSP_STATUS_RESET_REQUIRED

As per FSP External Architecture Specification version 2.0, Any reset required in the FSP flow will be reported as return status FSP_STATUS_RESET_REQUIREDx by the API.It is the bootloader responsibility to reset the system according to the reset type requested.

Below table specifies the return status returned by FSP API and the requested reset type.

FSP_STATUS_RESET_REQUIRED Code	Reset Type requested
0x40000001	Cold Reset
0x40000002	Warm Reset
0x40000003	Global Reset - Puts the system to Global reset through Heci or Full Reset through PCH
0x40000004	Reserved
0x40000005	Reserved
0x40000006	Reserved
0x40000007	Reserved
0x40000008	Reserved

Chapter 5

UPD PORTING GUIDE

5.1 5 UPD porting guide

UPD porting guide for recommendation values:

UPD	Dependency	Description	Value
CstateLatencyControl1Irtl	Server platform	Server platform should has different setting	0x6B
PchPcieHsioRxSetCtleEnable	Board design	Different board requires different value	tune
PchPcieHsioRxSetCtle	Board design	Different board requires different value	tune
PchSataHsioRxGen3EqBoostMag↩ Enable	Board design	Different board requires different value	tune
PchSataHsioRxGen3EqBoostMag	Board design	Different board requires different value	tune
PchSataHsioTxGen1DownscaleAmp↩ Enable	Board design	Different board requires different value	tune
PchSataHsioTxGen1DownscaleAmp	Board design	Different board requires different value	tune
PchSataHsioTxGen2DownscaleAmp↩ Enable	Board design	Different board requires different value	tune
PchSataHsioTxGen2DownscaleAmp	Board design	Different board requires different value	tune
PchNumRsvdSmbusAddresses	Board design	Different board requires different value	tune
RsvdSmbusAddressTablePtr	Board design	Different board requires different value	tune
BiosSize	Board design	Different board requires different value	tune

Chapter 6

FSP OUTPUT

6.1 6 FSP Output

The FSP builds a series of data structures called the Hand-Off-Blocks (HOBs) as it progresses through initializing the silicon.

Please refer to the Platform Initialization (PI) Specification - Volume 3: Shared Architectural Elements specification for PI Architectural HOBs. Please refer Chapter 9 in the FSP External Architecture Specification version 2.0 for details about FSP Architectural HOBs.

Below section describe the HOBs not covered in the above two specifications.

6.1.1 6.1 SMRAM Resource Descriptor HOB

The FSP will report the system SMRAM T-SEG range through a generic resource HOB if T-SEG is enabled. The owner field of the HOB identifies the owner as T-SEG.

```
#define FSP_HOB_RESOURCE_OWNER_TSEG_GUID  \
{ 0xd038747c, 0xd00c, 0x4980, { 0xb3, 0x19, 0x49, 0x01, 0x99, 0xa4, 0x7d, 0x55 } }
```

6.1.2 6.2 SMBIOS INFO HOB

The FSP will report the SMBIOS through a HOB with below GUID. This information can be consumed by the bootloader to produce the SMBIOS tables. These structures are included as part of MemInfoHob.h , SmbiosCacheInfoHob.h, SmbiosProcessorInfoHob.h & FirmwareVersionInfoHob.h

```
#define SI_MEMORY_INFO_DATA_HOB_GUID \
{ 0x9b2071d4, 0xb054, 0x4e0c, { 0x8d, 0x09, 0x11, 0xcf, 0x8b, 0x9f, 0x03, 0x23 } };

typedef struct {
  MrcDimmStatus Status;                     ///< See MrcDimmStatus for the definition of this field.
  UINT8         DimmId;
  UINT32        DimmCapacity;               ///< DIMM size in MBytes.
  UINT16        MfgId;
  UINT8         ModulePartNum[20];          ///< Module part number for DDR3 is 18 bytes however for DRR4
       20 bytes as per JEDEC Spec, so reserving 20 bytes
  UINT8         RankInDimm;                 ///< The number of ranks in this DIMM.
  UINT8         SpdDramDeviceType;          ///< Save SPD DramDeviceType information needed for SMBIOS
       structure creation.
  UINT8         SpdModuleType;              ///< Save SPD ModuleType information needed for SMBIOS
       structure creation.
  UINT8         SpdModuleMemoryBusWidth;    ///< Save SPD ModuleMemoryBusWidth information needed for
       SMBIOS structure creation.
  UINT8         SpdSave[MAX_SPD_SAVE_DATA]; ///< Save SPD Manufacturing information needed for SMBIOS
       structure creation.
} DIMM_INFO;

typedef struct {
  UINT8         Status;                     ///< Indicates whether this channel should be used.
  UINT8         ChannelId;
  UINT8         DimmCount;                  ///< Number of valid DIMMs that exist in the channel.
  MRC_CH_TIMING Timing[MAX_PROFILE];        ///< The channel timing values.
  DIMM_INFO     Dimm[MAX_DIMM];             ///< Save the DIMM output characteristics.
} CHANNEL_INFO;

typedef struct {
  UINT8            Status;                  ///< Indicates whether this controller should be used.
  UINT16           DeviceId;                ///< The PCI device id of this memory controller.
  UINT8            RevisionId;              ///< The PCI revision id of this memory controller.
  UINT8            ChannelCount;            ///< Number of valid channels that exist on the controller.
  CHANNEL_INFO     Channel[MAX_CH];         ///< The following are channel level definitions.
} CONTROLLER_INFO;

typedef struct {
  EFI_HOB_GUID_TYPE EfiHobGuidType;
  UINT8             Revision;
  UINT16            DataWidth;
  /// As defined in SMBIOS 3.0 spec
  /// Section 7.18.2 and Table 75
  UINT8             DdrType;                ///< DDR type: DDR3, DDR4, or LPDDR3
  UINT32            Frequency;              ///< The system's common memory controller frequency in MT/s.
  /// As defined in SMBIOS 3.0 spec
  /// Section 7.17.3 and Table 72
  UINT8             ErrorCorrectionType;

  SiMrcVersion      Version;
  UINT32            FreqMax;
  BOOLEAN           EccSupport;
  UINT8             MemoryProfile;
  UINT32            TotalPhysicalMemorySize;
  BOOLEAN           XmpProfileEnable;
  UINT8             Ratio;
  UINT8             RefClk;
  UINT32            VddVoltage[MAX_PROFILE];
  CONTROLLER_INFO   Controller[MAX_NODE];
} MEMORY_INFO_DATA_HOB;

#define  SI_MEMORY_PLATFORM_DATA_HOB \
  { 0x6210d62f, 0x418d, 0x4999, { 0xa2, 0x45, 0x22, 0x10, 0x0a, 0x5d, 0xea, 0x44 } }

typedef struct {
  UINT8             Revision;
  UINT8             Reserved[3];
  UINT32            BootMode;
  UINT32            TsegSize;
  UINT32            TsegBase;
  UINT32            PrmrrSize;
  UINT32            PrmrrBase;
  UINT32            GttBase;
  UINT32            MmioSize;
  UINT32            PciEBaseAddress;
} MEMORY_PLATFORM_DATA;

typedef struct {
  EFI_HOB_GUID_TYPE    EfiHobGuidType;
  MEMORY_PLATFORM_DATA Data;
  UINT8                *Buffer;
} MEMORY_PLATFORM_DATA_HOB;

#define SMBIOS_CACHE_INFO_HOB_GUID \
 { 0xd805b74e, 0x1460, 0x4755, {0xbb, 0x36, 0x1e, 0x8c, 0x8a, 0xd6, 0x78, 0xd7} }

///
/// SMBIOS Cache Info HOB Structure
///
typedef struct {
  UINT16     ProcessorSocketNumber;
  UINT16     NumberOfCacheLevels;         ///< Based on Number of Cache Types L1/L2/L3
  UINT8      SocketDesignationStrIndex;   ///< String Index in the string Buffer. Example "L1-CACHE"
  UINT16     CacheConfiguration;          ///< Format defined in SMBIOS Spec v3.0 Section7.8 Table36
  UINT16     MaxCacheSize;                ///< Format defined in SMBIOS Spec v3.0 Section7.8.1
  UINT16     InstalledSize;               ///< Format defined in SMBIOS Spec v3.0 Section7.8.1
  UINT16     SupportedSramType;           ///< Format defined in SMBIOS Spec v3.0 Section7.8.2
  UINT16     CurrentSramType;             ///< Format defined in SMBIOS Spec v3.0 Section7.8.2
  UINT8      CacheSpeed;                  ///< Cache Speed in nanoseconds. 0 if speed is unknown.
  UINT8      ErrorCorrectionType;         ///< ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.3
  UINT8      SystemCacheType;             ///< ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.4
  UINT8      Associativity;               ///< ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.5
  ///String Buffer - each string terminated by NULL "0x00"
  ///String buffer terminated by double NULL "0x0000"
} SMBIOS_CACHE_INFO;

#define SMBIOS_PROCESSOR_INFO_HOB_GUID \
  { 0xe6d73d92, 0xff56, 0x4146, {0xaf, 0xac, 0x1c, 0x18, 0x81, 0x7d, 0x68, 0x71} }

///
/// SMBIOS Processor Info HOB Structure
///
typedef struct {
  UINT16     TotalNumberOfSockets;
  UINT16     CurrentSocketNumber;
  UINT8      ProcessorType;                 ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.1
  ///This info is used for both ProcessorFamily and ProcessorFamily2 fields
  ///See ENUM defined in SMBIOS Spec v3.0 Section 7.5.2
  UINT16     ProcessorFamily;
  UINT8      ProcessorManufacturerStrIndex; ///< Index of the String in the String Buffer
  UINT64     ProcessorId;                   ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.3
  UINT8      ProcessorVersionStrIndex;      ///< Index of the String in the String Buffer
  UINT8      Voltage;                       ///< Format defined in SMBIOS Spec v3.0 Section 7.5.4
  UINT16     ExternalClockInMHz;            ///< External Clock Frequency. Set to 0 if unknown.
  UINT16     CurrentSpeedInMHz;             ///< Snapshot of current processor speed during boot
  UINT8      Status;                        ///< Format defined in the SMBIOS Spec v3.0 Table 21
  UINT8      ProcessorUpgrade;              ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.5
  ///This info is used for both CoreCount & CoreCount2 fields
  /// See detailed description in SMBIOS Spec v3.0 Section 7.5.6
  UINT16     CoreCount;
  ///This info is used for both CoreEnabled & CoreEnabled2 fields
  ///See detailed description in SMBIOS Spec v3.0 Section 7.5.7
  UINT16     EnabledCoreCount;
  ///This info is used for both ThreadCount & ThreadCount2 fields
  /// See detailed description in SMBIOS Spec v3.0 Section 7.5.8
  UINT16     ThreadCount;
  UINT16     ProcessorCharacteristics;      ///< Format defined in SMBIOS Spec v3.0 Section 7.5.9
  /// String Buffer - each string terminated by NULL "0x00"
  /// String buffer terminated by double NULL "0x0000"
} SMBIOS_PROCESSOR_INFO;

#define SMBIOS_FIRMWARE_VERSION_INFO_HOB_GUID \
  { 0x798e722e, 0x15b2, 0x4e13, { 0x8a, 0xe9, 0x6b, 0xa3, 0x0f, 0xf7, 0xf1, 0x67 }}

///
/// Firmware Version Structure
///
typedef struct {
  UINT8                          MajorVersion;
  UINT8                          MinorVersion;
  UINT8                          Revision;
  UINT16                         BuildNumber;
} FIRMWARE_VERSION;

///
/// Firmware Version Information Structure
///
typedef struct {
  UINT8                          ComponentNameIndex;        ///< Offset 0   Index of Component Name
  UINT8                          VersionStringIndex;        ///< Offset 1   Index of Version String
  FIRMWARE_VERSION               Version;                   ///< Offset 2-6 Firmware version
} FIRMWARE_VERSION_INFO;

///
/// The Smbios structure header.
///
typedef struct {
  UINT8                          Type;
  UINT8                          Length;
  UINT16                         Handle;
} SMBIOS_STRUCTURE;

///
/// Firmware Version Information HOB Structure
///
typedef struct {
  EFI_HOB_GUID_TYPE              Header;                    ///< Offset 0-23  The header of FVI HOB
  SMBIOS_STRUCTURE               SmbiosData;                ///< Offset 24-27  The SMBIOS header of FVI HOB
  UINT8                          Count;                     ///< Offset 28    Number of FVI elements
       included.
///
/// FIRMWARE_VERSION_INFO structures followed by the null terminated string buffer
///
} FIRMWARE_VERSION_INFO_HOB;
```

6.1.3 6.3 CHIPSETINIT INFO HOB

The FSP will report the ChipsetInit CRC through a HOB with below GUID. This information can be consumed by the bootloader to check if ChipsetInit CRC is matched between BIOS and ME. These structures are included as part of FspsUpd.h

```
#define CHIPSETINIT_INFO_HOB_GUID \
{ 0xc1392859, 0x1f65, 0x446e, { 0xb3, 0xf5, 0x84, 0x35, 0xfc, 0xc7, 0xd1, 0xc4 }}

///
/// The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.
///
typedef struct {
  UINT8             Revision;
  UINT8             Rsvd[3];
  UINT16            MeChipInitCrc;
  UINT16            BiosChipInitCrc;
} CHIPSET_INIT_INFO;
```

6.1.4 6.4 HOB USAGE INFO HOB

The FSP will report the Hob memory usage through a HOB with below GUID. This information can be consumed by the bootloader to check how many the temporary ram left.

```
#define HOB_USAGE_DATA_HOB_GUID \
{0xc764a821, 0xec41, 0x450d, { 0x9c, 0x99, 0x27, 0x20, 0xfc, 0x7c, 0xe1, 0xf6 }}

typedef struct {
  EFI_PHYSICAL_ADDRESS EfiMemoryTop;
  EFI_PHYSICAL_ADDRESS EfiMemoryBottom;
  EFI_PHYSICAL_ADDRESS EfiFreeMemoryTop;
  EFI_PHYSICAL_ADDRESS EfiFreeMemoryBottom;
  UINTN                FreeMemory;
} HOB_USAGE_DATA_HOB;
```

6.1.5 6.5 FSP_ERROR_INFO_HOB

In the case of an error occurring during the execution of the FSP, the FSP may produce this HOB which describes the error in more detail.

```
#define FSP_ERROR_INFO_HOB_GUID \
{0x611e6a88, 0xadb7, 0x4301, { 0x93, 0xff, 0xe4, 0x73, 0x04, 0xb4, 0x3d, 0xa6 }}

typedef struct {
  EFI_HOB_GUID_TYPE     GuidHob;
  EFI_STATUS_CODE_TYPE  Type;
  EFI_STATUS_CODE_VALUE Value;
  UINT32                Instance;
  EFI_GUID              CallerId;
  EFI_GUID              ErrorType;
  UINT32                Status;
} FSP_ERROR_INFO_HOB;

  Implemented CallerId                                                          | Description
  ------------------------------------------------------------------------------|------------------
  {0x1f4dc7e9, 0x26ca, 0x4336, {0x8c, 0xe3, 0x39, 0x31, 0x03, 0xb5, 0xf3, 0xd7}}| ME
  {0x98230916, 0xe632, 0x49ff, {0x81, 0x81, 0x55, 0xce, 0xe5, 0x10, 0x36, 0x89}}| System Agent
  {0x5a47c211, 0x642f, 0x4f92, {0x9c, 0xb3, 0x7f, 0xeb, 0x93, 0xda, 0xdd, 0xba}}| MRC


  Implemented ErrorType                                                         | Description
  ------------------------------------------------------------------------------|------------------
  {0x948585c4, 0x76a4, 0x45bb, {0xbe, 0x6c, 0x39, 0x61, 0xc3, 0xab, 0xde, 0x15}}|ME EOP failure
  {0x8106a5cc, 0x30ba, 0x41cf, {0xa1, 0x78, 0x63, 0x38, 0x91, 0x11, 0xae, 0xb2}}|SA PEI GOP Init failure
  {0x348cc7fe, 0x1e9a, 0x4c7a, {0x86, 0x28, 0xae, 0x48, 0x5b, 0x42, 0x10, 0xf0}}|SA PEI GOP GetMode failure
  {0x5de1c071, 0x2c9c, 0x4a53, {0x80, 0x21, 0x4e, 0x80, 0xd2, 0x5d, 0x44, 0xa8}}|MRC training failure
```

Chapter 7

FSP POSTCODE

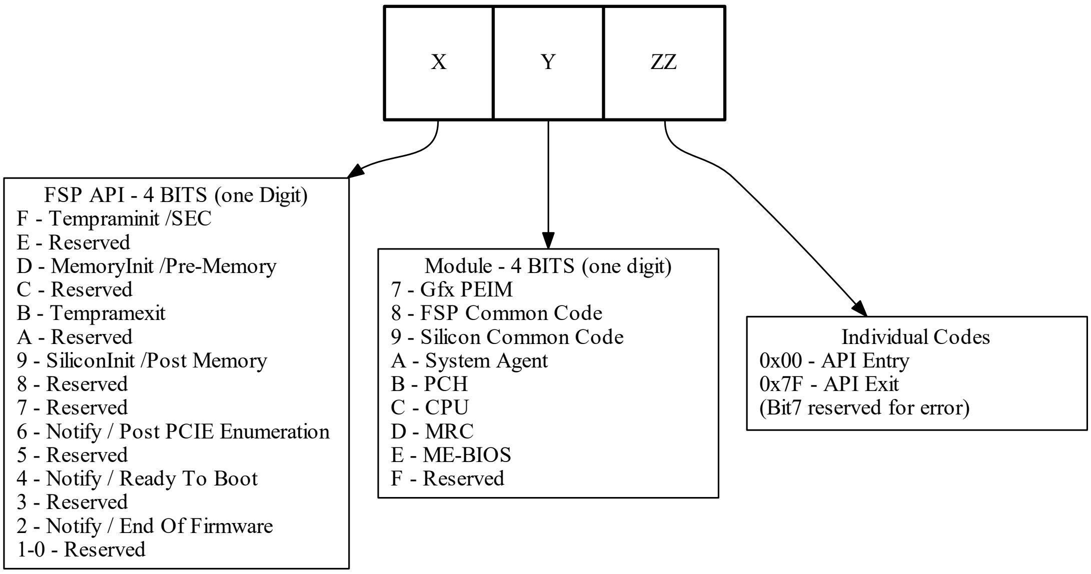
7.1 7 FSP PostCode

The FSP outputs 16 bit postcode to indicate which API and in which module the execution is happening.

Bit Range	Description
Bit15 - Bit12 (X)	used to indicate the phase/api under which the code is executing
Bit11 - Bit8 (Y)	used to indicate the module
Bit7 (ZZ bit 7)	reserved for error
Bit6 - Bit0 (ZZ)	individual codes

7.1.1 7.1 PostCode Info

Below diagram represents the 16 bit PostCode usage in FSP.



7.1.1.1 7.1.1 TempRamInit API Status Codes (0xFxxx)

PostCode	Module	Description -—
0x0000	FSP	TempRamInit API Entry (The change in upper byte is due to not enabling of the Port81 early in the boot)
0x007F	FSP	TempRamInit API Exit

7.1.1.2 7.1.2 FspMemoryInit API Status Codes (0xDxxx)

PostCode	Module	Description -—
0xD800	FSP	FspMemoryInit API Entry
0xD87F	FSP	FSpMemoryInit API Exit
0xDA00	SA	Pre-Mem SaInit Entry
0xDA02	SA	OverrideDev0Did Start
0xDA04	SA	OverrideDev2Did Start
0xDA06	SA	Programming SA Bars
0xDA08	SA	Install SA HOBs
0xDA0A	SA	Reporting SA PCIe code version
0xDA0C	SA	SaSvInit Start
0xDA10	SA	Initializing DMI
0xDA15	SA	Initialize TCSS PreMem
0xDA1F	SA	Initializing DMI/OPI Max PayLoad Size
0xDA20	SA	Initializing SwitchableGraphics
0xDA30	SA	Initializing SA PCIe
0xDA3F	SA	Programming PEG credit values Start
0xDA40	SA	Initializing DMI Tc/Vc mapping
0xDA42	SA	CheckOffboardPcieVga
0xDA44	SA	CheckAndInitializePegVga
0xDA50	SA	Initializing Graphics
0xDA52	SA	Initializing System Agent Overclocking
0xDA7F	SA	Pre-Mem SaInit Exit
0xDB00	PCH	Pre-Mem PchInit Entry
0xDB02	PCH	Pre-Mem Disable PCH fused controllers
0xDB15	PCH	Pre-Mem SMBUS configuration
0xDB48	PCH	Pre-Mem PchOnPolicyInstalled Entry
0xDB49	PCH	Pre-Mem Program HSIO
0xDB4A	PCH	Pre-Mem DCI configuration
0xDB4C	PCH	Pre-Mem Host DCI enabled
0xDB4D	PCH	Pre-Mem Trace Hub - Early configuration
0xDB4E	PCH	Pre-Mem Trace Hub - Device disabled
0xDB4F	PCH	Pre-Mem TraceHub - Programming MSR
0xDB50	PCH	Pre-Mem Trace Hub - Power gating configuration
0xDB51	PCH	Pre-Mem Trace Hub - Power gating Trace Hub device and locking HSWPGCR1 register
0xDB52	PCH	Pre-Mem Initialize HPET timer
0xDB55	PCH	Pre-Mem PchOnPolicyInstalled Exit
0xDB7F	PCH	Pre-Mem PchInit Exit
0xDC00	CPU	CPU Pre-Mem Entry
0xDC0F	CPU	CpuAddPreMemConfigBlocks Done
0xDC20	CPU	CpuOnPolicyInstalled Start

PostCode	Module	Description -—
0xDC2F	CPU	XmmInit Start
0xDC3F	CPU	TxtInit Start
0xDC4F	CPU	Init CPU Straps
0xDC5F	CPU	Init Overclocking
0xDC6F	CPU	CPU Pre-Mem Exit
0x∗∗55	SA	MRC_MEM_INIT_DONE
0x∗∗D5	SA	MRC_MEM_INIT_DONE_WITH_ERRORS
0xDD00	SA	MRC_INITIALIZATION_START
0xDD10	SA	MRC_CMD_PLOT_2D
0xDD1B	SA	MRC_FAST_BOOT_PERMITTED
0xDD1C	SA	MRC_RESTORE_NON_TRAINING
0xDD1D	SA	MRC_PRINT_INPUT_PARAMS
0xDD1E	SA	MRC_SET_OVERRIDES_PSPD
0xDD20	SA	MRC_SPD_PROCESSING
0xDD21	SA	MRC_SET_OVERRIDES
0xDD22	SA	MRC_MC_CAPABILITY
0xDD23	SA	MRC_MC_CONFIG
0xDD24	SA	MRC_MC_MEMORY_MAP
0xDD25	SA	MRC_JEDEC_INIT_LPDDR3
0xDD26	SA	MRC_RESET_SEQUENCE
0xDD27	SA	MRC_PRE_TRAINING
0xDD28	SA	MRC_EARLY_COMMAND
0xDD29	SA	MRC_SENSE_AMP_OFFSET
0xDD2A	SA	MRC_READ_MPR
0xDD2B	SA	MRC_RECEIVE_ENABLE
0xDD2C	SA	MRC_JEDEC_WRITE_LEVELING
0xDD2D	SA	MRC_LPDDR_LATENCY_SET_B
0xDD2E	SA	MRC_WRITE_TIMING_1D
0xDD2F	SA	MRC_READ_TIMING_1D
0xDD30	SA	MRC_DIMM_ODT
0xDD31	SA	MRC_EARLY_WRITE_TIMING_2D
0xDD32	SA	MRC_WRITE_DS
0xDD33	SA	MRC_WRITE_EQ
0xDD34	SA	MRC_EARLY_READ_TIMING_2D
0xDD35	SA	MRC_READ_ODT
0xDD36	SA	MRC_READ_EQ
0xDD37	SA	MRC_READ_AMP_POWER
0xDD38	SA	MRC_WRITE_TIMING_2D
0xDD39	SA	MRC_READ_TIMING_2D
0xDD3A	SA	MRC_CMD_VREF
0xDD3B	SA	MRC_WRITE_VREF_2D
0xDD3C	SA	MRC_READ_VREF_2D
0xDD3D	SA	MRC_POST_TRAINING
0xDD3E	SA	MRC_LATE_COMMAND
0xDD3F	SA	MRC_ROUND_TRIP_LAT
0xDD40	SA	MRC_TURN_AROUND
0xDD41	SA	MRC_CMP_OPT
0xDD42	SA	MRC_SAVE_MC_VALUES
0xDD43	SA	MRC_RESTORE_TRAINING
0xDD44	SA	MRC_RMT_TOOL
0xDD45	SA	MRC_WRITE_SR

PostCode	Module	Description -—
0xDD46	SA	MRC_DIMM_RON
0xDD47	SA	MRC_RCVEN_TIMING_1D
0xDD48	SA	MRC_MR_FILL
0xDD49	SA	MRC_PWR_MTR
0xDD4A	SA	MRC_DDR4_MAPPING
0xDD4B	SA	MRC_WRITE_VOLTAGE_1D
0xDD4C	SA	MRC_EARLY_RDMPR_TIMING_2D
0xDD4D	SA	MRC_FORCE_OLTM
0xDD50	SA	MRC_MC_ACTIVATE
0xDD51	SA	MRC_RH_PREVENTION
0xDD52	SA	MRC_GET_MRC_DATA
0xDD53	SA	Reserved
0xDD58	SA	MRC_RETRAIN_CHECK
0xDD5A	SA	MRC_SA_GV_SWITCH
0xDD5B	SA	MRC_ALIAS_CHECK
0xDD5C	SA	MRC_ECC_CLEAN_START
0xDD5D	SA	MRC_DONE
0xDD5F	SA	MRC_CPGC_MEMORY_TEST
0xDD60	SA	MRC_TXT_ALIAS_CHECK
0xDD61	SA	MRC_ENG_PERF_GAIN
0xDD68	SA	MRC_MEMORY_TEST
0xDD69	SA	MRC_FILL_RMT_STRUCTURE
0xDD70	SA	MRC_SELF_REFRESH_EXIT
0xDD71	SA	MRC_NORMAL_MODE
0xDD7D	SA	MRC_SSA_PRE_STOP_POINT
0xDD7F	SA	MRC_SSA_STOP_POINT, MRC_INITIALIZATION_END
0xDD90	SA	MRC_CMD_PLOT_2D_ERROR
0xDD9B	SA	MRC_FAST_BOOT_PERMITTED_ERROR
0xDD9C	SA	MRC_RESTORE_NON_TRAINING_ERROR
0xDD9D	SA	MRC_PRINT_INPUT_PARAMS_ERROR
0xDD9E	SA	MRC_SET_OVERRIDES_PSPD_ERROR
0xDDA0	SA	MRC_SPD_PROCESSING_ERROR
0xDDA1	SA	MRC_SET_OVERRIDES_ERROR
0xDDA2	SA	MRC_MC_CAPABILITY_ERROR
0xDDA3	SA	MRC_MC_CONFIG_ERROR
0xDDA4	SA	MRC_MC_MEMORY_MAP_ERROR
0xDDA5	SA	MRC_JEDEC_INIT_LPDDR3_ERROR
0xDDA6	SA	MRC_RESET_ERROR
0xDDA7	SA	MRC_PRE_TRAINING_ERROR
0xDDA8	SA	MRC_EARLY_COMMAND_ERROR
0xDDA9	SA	MRC_SENSE_AMP_OFFSET_ERROR
0xDDAA	SA	MRC_READ_MPR_ERROR
0xDDAB	SA	MRC_RECEIVE_ENABLE_ERROR
0xDDAC	SA	MRC_JEDEC_WRITE_LEVELING_ERROR
0xDDAD	SA	MRC_LPDDR_LATENCY_SET_B_ERROR
0xDDAE	SA	MRC_WRITE_TIMING_1D_ERROR
0xDDAF	SA	MRC_READ_TIMING_1D_ERROR
0xDDB0	SA	MRC_DIMM_ODT_ERROR
0xDDB1	SA	MRC_EARLY_WRITE_TIMING_ERROR
0xDDB2	SA	MRC_WRITE_DS_ERROR
0xDDB3	SA	MRC_WRITE_EQ_ERROR

PostCode	Module	Description -—
0xDDB4	SA	MRC_EARLY_READ_TIMING_ERROR
0xDDB5	SA	MRC_READ_ODT_ERROR
0xDDB6	SA	MRC_READ_EQ_ERROR
0xDDB7	SA	MRC_READ_AMP_POWER_ERROR
0xDDB8	SA	MRC_WRITE_TIMING_2D_ERROR
0xDDB9	SA	MRC_READ_TIMING_2D_ERROR
0xDDBA	SA	MRC_CMD_VREF_ERROR
0xDDBB	SA	MRC_WRITE_VREF_2D_ERROR
0xDDBC	SA	MRC_READ_VREF_2D_ERROR
0xDDBD	SA	MRC_POST_TRAINING_ERROR
0xDDBE	SA	MRC_LATE_COMMAND_ERROR
0xDDBF	SA	MRC_ROUND_TRIP_LAT_ERROR
0xDDC0	SA	MRC_TURN_AROUND_ERROR
0xDDC1	SA	MRC_CMP_OPT_ERROR
0xDDC2	SA	MRC_SAVE_MC_VALUES_ERROR
0xDDC3	SA	MRC_RESTORE_TRAINING_ERROR
0xDDC4	SA	MRC_RMT_TOOL_ERROR
0xDDC5	SA	MRC_WRITE_SR_ERROR
0xDDC6	SA	MRC_DIMM_RON_ERROR
0xDDC7	SA	MRC_RCVEN_TIMING_1D_ERROR
0xDDC8	SA	MRC_MR_FILL_ERROR
0xDDC9	SA	MRC_PWR_MTR_ERROR
0xDDCA	SA	MRC_DDR4_MAPPING_ERROR
0xDDCB	SA	MRC_WRITE_VOLTAGE_1D_ERROR
0xDDCC	SA	MRC_EARLY_RDMPR_TIMING_2D_ERROR
0xDDCD	SA	MRC_FORCE_OLTM_ERROR
0xDDD0	SA	MRC_MC_ACTIVATE_ERROR
0xDDD1	SA	MRC_RH_PREVENTION_ERROR
0xDDD2	SA	MRC_GET_MRC_DATA_ERROR
0xDDD3	SA	Reserved
0xDDD8	SA	MRC_RETRAIN_CHECK_ERROR
0xDDDA	SA	MRC_SA_GV_SWITCH_ERROR
0xDDDB	SA	MRC_ALIAS_CHECK_ERROR
0xDDDC	SA	MRC_ECC_CLEAN_ERROR
0xDDDD	SA	MRC_DONE_WITH_ERROR
0xDDDF	SA	MRC_CPGC_MEMORY_TEST_ERROR
0xDDE0	SA	MRC_TXT_ALIAS_CHECK_ERROR
0xDDE1	SA	MRC_ENG_PERF_GAIN_ERROR
0xDDE8	SA	MRC_MEMORY_TEST_ERROR
0xDDE9	SA	MRC_FILL_RMT_STRUCTURE_ERROR
0xDDF0	SA	MRC_SELF_REFRESH_EXIT_ERROR
0xDDF1	SA	MRC_MRC_NORMAL_MODE_ERROR
0xDDFD	SA	MRC_SSA_PRE_STOP_POINT_ERROR
0xDDFE	SA	MRC_NO_MEMORY_DETECTED

7.1.1.3 7.1.3 TempRamExit API Status Codes (0xBxxx)

PostCode	Module	Description -—
0xB800	FSP	TempRamExit API Entry
0xB87F	FSP	TempRamExit API Exit

7.1.1.4 7.1.4 FspSiliconInit API Status Codes (0x9xxx)

PostCode	Module	Description -—
0x9800	FSP	FspSiliconInit API Entry
0x987F	FSP	FspSiliconInit API Exit
0x9A00	SA	PostMem SaInit Entry
0x9A01	SA	DeviceConfigure Start
0x9A02	SA	UpdateSaHobPostMem Start
0x9A03	SA	Initializing Pei Display
0x9A04	SA	PeiGraphicsNotifyCallback Entry
0x9A05	SA	CallPpiAndFillFrameBuffer
0x9A06	SA	GraphicsPpiInit
0x9A07	SA	GraphicsPpiGetMode
0x9A08	SA	FillFrameBufferAndShowLogo
0x9A0F	SA	PeiGraphicsNotifyCallback Exit
0x9A14	SA	Initializing SA IPU device
0x9A16	SA	Initializing SA GNA device
0x9A1A	SA	SaProgramLlcWays Start
0x9A20	SA	Initializing PciExpressInitPostMem
0x9A22	SA	Initializing ConfigureNorthIntelTraceHub
0x9A30	SA	Initializing Vtd
0x9A31	SA	Initializing TCSS
0x9A32	SA	Initializing Pavp
0x9A34	SA	PeiInstallSmmAccessPpi Start
0x9A36	SA	EdramWa Start
0x9A4F	SA	Post-Mem SaInit Exit
0x9A50	SA	SaSecurityLock Start
0x9A5F	SA	SaSecurityLock End
0x9A60	SA	SaSResetComplete Entry
0x9A61	SA	Set BIOS_RESET_CPL to indicate all configurations complete
0x9A62	SA	SaSvInit2 Start
0x9A63	SA	GraphicsPmInit Start
0x9A64	SA	SaPciPrint Start
0x9A6F	SA	SaSResetComplete Exit
0x9A70	SA	SaS3ResumeAtEndOfPei Callback Entry
0x9A7F	SA	SaS3ResumeAtEndOfPei Callback Exit
0x9B00	PCH	Post-Mem PchInit Entry
0x9B03	PCH	Post-Mem Tune the USB 2.0 high-speed signals quality
0x9B04	PCH	Post-Mem Tune the USB 3.0 signals quality
0x9B05	PCH	Post-Mem Configure PCH xHCI
0x9B06	PCH	Post-Mem Performs configuration of PCH xHCI SSIC
0x9B07	PCH	Post-Mem Configure PCH xHCI after init
0x9B08	PCH	Post-Mem Configures PCH USB device (xDCI)
0x9B0A	PCH	Post-Mem DMI/OP-DMI configuration
0x9B0B	PCH	Post-Mem Initialize P2SB controller
0x9B0C	PCH	Post-Mem IOAPIC initialization
0x9B0D	PCH	Post-Mem PCH devices interrupt configuration
0x9B0E	PCH	Post-Mem HD Audio initizalization
0x9B0F	PCH	Post-Mem HD Audio Codec enumeration
0x9B10	PCH	Post-Mem HD Audio Codec not detected

PostCode	Module	Description -—
0x9B13	PCH	Post-Mem SCS initizalization
0x9B14	PCH	Post-Mem ISH initizalization
0x9B15	PCH	Post-Mem Configure SMBUS power management
0x9B16	PCH	Post-Mem Reserved
0x9B17	PCH	Post-Mem Performing global reset
0x9B18	PCH	Post-Mem Reserved
0x9B19	PCH	Post-Mem Reserved
0x9B40	PCH	Post-Mem OnEndOfPEI Entry
0x9B41	PCH	Post-Mem Initialize Thermal controller
0x9B42	PCH	Post-Mem Configure Memory Throttling
0x9B47	PCH	Post-Mem OnEndOfPEI Exit
0x9B4D	PCH	Post-Mem Trace Hub - Memory configuration
0x9B4E	PCH	Post-Mem Trace Hub - MSC0 configured
0x9B4F	PCH	Post-Mem Trace Hub - MSC1 configured
0x9B7F	PCH	Post-Mem PchInit Exit
0x9C00	CPU	CPU Post-Mem Entry
0x9C09	CPU	CpuAddConfigBlocks Done
0x9C0A	CPU	SetCpuStrapAndEarlyPowerOnConfig Start
0x9C13	CPU	SetCpuStrapAndEarlyPowerOnConfig Reset
0x9C14	CPU	SetCpuStrapAndEarlyPowerOnConfig Done
0x9C15	CPU	CpuInit Start
0x9C16	CPU	SgxInitializationPrePatchLoad Start
0x9C17	CPU	CollectProcessorFeature Start
0x9C18	CPU	ProgramProcessorFeature Start
0x9C19	CPU	ProgramProcessorFeature Done
0x9C20	CPU	CpuInitPreResetCpl Start
0x9C21	CPU	ProcessorsPrefetcherInitialization Start
0x9C22	CPU	InitRatl Start
0x9C23	CPU	ConfigureSvidVrs Start
0x9C24	CPU	ConfigurePidSettings Start
0x9C25	CPU	SetBootFrequency Start
0x9C26	CPU	CpuOcInitPreMem Start
0x9C27	CPU	CpuOcInit Reset
0x9C28	CPU	BiosGuardInit Start
0x9C29	CPU	BiosGuardInit Reset
0x9C3F	CPU	CpuInitPreResetCpl Done
0x9C42	CPU	SgxActivation Start
0x9C43	CPU	InitializeCpuDataHob Start
0x9C44	CPU	InitializeCpuDataHob Done
0x9C4F	CPU	CpuInit Done
0x9C50	CPU	S3InitializeCpu Start
0x9C55	CPU	MpRendezvousProcedure Start
0x9C56	CPU	MpRendezvousProcedure Done
0x9C69	CPU	S3InitializeCpu Done
0x9C6A	CPU	CpuPowerMgmtInit Start
0x9C71	CPU	InitPpm
0x9C7F	CPU	CPU Post-Mem Exit
0x9C80	CPU	ReloadMicrocodePatch Start
0x9C81	CPU	ReloadMicrocodePatch Done

PostCode	Module	Description -—
0x9C82	CPU	ApSafePostMicrocodePatchInit Start
0x9C83	CPU	ApSafePostMicrocodePatchInit Done

7.1.1.5 7.1.5 NotifyPhase API Status Codes (0x6xxx)

PostCode	Module	Description -—
0x6800	FSP	NotifyPhase API Entry
0x687F	FSP	NotifyPhase API Exit

Chapter 8

FSP DISPATCH MODE

8.1 8 FSP Dispatch mode support

8.1.1 8.1 Integration notes

The FSP Dispatch mode is supported by this platform FSP. The capability can be checked by FSP_INFO_HEAD↩
ER->ImageAttribute[1] = 1 (FSP Binary supports Dispatch mode) In Dispatch mode FSP Binary will be dispatched as standard FV and shares same PPIs, HOBs, and DynamicEx PCDs from UEFI boot loader.

Below are some integration notes:

1. Since FSP Binary can be integrated into anywhere in flash, boot loader has to report FSP FV to PEI and DXE dispatcher following standard way so those PEIMs and DXE drivers inside FSP Binary can be dispatched.
2. FSP binary package will include a DSC file which contains all DynamicEx PCDs consuemd by FSP binary. Boot loader should incorporate the DSC and build those PCD into PCD database so same PCDs can be shared bewteen boot loader and FSP.
3. In Dispatch mode, boot loader should not make FSP API calls. TempRamInit API is supported in both API mode and Dispatch mode, but rest of the APIs (MemoryInitApi, TempRamExitApi and SiliconinitApi) should not be invoked.
4. Dispatch mode FSP contains x64 DXE drivers for NotifyPhase callbacks. No thunkcall from 32bits to 64bits anymore and boot loader should remove S3EndOfPeiNotify and FspWrapperNotifyDxe as they are not used.
5. EFI_PEI_CORE_FV_LOCATION_PPI should be installed by boot loader SEC core and pointed to FSP-M FV location so the PeiCore inside FSP can be invoked. If this PPI was not installed or no PeiCore can be found by the pointer, the PeiCore from BFV will be invoked.
6. Some EDK2 overrides may be required for Dispatch mode support, please refer to override folders in reference code or the override EDK2 gihub repo for detail.
7. FSPM_ARCH_CONFIG_PPI->NvsBufferPtr now is a cross build type (FSP Dispatch mode and EDK2 builds) policy for MRC S3 data pointer, boot loader or platform code has to install this PPI to report MRC S3 data (SA_MISC_PEI_PREMEM_CONFIG->S3DataPtr is obsolete).
8. Policy initialization Flow Changes:
   - PEIMs from FSP-M/FSP-S should be dispatched earlier to produce the *DefaultPolicyInit* PPIs. -> Bootloader consumes the *DefaultPolicyInit* PPIs produced by the FSP binary to create the policy PPIs with default settings. -> Bootloader then locates and updates the policy PPIs as needed. -> Bootloader installs the *PolicyReadyPpi* after policy updates are completed. This signals to the FSP that silicon initialization may proceed.

- Bootloader shall consume two PPIs produced by FSP binary to create policy PPIs with default settings. These PPIs are:
  - _PEI_PREMEM_SI_DEFAULT_POLICY_INIT_PPI
  - _PEI_SI_DEFAULT_POLICY_INIT_PPI
- The bootloader shall call the two functions below after the bootloader has completed any needed policy updates:
  - SiPreMemInstallPolicyReadyPpi()
  - SiInstallPolicyReadyPpi()

9. Debug message handling in dispatch mode:

   - Before the ReportStatusCode service is ready, a debug built FSP will send debug messages using the FSP-T UPD configuration (passed as FSP-T API input parameter). FSP-T is recommended to be used regardless FSP API mode or Dispatch mode.
   - Once the ReportStatusCode service is ready, a debug built FSP will send debug messages using the ReportStatusCode service.
   - It is recommended that bootloader register a StatusCode listener immediately after the ReportStatusCode service is ready. It is important to register this listener as soon as possible so that all debug messages sent by the FSP are captured.
   - Please refer to section 9.4.7 in the Intel(R) Firmware Support Package External Architecture Specification v2.1 for details about the ReportStatusCode debug message format.

Chapter 9

Todo List

Member FSP_S_RESTRICTED_CONFIG::PchPmTestPchClearPowerSts

ADD DESCRIPTION.

Chapter 10

Deprecated List

Member FSP_S_CONFIG::SkipMpInitDeprecated

SkipMpInit has been moved to FspmUpd $EN_DIS

Member FSP_S_TEST_CONFIG::DebugInterfaceEnable

Enable or Disable processor debug features; **0: Disable**; 1: Enable.

Member FSP_S_TEST_CONFIG::EnableItbmDriver

Intel Turbo Boost Max Technology 3.0 Driver **0: Disabled**; 1: Enabled $EN_DIS

Member SI_CONFIG::SkipPostBootSai

since revision 3

Chapter 11

Class Index

11.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

Chapter 12

File Index

12.1 File List

Here is a list of all documented files with brief descriptions:

Chapter 13

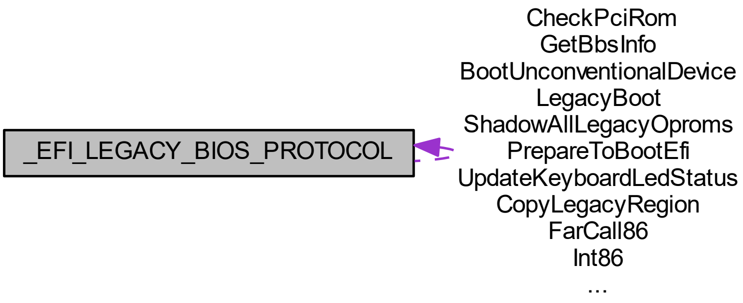
Class Documentation

13.1 _EFI_LEGACY_BIOS_PROTOCOL Struct Reference

Abstracts the traditional BIOS from the rest of EFI.

```
#include <LegacyBios.h>
```

Collaboration diagram for _EFI_LEGACY_BIOS_PROTOCOL:



Public Attributes

- EFI_LEGACY_BIOS_INT86 Int86

    Performs traditional software INT.

- EFI_LEGACY_BIOS_FARCALL86 FarCall86

    Performs a far call into Compatibility16 or traditional OpROM code.

- EFI_LEGACY_BIOS_CHECK_ROM CheckPciRom

    Checks if a traditional OpROM exists for this device.

- EFI_LEGACY_BIOS_INSTALL_ROM InstallPciRom

    Loads a traditional OpROM in traditional OpROM address space.

- EFI_LEGACY_BIOS_BOOT LegacyBoot

Boots a traditional OS.

- EFI_LEGACY_BIOS_UPDATE_KEYBOARD_LED_STATUS UpdateKeyboardLedStatus

  Updates BDA to reflect the current EFI keyboard LED status.
- EFI_LEGACY_BIOS_GET_BBS_INFO GetBbsInfo

  Allows an external agent, such as BIOS Setup, to get the BBS data.
- EFI_LEGACY_BIOS_SHADOW_ALL_LEGACY_OPROMS ShadowAllLegacyOproms

  Causes all legacy OpROMs to be shadowed.
- EFI_LEGACY_BIOS_PREPARE_TO_BOOT_EFI PrepareToBootEfi

  Performs all actions prior to boot.
- EFI_LEGACY_BIOS_GET_LEGACY_REGION GetLegacyRegion

  Allows EFI to reserve an area in the 0xE0000 or 0xF0000 block.
- EFI_LEGACY_BIOS_COPY_LEGACY_REGION CopyLegacyRegion

  Allows EFI to copy data to the area specified by GetLegacyRegion.
- EFI_LEGACY_BIOS_BOOT_UNCONVENTIONAL_DEVICE BootUnconventionalDevice

  Allows the user to boot off an unconventional device such as a PARTIES partition.

13.1.1 Detailed Description

Abstracts the traditional BIOS from the rest of EFI.

The LegacyBoot() member function allows the BDS to support booting a traditional OS. EFI thunks drivers that make EFI bindings for BIOS INT services use all the other member functions.

Definition at line 1458 of file LegacyBios.h.

13.1.2 Member Data Documentation

13.1.2.1 Int86

`EFI_LEGACY_BIOS_INT86 _EFI_LEGACY_BIOS_PROTOCOL::Int86`

Performs traditional software INT.

See the Int86() function description.

Definition at line 1462 of file LegacyBios.h.

13.1.2.2 PrepareToBootEfi

`EFI_LEGACY_BIOS_PREPARE_TO_BOOT_EFI _EFI_LEGACY_BIOS_PROTOCOL::PrepareToBootEfi`

Performs all actions prior to boot.

Used when booting an EFI-aware OS rather than a legacy OS.

Definition at line 1503 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.2 _EFI_SMM_VARIABLE_PROTOCOL Struct Reference

EFI SMM Variable Protocol is intended for use as a means to store data in the EFI SMM environment.

```
#include <SmmVariable.h>
```

13.2.1 Detailed Description

EFI SMM Variable Protocol is intended for use as a means to store data in the EFI SMM environment.

Definition at line 30 of file SmmVariable.h.

The documentation for this struct was generated from the following file:

- SmmVariable.h

13.3 _FSP_TEMP_RAM_EXIT_PPI Struct Reference

This PPI provides function to program MTRR values.

```
#include <TempRamExitPpi.h>
```

13.3.1 Detailed Description

This PPI provides function to program MTRR values.

Definition at line 63 of file TempRamExitPpi.h.

The documentation for this struct was generated from the following file:

- TempRamExitPpi.h

13.4 _PEI_PREMEM_SI_DEFAULT_POLICY_INIT_PPI Struct Reference

This PPI provides function to install default silicon policy.

```
#include <PeiPreMemSiDefaultPolicy.h>
```

13.4.1 Detailed Description

This PPI provides function to install default silicon policy.

Definition at line 55 of file PeiPreMemSiDefaultPolicy.h.

The documentation for this struct was generated from the following file:

- PeiPreMemSiDefaultPolicy.h

13.5 _PEI_SI_DEFAULT_POLICY_INIT_PPI Struct Reference

This PPI provides function to install default silicon policy.

```
#include <PeiSiDefaultPolicy.h>
```

13.5.1 Detailed Description

This PPI provides function to install default silicon policy.

Definition at line 55 of file PeiSiDefaultPolicy.h.

The documentation for this struct was generated from the following file:

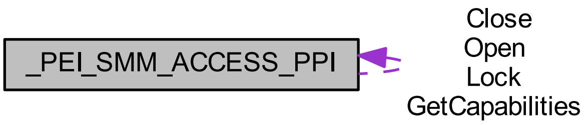
- PeiSiDefaultPolicy.h

13.6 _PEI_SMM_ACCESS_PPI Struct Reference

EFI SMM Access PPI is used to control the visibility of the SMRAM on the platform.

```
#include <SmmAccess.h>
```

Collaboration diagram for _PEI_SMM_ACCESS_PPI:



13.6.1 Detailed Description

EFI SMM Access PPI is used to control the visibility of the SMRAM on the platform.

It abstracts the location and characteristics of SMRAM. The expectation is that the north bridge or memory controller would publish this PPI.

Definition at line 134 of file SmmAccess.h.

The documentation for this struct was generated from the following file:

- SmmAccess.h

13.7 _PEI_SMM_CONTROL_PPI Struct Reference

PEI SMM Control PPI is used to initiate SMI/PMI activations.

```
#include <SmmControl.h>
```

Collaboration diagram for _PEI_SMM_CONTROL_PPI:

_PEI_SMM_CONTROL_PPI
Clear
Trigger

13.7.1 Detailed Description

PEI SMM Control PPI is used to initiate SMI/PMI activations.

This protocol could be published by either:

- A processor driver to abstract the SMI/PMI IPI
- The driver that abstracts the ASIC that is supporting the APM port, such as the ICH in an Intel chipset

Definition at line 89 of file SmmControl.h.

The documentation for this struct was generated from the following file:

- SmmControl.h

13.8 _SI_POLICY_STRUCT Struct Reference

SI Policy PPI
All SI config block change history will be listed here

.

```
#include <SiPolicyStruct.h>
```

13.8.1 Detailed Description

SI Policy PPI
All SI config block change history will be listed here

.

- **Revision 1**:
  - Initial version.

Definition at line 84 of file SiPolicyStruct.h.

The documentation for this struct was generated from the following file:

- SiPolicyStruct.h

13.9 _SI_PREMEM_POLICY_STRUCT Struct Reference

SI Policy PPI in Pre-Mem
All SI config block change history will be listed here

.

```
#include <SiPolicyStruct.h>
```

13.9.1 Detailed Description

SI Policy PPI in Pre-Mem
All SI config block change history will be listed here

.

- **Revision 1**:
  - Initial version.

Definition at line 70 of file SiPolicyStruct.h.

The documentation for this struct was generated from the following file:

- SiPolicyStruct.h

13.10 ATAPI_IDENTIFY Struct Reference

ATAPI_IDENTIFY.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 Raw [256]

  Raw data from the IDE IdentifyDrive command.

13.10.1 Detailed Description

ATAPI_IDENTIFY.

Definition at line 525 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

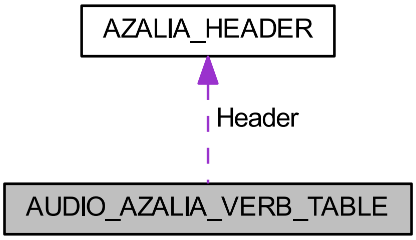
- LegacyBios.h

13.11 AUDIO_AZALIA_VERB_TABLE Struct Reference

Audio Azalia Verb Table structure.

```
#include <FspsUpd.h>
```

Collaboration diagram for AUDIO_AZALIA_VERB_TABLE:



Public Attributes

- AZALIA_HEADER Header

  AZALIA PCH header.
- UINT32 $*$ Data

  Pointer to the data buffer. Its length is specified in the header.

13.11.1 Detailed Description

Audio Azalia Verb Table structure.

Definition at line 56 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.12 AZALIA_HEADER Struct Reference

Azalia Header structure.

```
#include <FspsUpd.h>
```

Public Attributes

- UINT16 VendorId

  Codec Vendor ID.
- UINT16 DeviceId

  Codec Device ID.
- UINT8 RevisionId

  Revision ID of the codec. 0xFF matches any revision.
- UINT8 SdiNum

  SDI number, 0xFF matches any SDI.
- UINT16 DataDwords

  Number of data DWORDs pointed by the codec data buffer.
- UINT32 Reserved

  Reserved for future use. Must be set to 0.

13.12.1 Detailed Description

Azalia Header structure.

Definition at line 44 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.13 BBS_STATUS_FLAGS Struct Reference

BBS_STATUS_FLAGS;.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 OldPosition: 4

  Prior priority.
- UINT16 Reserved1: 4

  Reserved for future use.
- UINT16 Enabled: 1

  If 0, ignore this entry.
- UINT16 Failed: 1

  0 = Not known if boot failure occurred.
- UINT16 MediaPresent: 2

  State of media present.
- UINT16 Reserved2: 4

  Reserved for future use.

13.13.1 Detailed Description

BBS_STATUS_FLAGS;.

Definition at line 593 of file LegacyBios.h.

13.13.2 Member Data Documentation

13.13.2.1 Failed

```
UINT16 BBS_STATUS_FLAGS::Failed
```

0 = Not known if boot failure occurred.

1 = Boot attempted failed.

Definition at line 597 of file LegacyBios.h.

13.13.2.2 MediaPresent

```
UINT16 BBS_STATUS_FLAGS::MediaPresent
```

State of media present.

00 = No bootable media is present in the device. 01 = Unknown if a bootable media present. 10 = Media is present and appears bootable. 11 = Reserved.

Definition at line 607 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

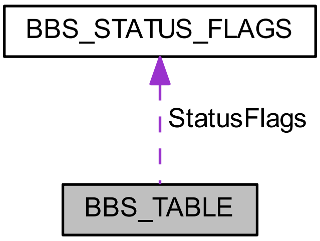
- LegacyBios.h

13.14 BBS_TABLE Struct Reference

BBS_TABLE, device type values & boot priority values.

```
#include <LegacyBios.h>
```

Collaboration diagram for BBS_TABLE:



Public Attributes

- UINT16 BootPriority

  The boot priority for this boot device.
- UINT32 Bus

  The PCI bus for this boot device.
- UINT32 Device

  The PCI device for this boot device.
- UINT32 Function

  The PCI function for the boot device.
- UINT8 Class

  The PCI class for this boot device.
- UINT8 SubClass

  The PCI Subclass for this boot device.
- UINT16 MfgStringOffset

  Segment:offset address of an ASCIIZ description string describing the manufacturer.
- UINT16 MfgStringSegment

  Segment:offset address of an ASCIIZ description string describing the manufacturer.
- UINT16 DeviceType

  BBS device type.
- BBS_STATUS_FLAGS StatusFlags

  Status of this boot device.
- UINT16 BootHandlerOffset

  Segment:Offset address of boot loader for IPL devices or install INT13 handler for BCV devices.
- UINT16 BootHandlerSegment

  Segment:Offset address of boot loader for IPL devices or install INT13 handler for BCV devices.
- UINT16 DescStringOffset

  Segment:offset address of an ASCIIZ description string describing this device.

- UINT16 DescStringSegment

  Segment:offset address of an ASCIIZ description string describing this device.
- UINT32 InitPerReserved

  Reserved.
- UINT32 AdditionalIrq13Handler

  The use of these fields is IBV dependent.
- UINT32 AdditionalIrq18Handler

  The use of these fields is IBV dependent.
- UINT32 AdditionalIrq19Handler

  The use of these fields is IBV dependent.
- UINT32 AdditionalIrq40Handler

  The use of these fields is IBV dependent.

13.14.1 Detailed Description

BBS_TABLE, device type values & boot priority values.

Definition at line 614 of file LegacyBios.h.

13.14.2 Member Data Documentation

13.14.2.1 AdditionalIrq13Handler

```
UINT32 BBS_TABLE::AdditionalIrq13Handler
```

The use of these fields is IBV dependent.

They can be used to flag that an OpROM has hooked the specified IRQ. The OpROM may be BBS compliant as some SCSI BBS-compliant OpROMs also hook IRQ vectors in order to run their BIOS Setup

Definition at line 697 of file LegacyBios.h.

13.14.2.2 AdditionalIrq18Handler

```
UINT32 BBS_TABLE::AdditionalIrq18Handler
```

The use of these fields is IBV dependent.

They can be used to flag that an OpROM has hooked the specified IRQ. The OpROM may be BBS compliant as some SCSI BBS-compliant OpROMs also hook IRQ vectors in order to run their BIOS Setup

Definition at line 704 of file LegacyBios.h.

13.14.2.3 AdditionalIrq19Handler

```
UINT32 BBS_TABLE::AdditionalIrq19Handler
```

The use of these fields is IBV dependent.

They can be used to flag that an OpROM has hooked the specified IRQ. The OpROM may be BBS compliant as some SCSI BBS-compliant OpROMs also hook IRQ vectors in order to run their BIOS Setup

Definition at line 711 of file LegacyBios.h.

13.14.2.4 AdditionalIrq40Handler

```
UINT32 BBS_TABLE::AdditionalIrq40Handler
```

The use of these fields is IBV dependent.

They can be used to flag that an OpROM has hooked the specified IRQ. The OpROM may be BBS compliant as some SCSI BBS-compliant OpROMs also hook IRQ vectors in order to run their BIOS Setup

Definition at line 718 of file LegacyBios.h.

13.14.2.5 BootPriority

```
UINT16 BBS_TABLE::BootPriority
```

The boot priority for this boot device.

Values are defined below.

Definition at line 618 of file LegacyBios.h.

13.14.2.6 DeviceType

```
UINT16 BBS_TABLE::DeviceType
```

BBS device type.

BBS device types are defined below.

Definition at line 658 of file LegacyBios.h.

13.14.2.7 StatusFlags

```
BBS_STATUS_FLAGS BBS_TABLE::StatusFlags
```

Status of this boot device.

Type BBS_STATUS_FLAGS is defined below.

Definition at line 663 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.15 CHIPSET_INIT_INFO Struct Reference

The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.

```
#include <FspmUpd.h>
```

Public Attributes

- UINT8 Revision

    Chipset Init Info Revision.
- UINT8 Rsvd [3]

    Reserved.
- UINT16 MeChipInitCrc

    16 bit CRC value of MeChipInit Table
- UINT16 BiosChipInitCrc

    16 bit CRC value of PchChipInit Table

13.15.1 Detailed Description

The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.

Definition at line 46 of file FspmUpd.h.

The documentation for this struct was generated from the following file:

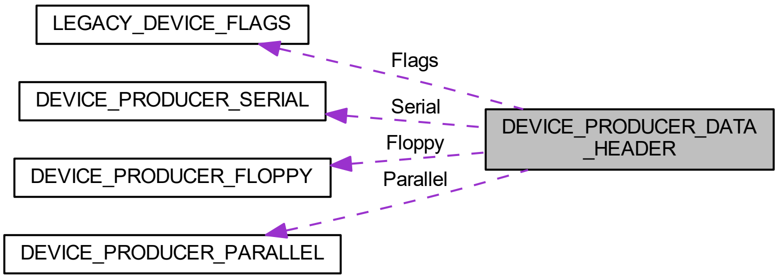
- FspmUpd.h

13.16 DEVICE_PRODUCER_DATA_HEADER Struct Reference

DEVICE_PRODUCER_DATA_HEADER.

```
#include <LegacyBios.h>
```

Collaboration diagram for DEVICE_PRODUCER_DATA_HEADER:



Public Attributes

- DEVICE_PRODUCER_SERIAL Serial [4]

  Data for serial port x. Type DEVICE_PRODUCER_SERIAL is defined below.
- DEVICE_PRODUCER_PARALLEL Parallel [3]

  Data for parallel port x. Type DEVICE_PRODUCER_PARALLEL is defined below.
- DEVICE_PRODUCER_FLOPPY Floppy

  Data for floppy. Type DEVICE_PRODUCER_FLOPPY is defined below.
- UINT8 MousePresent

  Flag to indicate if mouse is present.
- LEGACY_DEVICE_FLAGS Flags

  Miscellaneous Boolean state information passed to CSM.

13.16.1 Detailed Description

DEVICE_PRODUCER_DATA_HEADER.

Definition at line 514 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.17 DEVICE_PRODUCER_FLOPPY Struct Reference

DEVICE_PRODUCER_FLOPPY.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 Address

    I/O address assigned to the floppy.
- UINT8 Irq

    IRQ assigned to the floppy.
- UINT8 Dma

    DMA assigned to the floppy.
- UINT8 NumberOfFloppy

    Number of floppies in the system.

13.17.1 Detailed Description

DEVICE_PRODUCER_FLOPPY.

Definition at line 495 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.18 DEVICE_PRODUCER_PARALLEL Struct Reference

@)

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 Address

    I/O address assigned to the parallel port.
- UINT8 Irq

    IRQ assigned to the parallel port.
- UINT8 Dma

    DMA assigned to the parallel port.
- PARALLEL_MODE Mode

    Mode of the parallel port. Values are defined below.

13.18.1 Detailed Description

@)

DEVICE_PRODUCER_PARALLEL.

Definition at line 476 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.19 DEVICE_PRODUCER_SERIAL Struct Reference

DEVICE_PRODUCER_SERIAL.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 Address

  I/O address assigned to the serial port.
- UINT8 Irq

  IRQ assigned to the serial port.
- SERIAL_MODE Mode

  Mode of serial port. Values are defined below.

13.19.1 Detailed Description

DEVICE_PRODUCER_SERIAL.

Definition at line 457 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.20 DXE_SI_POLICY_PROTOCOL Struct Reference

The protocol allows the platform code to publish a set of configuration information that the Silicon drivers will use to configure the processor in the DXE phase.

```
#include <SiPolicyProtocol.h>
```

Public Attributes

- UINT8 Revision

  This member specifies the revision of the Si Policy protocol.
- UINT8 SmbiosOemTypeFirmwareVersionInfo

  SmbiosOemTypeFirmwareVersionInfo determines the SMBIOS OEM type (0x80 to 0xFF) defined in SMBIOS, values 0-0x7F will be treated as disable FVI reporting.
- UINT8 ReservedByte [6]

  Reserved bytes, align to multiple 8.
- ADAPTER_INFO_PLATFORM_SECURITY ∗ Hsti

  This member describes a pointer to Hsti results from previous boot.
- UINTN HstiSize

  Size of results, if setting Hsti policy to point to previous results.

13.20.1 Detailed Description

The protocol allows the platform code to publish a set of configuration information that the Silicon drivers will use to configure the processor in the DXE phase.

This Policy Protocol needs to be initialized for Silicon configuration.

Note

> The Protocol has to be published before processor DXE drivers are dispatched.

Definition at line 55 of file SiPolicyProtocol.h.

13.20.2 Member Data Documentation

13.20.2.1 Hsti

```
ADAPTER_INFO_PLATFORM_SECURITY* DXE_SI_POLICY_PROTOCOL::Hsti
```

This member describes a pointer to Hsti results from previous boot.

In order to mitigate the large performance cost of performing all of the platform security tests on each boot, we can save the results across boots and retrieve and point this policy to them prior to the launch of HstiSiliconDxe. Logic should be implemented to not populate this upon major platform changes (i.e changes to setup option or platform hw)to ensure that results accurately reflect the configuration of the platform.This is a pointer to Hsti results from previous boot

Definition at line 80 of file SiPolicyProtocol.h.

13.20.2.2 Revision

```
UINT8 DXE_SI_POLICY_PROTOCOL::Revision
```

This member specifies the revision of the Si Policy protocol.

This field is used to indicate backward compatible changes to the protocol. Any such changes to this protocol will result in an update in the revision number.

Revision 1:

- Initial version **Revision 2**:
- Added SmbiosOemTypeFirmwareVersionInfo to determines the SMBIOS OEM type

Definition at line 65 of file SiPolicyProtocol.h.

13.20.2.3 SmbiosOemTypeFirmwareVersionInfo

```
UINT8 DXE_SI_POLICY_PROTOCOL::SmbiosOemTypeFirmwareVersionInfo
```

SmbiosOemTypeFirmwareVersionInfo determines the SMBIOS OEM type (0x80 to 0xFF) defined in SMBIOS, values 0-0x7F will be treated as disable FVI reporting.

FVI structure uses it as SMBIOS OEM type to provide version information.

Definition at line 71 of file SiPolicyProtocol.h.

The documentation for this struct was generated from the following file:

- SiPolicyProtocol.h

13.21 EFI_BYTE_REGS Struct Reference

EFI_BYTE_REGS.

```
#include <LegacyBios.h>
```

13.21.1 Detailed Description

EFI_BYTE_REGS.

Definition at line 1120 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.22 EFI_COMPATIBILITY16_TABLE Struct Reference

There is a table located within the traditional BIOS in either the 0xF000:xxxx or 0xE000:xxxx physical address range.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT32 Signature

    The string "$EFI" denotes the start of the EfiCompatibility table.
- UINT8 TableChecksum

    The value required such that byte checksum of TableLength equals zero.
- UINT8 TableLength

    The length of this table.
- UINT8 EfiMajorRevision

    The major EFI revision for which this table was generated.
- UINT8 EfiMinorRevision

    The minor EFI revision for which this table was generated.
- UINT8 TableMajorRevision

    The major revision of this table.
- UINT8 TableMinorRevision

    The minor revision of this table.
- UINT16 Reserved

    Reserved for future usage.
- UINT16 Compatibility16CallSegment

    The segment of the entry point within the traditional BIOS for Compatibility16 functions.
- UINT16 Compatibility16CallOffset

    The offset of the entry point within the traditional BIOS for Compatibility16 functions.
- UINT16 PnPInstallationCheckSegment

    The segment of the entry point within the traditional BIOS for EfiCompatibility to invoke the PnP installation check.
- UINT16 PnPInstallationCheckOffset

    The Offset of the entry point within the traditional BIOS for EfiCompatibility to invoke the PnP installation check.
- UINT32 EfiSystemTable

    EFI system resources table.
- UINT32 OemIdStringPointer

    The address of an OEM-provided identifier string.
- UINT32 AcpiRsdPtrPointer

    The 32-bit physical address where ACPI RSD PTR is stored within the traditional BIOS.
- UINT16 OemRevision

    The OEM revision number.
- UINT32 E820Pointer

    The 32-bit physical address where INT15 E820 data is stored within the traditional BIOS.
- UINT32 E820Length

    The length of the E820 data and is filled in by the EfiCompatibility code.
- UINT32 IrqRoutingTablePointer

    The 32-bit physical address where the $PIR table is stored in the traditional BIOS.
- UINT32 IrqRoutingTableLength

    The length of the $PIR table and is filled in by the EfiCompatibility code.
- UINT32 MpTablePtr

    The 32-bit physical address where the MP table is stored in the traditional BIOS.
- UINT32 MpTableLength

    The length of the MP table and is filled in by the EfiCompatibility code.
- UINT16 OemIntSegment

    The segment of the OEM-specific INT table/code.
- UINT16 OemIntOffset

    The offset of the OEM-specific INT table/code.
- UINT16 Oem32Segment

The segment of the OEM-specific 32-bit table/code.
- UINT16 Oem32Offset

  The offset of the OEM-specific 32-bit table/code.
- UINT16 Oem16Segment

  The segment of the OEM-specific 16-bit table/code.
- UINT16 Oem16Offset

  The offset of the OEM-specific 16-bit table/code.
- UINT16 TpmSegment

  The segment of the TPM binary passed to 16-bit CSM.
- UINT16 TpmOffset

  The offset of the TPM binary passed to 16-bit CSM.
- UINT32 IbvPointer

  A pointer to a string identifying the independent BIOS vendor.
- UINT32 PciExpressBase

  This field is NULL for all systems not supporting PCI Express.
- UINT8 LastPciBus

  Maximum PCI bus number assigned.
- UINT32 UmaAddress

  Start Address of Upper Memory Area (UMA) to be set as Read/Write.
- UINT32 UmaSize

  Upper Memory Area size in bytes to be set as Read/Write.
- UINT32 HiPermanentMemoryAddress

  Start Address of high memory that can be used for permanent allocation.
- UINT32 HiPermanentMemorySize

  Size of high memory that can be used for permanent allocation in bytes.

13.22.1 Detailed Description

There is a table located within the traditional BIOS in either the 0xF000:xxxx or 0xE000:xxxx physical address range.

It is located on a 16-byte boundary and provides the physical address of the entry point for the Compatibility16 functions. These functions provide the platform-specific information that is required by the generic EfiCompatibility code. The functions are invoked via thunking by using EFI_LEGACY_BIOS_PROTOCOL.FarCall86() with the 32-bit physical entry point.

Definition at line 48 of file LegacyBios.h.

13.22.2 Member Data Documentation

13.22.2.1 AcpiRsdPtrPointer

```
UINT32 EFI_COMPATIBILITY16_TABLE::AcpiRsdPtrPointer
```

The 32-bit physical address where ACPI RSD PTR is stored within the traditional BIOS.

The remained of the ACPI tables are located at their EFI addresses. The size reserved is the maximum for ACPI 2.0. The EfiCompatibility will fill in the ACPI RSD PTR with either the ACPI 1.0b or 2.0 values.

Definition at line 129 of file LegacyBios.h.

13.22.2.2 E820Pointer

```
UINT32 EFI_COMPATIBILITY16_TABLE::E820Pointer
```

The 32-bit physical address where INT15 E820 data is stored within the traditional BIOS.

The EfiCompatibility code will fill in the E820Pointer value and copy the data to the indicated area.

Definition at line 141 of file LegacyBios.h.

13.22.2.3 EfiSystemTable

```
UINT32 EFI_COMPATIBILITY16_TABLE::EfiSystemTable
```

EFI system resources table.

Type EFI_SYSTEM_TABLE is defined in the IntelPlatform Innovation Framework for EFI Driver Execution Environment Core Interface Specification (DXE CIS).

Definition at line 116 of file LegacyBios.h.

13.22.2.4 HiPermanentMemoryAddress

```
UINT32 EFI_COMPATIBILITY16_TABLE::HiPermanentMemoryAddress
```

Start Address of high memory that can be used for permanent allocation.

If zero, high memory is not available for permanent allocation.

Definition at line 249 of file LegacyBios.h.

13.22.2.5 HiPermanentMemorySize

```
UINT32 EFI_COMPATIBILITY16_TABLE::HiPermanentMemorySize
```

Size of high memory that can be used for permanent allocation in bytes.

If zero, high memory is not available for permanent allocation.

Definition at line 255 of file LegacyBios.h.

13.22.2.6 IrqRoutingTablePointer

```
UINT32 EFI_COMPATIBILITY16_TABLE::IrqRoutingTablePointer
```

The 32-bit physical address where the $PIR table is stored in the traditional BIOS.

The EfiCompatibility code will fill in the IrqRoutingTablePointer value and copy the data to the indicated area.

Definition at line 153 of file LegacyBios.h.

13.22.2.7 MpTablePtr

```
UINT32 EFI_COMPATIBILITY16_TABLE::MpTablePtr
```

The 32-bit physical address where the MP table is stored in the traditional BIOS.

The EfiCompatibility code will fill in the MpTablePtr value and copy the data to the indicated area.

Definition at line 165 of file LegacyBios.h.

13.22.2.8 OemIdStringPointer

```
UINT32 EFI_COMPATIBILITY16_TABLE::OemIdStringPointer
```

The address of an OEM-provided identifier string.

The string is null terminated.

Definition at line 121 of file LegacyBios.h.

13.22.2.9 OemRevision

```
UINT16 EFI_COMPATIBILITY16_TABLE::OemRevision
```

The OEM revision number.

Usage is undefined but provided for OEM module usage.

Definition at line 134 of file LegacyBios.h.

13.22.2.10 PciExpressBase

```
UINT32 EFI_COMPATIBILITY16_TABLE::PciExpressBase
```

This field is NULL for all systems not supporting PCI Express.

This field is the base value of the start of the PCI Express memory-mapped configuration registers and must be filled in prior to EfiCompatibility code issuing the Compatibility16 function Compatibility16InitializeYourself(). Compatibility16InitializeYourself() is defined in Compatability16 Functions.

Definition at line 225 of file LegacyBios.h.

13.22.2.11 Signature

```
UINT32 EFI_COMPATIBILITY16_TABLE::Signature
```

The string "$EFI" denotes the start of the EfiCompatibility table.

Byte 0 is "I," byte 1 is "F," byte 2 is "E," and byte 3 is "$" and is normally accessed as a DWORD or UINT32.

Definition at line 53 of file LegacyBios.h.

13.22.2.12 UmaAddress

```
UINT32 EFI_COMPATIBILITY16_TABLE::UmaAddress
```

Start Address of Upper Memory Area (UMA) to be set as Read/Write.

If UmaAddress is a valid address in the shadow RAM, it also indicates that the region from 0xC0000 to (UmaAddress - 1) can be used for Option ROM.

Definition at line 237 of file LegacyBios.h.

13.22.2.13 UmaSize

```
UINT32 EFI_COMPATIBILITY16_TABLE::UmaSize
```

Upper Memory Area size in bytes to be set as Read/Write.

If zero, no UMA region will be set as Read/Write (i.e. all Shadow RAM is set as Read-Only).

Definition at line 243 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.23 EFI_DISPATCH_OPROM_TABLE Struct Reference

EFI_DISPATCH_OPROM_TABLE.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 PnPInstallationCheckSegment

  A pointer to the PnpInstallationCheck data structure.
- UINT16 PnPInstallationCheckOffset

  A pointer to the PnpInstallationCheck data structure.
- UINT16 OpromSegment

  The segment where the OpROM was placed. Offset is assumed to be 3.
- UINT8 PciBus

  The PCI bus.
- UINT8 PciDeviceFunction

  The PCI device $*$ 0x08 $|$ PCI function.
- UINT8 NumberBbsEntries

  The number of valid BBS table entries upon entry and exit.
- UINT32 BbsTablePointer

  A pointer to the BBS table.
- UINT16 RuntimeSegment

  The segment where the OpROM can be relocated to.

13.23.1 Detailed Description

EFI_DISPATCH_OPROM_TABLE.

Definition at line 376 of file LegacyBios.h.

13.23.2 Member Data Documentation

13.23.2.1 NumberBbsEntries

```
UINT8 EFI_DISPATCH_OPROM_TABLE::NumberBbsEntries
```

The number of valid BBS table entries upon entry and exit.

The IBV code may increase this number, if BBS-compliant devices also hook INTs in order to force the OpROM BIOS Setup to be executed.

Definition at line 382 of file LegacyBios.h.

13.23.2.2 RuntimeSegment

```
UINT16 EFI_DISPATCH_OPROM_TABLE::RuntimeSegment
```

The segment where the OpROM can be relocated to.

If this value is 0x0000, this means that the relocation of this run time code is not supported. Inconsistent with specification here: The member's name "OpromDestinationSegment" [defined in Intel Framework Compatibility Support Module Specification / 0.97 version] has been changed to "RuntimeSegment" since keeping backward compatible.

Definition at line 386 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

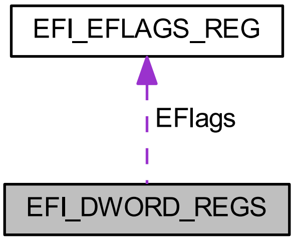
- LegacyBios.h

13.24 EFI_DWORD_REGS Struct Reference

EFI_DWORD_REGS.

```
#include <LegacyBios.h>
```

Collaboration diagram for EFI_DWORD_REGS:



13.24.1 Detailed Description

EFI_DWORD_REGS.

Definition at line 1048 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.25 EFI_EFLAGS_REG Struct Reference

EFI_EFLAGS_REG.

```
#include <LegacyBios.h>
```

13.25.1 Detailed Description

EFI_EFLAGS_REG.

Definition at line 1025 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.26 EFI_FLAGS_REG Struct Reference

EFI_FLAGS_REG.

```
#include <LegacyBios.h>
```

13.26.1 Detailed Description

EFI_FLAGS_REG.

Definition at line 1069 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

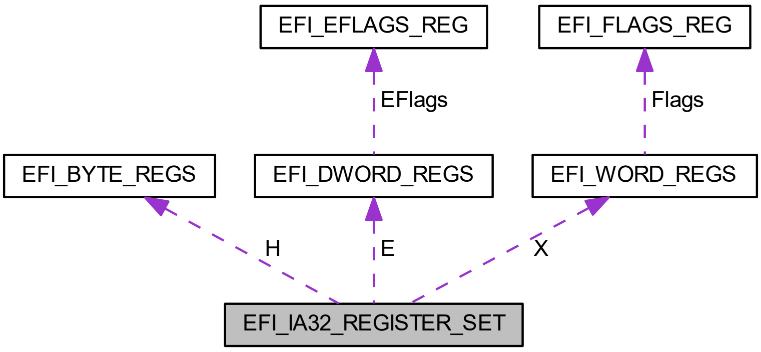
- LegacyBios.h

13.27 EFI_IA32_REGISTER_SET Union Reference

EFI_IA32_REGISTER_SET.

```
#include <LegacyBios.h>
```

Collaboration diagram for EFI_IA32_REGISTER_SET:



13.27.1 Detailed Description

EFI_IA32_REGISTER_SET.

Definition at line 1134 of file LegacyBios.h.

The documentation for this union was generated from the following file:

- LegacyBios.h

13.28 EFI_LEGACY_INSTALL_PCI_HANDLER Struct Reference

EFI_LEGACY_INSTALL_PCI_HANDLER.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT8 PciBus

  The PCI bus of the device.
- UINT8 PciDeviceFun

  The PCI device in bits 7:3 and function in bits 2:0.
- UINT8 PciSegment

  The PCI segment of the device.
- UINT8 PciClass

  The PCI class code of the device.
- UINT8 PciSubclass

  The PCI subclass code of the device.
- UINT8 PciInterface

  The PCI interface code of the device.
- UINT8 PrimaryIrq

  The primary device IRQ.
- UINT8 PrimaryReserved

  Reserved.
- UINT16 PrimaryControl

  The primary device control I/O base.
- UINT16 PrimaryBase

  The primary device I/O base.
- UINT16 PrimaryBusMaster

  The primary device bus master I/O base.
- UINT8 SecondaryIrq

  The secondary device IRQ.
- UINT8 SecondaryReserved

  Reserved.
- UINT16 SecondaryControl

  The secondary device control I/O base.
- UINT16 SecondaryBase

  The secondary device I/O base.
- UINT16 SecondaryBusMaster

  The secondary device bus master I/O base.

13.28.1 Detailed Description

EFI_LEGACY_INSTALL_PCI_HANDLER.

Definition at line 965 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

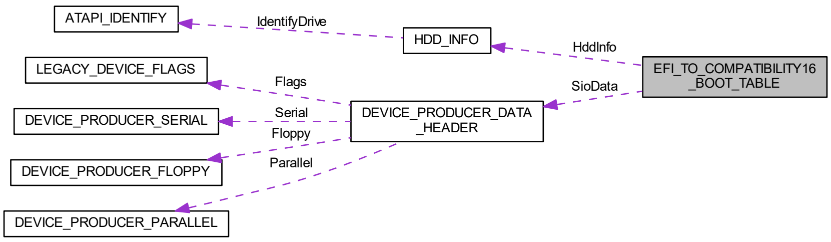
- LegacyBios.h

13.29 EFI_TO_COMPATIBILITY16_BOOT_TABLE Struct Reference

EFI_TO_COMPATIBILITY16_BOOT_TABLE.

```
#include <LegacyBios.h>
```

Collaboration diagram for EFI_TO_COMPATIBILITY16_BOOT_TABLE:



Public Attributes

- UINT16 MajorVersion

  The EfiCompatibility major version number.
- UINT16 MinorVersion

  The EfiCompatibility minor version number.
- UINT32 AcpiTable

  The location of the RSDT ACPI table. < 4G range.
- UINT32 SmbiosTable

  The location of the SMBIOS table in EFI memory. < 4G range.
- DEVICE_PRODUCER_DATA_HEADER SioData

  Standard traditional device information.
- UINT16 DevicePathType

  The default boot type.
- UINT16 PciIrqMask

  Mask of which IRQs have been assigned to PCI.
- UINT32 NumberE820Entries

  Number of E820 entries.
- HDD_INFO HddInfo [MAX_IDE_CONTROLLER]

  Hard disk drive information, including raw Identify Drive data.

- UINT32 NumberBbsEntries

  Number of entries in the BBS table.
- UINT32 BbsTable

  A pointer to the BBS table. Type BBS_TABLE is defined below.
- UINT32 SmmTable

  A pointer to the SMM table. Type SMM_TABLE is defined below.
- UINT32 OsMemoryAbove1Mb

  The amount of usable memory above 1 MB, i.e.
- UINT32 UnconventionalDeviceTable

  Information to boot off an unconventional device like a PARTIES partition.

13.29.1 Detailed Description

EFI_TO_COMPATIBILITY16_BOOT_TABLE.

Definition at line 934 of file LegacyBios.h.

13.29.2 Member Data Documentation

13.29.2.1 NumberE820Entries

```
UINT32 EFI_TO_COMPATIBILITY16_BOOT_TABLE::NumberE820Entries
```

Number of E820 entries.

The number can change from the Compatibility16InitializeYourself() function.

Definition at line 946 of file LegacyBios.h.

13.29.2.2 OsMemoryAbove1Mb

```
UINT32 EFI_TO_COMPATIBILITY16_BOOT_TABLE::OsMemoryAbove1Mb
```

The amount of usable memory above 1 MB, i.e.

E820 type 1 memory. This value can differ from the value in EFI_TO_COMPATIBILITY16_INIT_TABLE as more memory may have been discovered.

Definition at line 955 of file LegacyBios.h.

13.29.2.3 UnconventionalDeviceTable

```
UINT32 EFI_TO_COMPATIBILITY16_BOOT_TABLE::UnconventionalDeviceTable
```

Information to boot off an unconventional device like a PARTIES partition.

Type UD_TABLE is defined below.

Definition at line 958 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.30 EFI_TO_COMPATIBILITY16_INIT_TABLE Struct Reference

EFI_TO_COMPATIBILITY16_INIT_TABLE.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT32 BiosLessThan1MB

  Starting address of memory under 1 MB.
- UINT32 HiPmmMemory

  The starting address of the high memory block.
- UINT32 HiPmmMemorySizeInBytes

  The length of high memory block.
- UINT16 ReverseThunkCallSegment

  The segment of the reverse thunk call code.
- UINT16 ReverseThunkCallOffset

  The offset of the reverse thunk call code.
- UINT32 NumberE820Entries

  The number of E820 entries copied to the Compatibility16 BIOS.
- UINT32 OsMemoryAbove1Mb

  The amount of usable memory above 1 MB, e.g., E820 type 1 memory.
- UINT32 ThunkStart

  The start of thunk code in main memory.
- UINT32 ThunkSizeInBytes

  The size of the thunk code.
- UINT32 LowPmmMemory

  Starting address of memory under 1 MB.
- UINT32 LowPmmMemorySizeInBytes

  The length of low Memory block.

13.30.1 Detailed Description

EFI_TO_COMPATIBILITY16_INIT_TABLE.

Definition at line 397 of file LegacyBios.h.

13.30.2 Member Data Documentation

13.30.2.1 BiosLessThan1MB

```
UINT32 EFI_TO_COMPATIBILITY16_INIT_TABLE::BiosLessThan1MB
```

Starting address of memory under 1 MB.

The ending address is assumed to be 640 KB or 0x9FFFF.

Definition at line 401 of file LegacyBios.h.

13.30.2.2 ThunkStart

```
UINT32 EFI_TO_COMPATIBILITY16_INIT_TABLE::ThunkStart
```

The start of thunk code in main memory.

Memory cannot be used by BIOS or PMM.

Definition at line 436 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

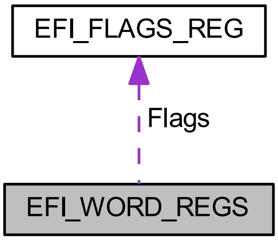
- LegacyBios.h

13.31 EFI_WORD_REGS Struct Reference

EFI_WORD_REGS.

```
#include <LegacyBios.h>
```

Collaboration diagram for EFI_WORD_REGS:



13.31.1 Detailed Description

EFI_WORD_REGS.

Definition at line 1090 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.32 FSP_ERROR_INFO_HOB Struct Reference

FSP Error Information Block.

```
#include <FspErrorInfo.h>
```

Public Attributes

- EFI_HOB_GUID_TYPE GuidHob

  GUID HOB header.
- EFI_STATUS_CODE_TYPE Type

  ReportStatusCode () type identifier.
- EFI_STATUS_CODE_VALUE Value

  ReportStatusCode () value.
- UINT32 Instance

  ReportStatusCode () Instance number.
- EFI_GUID CallerId

  Optional GUID which may be used to identify which internal component of the FSP was executing at the time of the error.
- EFI_GUID ErrorType

  GUID identifying the nature of the fatal error.
- UINT32 Status

  EFI_STATUS code describing the error encountered.

13.32.1 Detailed Description

FSP Error Information Block.

Definition at line 60 of file FspErrorInfo.h.

The documentation for this struct was generated from the following file:

- FspErrorInfo.h

13.33 FSP_M_CONFIG Struct Reference

Fsp M Configuration.

```
#include <FspmUpd.h>
```

Public Attributes

- UINT64 PlatformMemorySize

  Offset 0x0040 - Platform Reserved Memory Size The minimum platform memory size required to pass control into DXE.
- UINT32 MemorySpdPtr00

  Offset 0x0048 - Memory SPD Pointer Channel 0 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↩ Table SPD Address are marked as 00.
- UINT32 MemorySpdPtr01

  Offset 0x004C - Memory SPD Pointer Channel 0 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↩ Table SPD Address are marked as 00.
- UINT32 MemorySpdPtr10

  Offset 0x0050 - Memory SPD Pointer Channel 1 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↩ Table SPD Address are marked as 00.
- UINT32 MemorySpdPtr11

  Offset 0x0054 - Memory SPD Pointer Channel 1 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↩ Table SPD Address are marked as 00.
- UINT16 MemorySpdDataLen

  Offset 0x0058 - SPD Data Length Length of SPD Data 0x100:256 Bytes, 0x200:512 Bytes.
- UINT8 DqByteMapCh0 [12]

  Offset 0x005A - Dq Byte Map CH0 Dq byte mapping between CPU and DRAM, Channel 0: board-dependent.
- UINT8 DqByteMapCh1 [12]

  Offset 0x0066 - Dq Byte Map CH1 Dq byte mapping between CPU and DRAM, Channel 1: board-dependent.
- UINT8 DqsMapCpu2DramCh0 [8]

  Offset 0x0072 - Dqs Map CPU to DRAM CH 0 Set Dqs mapping relationship between CPU and DRAM, Channel 0: board-dependent.
- UINT8 DqsMapCpu2DramCh1 [8]

  Offset 0x007A - Dqs Map CPU to DRAM CH 1 Set Dqs mapping relationship between CPU and DRAM, Channel 1: board-dependent.
- UINT16 RcompResistor [3]

  Offset 0x0082 - RcompResistor settings Indicates RcompResistor settings: CML - 0's means MRC auto configured based on Design Guidelines, otherwise input an Ohmic value per segment.
- UINT16 RcompTarget [5]

  Offset 0x0088 - RcompTarget settings RcompTarget settings: CML - 0's mean MRC auto configured based on Design Guidelines, otherwise input an Ohmic value per segment.
- UINT8 DqPinsInterleaved

  Offset 0x0092 - Dqs Pins Interleaved Setting Indicates DqPinsInterleaved setting: board-dependent $EN_DIS.
- UINT8 CaVrefConfig

  Offset 0x0093 - VREF_CA CA Vref routing: board-dependent 0:VREF_CA goes to both CH_A and CH_B, 1: VRE↩ F_CA to CH_A and VREF_DQ_A to CH_B, 2:VREF_CA to CH_A and VREF_DQ_B to CH_B.
- UINT8 SmramMask

  Offset 0x0094 - Smram Mask The SMM Regions AB-SEG and/or H-SEG reserved 0: Neither, 1:AB-SEG, 2:H-SEG, 3: Both.
- UINT8 MrcTimeMeasure

  Offset 0x0095 - Time Measure Time Measure: 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 MrcFastBoot

  Offset 0x0096 - MRC Fast Boot Enables/Disable the MRC fast path thru the MRC $EN_DIS.
- UINT8 RmtPerTask

  Offset 0x0097 - Rank Margin Tool per Task This option enables the user to execute Rank Margin Tool per major training step in the MRC.
- UINT8 TrainTrace

  Offset 0x0098 - Training Trace This option enables the trained state tracing feature in MRC.
- UINT8 UnusedUpdSpace0 [3]

Offset 0x0099.

- UINT32 IedSize

    Offset 0x009C - Intel Enhanced Debug Intel Enhanced Debug (IED): 0=Disabled, 0x400000=Enabled and 4MB S↩ MRAM occupied 0 : Disable, 0x400000 : Enable.
- UINT32 TsegSize

    Offset 0x00A0 - Tseg Size Size of SMRAM memory reserved.
- UINT16 MmioSize

    Offset 0x00A4 - MMIO Size Size of MMIO space reserved for devices.
- UINT8 ProbelessTrace

    Offset 0x00A6 - Probeless Trace Probeless Trace: 0=Disabled, 1=Enable.
- UINT8 GdxcIotSize

    Offset 0x00A7 - GDXC IOT SIZE Size of IOT and MOT is in 8 MB chunks.
- UINT8 GdxcMotSize

    Offset 0x00A8 - GDXC MOT SIZE Size of IOT and MOT is in 8 MB chunks.
- UINT8 SpdAddressTable [4]

    Offset 0x00A9 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.
- UINT8 IgdDvmt50PreAlloc

    Offset 0x00AD - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.
- UINT8 InternalGfx

    Offset 0x00AE - Internal Graphics Enable/disable internal graphics.
- UINT8 ApertureSize

    Offset 0x00AF - Aperture Size Select the Aperture Size.
- UINT8 UserBd

    Offset 0x00B0 - Board Type MrcBoardType, Options are 0=Mobile/Mobile Halo, 1=Desktop/DT Halo, 5=ULT/ULX/↩ Mobile Halo, 7=UP Server 0:Mobile/Mobile Halo, 1:Desktop/DT Halo, 5:ULT/ULX/Mobile Halo, 7:UP Server.
- UINT8 SaGv

    Offset 0x00B1 - SA GV System Agent dynamic frequency support and when enabled memory will be training at two different frequencies.
- UINT16 DdrFreqLimit

    Offset 0x00B2 - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.
- UINT16 FreqSaGvLow

    Offset 0x00B4 - Low Frequency SAGV Low Frequency Selections in Mhz.
- UINT8 RMT

    Offset 0x00B6 - Rank Margin Tool Enable/disable Rank Margin Tool.
- UINT8 DisableDimmChannel0

    Offset 0x00B7 - Channel A DIMM Control Channel A DIMM Control Support - Enable or Disable Dimms on Channel A.
- UINT8 DisableDimmChannel1

    Offset 0x00B8 - Channel B DIMM Control Channel B DIMM Control Support - Enable or Disable Dimms on Channel B.
- UINT8 ScramblerSupport

    Offset 0x00B9 - Scrambler Support This option enables data scrambling in memory.
- UINT8 SkipMpInit

    Offset 0x00BA - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SiliconInit API.
- UINT8 SpdProfileSelected

    Offset 0x00BB - SPD Profile Selected Select DIMM timing profile.
- UINT8 RefClk

    Offset 0x00BC - Memory Reference Clock 100MHz, 133MHz.
- UINT8 UnusedUpdSpace1

    Offset 0x00BD.
- UINT16 VddVoltage

Offset 0x00BE - Memory Voltage Memory Voltage Override (Vddq).

- UINT8 Ratio

  Offset 0x00C0 - Memory Ratio Automatic or the frequency will equal ratio times reference clock.

- UINT8 OddRatioMode

  Offset 0x00C1 - QCLK Odd Ratio Adds 133 or 100 MHz to QCLK frequency, depending on RefClk $EN_DIS.

- UINT8 tCL

  Offset 0x00C2 - tCL CAS Latency, 0: AUTO, max: 31.

- UINT8 tCWL

  Offset 0x00C3 - tCWL Min CAS Write Latency Delay Time, 0: AUTO, max: 34.

- UINT8 tRCDtRP

  Offset 0x00C4 - tRCD/tRP RAS to CAS delay time and Row Precharge delay time, 0: AUTO, max: 63.

- UINT8 tRRD

  Offset 0x00C5 - tRRD Min Row Active to Row Active Delay Time, 0: AUTO, max: 15.

- UINT16 tFAW

  Offset 0x00C6 - tFAW Min Four Activate Window Delay Time, 0: AUTO, max: 63.

- UINT16 tRAS

  Offset 0x00C8 - tRAS RAS Active Time, 0: AUTO, max: 64.

- UINT16 tREFI

  Offset 0x00CA - tREFI Refresh Interval, 0: AUTO, max: 65535.

- UINT16 tRFC

  Offset 0x00CC - tRFC Min Refresh Recovery Delay Time, 0: AUTO, max: 1023.

- UINT8 tRTP

  Offset 0x00CE - tRTP Min Internal Read to Precharge Command Delay Time, 0: AUTO, max: 15.

- UINT8 tWR

  Offset 0x00CF - tWR Min Write Recovery Time, 0: AUTO, legal values: 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 24, 30, 34, 40 0:Auto, 5:5, 6:6, 7:7, 8:8, 10:10, 12:12, 14:14, 16:16, 18:18, 20:20, 24:24, 30:30, 34:34, 40:40.

- UINT8 tWTR

  Offset 0x00D0 - tWTR Min Internal Write to Read Command Delay Time, 0: AUTO, max: 28.

- UINT8 NModeSupport

  Offset 0x00D1 - NMode System command rate, range 0-2, 0 means auto, 1 = 1N, 2 = 2N.

- UINT8 DllBwEn0

  Offset 0x00D2 - DllBwEn[0] DllBwEn[0], for 1067 (0..7)

- UINT8 DllBwEn1

  Offset 0x00D3 - DllBwEn[1] DllBwEn[1], for 1333 (0..7)

- UINT8 DllBwEn2

  Offset 0x00D4 - DllBwEn[2] DllBwEn[2], for 1600 (0..7)

- UINT8 DllBwEn3

  Offset 0x00D5 - DllBwEn[3] DllBwEn[3], for 1867 and up (0..7)

- UINT8 IsvtIoPort

  Offset 0x00D6 - ISVT IO Port Address ISVT IO Port Address.

- UINT8 MarginLimitCheck

  Offset 0x00D7 - Margin Limit Check Margin Limit Check.

- UINT16 MarginLimitL2

  Offset 0x00D8 - Margin Limit L2 % of L1 check for margin limit check.

- UINT8 CpuTraceHubMode

  Offset 0x00DA - CPU Trace Hub Mode Select 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

- UINT8 CpuTraceHubMemReg0Size

  Offset 0x00DB - CPU Trace Hub Memory Region 0 CPU Trace Hub Memory Region 0, The avaliable memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

- UINT8 CpuTraceHubMemReg1Size

Offset 0x00DC - CPU Trace Hub Memory Region 1 CPU Trace Hub Memory Region 1.

- UINT8 PeciC10Reset

  Offset 0x00DD - Enable or Disable Peci C10 Reset command Enable or Disable Peci C10 Reset command.
- UINT8 PeciSxReset

  *Offset 0x00DE - Enable or Disable Peci Sx Reset command Enable or Disable Peci Sx Reset command; **0: Disable;** 1: Enable.*
- UINT8 HeciTimeouts

  Offset 0x00DF - HECI Timeouts 0: Disable, 1: Enable (Default) timeout check for HECI $EN_DIS.
- UINT32 Heci1BarAddress

  Offset 0x00E0 - HECI1 BAR address BAR address of HECI1.
- UINT32 Heci2BarAddress

  Offset 0x00E4 - HECI2 BAR address BAR address of HECI2.
- UINT32 Heci3BarAddress

  Offset 0x00E8 - HECI3 BAR address BAR address of HECI3.
- UINT16 SgDelayAfterPwrEn

  Offset 0x00EC - SG dGPU Power Delay SG dGPU delay interval after power enabling: 0=Minimal, 1000=Maximum, default is 300=300 microseconds.
- UINT16 SgDelayAfterHoldReset

  Offset 0x00EE - SG dGPU Reset Delay SG dGPU delay interval for Reset complete: 0=Minimal, 1000=Maximum, default is 100=100 microseconds.
- UINT16 MmioSizeAdjustment

  Offset 0x00F0 - MMIO size adjustment for AUTO mode Positive number means increasing MMIO size, Negative value means decreasing MMIO size: 0 (Default)=no change to AUTO mode MMIO size.
- UINT8 DmiGen3ProgramStaticEq

  Offset 0x00F2 - Enable/Disable DMI GEN3 Static EQ Phase1 programming Program DMI Gen3 EQ Phase1 Static Presets.
- UINT8 Peg0Enable

  Offset 0x00F3 - Enable/Disable PEG 0 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.
- UINT8 Peg1Enable

  Offset 0x00F4 - Enable/Disable PEG 1 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.
- UINT8 Peg2Enable

  Offset 0x00F5 - Enable/Disable PEG 2 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.
- UINT8 Peg3Enable

  Offset 0x00F6 - Enable/Disable PEG 3 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.
- UINT8 Peg0MaxLinkSpeed

  Offset 0x00F7 - PEG 0 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.
- UINT8 Peg1MaxLinkSpeed

  Offset 0x00F8 - PEG 1 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.
- UINT8 Peg2MaxLinkSpeed

  Offset 0x00F9 - PEG 2 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.
- UINT8 Peg3MaxLinkSpeed

Offset 0x00FA - PEG 3 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.

- UINT8 Peg0MaxLinkWidth

  Offset 0x00FB - PEG 0 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4, (0x4): Limit Link to x8 0:Auto, 1:x1, 2:x2, 3:x4, 4:x8.

- UINT8 Peg1MaxLinkWidth

  Offset 0x00FC - PEG 1 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4 0:Auto, 1:x1, 2:x2, 3:x4.

- UINT8 Peg2MaxLinkWidth

  Offset 0x00FD - PEG 2 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2 0:Auto, 1:x1, 2:x2.

- UINT8 Peg3MaxLinkWidth

  Offset 0x00FE - PEG 3 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2 0:Auto, 1:x1, 2:x2.

- UINT8 Peg0PowerDownUnusedLanes

  Offset 0x00FF - Power down unused lanes on PEG 0 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

- UINT8 Peg1PowerDownUnusedLanes

  Offset 0x0100 - Power down unused lanes on PEG 1 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

- UINT8 Peg2PowerDownUnusedLanes

  Offset 0x0101 - Power down unused lanes on PEG 2 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

- UINT8 Peg3PowerDownUnusedLanes

  Offset 0x0102 - Power down unused lanes on PEG 3 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

- UINT8 InitPcieAspmAfterOprom

  Offset 0x0103 - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.

- UINT8 PegDisableSpreadSpectrumClocking

  Offset 0x0104 - PCIe Disable Spread Spectrum Clocking PCIe Disable Spread Spectrum Clocking.

- UINT8 DmiGen3RootPortPreset [8]

  Offset 0x0105 - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.

- UINT8 DmiGen3EndPointPreset [8]

  Offset 0x010D - DMI Gen3 End port preset values per lane Used for programming DMI Gen3 preset values per lane.

- UINT8 DmiGen3EndPointHint [8]

  Offset 0x0115 - DMI Gen3 End port Hint values per lane Used for programming DMI Gen3 Hint values per lane.

- UINT8 DmiGen3RxCtlePeaking [4]

  Offset 0x011D - DMI Gen3 RxCTLEp per-Bundle control Range: 0-15, 0 is default for each bundle, must be specified based upon platform design.

- UINT8 TvbRatioClipping

  Offset 0x0121 - Thermal Velocity Boost Ratio clipping 0(Default): Disabled, 1: Enabled.

- UINT8 TvbVoltageOptimization

  Offset 0x0122 - Thermal Velocity Boost voltage optimization 0: Disabled, 1: Enabled(Default).

- UINT8 PegGen3RxCtlePeaking [10]

  Offset 0x0123 - PEG Gen3 RxCTLEp per-Bundle control Range: 0-15, 12 is default for each bundle, must be specified based upon platform design.

- UINT8 UnusedUpdSpace2 [3]

  Offset 0x012D.

- UINT32 PegDataPtr

  Offset 0x0130 - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA_PEG_DATA) and platform code can save/restore this data to skip preset search in the following boots.

- UINT8 PegGpioData [28]

  Offset 0x0134 - PEG PERST# GPIO information The reference code will use the information in this structure in order to reset PCIe Gen3 devices during equalization, if necessary.
- UINT8 PegRootPortHPE [4]

  Offset 0x0150 - PCIe Hot Plug Enable/Disable per port 0(Default): Disable, 1: Enable.
- UINT8 DmiDeEmphasis

  Offset 0x0154 - DeEmphasis control for DMI DeEmphasis control for DMI.
- UINT8 PrimaryDisplay

  Offset 0x0155 - Selection of the primary display device 0=iGFX, 1=PEG, 2=PCIe Graphics on PCH, 3(Default)=AUTO, 4=Switchable Graphics 0:iGFX, 1:PEG, 2:PCIe Graphics on PCH, 3:AUTO, 4:Switchable Graphics.
- UINT16 GttSize

  Offset 0x0156 - Selection of iGFX GTT Memory size 1=2MB, 2=4MB, 3=8MB, Default is 3 1:2MB, 2:4MB, 3:8MB.
- UINT32 GmAdr

  Offset 0x0158 - Temporary MMIO address for GMADR The reference code will use this as Temporary MMIO address space to access GMADR Registers.Platform should provide conflict free Temporary MMIO Range: GmAdr to (GmAdr + ApertureSize).
- UINT32 GttMmAdr

  Offset 0x015C - Temporary MMIO address for GTTMMADR The reference code will use this as Temporary MM↩ IO address space to access GTTMMADR Registers.Platform should provide conflict free Temporary MMIO Range: GttMmAdr to (GttMmAdr + 2MB MMIO + 6MB Reserved + GttSize).
- UINT8 PsmiRegionSize

  Offset 0x0160 - Selection of PSMI Region size 0=32MB, 1=288MB, 2=544MB, 3=800MB, 4=1024MB Default is 0 0:32MB, 1:288MB, 2:544MB, 3:800MB, 4:1024MB.
- UINT8 SaRtd3Pcie0Gpio [24]

  Offset 0x0161 - Switchable Graphics GPIO information for PEG 0 Switchable Graphics GPIO information for PEG 0, for Reset, power and wake GPIOs.
- UINT8 SaRtd3Pcie1Gpio [24]

  Offset 0x0179 - Switchable Graphics GPIO information for PEG 1 Switchable Graphics GPIO information for PEG 1, for Reset, power and wake GPIOs.
- UINT8 SaRtd3Pcie2Gpio [24]

  Offset 0x0191 - Switchable Graphics GPIO information for PEG 2 Switchable Graphics GPIO information for PEG 2, for Reset, power and wake GPIOs.
- UINT8 SaRtd3Pcie3Gpio [24]

  Offset 0x01A9 - Switchable Graphics GPIO information for PEG 3 Switchable Graphics GPIO information for PEG 3, for Reset, power and wake GPIOs.
- UINT8 TxtImplemented

  Offset 0x01C1 - Enable/Disable MRC TXT dependency When enabled MRC execution will wait for TXT initialization to be done first.
- UINT8 SaOcSupport

  Offset 0x01C2 - Enable/Disable SA OcSupport Enable: Enable SA OcSupport, Disable(Default): Disable SA Oc↩ Support $EN_DIS.
- UINT8 GtVoltageMode

  Offset 0x01C3 - GT slice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.
- UINT8 GtMaxOcRatio

  Offset 0x01C4 - Maximum GTs turbo ratio override 0(Default)=Minimal/Auto, 60=Maximum.
- UINT8 UnusedUpdSpace3

  Offset 0x01C5.
- UINT16 GtVoltageOffset

  Offset 0x01C6 - The voltage offset applied to GT slice 0(Default)=Minimal, 1000=Maximum.
- UINT16 GtVoltageOverride

  Offset 0x01C8 - The GT slice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.
- UINT16 GtExtraTurboVoltage

Offset 0x01CA - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 SaVoltageOffset

  Offset 0x01CC - voltage offset applied to the SA 0(Default)=Minimal, 1000=Maximum.

- UINT8 RootPortIndex

  Offset 0x01CE - PCIe root port Function number for Switchable Graphics dGPU Root port Index number to indicate which PCIe root port has dGPU.

- UINT8 RealtimeMemoryTiming

  Offset 0x01CF - Realtime Memory Timing 0(Default): Disabled, 1: Enabled.

- UINT8 SaIpuEnable

  Offset 0x01D0 - Enable/Disable SA IPU Enable(Default): Enable SA IPU, Disable: Disable SA IPU $EN_DIS.

- UINT8 SaIpuImrConfiguration

  Offset 0x01D1 - IPU IMR Configuration 0:IPU Camera, 1:IPU Gen Default is 0 0:IPU Camera, 1:IPU Gen.

- UINT8 GtPsmiSupport

  Offset 0x01D2 - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.

- UINT8 GtusVoltageMode

  Offset 0x01D3 - GT unslice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.

- UINT16 GtusVoltageOffset

  Offset 0x01D4 - voltage offset applied to GT unslice 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtusVoltageOverride

  Offset 0x01D6 - GT unslice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtusExtraTurboVoltage

  Offset 0x01D8 - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT8 GtusMaxOcRatio

  Offset 0x01DA - Maximum GTus turbo ratio override 0(Default)=Minimal, 60=Maximum.

- UINT8 SaPreMemProductionRsvd [1]

  Offset 0x01DB - SaPreMemProductionRsvd Reserved for SA Pre-Mem Production $EN_DIS.

- UINT16 PerCoreHtDisable

  Offset 0x01DC - Per-core HT Disable Defines the per-core HT disable mask where: 1 - Disable selected logical core HT, 0 - is ignored.

- UINT8 BistOnReset

  *Offset 0x01DE - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.*

- UINT8 SkipStopPbet

  *Offset 0x01DF - Skip Stop PBET Timer Enable/Disable Skip Stop PBET Timer; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 EnableC6Dram

  Offset 0x01E0 - C6DRAM power gating feature This policy indicates whether or not BIOS should allocate PRMRR memory for C6DRAM power gating feature.

- UINT8 OcSupport

  *Offset 0x01E1 - Over clocking support Over clocking support; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 OcLock

  *Offset 0x01E2 - Over clocking Lock Over clocking Lock Enable/Disable; 0: Disable; **1: Enable**.*

- UINT8 CoreMaxOcRatio

  Offset 0x01E3 - Maximum Core Turbo Ratio Override Maximum core turbo ratio override allows to increase CPU core frequency beyond the fused max turbo ratio limit.

- UINT8 CoreVoltageMode

  *Offset 0x01E4 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.*

- UINT8 DisableMtrrProgram

  *Offset 0x01E5 - Program Cache Attributes Program Cache Attributes; **0: Program**; 1: Disable Program.*

- UINT8 RingMaxOcRatio

  Offset 0x01E6 - Maximum clr turbo ratio override Maximum clr turbo ratio override allows to increase CPU clr frequency beyond the fused max turbo ratio limit.

- UINT8 HyperThreading

*Offset 0x01E7 - Hyper Threading Enable/Disable Enable or Disable Hyper Threading; 0: Disable; **1: Enable** $EN_↩ DIS.*

- UINT8 CpuRatio

  Offset 0x01E8 - CPU ratio value CPU ratio value.
- UINT8 BootFrequency

  Offset 0x01E9 - Boot frequency Sets the boot frequency starting from reset vector.
- UINT8 ActiveCoreCount

  Offset 0x01EA - Number of active cores Number of active cores(Depends on Number of cores).
- UINT8 FClkFrequency

  *Offset 0x01EB - Processor Early Power On Configuration FCLK setting **0: 800 MHz (ULT/ULX)**.*
- UINT8 JtagC10PowerGateDisable

  Offset 0x01EC - Set JTAG power in C10 and deeper power states False: JTAG is power gated in C10 state.
- UINT8 VmxEnable

  *Offset 0x01ED - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.*
- UINT8 Avx2RatioOffset

  Offset 0x01EE - AVX2 Ratio Offset 0(Default)= No Offset.
- UINT8 Avx3RatioOffset

  Offset 0x01EF - AVX3 Ratio Offset 0(Default)= No Offset.
- UINT8 BclkAdaptiveVoltage

  Offset 0x01F0 - BCLK Adaptive Voltage Enable When enabled, the CPU V/F curves are aware of BCLK frequency when calculated.
- UINT8 CorePllVoltageOffset

  Offset 0x01F1 - Core PLL voltage offset Core PLL voltage offset.
- UINT16 CoreVoltageOverride

  Offset 0x01F2 - core voltage override The core voltage override which is applied to the entire range of cpu core frequencies.
- UINT16 CoreVoltageAdaptive

  Offset 0x01F4 - Core Turbo voltage Adaptive Extra Turbo voltage applied to the cpu core when the cpu is operating in turbo mode.
- UINT16 CoreVoltageOffset

  Offset 0x01F6 - Core Turbo voltage Offset The voltage offset applied to the core while operating in turbo mode.Valid Range 0 to 1000.
- UINT8 RingDownBin

  Offset 0x01F8 - Ring Downbin Ring Downbin enable/disable.
- UINT8 RingVoltageMode

  *Offset 0x01F9 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.*
- UINT16 RingVoltageOverride

  Offset 0x01FA - Ring voltage override The ring voltage override which is applied to the entire range of cpu ring frequencies.
- UINT16 RingVoltageAdaptive

  Offset 0x01FC - Ring Turbo voltage Adaptive Extra Turbo voltage applied to the cpu ring when the cpu is operating in turbo mode.
- UINT16 RingVoltageOffset

  Offset 0x01FE - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.
- UINT8 TjMaxOffset

  Offset 0x0200 - TjMax Offset TjMax offset.Specified value here is clipped by pCode (125 - TjMax Offset) to support TjMax in the range of 62 to 115 deg Celsius.
- UINT8 BiosGuard

  Offset 0x0201 - BiosGuard Enable/Disable.
- UINT8 BiosGuardToolsInterface

  Offset 0x0202.
- UINT8 EnableSgx

Offset 0x0203 - EnableSgx Enable/Disable.

- UINT8 Txt

  Offset 0x0204 - Txt Enable/Disable.

- UINT8 UnusedUpdSpace4 [3]

  Offset 0x0205.

- UINT32 PrmrrSize

  Offset 0x0208 - PrmrrSize 0=Invalid, 32MB=0x2000000, 64MB=0x4000000, 128MB=0x8000000, 256↩ MB=0x10000000.

- UINT32 SinitMemorySize

  Offset 0x020C - SinitMemorySize Enable/Disable.

- UINT32 TxtHeapMemorySize

  Offset 0x0210 - TxtHeapMemorySize Enable/Disable.

- UINT32 TxtDprMemorySize

  Offset 0x0214 - TxtDprMemorySize Enable/Disable.

- UINT64 TxtDprMemoryBase

  Offset 0x0218 - TxtDprMemoryBase Enable/Disable.

- UINT32 BiosAcmBase

  Offset 0x0220 - BiosAcmBase Enable/Disable.

- UINT32 BiosAcmSize

  Offset 0x0224 - BiosAcmSize Enable/Disable.

- UINT32 ApStartupBase

  Offset 0x0228 - ApStartupBase Enable/Disable.

- UINT32 TgaSize

  Offset 0x022C - TgaSize Enable/Disable.

- UINT64 TxtLcpPdBase

  Offset 0x0230 - TxtLcpPdBase Enable/Disable.

- UINT64 TxtLcpPdSize

  Offset 0x0238 - TxtLcpPdSize Enable/Disable.

- UINT8 IsTPMPresence

  Offset 0x0240 - IsTPMPresence IsTPMPresence default values.

- UINT8 AutoEasyOverclock

  Offset 0x0241 - Intel Speed Optimizer Enable : CML won't support BIOS ISO.

- UINT8 VmaxStress

  Offset 0x0242 - Vmax Stress Vmax Stress enable/disable.

- UINT8 ReservedSecurityPreMem [1]

  Offset 0x0243 - ReservedSecurityPreMem Reserved for Security Pre-Mem $EN_DIS.

- UINT32 VtdBaseAddress [3]

  Offset 0x0244 - Base addresses for VT-d function MMIO access Base addresses for VT-d MMIO access per VT-d engine.

- UINT8 SmbusEnable

  Offset 0x0250 - Enable SMBus Enable/disable SMBus controller.

- UINT8 PlatformDebugConsent

  Offset 0x0251 - Platform Debug Consent To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type.

- UINT8 DciUsb3TypecUfpDbg

  Offset 0x0252 - USB3 Type-C UFP2DFP Kernel/Platform Debug Support This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting.

- UINT8 PchTraceHubMode

  Offset 0x0253 - PCH Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

- UINT8 PchTraceHubMemReg0Size

Offset 0x0254 - PCH Trace Hub Memory Region 0 buffer Size Specify size of Pch trace memory region 0 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

- UINT8 PchTraceHubMemReg1Size

  Offset 0x0255 - PCH Trace Hub Memory Region 1 buffer Size Specify size of Pch trace memory region 1 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

- UINT8 PchHdaEnable

  Offset 0x0256 - Enable Intel HD Audio (Azalia) 0: Disable, 1: Enable (Default) Azalia controller $EN_DIS.

- UINT8 PchIshEnable

  Offset 0x0257 - Enable PCH ISH Controller 0: Disable, 1: Enable (Default) ISH Controller $EN_DIS.

- UINT8 PchPcieHsioRxSetCtleEnable [24]

  Offset 0x0258 - Enable PCH HSIO PCIE Rx Set Ctle Enable PCH PCIe Gen 3 Set CTLE Value.

- UINT8 PchPcieHsioRxSetCtle [24]

  Offset 0x0270 - PCH HSIO PCIE Rx Set Ctle Value PCH PCIe Gen 3 Set CTLE Value.

- UINT8 PchPcieHsioTxGen1DownscaleAmpEnable [24]

  Offset 0x0288 - Enble PCH HSIO PCIE TX Gen 1 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen1DownscaleAmp [24]

  Offset 0x02A0 - PCH HSIO PCIE Gen 2 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 2 TX Output Downscale Amplitude Adjustment value.

- UINT8 PchPcieHsioTxGen2DownscaleAmpEnable [24]

  Offset 0x02B8 - Enable PCH HSIO PCIE TX Gen 2 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DownscaleAmp [24]

  Offset 0x02D0 - PCH HSIO PCIE Gen 2 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 2 TX Output Downscale Amplitude Adjustment value.

- UINT8 PchPcieHsioTxGen3DownscaleAmpEnable [24]

  Offset 0x02E8 - Enable PCH HSIO PCIE TX Gen 3 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen3DownscaleAmp [24]

  Offset 0x0300 - PCH HSIO PCIE Gen 3 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 3 TX Output Downscale Amplitude Adjustment value.

- UINT8 PchPcieHsioTxGen1DeEmphEnable [24]

  Offset 0x0318 - Enable PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen1DeEmph [24]

  Offset 0x0330 - PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment value PCH PCIe Gen 1 TX Output De-Emphasis Adjustment Setting.

- UINT8 PchPcieHsioTxGen2DeEmph3p5Enable [24]

  Offset 0x0348 - Enable PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DeEmph3p5 [24]

  Offset 0x0360 - PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment value PCH PCIe Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting.

- UINT8 PchPcieHsioTxGen2DeEmph6p0Enable [24]

  Offset 0x0378 - Enable PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DeEmph6p0 [24]

  Offset 0x0390 - PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment value PCH PCIe Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting.

- UINT8 PchSataHsioRxGen1EqBoostMagEnable [8]

  Offset 0x03A8 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↩ : Disable; 1: Enable.

- UINT8 PchSataHsioRxGen1EqBoostMag [8]

Offset 0x03B0 - PCH HSIO SATA 1.5 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 1.5 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

- UINT8 PchSataHsioRxGen2EqBoostMagEnable [8]

  Offset 0x03B8 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↵ : Disable; 1: Enable.

- UINT8 PchSataHsioRxGen2EqBoostMag [8]

  Offset 0x03C0 - PCH HSIO SATA 3.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 3.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

- UINT8 PchSataHsioRxGen3EqBoostMagEnable [8]

  Offset 0x03C8 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↵ : Disable; 1: Enable.

- UINT8 PchSataHsioRxGen3EqBoostMag [8]

  Offset 0x03D0 - PCH HSIO SATA 6.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 6.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

- UINT8 PchSataHsioTxGen1DownscaleAmpEnable [8]

  Offset 0x03D8 - Enable PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen1DownscaleAmp [8]

  Offset 0x03E0 - PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value.

- UINT8 PchSataHsioTxGen2DownscaleAmpEnable [8]

  Offset 0x03E8 - Enable PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen2DownscaleAmp [8]

  Offset 0x03F0 - PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value.

- UINT8 PchSataHsioTxGen3DownscaleAmpEnable [8]

  Offset 0x03F8 - Enable PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen3DownscaleAmp [8]

  Offset 0x0400 - PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value.

- UINT8 PchSataHsioTxGen1DeEmphEnable [8]

  Offset 0x0408 - Enable PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen1DeEmph [8]

  Offset 0x0410 - PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting.

- UINT8 PchSataHsioTxGen2DeEmphEnable [8]

  Offset 0x0418 - Enable PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen2DeEmph [8]

  Offset 0x0420 - PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting.

- UINT8 PchSataHsioTxGen3DeEmphEnable [8]

  Offset 0x0428 - Enable PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen3DeEmph [8]

  Offset 0x0430 - PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting.

- UINT8 PchLpcEnhancePort8xhDecoding

  Offset 0x0438 - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.

- UINT8 PchPort80Route

  Offset 0x0439 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.

- UINT8 SmbusArpEnable

  Offset 0x043A - Enable SMBus ARP support Enable SMBus ARP support.
- UINT8 PchNumRsvdSmbusAddresses

  Offset 0x043B - Number of RsvdSmbusAddressTable.
- UINT16 PchSmbusIoBase

  Offset 0x043C - SMBUS Base Address SMBUS Base Address (IO space).
- UINT16 PcieImrSize

  Offset 0x043E - Size of PCIe IMR.
- UINT32 RsvdSmbusAddressTablePtr

  Offset 0x0440 - Point of RsvdSmbusAddressTable Array of addresses reserved for non-ARP-capable SMBus devices.
- UINT32 PcieRpEnableMask

  Offset 0x0444 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.
- UINT8 PcieImrEnabled

  Offset 0x0448 - Enable PCIe IMR 0:Disable, 1:Enable $EN_DIS.
- UINT8 ImrRpSelection

  Offset 0x0449 - Root port number for IMR.
- UINT8 PchSmbAlertEnable

  Offset 0x044A - Enable SMBus Alert Pin Enable SMBus Alert Pin.
- UINT8 PcdDebugInterfaceFlags

  Offset 0x044B - Debug Interfaces Debug Interfaces.
- UINT8 SerialIoUartDebugControllerNumber

  Offset 0x044C - Serial Io Uart Debug Controller Number Select SerialIo Uart Controller for debug.
- UINT8 SerialIoUartDebugAutoFlow

  Offset 0x044D - Serial Io Uart Debug Auto Flow Enables UART hardware flow control, CTS and RTS lines.
- UINT8 UnusedUpdSpace5 [2]

  Offset 0x044E.
- UINT32 SerialIoUartDebugBaudRate

  Offset 0x0450 - Serial Io Uart Debug BaudRate Set default BaudRate Supported from 0 - default to 6000000.
- UINT8 SerialIoUartDebugParity

  Offset 0x0454 - Serial Io Uart Debug Parity Set default Parity.
- UINT8 SerialIoUartDebugStopBits

  Offset 0x0455 - Serial Io Uart Debug Stop Bits Set default stop bits.
- UINT8 SerialIoUartDebugDataBits

  Offset 0x0456 - Serial Io Uart Debug Data Bits Set default word length.
- UINT8 PchHdaDspEnable

  Offset 0x0457 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.
- UINT8 PchHdaVcType

  Offset 0x0458 - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.
- UINT8 PchHdaDspUaaCompliance

  Offset 0x0459 - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).
- UINT8 PchHdaAudioLinkHda

  Offset 0x045A - Enable HD Audio Link Enable/disable HD Audio Link.
- UINT8 PchHdaAudioLinkDmic0

  Offset 0x045B - Enable HD Audio DMIC0 Link Deprecated.
- UINT8 PchHdaAudioLinkDmic1

  Offset 0x045C - Enable HD Audio DMIC1 Link Deprecated.
- UINT8 PchHdaAudioLinkSsp0

  Offset 0x045D - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.
- UINT8 PchHdaAudioLinkSsp1

  Offset 0x045E - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.

- UINT8 PchHdaAudioLinkSsp2

  Offset 0x045F - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.
- UINT8 PchHdaAudioLinkSndw1

  Offset 0x0460 - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.
- UINT8 PchHdaAudioLinkSndw2

  Offset 0x0461 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.
- UINT8 PchHdaAudioLinkSndw3

  Offset 0x0462 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.
- UINT8 PchHdaAudioLinkSndw4

  Offset 0x0463 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.
- UINT8 PchHdaSndwBufferRcomp

  Offset 0x0464 - Soundwire Clock Buffer GPIO RCOMP Setting 0: non-ACT - 50 Ohm driver impedance, 1: ACT - 8 Ohm driver impedance.
- UINT8 ReservedPchPreMem [2]

  Offset 0x0465 - ReservedPchPreMem Reserved for Pch Pre-Mem $EN_DIS.
- UINT8 PcdIsaSerialUartBase

  Offset 0x0467 - ISA Serial Base selection Select ISA Serial Base address.
- UINT8 GtPllVoltageOffset

  Offset 0x0468 - GT PLL voltage offset Core PLL voltage offset.
- UINT8 RingPllVoltageOffset

  Offset 0x0469 - Ring PLL voltage offset Core PLL voltage offset.
- UINT8 SaPllVoltageOffset

  Offset 0x046A - System Agent PLL voltage offset Core PLL voltage offset.
- UINT8 McPllVoltageOffset

  Offset 0x046B - Memory Controller PLL voltage offset Core PLL voltage offset.
- UINT8 MrcSafeConfig

  Offset 0x046C - MRC Safe Config Enables/Disable MRC Safe Config $EN_DIS.
- UINT8 PcdSerialDebugBaudRate

  Offset 0x046D - PcdSerialDebugBaudRate Baud Rate for Serial Debug Messages.
- UINT8 HobBufferSize

  Offset 0x046E - HobBufferSize Size to set HOB Buffer.
- UINT8 ECT

  Offset 0x046F - Early Command Training Enables/Disable Early Command Training $EN_DIS.
- UINT8 SOT

  Offset 0x0470 - SenseAmp Offset Training Enables/Disable SenseAmp Offset Training $EN_DIS.
- UINT8 ERDMPRTC2D

  Offset 0x0471 - Early ReadMPR Timing Centering 2D Enables/Disable Early ReadMPR Timing Centering 2D $EN↩ _DIS.
- UINT8 RDMPRT

  Offset 0x0472 - Read MPR Training Enables/Disable Read MPR Training $EN_DIS.
- UINT8 RCVET

  Offset 0x0473 - Receive Enable Training Enables/Disable Receive Enable Training $EN_DIS.
- UINT8 JWRL

  Offset 0x0474 - Jedec Write Leveling Enables/Disable Jedec Write Leveling $EN_DIS.
- UINT8 EWRTC2D

  Offset 0x0475 - Early Write Time Centering 2D Enables/Disable Early Write Time Centering 2D $EN_DIS.
- UINT8 ERDTC2D

  Offset 0x0476 - Early Read Time Centering 2D Enables/Disable Early Read Time Centering 2D $EN_DIS.
- UINT8 WRTC1D

  Offset 0x0477 - Write Timing Centering 1D Enables/Disable Write Timing Centering 1D $EN_DIS.
- UINT8 WRVC1D

Offset 0x0478 - Write Voltage Centering 1D Enables/Disable Write Voltage Centering 1D $EN_DIS.

- UINT8 RDTC1D

  Offset 0x0479 - Read Timing Centering 1D Enables/Disable Read Timing Centering 1D $EN_DIS.
- UINT8 DIMMODTT

  Offset 0x047A - Dimm ODT Training Enables/Disable Dimm ODT Training $EN_DIS.
- UINT8 DIMMRONT

  Offset 0x047B - DIMM RON Training Enables/Disable DIMM RON Training $EN_DIS.
- UINT8 WRDSEQT

  Offset 0x047C - Write Drive Strength/Equalization 2D Enables/Disable Write Drive Strength/Equalization 2D $EN_↩ DIS.
- UINT8 WRSRT

  Offset 0x047D - Write Slew Rate Training Enables/Disable Write Slew Rate Training $EN_DIS.
- UINT8 RDODTT

  Offset 0x047E - Read ODT Training Enables/Disable Read ODT Training $EN_DIS.
- UINT8 RDEQT

  Offset 0x047F - Read Equalization Training Enables/Disable Read Equalization Training $EN_DIS.
- UINT8 RDAPT

  Offset 0x0480 - Read Amplifier Training Enables/Disable Read Amplifier Training $EN_DIS.
- UINT8 WRTC2D

  Offset 0x0481 - Write Timing Centering 2D Enables/Disable Write Timing Centering 2D $EN_DIS.
- UINT8 RDTC2D

  Offset 0x0482 - Read Timing Centering 2D Enables/Disable Read Timing Centering 2D $EN_DIS.
- UINT8 WRVC2D

  Offset 0x0483 - Write Voltage Centering 2D Enables/Disable Write Voltage Centering 2D $EN_DIS.
- UINT8 RDVC2D

  Offset 0x0484 - Read Voltage Centering 2D Enables/Disable Read Voltage Centering 2D $EN_DIS.
- UINT8 CMDVC

  Offset 0x0485 - Command Voltage Centering Enables/Disable Command Voltage Centering $EN_DIS.
- UINT8 LCT

  Offset 0x0486 - Late Command Training Enables/Disable Late Command Training $EN_DIS.
- UINT8 RTL

  Offset 0x0487 - Round Trip Latency Training Enables/Disable Round Trip Latency Training $EN_DIS.
- UINT8 TAT

  Offset 0x0488 - Turn Around Timing Training Enables/Disable Turn Around Timing Training $EN_DIS.
- UINT8 MEMTST

  Offset 0x0489 - Memory Test Enables/Disable Memory Test $EN_DIS.
- UINT8 ALIASCHK

  Offset 0x048A - DIMM SPD Alias Test Enables/Disable DIMM SPD Alias Test $EN_DIS.
- UINT8 RCVENC1D

  Offset 0x048B - Receive Enable Centering 1D Enables/Disable Receive Enable Centering 1D $EN_DIS.
- UINT8 RMC

  Offset 0x048C - Retrain Margin Check Enables/Disable Retrain Margin Check $EN_DIS.
- UINT8 WRDSUDT

  Offset 0x048D - Write Drive Strength Up/Dn independently Enables/Disable Write Drive Strength Up/Dn independently $EN_DIS.
- UINT8 EccSupport

  Offset 0x048E - ECC Support Enables/Disable ECC Support $EN_DIS.
- UINT8 RemapEnable

  Offset 0x048F - Memory Remap Enables/Disable Memory Remap $EN_DIS.
- UINT8 RankInterleave

  Offset 0x0490 - Rank Interleave support Enables/Disable Rank Interleave support.

- UINT8 EnhancedInterleave

  Offset 0x0491 - Enhanced Interleave support Enables/Disable Enhanced Interleave support $EN_DIS.
- UINT8 MemoryTrace

  Offset 0x0492 - Memory Trace Enable Memory Trace of Ch 0 to Ch 1 using Stacked Mode.
- UINT8 ChHashEnable

  Offset 0x0493 - Ch Hash Support Enable/Disable Channel Hash Support.
- UINT8 EnableExtts

  Offset 0x0494 - Extern Therm Status Enables/Disable Extern Therm Status $EN_DIS.
- UINT8 EnableCltm

  Offset 0x0495 - Closed Loop Therm Manage Enables/Disable Closed Loop Therm Manage $EN_DIS.
- UINT8 EnableOltm

  Offset 0x0496 - Open Loop Therm Manage Enables/Disable Open Loop Therm Manage $EN_DIS.
- UINT8 EnablePwrDn

  Offset 0x0497 - DDR PowerDown and idle counter Enables/Disable DDR PowerDown and idle counter $EN_DIS.
- UINT8 EnablePwrDnLpddr

  Offset 0x0498 - DDR PowerDown and idle counter - LPDDR Enables/Disable DDR PowerDown and idle counter(For LPDDR Only) $EN_DIS.
- UINT8 UserPowerWeightsEn

  Offset 0x0499 - Use user provided power weights, scale factor, and channel power floor values Enables/Disable Use user provided power weights, scale factor, and channel power floor values $EN_DIS.
- UINT8 RaplLim2Lock

  Offset 0x049A - RAPL PL Lock Enables/Disable RAPL PL Lock $EN_DIS.
- UINT8 RaplLim2Ena

  Offset 0x049B - RAPL PL 2 enable Enables/Disable RAPL PL 2 enable $EN_DIS.
- UINT8 RaplLim1Ena

  Offset 0x049C - RAPL PL 1 enable Enables/Disable RAPL PL 1 enable $EN_DIS.
- UINT8 SrefCfgEna

  Offset 0x049D - SelfRefresh Enable Enables/Disable SelfRefresh Enable $EN_DIS.
- UINT8 ThrtCkeMinDefeatLpddr

  Offset 0x049E - Throttler CKEMin Defeature - LPDDR Enables/Disable Throttler CKEMin Defeature(For LPDDR Only) $EN_DIS.
- UINT8 ThrtCkeMinDefeat

  Offset 0x049F - Throttler CKEMin Defeature Enables/Disable Throttler CKEMin Defeature $EN_DIS.
- UINT8 RhPrevention

  Offset 0x04A0 - Enable RH Prevention Enables/Disable RH Prevention $EN_DIS.
- UINT8 ExitOnFailure

  Offset 0x04A1 - Exit On Failure (MRC) Enables/Disable Exit On Failure (MRC) $EN_DIS.
- UINT8 DdrThermalSensor

  Offset 0x04A2 - LPDDR Thermal Sensor Enables/Disable LPDDR Thermal Sensor $EN_DIS.
- UINT8 Ddr4DdpSharedClock

  Offset 0x04A3 - Select if CLK0 is shared between Rank0 and Rank1 in DDR4 DDP Select if CLK0 is shared between Rank0 and Rank1 in DDR4 DDP $EN_DIS.
- UINT8 Ddr4DdpSharedZq

  Offset 0x04A4 - Select if ZQ pin is shared between Rank0 and Rank1 in DDR4 DDP ESelect if ZQ pin is shared between Rank0 and Rank1 in DDR4 DDP $EN_DIS.
- UINT8 UnusedUpdSpace6

  Offset 0x04A5.
- UINT16 ChHashMask

  Offset 0x04A6 - Ch Hash Mask Set the BIT(s) to be included in the XOR function.
- UINT32 BClkFrequency

  Offset 0x04A8 - Base reference clock value Base reference clock value, in Hertz(Default is 125Hz) 100000000:100Hz, 125000000:125Hz, 167000000:167Hz, 250000000:250Hz.

- UINT8 ChHashInterleaveBit

  Offset 0x04AC - Ch Hash Interleaved Bit Select the BIT to be used for Channel Interleaved mode.
- UINT8 EnergyScaleFact

  Offset 0x04AD - Energy Scale Factor Energy Scale Factor, Default is 4.
- UINT16 Idd3n

  Offset 0x04AE - EPG DIMM Idd3N Active standby current (Idd3N) in milliamps from datasheet.
- UINT16 Idd3p

  Offset 0x04B0 - EPG DIMM Idd3P Active power-down current (Idd3P) in milliamps from datasheet.
- UINT8 CMDSR

  Offset 0x04B2 - CMD Slew Rate Training Enable/Disable CMD Slew Rate Training $EN_DIS.
- UINT8 CMDDSEQ

  Offset 0x04B3 - CMD Drive Strength and Tx Equalization Enable/Disable CMD Drive Strength and Tx Equalization $EN_DIS.
- UINT8 CMDNORM

  Offset 0x04B4 - CMD Normalization Enable/Disable CMD Normalization $EN_DIS.
- UINT8 EWRDSEQ

  Offset 0x04B5 - Early DQ Write Drive Strength and Equalization Training Enable/Disable Early DQ Write Drive Strength and Equalization Training $EN_DIS.
- UINT8 RhActProbability

  Offset 0x04B6 - RH Activation Probability RH Activation Probability, Probability value is 1/2^(inputvalue)
- UINT8 RaplLim2WindX

  Offset 0x04B7 - RAPL PL 2 WindowX Power PL 2 time window X value, (1/1024)∗(1+(x/4))∗(2^y) (1=Def)
- UINT8 RaplLim2WindY

  Offset 0x04B8 - RAPL PL 2 WindowY Power PL 2 time window Y value, (1/1024)∗(1+(x/4))∗(2^y) (1=Def)
- UINT8 RaplLim1WindX

  Offset 0x04B9 - RAPL PL 1 WindowX Power PL 1 time window X value, (1/1024)∗(1+(x/4))∗(2^y) (0=Def)
- UINT8 RaplLim1WindY

  Offset 0x04BA - RAPL PL 1 WindowY Power PL 1 time window Y value, (1/1024)∗(1+(x/4))∗(2^y) (0=Def)
- UINT8 UnusedUpdSpace7

  Offset 0x04BB.
- UINT16 RaplLim2Pwr

  Offset 0x04BC - RAPL PL 2 Power range[0;2^14-1]= [2047.875;0]in W, (222= Def)
- UINT16 RaplLim1Pwr

  Offset 0x04BE - RAPL PL 1 Power range[0;2^14-1]= [2047.875;0]in W, (0= Def)
- UINT8 WarmThresholdCh0Dimm0

  Offset 0x04C0 - Warm Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmThresholdCh0Dimm1

  Offset 0x04C1 - Warm Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmThresholdCh1Dimm0

  Offset 0x04C2 - Warm Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmThresholdCh1Dimm1

  Offset 0x04C3 - Warm Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotThresholdCh0Dimm0

  Offset 0x04C4 - Hot Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotThresholdCh0Dimm1

  Offset 0x04C5 - Hot Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotThresholdCh1Dimm0

  Offset 0x04C6 - Hot Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotThresholdCh1Dimm1

  Offset 0x04C7 - Hot Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmBudgetCh0Dimm0

Offset 0x04C8 - Warm Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

- UINT8 WarmBudgetCh0Dimm1

  Offset 0x04C9 - Warm Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmBudgetCh1Dimm0

  Offset 0x04CA - Warm Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 WarmBudgetCh1Dimm1

  Offset 0x04CB - Warm Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotBudgetCh0Dimm0

  Offset 0x04CC - Hot Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotBudgetCh0Dimm1

  Offset 0x04CD - Hot Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotBudgetCh1Dimm0

  Offset 0x04CE - Hot Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 HotBudgetCh1Dimm1

  Offset 0x04CF - Hot Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
- UINT8 IdleEnergyCh0Dimm0

  Offset 0x04D0 - Idle Energy Ch0Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
- UINT8 IdleEnergyCh0Dimm1

  Offset 0x04D1 - Idle Energy Ch0Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
- UINT8 IdleEnergyCh1Dimm0

  Offset 0x04D2 - Idle Energy Ch1Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
- UINT8 IdleEnergyCh1Dimm1

  Offset 0x04D3 - Idle Energy Ch1Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
- UINT8 PdEnergyCh0Dimm0

  Offset 0x04D4 - PowerDown Energy Ch0Dimm0 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
- UINT8 PdEnergyCh0Dimm1

  Offset 0x04D5 - PowerDown Energy Ch0Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
- UINT8 PdEnergyCh1Dimm0

  Offset 0x04D6 - PowerDown Energy Ch1Dimm0 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
- UINT8 PdEnergyCh1Dimm1

  Offset 0x04D7 - PowerDown Energy Ch1Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
- UINT8 ActEnergyCh0Dimm0

  Offset 0x04D8 - Activate Energy Ch0Dimm0 Activate Energy Contribution, range[255;0],(172= Def)
- UINT8 ActEnergyCh0Dimm1

  Offset 0x04D9 - Activate Energy Ch0Dimm1 Activate Energy Contribution, range[255;0],(172= Def)
- UINT8 ActEnergyCh1Dimm0

  Offset 0x04DA - Activate Energy Ch1Dimm0 Activate Energy Contribution, range[255;0],(172= Def)
- UINT8 ActEnergyCh1Dimm1

  Offset 0x04DB - Activate Energy Ch1Dimm1 Activate Energy Contribution, range[255;0],(172= Def)
- UINT8 RdEnergyCh0Dimm0

  Offset 0x04DC - Read Energy Ch0Dimm0 Read Energy Contribution, range[255;0],(212= Def)
- UINT8 RdEnergyCh0Dimm1

  Offset 0x04DD - Read Energy Ch0Dimm1 Read Energy Contribution, range[255;0],(212= Def)
- UINT8 RdEnergyCh1Dimm0

  Offset 0x04DE - Read Energy Ch1Dimm0 Read Energy Contribution, range[255;0],(212= Def)
- UINT8 RdEnergyCh1Dimm1

  Offset 0x04DF - Read Energy Ch1Dimm1 Read Energy Contribution, range[255;0],(212= Def)

- UINT8 WrEnergyCh0Dimm0

  Offset 0x04E0 - Write Energy Ch0Dimm0 Write Energy Contribution, range[255;0],(221= Def)
- UINT8 WrEnergyCh0Dimm1

  Offset 0x04E1 - Write Energy Ch0Dimm1 Write Energy Contribution, range[255;0],(221= Def)
- UINT8 WrEnergyCh1Dimm0

  Offset 0x04E2 - Write Energy Ch1Dimm0 Write Energy Contribution, range[255;0],(221= Def)
- UINT8 WrEnergyCh1Dimm1

  Offset 0x04E3 - Write Energy Ch1Dimm1 Write Energy Contribution, range[255;0],(221= Def)
- UINT8 ThrtCkeMinTmr

  Offset 0x04E4 - Throttler CKEMin Timer Timer value for CKEMin, range[255;0].
- UINT8 CkeRankMapping

  Offset 0x04E5 - Cke Rank Mapping Bits [7:4] - Channel 1, bits [3:0] - Channel 0.
- UINT8 RaplPwrFlCh0

  Offset 0x04E6 - Rapl Power Floor Ch0 Power budget ,range[255;0],(0= 5.3W Def)
- UINT8 RaplPwrFlCh1

  Offset 0x04E7 - Rapl Power Floor Ch1 Power budget ,range[255;0],(0= 5.3W Def)
- UINT8 EnCmdRate

  Offset 0x04E8 - Command Rate Support CMD Rate and Limit Support Option.
- UINT8 Refresh2X

  Offset 0x04E9 - REFRESH_2X_MODE 0- (Default)Disabled 1-iMC enables 2xRef when Warm and Hot 2- iMC enables 2xRef when Hot 0:Disable, 1:Enabled for WARM or HOT, 2:Enabled HOT only.
- UINT8 EpgEnable

  Offset 0x04EA - Energy Performance Gain Enable/disable(default) Energy Performance Gain.
- UINT8 RhSolution

  Offset 0x04EB - Row Hammer Solution Type of method used to prevent Row Hammer.
- UINT8 UserThresholdEnable

  Offset 0x04EC - User Manual Threshold Disabled: Predefined threshold will be used.
- UINT8 UserBudgetEnable

  Offset 0x04ED - User Manual Budget Disabled: Configuration of memories will defined the Budget value.
- UINT8 TsodTcritMax

  Offset 0x04EE - TcritMax Maximum Critical Temperature in Centigrade of the On-DIMM Thermal Sensor.
- UINT8 TsodEventMode

  Offset 0x04EF - Event mode Disable:Comparator mode.
- UINT8 TsodEventPolarity

  Offset 0x04F0 - EVENT polarity Disable:Active LOW.
- UINT8 TsodCriticalEventOnly

  Offset 0x04F1 - Critical event only Disable:Trips on alarm or critical.
- UINT8 TsodEventOutputControl

  Offset 0x04F2 - Event output control Disable:Event output disable.
- UINT8 TsodAlarmwindowLockBit

  Offset 0x04F3 - Alarm window lock bit Disable:Alarm trips are not locked and can be changed.
- UINT8 TsodCriticaltripLockBit

  Offset 0x04F4 - Critical trip lock bit Disable:Critical trip is not locked and can be changed.
- UINT8 TsodShutdownMode

  Offset 0x04F5 - Shutdown mode Disable:Temperature sensor enable.
- UINT8 TsodThigMax

  Offset 0x04F6 - ThighMax Thigh = ThighMax (Default is 93)
- UINT8 TsodManualEnable

  Offset 0x04F7 - User Manual Thig and Tcrit Disabled(Default): Temperature will be given by the configuration of memories and 1x or 2xrefresh rate.
- UINT8 ForceOltmOrRefresh2x

Offset 0x04F8 - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.

- UINT8 PwdwnIdleCounter

  Offset 0x04F9 - Pwr Down Idle Timer The minimum value should = to the worst case Roundtrip delay + Burst_Length.

- UINT8 CmdRanksTerminated

  Offset 0x04FA - Bitmask of ranks that have CA bus terminated Offset 225 LPDDR4: Bitmask of ranks that have CA bus terminated.

- UINT8 GdxcEnable

  Offset 0x04FB - GDXC MOT enable GDXC MOT enable.

- UINT8 PcdSerialDebugLevel

  Offset 0x04FC - PcdSerialDebugLevel Serial Debug Message Level.

- UINT8 FivrFaults

  Offset 0x04FD - Fivr Faults Fivr Faults; 0: Disabled; ***1: Enabled.***

- UINT8 FivrEfficiency

  Offset 0x04FE - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; ***1: Enabled.***

- UINT8 SafeMode

  Offset 0x04FF - Safe Mode Support This option configures the varous items in the IO and MC to be more conservative.

- UINT8 CleanMemory

  Offset 0x0500 - Ask MRC to clear memory content Ask MRC to clear memory content ***0: Do not Clear Memory;*** *1: Clear Memory.*

- UINT8 LpDdrDqDqsReTraining

  Offset 0x0501 - LpDdrDqDqsReTraining Enables/Disable LpDdrDqDqsReTraining $EN_DIS.

- UINT16 PostCodeOutputPort

  Offset 0x0502 - Post Code Output Port This option configures Post Code Output Port.

- UINT8 RMTLoopCount

  Offset 0x0504 - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.

- UINT8 EnBER

  Offset 0x0505 - BER Support Enable/Disable the Rank Margin Tool interpolation/extrapolation.

- UINT8 DualDimmPerChannelBoardType

  Offset 0x0506 - Dual Dimm Per-Channel Board Type Option to indicate if Board Layout includes One/Two DIMMs per channel.

- UINT8 Ddr4Mixed2DpcLimit

  Offset 0x0507 - DDR4 Mixed U-DIMM 2DPC Limitation Enable/Disable Frequency Limitation for DDR4 Mixed Dimm 2DPC Memory Configurations.

- UINT8 FastBootRmt

  Offset 0x0508 - RMT on Fast flow Enable/Disable RMT on Fast flow.

- UINT8 ReservedFspmUpdCfl

  Offset 0x0509 - CFL Reserved Reserved FspmConfig CFL $EN_DIS.

- UINT8 MemTestOnWarmBoot

  Offset 0x050A - Memory Test on Warm Boot Run Base Memory Test on Warm Boot 0:Disable, 1:Enable.

- UINT8 ThrtCkeMinTmrLpddr

  Offset 0x050B - Throttler CKEMin Timer - LPDDR Timer value for CKEMin (For LPDDR Only), range[255;0].

- UINT8 X2ApicOptOut

  Offset 0x050C - State of X2APIC_OPT_OUT bit in the DMAR table 0=Disable/Clear, 1=Enable/Set $EN_DIS.

- UINT8 MrcTrainOnWarm

  Offset 0x050D - MRC Force training on Warm Enables/Disable the MRC training on warm boot $EN_DIS.

- UINT8 LpddrDramOdt

  Offset 0x050E - Lpddr Dram Odt Override Enable/Disable for the ODT logic for LPDDR3 memory.

- UINT8 Ddr4SkipRefreshEn

  Offset 0x050F - DDR4 Skip Refresh Enable Enable/Disable of DDR4 Temperature Controlled Refresh on DRAM.

- UINT8 SerialDebugMrcLevel

  Offset 0x0510 - SerialDebugMrcLevel MRC Serial Debug Message Level.

- UINT8 PchHdaSndwLinkIoControlEnabled [4]

    Offset 0x0511 - Enable HD Audio Sndw Link IO Control deprecated.
- UINT8 CoreVfPointOffsetMode

    *Offset 0x0515 - Core VF Point Offset Mode Selects Core Voltage & Frequency Point Offset between Legacy and Selection modes; **0: Legacy**; 1: Selection.*
- UINT16 CoreVfPointOffset [15]

    Offset 0x0516 - Core VF Point Offset Array used to specifies the Offset Voltage applied to the each selected Core VF Point.
- UINT8 CoreVfPointOffsetPrefix [15]

    *Offset 0x0534 - Core VF Point Offset Prefix Sets the CoreVfPointOffset value as positive or negative for corresponding core VF Point; **0: Positive** ; 1: Negative.*
- UINT8 CoreVfPointRatio [15]

    Offset 0x0543 - Core VF Point Ratio Array for the each selected Core VF Point to display the ration.
- UINT8 CoreVfPointCount

    Offset 0x0552 - Core VF Point Count Number of supported Core Voltage & Frequency Point Offset.
- UINT8 RefreshPanicWm

    Offset 0x0553 - REFRESH_PANIC_WM Refresh Panic Watermark, range 1-9.
- UINT8 RefreshHpWm

    Offset 0x0554 - REFRESH_HP_WM Refresh High Priority Watermark, range 1-9.
- UINT8 RetrainOnFastFail

    Offset 0x0555 - Retrain On Fast Fail Restart MRC in Cold mode if SW MemTest fails during Fast flow.
- UINT8 DllBwEnOverride

    Offset 0x0556 - DllBwEnOverride DllBwEnOverride 0: Disable(Default), 1: Enable $EN_DIS.
- UINT8 ReservedFspmUpd [1]

    Offset 0x0557.

13.33.1 Detailed Description

Fsp M Configuration.

Definition at line 56 of file FspmUpd.h.

13.33.2 Member Data Documentation

13.33.2.1 ActiveCoreCount

```
UINT8 FSP_M_CONFIG::ActiveCoreCount
```

Offset 0x01EA - Number of active cores Number of active cores(Depends on Number of cores).

0: All;**1: 1** ;**2: 2** ;**3: 3** 0:All, 1:1, 2:2, 3:3

Definition at line 955 of file FspmUpd.h.

13.33.2.2 ApertureSize

```
UINT8 FSP_M_CONFIG::ApertureSize
```

Offset 0x00AF - Aperture Size Select the Aperture Size.

0:128 MB, 1:256 MB, 3:512 MB, 7:1024 MB, 15: 2048 MB

Definition at line 227 of file FspmUpd.h.

13.33.2.3 ApStartupBase

```
UINT32 FSP_M_CONFIG::ApStartupBase
```

Offset 0x0228 - ApStartupBase Enable/Disable.

0: Disable, define default value of BiosAcmBase , 1: enable

Definition at line 1118 of file FspmUpd.h.

13.33.2.4 AutoEasyOverclock

```
UINT8 FSP_M_CONFIG::AutoEasyOverclock
```

Offset 0x0241 - Intel Speed Optimizer Enable : CML won't support BIOS ISO.

And XTU ISO supported depends on Board thermal design. When enabled this feature automatically overclocks your processor. It changes the All Core Frequency along with PL1, PL2, and IccMax. 0: Disable;**1: Enable $EN↩ _DIS**

Definition at line 1146 of file FspmUpd.h.

13.33.2.5 Avx2RatioOffset

```
UINT8 FSP_M_CONFIG::Avx2RatioOffset
```

Offset 0x01EE - AVX2 Ratio Offset 0(Default)= No Offset.

Range 0 - 31. Specifies number of bins to decrease AVX ratio vs. Core Ratio. Uses Mailbox MSR 0x150, cmd 0x1B.

Definition at line 981 of file FspmUpd.h.

13.33.2.6 Avx3RatioOffset

```
UINT8 FSP_M_CONFIG::Avx3RatioOffset
```

Offset 0x01EF - AVX3 Ratio Offset 0(Default)= No Offset.

Range 0 - 31. Specifies number of bins to decrease AVX ratio vs. Core Ratio. Uses Mailbox MSR 0x150, cmd 0x1B.

Definition at line 987 of file FspmUpd.h.

13.33.2.7 BclkAdaptiveVoltage

```
UINT8 FSP_M_CONFIG::BclkAdaptiveVoltage
```

Offset 0x01F0 - BCLK Adaptive Voltage Enable When enabled, the CPU V/F curves are aware of BCLK frequency when calculated.

0: Disable;**1: Enable $EN_DIS**

Definition at line 994 of file FspmUpd.h.

13.33.2.8 BiosAcmBase

```
UINT32 FSP_M_CONFIG::BiosAcmBase
```

Offset 0x0220 - BiosAcmBase Enable/Disable.

0: Disable, define default value of BiosAcmBase , 1: enable

Definition at line 1108 of file FspmUpd.h.

13.33.2.9 BiosAcmSize

```
UINT32 FSP_M_CONFIG::BiosAcmSize
```

Offset 0x0224 - BiosAcmSize Enable/Disable.

0: Disable, define default value of BiosAcmSize , 1: enable

Definition at line 1113 of file FspmUpd.h.

13.33.2.10 BiosGuard

`UINT8 FSP_M_CONFIG::BiosGuard`

Offset 0x0201 - BiosGuard Enable/Disable.

0: Disable, Enable/Disable BIOS Guard feature, 1: enable $EN_DIS

Definition at line 1058 of file FspmUpd.h.

13.33.2.11 BistOnReset

`UINT8 FSP_M_CONFIG::BistOnReset`

Offset 0x01DE - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 879 of file FspmUpd.h.

13.33.2.12 BootFrequency

`UINT8 FSP_M_CONFIG::BootFrequency`

Offset 0x01E9 - Boot frequency Sets the boot frequency starting from reset vector.

- 0: Maximum battery performance.- **1: Maximum non-turbo performance**.- 2: Turbo performance.

  Note

  > If Turbo is selected BIOS will start in max non-turbo mode and switch to Turbo mode. 0:0, 1:1, 2:2

Definition at line 948 of file FspmUpd.h.

13.33.2.13 ChHashEnable

`UINT8 FSP_M_CONFIG::ChHashEnable`

Offset 0x0493 - Ch Hash Support Enable/Disable Channel Hash Support.

NOTE: ONLY if Memory interleaved Mode $EN_DIS

Definition at line 1848 of file FspmUpd.h.

13.33.2.14 ChHashInterleaveBit

```
UINT8 FSP_M_CONFIG::ChHashInterleaveBit
```

Offset 0x04AC - Ch Hash Interleaved Bit Select the BIT to be used for Channel Interleaved mode.

NOTE: BIT7 will interlave the channels at a 2 cacheline granularity, BIT8 at 4 and BIT9 at 8. Default is BIT8 0:BIT6, 1:BIT7, 2:BIT8, 3:BIT9, 4:BIT10, 5:BIT11, 6:BIT12, 7:BIT13

Definition at line 1974 of file FspmUpd.h.

13.33.2.15 ChHashMask

```
UINT16 FSP_M_CONFIG::ChHashMask
```

Offset 0x04A6 - Ch Hash Mask Set the BIT(s) to be included in the XOR function.

NOTE BIT mask corresponds to BITS [19:6

Definition at line 1961 of file FspmUpd.h.

13.33.2.16 CkeRankMapping

```
UINT8 FSP_M_CONFIG::CkeRankMapping
```

Offset 0x04E5 - Cke Rank Mapping Bits [7:4] - Channel 1, bits [3:0] - Channel 0.

0xAA=Default Bit [i] specifies which rank CKE[i] goes to.

Definition at line 2246 of file FspmUpd.h.

13.33.2.17 CleanMemory

```
UINT8 FSP_M_CONFIG::CleanMemory
```

Offset 0x0500 - Ask MRC to clear memory content Ask MRC to clear memory content **0: Do not Clear Memory;** 1: Clear Memory.

$EN_DIS

Definition at line 2421 of file FspmUpd.h.

13.33.2.18 CmdRanksTerminated

```
UINT8 FSP_M_CONFIG::CmdRanksTerminated
```

Offset 0x04FA - Bitmask of ranks that have CA bus terminated Offset 225 LPDDR4: Bitmask of ranks that have CA bus terminated.

0x01=Default, Rank0 is terminating and Rank1 is non-terminating

Definition at line 2382 of file FspmUpd.h.

13.33.2.19 CoreMaxOcRatio

```
UINT8 FSP_M_CONFIG::CoreMaxOcRatio
```

Offset 0x01E3 - Maximum Core Turbo Ratio Override Maximum core turbo ratio override allows to increase CPU core frequency beyond the fused max turbo ratio limit.

0: Hardware defaults. Range: 0-255

Definition at line 911 of file FspmUpd.h.

13.33.2.20 CorePllVoltageOffset

```
UINT8 FSP_M_CONFIG::CorePllVoltageOffset
```

Offset 0x01F1 - Core PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 999 of file FspmUpd.h.

13.33.2.21 CoreVfPointOffset

```
UINT16 FSP_M_CONFIG::CoreVfPointOffset[15]
```

Offset 0x0516 - Core VF Point Offset Array used to specifies the Offset Voltage applied to the each selected Core VF Point.

This voltage is specified in millivolts.

Definition at line 2532 of file FspmUpd.h.

13.33.2.22 CoreVfPointOffsetMode

```
UINT8 FSP_M_CONFIG::CoreVfPointOffsetMode
```

Offset 0x0515 - Core VF Point Offset Mode Selects Core Voltage & Frequency Point Offset between Legacy and Selection modes; **0: Legacy**; 1: Selection.

0:Legacy, 1:Selection

Definition at line 2526 of file FspmUpd.h.

13.33.2.23 CoreVfPointOffsetPrefix

```
UINT8 FSP_M_CONFIG::CoreVfPointOffsetPrefix[15]
```

Offset 0x0534 - Core VF Point Offset Prefix Sets the CoreVfPointOffset value as positive or negative for corresponding core VF Point; **0: Positive** ; 1: Negative.

0:Positive, 1:Negative

Definition at line 2539 of file FspmUpd.h.

13.33.2.24 CoreVoltageAdaptive

```
UINT16 FSP_M_CONFIG::CoreVoltageAdaptive
```

Offset 0x01F4 - Core Turbo voltage Adaptive Extra Turbo voltage applied to the cpu core when the cpu is operating in turbo mode.

Valid Range 0 to 2000

Definition at line 1011 of file FspmUpd.h.

13.33.2.25 CoreVoltageMode

```
UINT8 FSP_M_CONFIG::CoreVoltageMode
```

Offset 0x01E4 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.

$EN_DIS

Definition at line 917 of file FspmUpd.h.

13.33.2.26 CoreVoltageOverride

```
UINT16 FSP_M_CONFIG::CoreVoltageOverride
```

Offset 0x01F2 - core voltage override The core voltage override which is applied to the entire range of cpu core frequencies.

Valid Range 0 to 2000

Definition at line 1005 of file FspmUpd.h.

13.33.2.27 CpuRatio

```
UINT8 FSP_M_CONFIG::CpuRatio
```

Offset 0x01E8 - CPU ratio value CPU ratio value.

Valid Range 0 to 63. CPU Ratio is 0 when disabled.

Definition at line 940 of file FspmUpd.h.

13.33.2.28 CpuTraceHubMemReg0Size

```
UINT8 FSP_M_CONFIG::CpuTraceHubMemReg0Size
```

Offset 0x00DB - CPU Trace Hub Memory Region 0 CPU Trace Hub Memory Region 0, The avaliable memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

Note : Limitation of total buffer size (CPU + PCH) is 512MB. 0:0, 1:1MB, 2:8MB, 3:64MB, 4:128MB, 5:256MB, 6:512MB

Definition at line 439 of file FspmUpd.h.

13.33.2.29 CpuTraceHubMemReg1Size

```
UINT8 FSP_M_CONFIG::CpuTraceHubMemReg1Size
```

Offset 0x00DC - CPU Trace Hub Memory Region 1 CPU Trace Hub Memory Region 1.

The avaliable memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB. Note : Limitation of total buffer size (CPU + PCH) is 512MB. 0:0, 1:1MB, 2:8MB, 3:64MB, 4:128MB, 5:256MB, 6:512MB

Definition at line 446 of file FspmUpd.h.

13.33.2.30 CpuTraceHubMode

```
UINT8 FSP_M_CONFIG::CpuTraceHubMode
```

Offset 0x00DA - CPU Trace Hub Mode Select 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

0: Disable, 1:Target Debugger Mode

Definition at line 432 of file FspmUpd.h.

13.33.2.31 DciUsb3TypecUfpDbg

```
UINT8 FSP_M_CONFIG::DciUsb3TypecUfpDbg
```

Offset 0x0252 - USB3 Type-C UFP2DFP Kernel/Platform Debug Support This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting.

0:Disabled, 1:Enabled, 2:No Change

Definition at line 1187 of file FspmUpd.h.

13.33.2.32 Ddr4Mixed2DpcLimit

```
UINT8 FSP_M_CONFIG::Ddr4Mixed2DpcLimit
```

Offset 0x0507 - DDR4 Mixed U-DIMM 2DPC Limitation Enable/Disable Frequency Limitation for DDR4 Mixed Dimm 2DPC Memory Configurations.

Disable=0, Enable(Default)=1 $EN_DIS

Definition at line 2457 of file FspmUpd.h.

13.33.2.33 Ddr4SkipRefreshEn

```
UINT8 FSP_M_CONFIG::Ddr4SkipRefreshEn
```

Offset 0x050F - DDR4 Skip Refresh Enable Enable/Disable of DDR4 Temperature Controlled Refresh on DRAM.

Default is 1 (Enabled) 0:Disable, 1:Enable

Definition at line 2505 of file FspmUpd.h.

13.33.2.34 DdrFreqLimit

```
UINT16 FSP_M_CONFIG::DdrFreqLimit
```

Offset 0x00B2 - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.

Valid values should match the refclk, i.e. divide by 133 or 100 1067:1067, 1333:1333, 1400:1400, 1600:1600, 1800:1800, 1867:1867, 2000:2000, 2133:2133, 2200:2200, 2400:2400, 2600:2600, 2667:2667, 2800:2800, 2933↩ :2933, 3000:3000, 3200:3200, 0:Auto

Definition at line 250 of file FspmUpd.h.

13.33.2.35 DisableDimmChannel0

```
UINT8 FSP_M_CONFIG::DisableDimmChannel0
```

Offset 0x00B7 - Channel A DIMM Control Channel A DIMM Control Support - Enable or Disable Dimms on Channel A.

0:Enable both DIMMs, 1:Disable DIMM0, 2:Disable DIMM1, 3:Disable both DIMMs

Definition at line 269 of file FspmUpd.h.

13.33.2.36 DisableDimmChannel1

```
UINT8 FSP_M_CONFIG::DisableDimmChannel1
```

Offset 0x00B8 - Channel B DIMM Control Channel B DIMM Control Support - Enable or Disable Dimms on Channel B.

0:Enable both DIMMs, 1:Disable DIMM0, 2:Disable DIMM1, 3:Disable both DIMMs

Definition at line 275 of file FspmUpd.h.

13.33.2.37 DisableMtrrProgram

```
UINT8 FSP_M_CONFIG::DisableMtrrProgram
```

Offset 0x01E5 - Program Cache Attributes Program Cache Attributes; **0: Program**; 1: Disable Program.

$EN_DIS

Definition at line 923 of file FspmUpd.h.

13.33.2.38 DmiDeEmphasis

```
UINT8 FSP_M_CONFIG::DmiDeEmphasis
```

Offset 0x0154 - DeEmphasis control for DMI DeEmphasis control for DMI.

0=-6dB, 1(Default)=-3.5 dB 0: -6dB, 1: -3.5dB

Definition at line 701 of file FspmUpd.h.

13.33.2.39 DmiGen3EndPointHint

```
UINT8 FSP_M_CONFIG::DmiGen3EndPointHint[8]
```

Offset 0x0115 - DMI Gen3 End port Hint values per lane Used for programming DMI Gen3 Hint values per lane.

Range: 0-6, 2 is default for each lane

Definition at line 648 of file FspmUpd.h.

13.33.2.40 DmiGen3EndPointPreset

```
UINT8 FSP_M_CONFIG::DmiGen3EndPointPreset[8]
```

Offset 0x010D - DMI Gen3 End port preset values per lane Used for programming DMI Gen3 preset values per lane.

Range: 0-9, 7 is default for each lane

Definition at line 643 of file FspmUpd.h.

13.33.2.41 DmiGen3ProgramStaticEq

```
UINT8 FSP_M_CONFIG::DmiGen3ProgramStaticEq
```

Offset 0x00F2 - Enable/Disable DMI GEN3 Static EQ Phase1 programming Program DMI Gen3 EQ Phase1 Static Presets.

Disabled(0x0): Disable EQ Phase1 Static Presets Programming, Enabled(0x1)(Default): Enable EQ Phase1 Static Presets Programming $EN_DIS

Definition at line 506 of file FspmUpd.h.

13.33.2.42 DmiGen3RootPortPreset

```
UINT8 FSP_M_CONFIG::DmiGen3RootPortPreset[8]
```

Offset 0x0105 - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.

Range: 0-9, 8 is default for each lane

Definition at line 638 of file FspmUpd.h.

13.33.2.43 DualDimmPerChannelBoardType

```
UINT8 FSP_M_CONFIG::DualDimmPerChannelBoardType
```

Offset 0x0506 - Dual Dimm Per-Channel Board Type Option to indicate if Board Layout includes One/Two DIMMs per channel.

This is used to limit maximum frequency for some SKUs. 0:1DPC, 1:2DPC

Definition at line 2450 of file FspmUpd.h.

13.33.2.44 EnableC6Dram

```
UINT8 FSP_M_CONFIG::EnableC6Dram
```

Offset 0x01E0 - C6DRAM power gating feature This policy indicates whether or not BIOS should allocate PRMRR memory for C6DRAM power gating feature.

- 0: Don't allocate any PRMRR memory for C6DRAM power gating feature.- **1: Allocate PRMRR memory for C6DRAM power gating feature**. $EN_DIS

Definition at line 893 of file FspmUpd.h.

13.33.2.45 EnableSgx

```
UINT8 FSP_M_CONFIG::EnableSgx
```

Offset 0x0203 - EnableSgx Enable/Disable.

0: Disable, Enable/Disable SGX feature, 1: enable, 2: Software Control 0: Disable, 1: Enable, 2: Software Control

Definition at line 1068 of file FspmUpd.h.

13.33.2.46 EnBER

```
UINT8 FSP_M_CONFIG::EnBER
```

Offset 0x0505 - BER Support Enable/Disable the Rank Margin Tool interpolation/extrapolation.

0:Disable, 1:Enable

Definition at line 2443 of file FspmUpd.h.

13.33.2.47 EnCmdRate

```
UINT8 FSP_M_CONFIG::EnCmdRate
```

Offset 0x04E8 - Command Rate Support CMD Rate and Limit Support Option.

NOTE: ONLY supported in 1N Mode, Default is 3 CMDs 0:Disable, 1:1 CMD, 2:2 CMDS, 3:3 CMDS, 4:4 CMDS, 5:5 CMDS, 6:6 CMDS, 7:7 CMDS

Definition at line 2262 of file FspmUpd.h.

13.33.2.48 EpgEnable

```
UINT8 FSP_M_CONFIG::EpgEnable
```

Offset 0x04EA - Energy Performance Gain Enable/disable(default) Energy Performance Gain.

$EN_DIS

Definition at line 2274 of file FspmUpd.h.

13.33.2.49 FastBootRmt

```
UINT8 FSP_M_CONFIG::FastBootRmt
```

Offset 0x0508 - RMT on Fast flow Enable/Disable RMT on Fast flow.

Default: Disabled $EN_DIS

Definition at line 2463 of file FspmUpd.h.

13.33.2.50 FClkFrequency

```
UINT8 FSP_M_CONFIG::FClkFrequency
```

Offset 0x01EB - Processor Early Power On Configuration FCLK setting **0: 800 MHz (ULT/ULX)**.

1: 1 GHz (DT/Halo). Not supported on ULT/ULX.- 2: 400 MHz. - 3: Reserved 0:800 MHz, 1: 1 GHz, 2: 400 MHz, 3: Reserved

Definition at line 962 of file FspmUpd.h.

13.33.2.51 FivrEfficiency

```
UINT8 FSP_M_CONFIG::FivrEfficiency
```

Offset 0x04FE - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; **1: Enabled.**

$EN_DIS

Definition at line 2409 of file FspmUpd.h.

13.33.2.52 FivrFaults

```
UINT8 FSP_M_CONFIG::FivrFaults
```

Offset 0x04FD - Fivr Faults Fivr Faults; 0: Disabled; **1: Enabled.**

$EN_DIS

Definition at line 2403 of file FspmUpd.h.

13.33.2.53 ForceOltmOrRefresh2x

```
UINT8 FSP_M_CONFIG::ForceOltmOrRefresh2x
```

Offset 0x04F8 - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.

Enabled: = Force 2x Refresh. $EN_DIS

Definition at line 2370 of file FspmUpd.h.

13.33.2.54 FreqSaGvLow

```
UINT16 FSP_M_CONFIG::FreqSaGvLow
```

Offset 0x00B4 - Low Frequency SAGV Low Frequency Selections in Mhz.

Options are 1067, 1333, 1600, 1867, 2133, 2400, 2667, 2933 and 0 for Auto. 1067:1067, 1333:1333, 1600:1600, 1867:1867, 2133:2133, 2400:2400, 2667:2667, 2933:2933, 0:Auto

Definition at line 257 of file FspmUpd.h.

13.33.2.55 GdxcEnable

```
UINT8 FSP_M_CONFIG::GdxcEnable
```

Offset 0x04FB - GDXC MOT enable GDXC MOT enable.

$EN_DIS

Definition at line 2388 of file FspmUpd.h.

13.33.2.56 GmAdr

```
UINT32 FSP_M_CONFIG::GmAdr
```

Offset 0x0158 - Temporary MMIO address for GMADR The reference code will use this as Temporary MMIO address space to access GMADR Registers.Platform should provide conflict free Temporary MMIO Range: GmAdr to (GmAdr + ApertureSize).

Default is (PciExpressBaseAddress - ApertureSize) to (PciExpressBaseAddress

- 0x1) (Where ApertureSize = 256MB)

Definition at line 721 of file FspmUpd.h.

13.33.2.57 GtPllVoltageOffset

```
UINT8 FSP_M_CONFIG::GtPllVoltageOffset
```

Offset 0x0468 - GT PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1590 of file FspmUpd.h.

13.33.2.58 GtPsmiSupport

```
UINT8 FSP_M_CONFIG::GtPsmiSupport
```

Offset 0x01D2 - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.

When TRUE, it will allow the PSMI Support $EN_DIS

Definition at line 833 of file FspmUpd.h.

13.33.2.59 GttMmAdr

```
UINT32 FSP_M_CONFIG::GttMmAdr
```

Offset 0x015C - Temporary MMIO address for GTTMMADR The reference code will use this as Temporary MMIO address space to access GTTMMADR Registers.Platform should provide conflict free Temporary MMIO Range: GttMmAdr to (GttMmAdr + 2MB MMIO + 6MB Reserved + GttSize).

Default is (GmAdr - (2MB MMIO

- 6MB Reserved + GttSize)) to (GmAdr - 0x1) (Where GttSize = 8MB)

Definition at line 729 of file FspmUpd.h.

13.33.2.60 HobBufferSize

```
UINT8 FSP_M_CONFIG::HobBufferSize
```

Offset 0x046E - HobBufferSize Size to set HOB Buffer.

0:Default, 1: 1 Byte, 2: 1 KB, 3: Max value(assuming 63KB total HOB size). 0:Default, 1: 1 Byte, 2: 1 KB, 3: Max value

Definition at line 1624 of file FspmUpd.h.

13.33.2.61 HotThresholdCh0Dimm0

```
UINT8 FSP_M_CONFIG::HotThresholdCh0Dimm0
```

Offset 0x04C4 - Hot Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2079 of file FspmUpd.h.

13.33.2.62 HotThresholdCh0Dimm1

```
UINT8 FSP_M_CONFIG::HotThresholdCh0Dimm1
```

Offset 0x04C5 - Hot Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2084 of file FspmUpd.h.

13.33.2.63 HotThresholdCh1Dimm0

```
UINT8 FSP_M_CONFIG::HotThresholdCh1Dimm0
```

Offset 0x04C6 - Hot Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2089 of file FspmUpd.h.

13.33.2.64 HotThresholdCh1Dimm1

```
UINT8 FSP_M_CONFIG::HotThresholdCh1Dimm1
```

Offset 0x04C7 - Hot Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2094 of file FspmUpd.h.

13.33.2.65 Idd3n

```
UINT16 FSP_M_CONFIG::Idd3n
```

Offset 0x04AE - EPG DIMM Idd3N Active standby current (Idd3N) in milliamps from datasheet.

Must be calculated on a per DIMM basis. Default is 26

Definition at line 1985 of file FspmUpd.h.

13.33.2.66 Idd3p

```
UINT16 FSP_M_CONFIG::Idd3p
```

Offset 0x04B0 - EPG DIMM Idd3P Active power-down current (Idd3P) in milliamps from datasheet.

Must be calculated on a per DIMM basis. Default is 11

Definition at line 1991 of file FspmUpd.h.

13.33.2.67 IgdDvmt50PreAlloc

```
UINT8 FSP_M_CONFIG::IgdDvmt50PreAlloc
```

Offset 0x00AD - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.

0x00:0 MB, 0x01:32 MB, 0x02:64 MB

Definition at line 215 of file FspmUpd.h.

13.33.2.68 ImrRpSelection

```
UINT8 FSP_M_CONFIG::ImrRpSelection
```

Offset 0x0449 - Root port number for IMR.

Root port number for IMR.

Definition at line 1435 of file FspmUpd.h.

13.33.2.69 InitPcieAspmAfterOprom

```
UINT8 FSP_M_CONFIG::InitPcieAspmAfterOprom
```

Offset 0x0103 - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.

Before(0x0)(Default): Do PCIe ASPM programming before Oprom, After(0x1): Do PCIe ASPM programming after Oprom, requires an SMI handler to save/restore ASPM settings during S3 resume 0:Before, 1:After

Definition at line 626 of file FspmUpd.h.

13.33.2.70 InternalGfx

```
UINT8 FSP_M_CONFIG::InternalGfx
```

Offset 0x00AE - Internal Graphics Enable/disable internal graphics.

$EN_DIS

Definition at line 221 of file FspmUpd.h.

13.33.2.71 IsvtIoPort

```
UINT8 FSP_M_CONFIG::IsvtIoPort
```

Offset 0x00D6 - ISVT IO Port Address ISVT IO Port Address.

0=Minimal, 0xFF=Maximum, 0x99=Default

Definition at line 414 of file FspmUpd.h.

13.33.2.72 JtagC10PowerGateDisable

```
UINT8 FSP_M_CONFIG::JtagC10PowerGateDisable
```

Offset 0x01EC - Set JTAG power in C10 and deeper power states False: JTAG is power gated in C10 state.

True: keeps the JTAG power up during C10 and deeper power states for debug purpose. **0: False**; 1: True. 0: False, 1: True

Definition at line 969 of file FspmUpd.h.

13.33.2.73 LpddrDramOdt

```
UINT8 FSP_M_CONFIG::LpddrDramOdt
```

Offset 0x050E - Lpddr Dram Odt Override Enable/Disable for the ODT logic for LPDDR3 memory.

Default is 2 (AUTO) 0:Disable, 1:Enable, 2:AUTO

Definition at line 2499 of file FspmUpd.h.

13.33.2.74 MarginLimitCheck

```
UINT8 FSP_M_CONFIG::MarginLimitCheck
```

Offset 0x00D7 - Margin Limit Check Margin Limit Check.

Choose level of margin check 0:Disable, 1:L1, 2:L2, 3:Both

Definition at line 420 of file FspmUpd.h.

13.33.2.75 McPllVoltageOffset

```
UINT8 FSP_M_CONFIG::McPllVoltageOffset
```

Offset 0x046B - Memory Controller PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1605 of file FspmUpd.h.

13.33.2.76 MemoryTrace

```
UINT8 FSP_M_CONFIG::MemoryTrace
```

Offset 0x0492 - Memory Trace Enable Memory Trace of Ch 0 to Ch 1 using Stacked Mode.

Both channels must be of equal size. This option may change TOLUD and REMAP values as needed. $EN_DIS

Definition at line 1842 of file FspmUpd.h.

13.33.2.77 MmioSize

```
UINT16 FSP_M_CONFIG::MmioSize
```

Offset 0x00A4 - MMIO Size Size of MMIO space reserved for devices.

0(Default)=Auto, non-Zero=size in MB

Definition at line 186 of file FspmUpd.h.

13.33.2.78 OcLock

```
UINT8 FSP_M_CONFIG::OcLock
```

Offset 0x01E2 - Over clocking Lock Over clocking Lock Enable/Disable; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 905 of file FspmUpd.h.

13.33.2.79 PcdDebugInterfaceFlags

```
UINT8 FSP_M_CONFIG::PcdDebugInterfaceFlags
```

Offset 0x044B - Debug Interfaces Debug Interfaces.

BIT0-RAM, BIT1-UART, BIT3-USB3, BIT4-Serial IO, BIT5-TraceHub, BIT2 - Not used.

Definition at line 1447 of file FspmUpd.h.

13.33.2.80 PcdIsaSerialUartBase

```
UINT8 FSP_M_CONFIG::PcdIsaSerialUartBase
```

Offset 0x0467 - ISA Serial Base selection Select ISA Serial Base address.

Default is 0x3F8. 0:0x3F8, 1:0x2F8

Definition at line 1585 of file FspmUpd.h.

13.33.2.81 PcdSerialDebugBaudRate

```
UINT8 FSP_M_CONFIG::PcdSerialDebugBaudRate
```

Offset 0x046D - PcdSerialDebugBaudRate Baud Rate for Serial Debug Messages.

3:9600, 4:19200, 6:56700, 7:115200. 3:9600, 4:19200, 6:56700, 7:115200

Definition at line 1617 of file FspmUpd.h.

13.33.2.82 PcdSerialDebugLevel

```
UINT8 FSP_M_CONFIG::PcdSerialDebugLevel
```

Offset 0x04FC - PcdSerialDebugLevel Serial Debug Message Level.

0:Disable, 1:Error Only, 2:Error & Warnings, 3:Load, Error, Warnings & Info, 4:Load, Error, Warnings, Info & Event, 5:Load, Error, Warnings, Info & Verbose. 0:Disable, 1:Error Only, 2:Error and Warnings, 3:Load Error Warnings and Info, 4:Load Error Warnings and Info & Event, 5:Load Error Warnings Info and Verbose

Definition at line 2397 of file FspmUpd.h.

13.33.2.83 PchHdaAudioLinkDmic0

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkDmic0
```

Offset 0x045B - Enable HD Audio DMIC0 Link Deprecated.

$EN_DIS

Definition at line 1519 of file FspmUpd.h.

13.33.2.84 PchHdaAudioLinkDmic1

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkDmic1
```

Offset 0x045C - Enable HD Audio DMIC1 Link Deprecated.

$EN_DIS

Definition at line 1525 of file FspmUpd.h.

13.33.2.85 PchHdaAudioLinkHda

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkHda
```

Offset 0x045A - Enable HD Audio Link Enable/disable HD Audio Link.

Muxed with SSP0/SSP1/SNDW1. $EN_DIS

Definition at line 1513 of file FspmUpd.h.

13.33.2.86 PchHdaAudioLinkSndw1

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSndw1
```

Offset 0x0460 - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.

Muxed with HDA. $EN_DIS

Definition at line 1549 of file FspmUpd.h.

13.33.2.87 PchHdaAudioLinkSndw2

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSndw2
```

Offset 0x0461 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.

Muxed with SSP1. $EN_DIS

Definition at line 1555 of file FspmUpd.h.

13.33.2.88 PchHdaAudioLinkSndw3

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSndw3
```

Offset 0x0462 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.

Muxed with DMIC1. $EN_DIS

Definition at line 1561 of file FspmUpd.h.

13.33.2.89 PchHdaAudioLinkSndw4

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSndw4
```

Offset 0x0463 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.

Muxed with DMIC0. $EN_DIS

Definition at line 1567 of file FspmUpd.h.

13.33.2.90 PchHdaAudioLinkSsp0

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSsp0
```

Offset 0x045D - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.

Muxed with HDA. $EN_DIS

Definition at line 1531 of file FspmUpd.h.

13.33.2.91 PchHdaAudioLinkSsp1

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSsp1
```

Offset 0x045E - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.

Muxed with HDA/SNDW2. $EN_DIS

Definition at line 1537 of file FspmUpd.h.

13.33.2.92 PchHdaAudioLinkSsp2

```
UINT8 FSP_M_CONFIG::PchHdaAudioLinkSsp2
```

Offset 0x045F - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.

$EN_DIS

Definition at line 1543 of file FspmUpd.h.

13.33.2.93 PchHdaDspEnable

```
UINT8 FSP_M_CONFIG::PchHdaDspEnable
```

Offset 0x0457 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

$EN_DIS

Definition at line 1494 of file FspmUpd.h.

13.33.2.94 PchHdaDspUaaCompliance

```
UINT8 FSP_M_CONFIG::PchHdaDspUaaCompliance
```

Offset 0x0459 - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).

$EN_DIS

Definition at line 1507 of file FspmUpd.h.

13.33.2.95 PchHdaSndwBufferRcomp

```
UINT8 FSP_M_CONFIG::PchHdaSndwBufferRcomp
```

Offset 0x0464 - Soundwire Clock Buffer GPIO RCOMP Setting 0: non-ACT - 50 Ohm driver impedance, 1: ACT - 8 Ohm driver impedance.

$EN_DIS

Definition at line 1573 of file FspmUpd.h.

13.33.2.96 PchHdaVcType

```
UINT8 FSP_M_CONFIG::PchHdaVcType
```

Offset 0x0458 - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.

0: VC0, 1: VC1

Definition at line 1500 of file FspmUpd.h.

13.33.2.97 PchLpcEnhancePort8xhDecoding

```
UINT8 FSP_M_CONFIG::PchLpcEnhancePort8xhDecoding
```

Offset 0x0438 - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.

$EN_DIS

Definition at line 1386 of file FspmUpd.h.

13.33.2.98 PchNumRsvdSmbusAddresses

```
UINT8 FSP_M_CONFIG::PchNumRsvdSmbusAddresses
```

Offset 0x043B - Number of RsvdSmbusAddressTable.

The number of elements in the RsvdSmbusAddressTable.

Definition at line 1403 of file FspmUpd.h.

13.33.2.99 PchPort80Route

```
UINT8 FSP_M_CONFIG::PchPort80Route
```

Offset 0x0439 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.

$EN_DIS

Definition at line 1392 of file FspmUpd.h.

13.33.2.100 PchSmbAlertEnable

```
UINT8 FSP_M_CONFIG::PchSmbAlertEnable
```

Offset 0x044A - Enable SMBus Alert Pin Enable SMBus Alert Pin.

$EN_DIS

Definition at line 1441 of file FspmUpd.h.

13.33.2.101 PchTraceHubMemReg0Size

```
UINT8 FSP_M_CONFIG::PchTraceHubMemReg0Size
```

Offset 0x0254 - PCH Trace Hub Memory Region 0 buffer Size Specify size of Pch trace memory region 0 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

Note : Limitation of total buffer size (PCH + CPU) is 512MB. 0:0, 1:1MB, 2:8MB, 3:64MB, 4:128MB, 5:256MB, 6:512MB

Definition at line 1201 of file FspmUpd.h.

13.33.2.102 PchTraceHubMemReg1Size

```
UINT8 FSP_M_CONFIG::PchTraceHubMemReg1Size
```

Offset 0x0255 - PCH Trace Hub Memory Region 1 buffer Size Specify size of Pch trace memory region 1 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

Note : Limitation of total buffer size (PCH + CPU) is 512MB. 0:0, 1:1MB, 2:8MB, 3:64MB, 4:128MB, 5:256MB, 6:512MB

Definition at line 1208 of file FspmUpd.h.

13.33.2.103 PchTraceHubMode

```
UINT8 FSP_M_CONFIG::PchTraceHubMode
```

Offset 0x0253 - PCH Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

0: Disable, 1: Target Debugger Mode, 2: Host Debugger Mode

Definition at line 1194 of file FspmUpd.h.

13.33.2.104 PcieImrSize

```
UINT16 FSP_M_CONFIG::PcieImrSize
```

Offset 0x043E - Size of PCIe IMR.

Size of PCIe IMR in megabytes

Definition at line 1413 of file FspmUpd.h.

13.33.2.105 PcieRpEnableMask

```
UINT32 FSP_M_CONFIG::PcieRpEnableMask
```

Offset 0x0444 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 1424 of file FspmUpd.h.

13.33.2.106 PeciC10Reset

```
UINT8 FSP_M_CONFIG::PeciC10Reset
```

Offset 0x00DD - Enable or Disable Peci C10 Reset command Enable or Disable Peci C10 Reset command.

If Enabled, BIOS will send the CPU message to disable peci reset on C10 exit. The default value is **0: Disable** for CNL, and **1: Enable** for all other CPU's $EN_DIS

Definition at line 454 of file FspmUpd.h.

13.33.2.107 PeciSxReset

```
UINT8 FSP_M_CONFIG::PeciSxReset
```

Offset 0x00DE - Enable or Disable Peci Sx Reset command Enable or Disable Peci Sx Reset command; **0: Disable;** 1: Enable.

$EN_DIS

Definition at line 460 of file FspmUpd.h.

13.33.2.108 PegDataPtr

```
UINT32 FSP_M_CONFIG::PegDataPtr
```

Offset 0x0130 - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA_PEG_DATA) and platform code can save/restore this data to skip preset search in the following boots.

Range: 0-0xFFFFFFFF, default is 0

Definition at line 684 of file FspmUpd.h.

13.33.2.109 PegDisableSpreadSpectrumClocking

```
UINT8 FSP_M_CONFIG::PegDisableSpreadSpectrumClocking
```

Offset 0x0104 - PCIe Disable Spread Spectrum Clocking PCIe Disable Spread Spectrum Clocking.

Normal Operation(0x0)(Default) - SSC enabled, Disable SSC(0X1) - Disable SSC per platform design or for compliance testing 0:Normal Operation, 1:Disable SSC

Definition at line 633 of file FspmUpd.h.

13.33.2.110 PerCoreHtDisable

```
UINT16 FSP_M_CONFIG::PerCoreHtDisable
```

Offset 0x01DC - Per-core HT Disable Defines the per-core HT disable mask where: 1 - Disable selected logical core HT, 0 - is ignored.

Input is in HEX and each bit maps to a logical core. Ex. A value of '1F' would disable HT for cores 4,3,2,1 and 0. Default is 0, all cores have HT enabled. Range is 0 - 0x1FF. You can only disable up to MAX_CORE_COUNT - 1.

Definition at line 873 of file FspmUpd.h.

13.33.2.111 PlatformDebugConsent

```
UINT8 FSP_M_CONFIG::PlatformDebugConsent
```

Offset 0x0251 - Platform Debug Consent To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type.

Enabling this BIOS option may alter the default value of other debug-related BIOS options. Note: DCI OOB (aka BSSB) uses CCA probe; [DCI OOB+DbC] and [USB2 DbC] have the same setting 0:Disabled, 1:Enabled (DCI OOB+[DbC]), 2:Enabled (DCI OOB), 3:Enabled (USB3 DbC), 4:Enabled (XDP/MIPI60), 5:Enabled (USB2 DbC)

Definition at line 1180 of file FspmUpd.h.

13.33.2.112 ProbelessTrace

```
UINT8 FSP_M_CONFIG::ProbelessTrace
```

Offset 0x00A6 - Probeless Trace Probeless Trace: 0=Disabled, 1=Enable.

Enabling Probeless Trace will reserve 128MB. This also requires IED to be enabled. $EN_DIS

Definition at line 193 of file FspmUpd.h.

13.33.2.113 PwdwnIdleCounter

```
UINT8 FSP_M_CONFIG::PwdwnIdleCounter
```

Offset 0x04F9 - Pwr Down Idle Timer The minimum value should = to the worst case Roundtrip delay + Burst_↩ Length.

0 means AUTO: 64 for ULX/ULT, 128 for DT/Halo

Definition at line 2376 of file FspmUpd.h.

13.33.2.114 RankInterleave

```
UINT8 FSP_M_CONFIG::RankInterleave
```

Offset 0x0490 - Rank Interleave support Enables/Disable Rank Interleave support.

NOTE: RI and HORI can not be enabled at the same time. $EN_DIS

Definition at line 1829 of file FspmUpd.h.

13.33.2.115 Ratio

```
UINT8 FSP_M_CONFIG::Ratio
```

Offset 0x00C0 - Memory Ratio Automatic or the frequency will equal ratio times reference clock.

Set to Auto to recalculate memory timings listed below. 0:Auto, 4:4, 5:5, 6:6, 7:7, 8:8, 9:9, 10:10, 11:11, 12:12, 13:13, 14:14, 15:15

Definition at line 319 of file FspmUpd.h.

13.33.2.116 RcompResistor

```
UINT16 FSP_M_CONFIG::RcompResistor[3]
```

Offset 0x0082 - RcompResistor settings Indicates RcompResistor settings: CML - 0's means MRC auto configured based on Design Guidelines, otherwise input an Ohmic value per segment.

CFL will need to provide the appropriate values.

Definition at line 114 of file FspmUpd.h.

13.33.2.117 RcompTarget

```
UINT16 FSP_M_CONFIG::RcompTarget[5]
```

Offset 0x0088 - RcompTarget settings RcompTarget settings: CML - 0's mean MRC auto configured based on Design Guidelines, otherwise input an Ohmic value per segment.

CFL will need to provide the appropriate values.

Definition at line 120 of file FspmUpd.h.

13.33.2.118 RealtimeMemoryTiming

```
UINT8 FSP_M_CONFIG::RealtimeMemoryTiming
```

Offset 0x01CF - Realtime Memory Timing 0(Default): Disabled, 1: Enabled.

When enabled, it will allow the system to perform realtime memory timing changes after MRC_DONE. 0: Disabled, 1: Enabled

Definition at line 815 of file FspmUpd.h.

13.33.2.119 RefClk

```
UINT8 FSP_M_CONFIG::RefClk
```

Offset 0x00BC - Memory Reference Clock 100MHz, 133MHz.

0:133MHz, 1:100MHz

Definition at line 301 of file FspmUpd.h.

13.33.2.120 RetrainOnFastFail

```
UINT8 FSP_M_CONFIG::RetrainOnFastFail
```

Offset 0x0555 - Retrain On Fast Fail Restart MRC in Cold mode if SW MemTest fails during Fast flow.

Default = Enabled

Definition at line 2564 of file FspmUpd.h.

13.33.2.121 RhSolution

```
UINT8 FSP_M_CONFIG::RhSolution
```

Offset 0x04EB - Row Hammer Solution Type of method used to prevent Row Hammer.

Default is Hardware RHP 0:Hardware RHP, 1:2x Refresh

Definition at line 2280 of file FspmUpd.h.

13.33.2.122 RingDownBin

```
UINT8 FSP_M_CONFIG::RingDownBin
```

Offset 0x01F8 - Ring Downbin Ring Downbin enable/disable.

When enabled, CPU will ensure the ring ratio is always lower than the core ratio.0: Disable; **1: Enable.** $EN_DIS

Definition at line 1023 of file FspmUpd.h.

13.33.2.123 RingMaxOcRatio

```
UINT8 FSP_M_CONFIG::RingMaxOcRatio
```

Offset 0x01E6 - Maximum clr turbo ratio override Maximum clr turbo ratio override allows to increase CPU clr frequency beyond the fused max turbo ratio limit.

0: Hardware defaults. Range: 0-255

Definition at line 929 of file FspmUpd.h.

13.33.2.124 RingPllVoltageOffset

```
UINT8 FSP_M_CONFIG::RingPllVoltageOffset
```

Offset 0x0469 - Ring PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1595 of file FspmUpd.h.

13.33.2.125 RingVoltageAdaptive

```
UINT16 FSP_M_CONFIG::RingVoltageAdaptive
```

Offset 0x01FC - Ring Turbo voltage Adaptive Extra Turbo voltage applied to the cpu ring when the cpu is operating in turbo mode.

Valid Range 0 to 2000

Definition at line 1041 of file FspmUpd.h.

13.33.2.126 RingVoltageMode

```
UINT8 FSP_M_CONFIG::RingVoltageMode
```

Offset 0x01F9 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.

$EN_DIS

Definition at line 1029 of file FspmUpd.h.

13.33.2.127 RingVoltageOffset

```
UINT16 FSP_M_CONFIG::RingVoltageOffset
```

Offset 0x01FE - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.

Valid Range 0 to 1000

Definition at line 1046 of file FspmUpd.h.

13.33.2.128 RingVoltageOverride

```
UINT16 FSP_M_CONFIG::RingVoltageOverride
```

Offset 0x01FA - Ring voltage override The ring voltage override which is applied to the entire range of cpu ring frequencies.

Valid Range 0 to 2000

Definition at line 1035 of file FspmUpd.h.

13.33.2.129 RMT

```
UINT8 FSP_M_CONFIG::RMT
```

Offset 0x00B6 - Rank Margin Tool Enable/disable Rank Margin Tool.

$EN_DIS

Definition at line 263 of file FspmUpd.h.

13.33.2.130 RMTLoopCount

```
UINT8 FSP_M_CONFIG::RMTLoopCount
```

Offset 0x0504 - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.

0 - AUTO

Definition at line 2437 of file FspmUpd.h.

13.33.2.131 RmtPerTask

```
UINT8 FSP_M_CONFIG::RmtPerTask
```

Offset 0x0097 - Rank Margin Tool per Task This option enables the user to execute Rank Margin Tool per major training step in the MRC.

$EN_DIS

Definition at line 158 of file FspmUpd.h.

13.33.2.132 SafeMode

```
UINT8 FSP_M_CONFIG::SafeMode
```

Offset 0x04FF - Safe Mode Support This option configures the varous items in the IO and MC to be more conservative.

(def=Disable) $EN_DIS

Definition at line 2415 of file FspmUpd.h.

13.33.2.133 SaGv

```
UINT8 FSP_M_CONFIG::SaGv
```

Offset 0x00B1 - SA GV System Agent dynamic frequency support and when enabled memory will be training at two different frequencies.

Only effects ULX/ULT CPUs. 0=Disabled, 1=FixedLow, 2=FixedHigh, and 3=Enabled. 0:Disabled, 1:FixedLow, 2:FixedHigh, 3:Enabled

Definition at line 242 of file FspmUpd.h.

13.33.2.134 SaPllVoltageOffset

```
UINT8 FSP_M_CONFIG::SaPllVoltageOffset
```

Offset 0x046A - System Agent PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1600 of file FspmUpd.h.

13.33.2.135 ScramblerSupport

```
UINT8 FSP_M_CONFIG::ScramblerSupport
```

Offset 0x00B9 - Scrambler Support This option enables data scrambling in memory.

$EN_DIS

Definition at line 281 of file FspmUpd.h.

13.33.2.136 SerialDebugMrcLevel

```
UINT8 FSP_M_CONFIG::SerialDebugMrcLevel
```

Offset 0x0510 - SerialDebugMrcLevel MRC Serial Debug Message Level.

0:Disable, 1:Error Only, 2:Error & Warnings, 3:Load, Error, Warnings & Info, 4:Load, Error, Warnings, Info & Event, 5:Load, Error, Warnings, Info & Verbose. 0:Disable, 1:Error Only, 2:Error and Warnings, 3:Load Error Warnings and Info, 4:Load Error Warnings and Info & Event, 5:Load Error Warnings Info and Verbose

Definition at line 2514 of file FspmUpd.h.

13.33.2.137 SerialIoUartDebugAutoFlow

```
UINT8 FSP_M_CONFIG::SerialIoUartDebugAutoFlow
```

Offset 0x044D - Serial Io Uart Debug Auto Flow Enables UART hardware flow control, CTS and RTS lines.

$EN_DIS

Definition at line 1460 of file FspmUpd.h.

13.33.2.138 SerialIoUartDebugBaudRate

```
UINT32 FSP_M_CONFIG::SerialIoUartDebugBaudRate
```

Offset 0x0450 - Serial Io Uart Debug BaudRate Set default BaudRate Supported from 0 - default to 6000000.

Recommended values 9600, 19200, 57600, 115200, 460800, 921600, 1500000, 1843200, 3000000, 3686400, 6000000

Definition at line 1470 of file FspmUpd.h.

13.33.2.139 SerialIoUartDebugControllerNumber

```
UINT8 FSP_M_CONFIG::SerialIoUartDebugControllerNumber
```

Offset 0x044C - Serial Io Uart Debug Controller Number Select SerialIo Uart Controller for debug.

Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 1454 of file FspmUpd.h.

13.33.2.140 SerialIoUartDebugDataBits

```
UINT8 FSP_M_CONFIG::SerialIoUartDebugDataBits
```

Offset 0x0456 - Serial Io Uart Debug Data Bits Set default word length.

0: Default, 5,6,7,8 5:5BITS, 6:6BITS, 7:7BITS, 8:8BITS

Definition at line 1488 of file FspmUpd.h.

13.33.2.141 SerialIoUartDebugParity

```
UINT8 FSP_M_CONFIG::SerialIoUartDebugParity
```

Offset 0x0454 - Serial Io Uart Debug Parity Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 1476 of file FspmUpd.h.

13.33.2.142 SerialIoUartDebugStopBits

```
UINT8 FSP_M_CONFIG::SerialIoUartDebugStopBits
```

Offset 0x0455 - Serial Io Uart Debug Stop Bits Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 1482 of file FspmUpd.h.

13.33.2.143 SinitMemorySize

```
UINT32 FSP_M_CONFIG::SinitMemorySize
```

Offset 0x020C - SinitMemorySize Enable/Disable.

0: Disable, define default value of SinitMemorySize , 1: enable

Definition at line 1088 of file FspmUpd.h.

13.33.2.144 SkipMpInit

```
UINT8 FSP_M_CONFIG::SkipMpInit
```

Offset 0x00BA - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SilicionInit API.

0: Initialize; **1: Skip $EN_DIS**

Definition at line 288 of file FspmUpd.h.

13.33.2.145 SmbusArpEnable

```
UINT8 FSP_M_CONFIG::SmbusArpEnable
```

Offset 0x043A - Enable SMBus ARP support Enable SMBus ARP support.

$EN_DIS

Definition at line 1398 of file FspmUpd.h.

13.33.2.146 SmbusEnable

```
UINT8 FSP_M_CONFIG::SmbusEnable
```

Offset 0x0250 - Enable SMBus Enable/disable SMBus controller.

$EN_DIS

Definition at line 1170 of file FspmUpd.h.

13.33.2.147 SpdAddressTable

```
UINT8 FSP_M_CONFIG::SpdAddressTable[4]
```

Offset 0x00A9 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.

MemorySpdPtr will be used if SPD Address is 00

Definition at line 209 of file FspmUpd.h.

13.33.2.148 SpdProfileSelected

```
UINT8 FSP_M_CONFIG::SpdProfileSelected
```

Offset 0x00BB - SPD Profile Selected Select DIMM timing profile.

Options are 0=Default profile, 1=Custom profile, 2=XMP Profile 1, 3=XMP Profile 2 0:Default profile, 1:Custom profile, 2:XMP profile 1, 3:XMP profile 2

Definition at line 295 of file FspmUpd.h.

13.33.2.149 TgaSize

```
UINT32 FSP_M_CONFIG::TgaSize
```

Offset 0x022C - TgaSize Enable/Disable.

0: Disable, define default value of TgaSize , 1: enable

Definition at line 1123 of file FspmUpd.h.

13.33.2.150 ThrtCkeMinTmr

```
UINT8 FSP_M_CONFIG::ThrtCkeMinTmr
```

Offset 0x04E4 - Throttler CKEMin Timer Timer value for CKEMin, range[255;0].

Req'd min of SC_ROUND_T + BYTE_LENGTH (4). Default is 0x30

Definition at line 2240 of file FspmUpd.h.

13.33.2.151 ThrtCkeMinTmrLpddr

```
UINT8 FSP_M_CONFIG::ThrtCkeMinTmrLpddr
```

Offset 0x050B - Throttler CKEMin Timer - LPDDR Timer value for CKEMin (For LPDDR Only), range[255;0].

Req'd min of SC_ROUND_T + BYTE_LENGTH (4). Default is 0x40

Definition at line 2481 of file FspmUpd.h.

13.33.2.152 TjMaxOffset

```
UINT8 FSP_M_CONFIG::TjMaxOffset
```

Offset 0x0200 - TjMax Offset TjMax offset.Specified value here is clipped by pCode (125 - TjMax Offset) to support TjMax in the range of 62 to 115 deg Celsius.

Valid Range 10 - 63

Definition at line 1052 of file FspmUpd.h.

13.33.2.153 TrainTrace

```
UINT8 FSP_M_CONFIG::TrainTrace
```

Offset 0x0098 - Training Trace This option enables the trained state tracing feature in MRC.

This feature will print out the key training parameters state across major training steps. $EN_DIS

Definition at line 165 of file FspmUpd.h.

13.33.2.154 tRTP

```
UINT8 FSP_M_CONFIG::tRTP
```

Offset 0x00CE - tRTP Min Internal Read to Precharge Command Delay Time, 0: AUTO, max: 15.

DDR4 legal values: 5, 6, 7, 8, 9, 10, 12

Definition at line 371 of file FspmUpd.h.

13.33.2.155 TsegSize

```
UINT32 FSP_M_CONFIG::TsegSize
```

Offset 0x00A0 - Tseg Size Size of SMRAM memory reserved.

0x400000 for Release build and 0x1000000 for Debug build 0x0400000:4MB, 0x01000000:16MB

Definition at line 181 of file FspmUpd.h.

13.33.2.156 TsodAlarmwindowLockBit

```
UINT8 FSP_M_CONFIG::TsodAlarmwindowLockBit
```

Offset 0x04F3 - Alarm window lock bit Disable:Alarm trips are not locked and can be changed.

Enable:Alarm trips are locked and cannot be changed $EN_DIS

Definition at line 2336 of file FspmUpd.h.

13.33.2.157 TsodCriticalEventOnly

```
UINT8 FSP_M_CONFIG::TsodCriticalEventOnly
```

Offset 0x04F1 - Critical event only Disable:Trips on alarm or critical.

Enable:Trips only if criticaal temperature is reached $EN_DIS

Definition at line 2322 of file FspmUpd.h.

13.33.2.158 TsodCriticaltripLockBit

```
UINT8 FSP_M_CONFIG::TsodCriticaltripLockBit
```

Offset 0x04F4 - Critical trip lock bit Disable:Critical trip is not locked and can be changed.

Enable:Critical trip is locked and cannot be changed $EN_DIS

Definition at line 2343 of file FspmUpd.h.

13.33.2.159 TsodEventMode

```
UINT8 FSP_M_CONFIG::TsodEventMode
```

Offset 0x04EF - Event mode Disable:Comparator mode.

Enable:Interrupt mode $EN_DIS

Definition at line 2308 of file FspmUpd.h.

13.33.2.160 TsodEventOutputControl

```
UINT8 FSP_M_CONFIG::TsodEventOutputControl
```

Offset 0x04F2 - Event output control Disable:Event output disable.

Enable:Event output enabled $EN_DIS

Definition at line 2329 of file FspmUpd.h.

13.33.2.161 TsodEventPolarity

```
UINT8 FSP_M_CONFIG::TsodEventPolarity
```

Offset 0x04F0 - EVENT polarity Disable:Active LOW.

Enable:Active HIGH $EN_DIS

Definition at line 2315 of file FspmUpd.h.

13.33.2.162 TsodManualEnable

```
UINT8 FSP_M_CONFIG::TsodManualEnable
```

Offset 0x04F7 - User Manual Thig and Tcrit Disabled(Default): Temperature will be given by the configuration of memories and 1x or 2xrefresh rate.

Enabled: User Input will define for Thigh and Tcrit. $EN_DIS

Definition at line 2363 of file FspmUpd.h.

13.33.2.163 TsodShutdownMode

```
UINT8 FSP_M_CONFIG::TsodShutdownMode
```

Offset 0x04F5 - Shutdown mode Disable:Temperature sensor enable.

Enable:Temperature sensor disable $EN_DIS

Definition at line 2350 of file FspmUpd.h.

13.33.2.164 TsodTcritMax

```
UINT8 FSP_M_CONFIG::TsodTcritMax
```

Offset 0x04EE - TcritMax Maximum Critical Temperature in Centigrade of the On-DIMM Thermal Sensor.

TCRITMax has to be greater than THIGHMax .
Critical temperature will be TcritMax

Definition at line 2301 of file FspmUpd.h.

13.33.2.165 TvbRatioClipping

```
UINT8 FSP_M_CONFIG::TvbRatioClipping
```

Offset 0x0121 - Thermal Velocity Boost Ratio clipping 0(Default): Disabled, 1: Enabled.

This service controls Core frequency reduction caused by high package temperatures for processors that implement the Intel Thermal Velocity Boost (TVB) feature 0: Disabled, 1: Enabled

Definition at line 661 of file FspmUpd.h.

13.33.2.166 TvbVoltageOptimization

```
UINT8 FSP_M_CONFIG::TvbVoltageOptimization
```

Offset 0x0122 - Thermal Velocity Boost voltage optimization 0: Disabled, 1: Enabled(Default).

This service controls thermal based voltage optimizations for processors that implement the Intel Thermal Velocity Boost (TVB) feature. 0: Disabled, 1: Enabled

Definition at line 668 of file FspmUpd.h.

13.33.2.167 Txt

```
UINT8 FSP_M_CONFIG::Txt
```

Offset 0x0204 - Txt Enable/Disable.

0: Disable, Enable/Disable Txt feature, 1: enable $EN_DIS

Definition at line 1074 of file FspmUpd.h.

13.33.2.168 TxtDprMemoryBase

```
UINT64 FSP_M_CONFIG::TxtDprMemoryBase
```

Offset 0x0218 - TxtDprMemoryBase Enable/Disable.

0: Disable, define default value of TxtDprMemoryBase , 1: enable

Definition at line 1103 of file FspmUpd.h.

13.33.2.169 TxtDprMemorySize

```
UINT32 FSP_M_CONFIG::TxtDprMemorySize
```

Offset 0x0214 - TxtDprMemorySize Enable/Disable.

0: Disable, define default value of TxtDprMemorySize , 1: enable

Definition at line 1098 of file FspmUpd.h.

13.33.2.170 TxtHeapMemorySize

```
UINT32 FSP_M_CONFIG::TxtHeapMemorySize
```

Offset 0x0210 - TxtHeapMemorySize Enable/Disable.

0: Disable, define default value of TxtHeapMemorySize , 1: enable

Definition at line 1093 of file FspmUpd.h.

13.33.2.171 TxtImplemented

```
UINT8 FSP_M_CONFIG::TxtImplemented
```

Offset 0x01C1 - Enable/Disable MRC TXT dependency When enabled MRC execution will wait for TXT initialization to be done first.

Disabled(0x0)(Default): MRC will not wait for TXT initialization, Enabled(0x1): MRC will wait for TXT initialization $EN_DIS

Definition at line 762 of file FspmUpd.h.

13.33.2.172 TxtLcpPdBase

```
UINT64 FSP_M_CONFIG::TxtLcpPdBase
```

Offset 0x0230 - TxtLcpPdBase Enable/Disable.

0: Disable, define default value of TxtLcpPdBase , 1: enable

Definition at line 1128 of file FspmUpd.h.

13.33.2.173 TxtLcpPdSize

```
UINT64 FSP_M_CONFIG::TxtLcpPdSize
```

Offset 0x0238 - TxtLcpPdSize Enable/Disable.

0: Disable, define default value of TxtLcpPdSize , 1: enable

Definition at line 1133 of file FspmUpd.h.

13.33.2.174 UserBudgetEnable

```
UINT8 FSP_M_CONFIG::UserBudgetEnable
```

Offset 0x04ED - User Manual Budget Disabled: Configuration of memories will defined the Budget value.

Enabled: User Input will be used. $EN_DIS

Definition at line 2294 of file FspmUpd.h.

13.33.2.175 UserThresholdEnable

```
UINT8 FSP_M_CONFIG::UserThresholdEnable
```

Offset 0x04EC - User Manual Threshold Disabled: Predefined threshold will be used.

Enabled: User Input will be used. $EN_DIS

Definition at line 2287 of file FspmUpd.h.

13.33.2.176 VddVoltage

```
UINT16 FSP_M_CONFIG::VddVoltage
```

Offset 0x00BE - Memory Voltage Memory Voltage Override (Vddq).

Default = no override 0:Default, 1200:1.20 Volts, 1250:1.25 Volts, 1300:1.30 Volts, 1350:1.35 Volts, 1400:1.40 Volts, 1450:1.45 Volts, 1500:1.50 Volts, 1550:1.55 Volts, 1600:1.60 Volts, 1650:1.65 Volts

Definition at line 312 of file FspmUpd.h.

13.33.2.177 VmaxStress

```
UINT8 FSP_M_CONFIG::VmaxStress
```

Offset 0x0242 - Vmax Stress Vmax Stress enable/disable.

When enabled, frequency may be clipped the effective max voltage on the silicon is too high.0: Disable; **1: Enable.** $EN_DIS

Definition at line 1153 of file FspmUpd.h.

13.33.2.178 VmxEnable

```
UINT8 FSP_M_CONFIG::VmxEnable
```

Offset 0x01ED - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 975 of file FspmUpd.h.

13.33.2.179 WarmThresholdCh0Dimm0

```
UINT8 FSP_M_CONFIG::WarmThresholdCh0Dimm0
```

Offset 0x04C0 - Warm Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2059 of file FspmUpd.h.

13.33.2.180 WarmThresholdCh0Dimm1

```
UINT8 FSP_M_CONFIG::WarmThresholdCh0Dimm1
```

Offset 0x04C1 - Warm Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2064 of file FspmUpd.h.

13.33.2.181 WarmThresholdCh1Dimm0

```
UINT8 FSP_M_CONFIG::WarmThresholdCh1Dimm0
```

Offset 0x04C2 - Warm Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2069 of file FspmUpd.h.

13.33.2.182 WarmThresholdCh1Dimm1

`UINT8 FSP_M_CONFIG::WarmThresholdCh1Dimm1`

Offset 0x04C3 - Warm Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 2074 of file FspmUpd.h.

The documentation for this struct was generated from the following file:

- FspmUpd.h

13.34 FSP_M_RESTRICTED_CONFIG Struct Reference

Fsp M Restricted Configuration.

`#include <FspmUpd.h>`

Public Attributes

- UINT32 Signature

  Offset 0x0620.
- UINT16 SaSvRemapBaseOverride

  Offset 0x0624 - Sa Sv Remap Base Override SvRemapBaseOverride.
- UINT8 SaSystemAgentClockGatingEnable

  Offset 0x0626 - Sa System Agent ClockGating Enable SystemAgentClockGatingEnable.
- UINT8 SaPciePllShutdownEnable

  Offset 0x0627 - Sa Pcie Pll Shutdown Enable PciePllShutdownEnable.
- UINT8 SaSV_DMI_GEN1_halt

  Offset 0x0628 - Sa SV_DMI_GEN1_halt SV_DMI_GEN1_halt.
- UINT8 SaSV_nFTS_DMI_auto

  Offset 0x0629 - Sa SV_nFTS_DMI_auto SV_nFTS_DMI_auto.
- UINT8 SaSvDMI_nFTS

  Offset 0x062A - Sa Sv DMI_nFTS SvDMI_nFTS.
- UINT8 SanFTS_auto

  Offset 0x062B - Sa nFTS_auto nFTS_auto.
- UINT8 SaSvPEG_nFTS [4]

  Offset 0x062C - Sa SvPEG_nFTS SvPEG_nFTS.
- UINT8 SaSvPEG_gen3_ccFTS [4]

  Offset 0x0630 - Sa SvPEG_gen3_ccFTS SvPEG_gen3_ccFTS.
- UINT8 SaSvPEG_gen3_nccFTS [4]

  Offset 0x0634 - Sa SvPEG_gen3_nccFTS SvPEG_gen3_nccFTS.
- UINT8 SanFTS_gen3_auto

  Offset 0x0638 - Sa nFTS_gen3_auto nFTS_gen3_auto.
- UINT8 SaSVIAER

  Offset 0x0639 - Sa SVIAER SVIAER.
- UINT8 SaSvScramblerDmi

Offset 0x063A - Sa Sv Scrambler Dmi SvScramblerDmi.

- UINT8 SaSvScramblerPeg [4]

  Offset 0x063B - Sa Sv Scrambler Peg SvScramblerPeg.
- UINT8 SaSvDmiSerr

  Offset 0x063F - Sa Sv Dmi Serr SvDmiSerr.
- UINT8 SaSvScramblerPegGen3 [4]

  Offset 0x0640 - Sa Sv Scrambler Peg Gen3 SvScramblerPegGen3.
- UINT8 SaSvPegSerr [4]

  Offset 0x0644 - Sa Sv Peg Serr SvPegSerr.
- UINT8 SaTestTxClkGating

  Offset 0x0648 - Sa Test Tx ClkGating TestTxClkGating.
- UINT8 SaTestRxClkGating

  Offset 0x0649 - Sa Test Rx ClkGating TestRxClkGating.
- UINT8 SaTestLowPwrMode

  Offset 0x064A - Sa Test Low Pwr Mode TestLowPwrMode.
- UINT8 SaSrMode

  Offset 0x064B - Sa Sr Mode SrMode.
- UINT8 SaSrSeq

  Offset 0x064C - Sa Sr Seq SrSeq.
- UINT8 SaBurstSpacing

  Offset 0x064D - Sa Burst Spacing BurstSpacing.
- UINT8 SaRestrictedSvPolicyEnable

  Offset 0x064E - SvPolicyEnable Enable: SV policy is enabled, Disable(Default): SV policy is disabled $EN_DIS.
- UINT8 SaCpuSvBootMode

  Offset 0x064F - Cpu Sv Boot Mode 0: Auto (Default), 1: Commercial boot mode, 2: SV boot mode, 3: SV boot JTAG mode with SB loop, 4: SV boot JTAG mode without SB loop 0: Auto , 1: Commercial boot mode, 2: SV boot mode, 3: SV boot JTAG mode with SB loop, 4: SV boot JTAG mode without SB loop.
- UINT8 XmlCliEnable

  Offset 0x0650 - CpuSvBootMode Enable: XmlCli is enabled, Disble(Default): XmlCli is disabled $EN_DIS.
- UINT8 LoadValidationFv

  Offset 0x0651 - LoadValidationFv Enable: Enable loading of ValidationFV, Disable(Default) $EN_DIS.
- UINT8 SvReserveMemoryBelowPrmrr

  Offset 0x0652 - SvReserveMemoryBelowPrmrr Enable: Enable reserve SV memory below PMRR, Disable(Default) $EN_DIS.
- UINT8 SaTestSamplePartStatusOverride

  Offset 0x0653 - Sa Test Sample Part Status Override 0-Passthrough, 1-Production part, 2-Preproduction part.
- UINT8 SaTestGrunitClockGating

  Offset 0x0654 - Sa Test Grunit ClockGating Enable Sa Test Grunit ClockGating $EN_DIS.
- UINT8 SaTestDmiCapRegLock

  Offset 0x0655 - Sa Test Dmi Cap Reg Lock DMI Capability Register Lock.
- UINT8 SaTestDmiMaxPayloadSize

  Offset 0x0656 - Sa Test Dmi Max Payload Size DMI Max Payload Size.
- UINT8 SaPcieVcLimLock

  Offset 0x0657 - Sa Pcie VcLim Lock Lock bit.
- UINT8 SaPcieVCmCmpLim

  Offset 0x0658 - Sa Pcie VCm Cmp Lim VCm Completions override.
- UINT8 SaPcieVCmPLim

  Offset 0x0659 - Sa Pcie VCm PLim posted VCm Requests override.
- UINT8 SaPcieVCmNpLim

  Offset 0x065A - Sa Pcie VCm NpLim non-posted VCm Requests override.
- UINT8 SaLagunaCreditWA

Offset 0x065B - Sa Laguna Credit WA Laguna Credit WA.

- UINT8 SaSvDmiComplianceDeemphasis

  Offset 0x065C - Sa Sv Dmi Compliance Deemphasis SvDmiComplianceDeemphasis.
- UINT8 PrefetchNonPrefetchRatio

  Offset 0x065D - Prefetch NonPrefetch Ratio 0: All prefetch, 1: Seven of Eight Prefetch, 2: Three of Four Prefetch, 3: Half Prefetch Half Non-Prefetch(Default), 4: Three of Four Non-Prefetch, 5: Seven of Eight Prefetch, 6: All Non-prefetch 0: All prefetch, 1: Seven of Eight Prefetch, 2: Three of Four Prefetch, 3: Half Prefetch Half Non-Prefetch, 4: Three of Four Non-Prefetch, 5: Seven of Eight Prefetch, 6: All Non-prefetch.
- UINT8 SaTestDev0DidOverride

  Offset 0x065E - Sa Test Dev0 Did Override Dev 0 Device ID override.
- UINT8 SaTestMobileSaDidOverride

  Offset 0x065F - Sa Test Mobile Sa Did Override Dev 0 Mobile (ULT/ULX) Device ID override.
- UINT8 SaTestNonMobileSaDidOverride

  Offset 0x0660 - Sa Test NonMobile Sa Did Override Dev 0 Non Mobile (DT, DT_Halo, M_Halo, Server) Device ID override.
- UINT8 SaTestDev2GtDidOverride

  Offset 0x0661 - Sa Test Dev2 Gt Did Override Dev 2 GT Device ID override.
- UINT8 SaTestGt4HaloDidOverride

  Offset 0x0662 - Sa Test Gt4 Halo Did Override Dev 2 GT4 Halo Device ID override.
- UINT8 SaTestGt3UltDidOverride

  Offset 0x0663 - Sa Test Gt3 Ult Did Override Dev 2 GT3 ULT Device ID override.
- UINT8 SaTestGt2UlxDidOverride

  Offset 0x0664 - Sa Test Gt2 Ulx Did Override Dev 2 GT2 ULX Device ID override.
- UINT8 SaTestGt2UltDidOverride

  Offset 0x0665 - Sa Test Gt2 Ult Did Override Dev 2 GT2 ULT Device ID override.
- UINT8 SaPreMemRestrictedRsvd [14]

  Offset 0x0666 - SaPreMemRestrictedRsvd Reserved for SA Pre-Mem Restricted $EN_DIS.
- UINT8 UnusedUpdSpace10 [4]

  Offset 0x0674.
- UINT64 MsegSize

  Offset 0x0678 - MSEG Size MSEG Size.
- UINT8 ForceTxtEnable

  Offset 0x0680 - Force TXT Enable Force TXT Enable; 0: disable, 1: enable $EN_DIS.
- UINT8 UnlockMchbarCtrlRegs

  Offset 0x0681 - Unlock MCHBAR control registers Unlock MCHBAR control registers; 0: disable, 1: enable $EN_DIS.
- UINT8 CpuPreMemRestrictedRsvd [6]

  Offset 0x0682 - SaPreMemRestrictedRsvd Reserved for SA Pre-Mem Restricted $EN_DIS.
- UINT8 DmaPassThrough

  Offset 0x0688 - Enable or disable VT-d DmaPassThrough 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 CCHit2pend

  Offset 0x0689 - Enable or disable VT-d CCHit2pend 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 ContextInvalidation

  Offset 0x068A - Enable or disable VT-d ContextInvalidation 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 IotlbInvalidation

  Offset 0x068B - Enable or disable VT-d IotlbInvalidation 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 ContextCacheDis

  Offset 0x068C - Enable or disable VT-d ContextCacheDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L1Disable

  Offset 0x068D - Enable or disable VT-d L1Disable 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L2Disable

  Offset 0x068E - Enable or disable VT-d L2Disable 0=Disable, 1(Default)=Enable $EN_DIS.

- UINT8 L3Disable

  Offset 0x068F - Enable or disable VT-d L3Disable 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L1Hit2PendDis

  Offset 0x0690 - Enable or disable VT-d L1Hit2PendDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L3Hit2PendDis

  Offset 0x0691 - Enable or disable VT-d L3Hit2PendDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 InvQueueCohDis

  Offset 0x0692 - Enable or disable VT-d InvQueueCohDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 SuperPageCap

  Offset 0x0693 - Enable or disable VT-d SuperPageCap 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 QueueInvCapDis

  Offset 0x0694 - Enable or disable VT-d QueueInvCapDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 TestIntrRemapCapDis

  Offset 0x0695 - Enable or disable VT-d IntrRemapCapDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 SnoopControl

  Offset 0x0696 - Enable or disable VT-d SnoopControl 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 RemapReverseCtrl

  Offset 0x0697 - Enable or disable VT-d RemapReverseCtrl 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 PchTestDmiTranCoOverEn [4]

  Offset 0x0698 - Dmi Test Tran Co Over En Enable/Disable Lane Transmitter Coefficient.
- UINT8 PchTestDmiTranCoOverPostCur [4]

  Offset 0x069C - Dmi Test Tran Co Over Post Cur Lane Transmitter Post-Cursor Coefficient Override.
- UINT8 PchTestDmiTranCoOverPreCur [4]

  Offset 0x06A0 - Dmi Test Tran Co Over Pre Cur Lane Transmitter Pre-Cursor Coefficient Override.
- UINT8 PchTestDmiUpPortTranPreset [4]

  Offset 0x06A4 - Dmi Test Up Port Tran Preset Upstream Port Lane Transmitter Preset.
- UINT8 PchTestDmiUpPortTranPresetEn

  Offset 0x06A8 - Dmi Test UpPort Tran Preset En 0: POR setting, 1: force enable, 2: force disable.
- UINT8 PchTestDmiRtlepceb

  Offset 0x06A9 - Dmi Test Rtlepceb DMI Remote Transmit Link Equalization Preset/Coefficient Evaluation Bypass (RTLEPCEB).
- UINT8 PchTestDmiMeUmaRootSpaceCheck

  Offset 0x06AA - DMI ME UMA Root Space Check DMI IOSF Root Space attribute check for RS3 for cycles targeting MEUMA.
- UINT8 PchHdaTestConfigLockdown

  Offset 0x06AB - Configuration Lockdown (BCLD) 0: POR (Enable), 1: Enable, 2: Disable.
- UINT8 PchHdaTestLowFreqLinkClkSrc

  Offset 0x06AC - Low Frequency Link Clock Source (LFLCS) 0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL).
- UINT8 PchHdaTestPowerClockGating

  Offset 0x06AD - HDA Power/Clock Gating (PGD/CGD) POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE.
- UINT8 HeciCommunication

  Offset 0x06AE - HECI Communication Test, 0: POR, 1: enable, 2: disable, Disables HECI communication causing ME to enter error state.
- UINT8 HeciCommunication3

  Offset 0x06AF - HECI3 Interface Communication Test, 0: POR, 1: enable, 2: disable, Adds or Removes HECI3 Device from PCI space.
- UINT8 HostResetNotification

  Offset 0x06B0 - Notification test for Host Reset Test, 0: POR, 1: enable, 2: disable, Enable test for notification when Host Reset $EN_DIS.
- UINT8 ManufRstAndHaltOnS3Resume

Offset 0x06B1 - Send Manufacturing Reset And Halt On S3 Resume Test, 0: POR, 1: enable, 2: disable, Enable sending Manufacturing Reset and Halt on S3 Resume $EN_DIS.

- UINT8 ForceUnlockAes

  Offset 0x06B2 - Force Unlock AES 0(Default)=Disable, 1=Enable $EN_DIS.

- UINT8 PreMemRestrictedRsvd2 [23]

  Offset 0x06B3 - PreMemRestrictedRsvd2 Reserved for Pre-Mem RestrictedReserved $EN_DIS.

- UINT8 AsyncOdtDis

  Offset 0x06CA - Asynchronous ODT This option configures the Memory Controler Asynchronous ODT control 0↩ :Enabled, 1:Disabled.

- UINT8 PowerDownMode

  Offset 0x06CB - Power Down Mode This option controls command bus tristating during idle periods 0x0:No Power Down, 0x1:APD, 0x6:PPD DLL OFF, 0xFF:Auto.

- UINT8 WeaklockEn

  Offset 0x06CC - DLL Weak Lock Support Enables/Disable DLL Weak Lock Support $EN_DIS.

- UINT8 Force1Dpc

  Offset 0x06CD - Fore 1 DPC config Enables/Disable Fore 1 DPC config $EN_DIS.

- UINT8 ForceSingleRank

  Offset 0x06CE - Fore Single Rank config Enables/Disable Fore Single Rank config $EN_DIS.

- UINT8 UnusedUpdSpace11

  Offset 0x06CF.

- UINT16 SrefCfgIdleTmr

  Offset 0x06D0 - SelfRefresh IdleTimer Self Refresh idle timer in nCK units: 0 = Auto (default), or value in range [512 .

- UINT8 StrongWkLeaker

  Offset 0x06D2 - Strong Weak Leaker Strong Weak Leaker value.

- UINT8 IgnoreDdr4FreqLimit3200

  Offset 0x06D3 - Ignore DDR4 Frequency Limitation Option to ignore the DDR4-3200 frequency limitation based on board type and memory popualation $EN_DIS.

- UINT8 OpportunisticRead

  Offset 0x06D4 - Opportunistic Read Enables/Disable Opportunistic Read (Def= Enable) $EN_DIS.

- UINT8 MemStackMode

  Offset 0x06D5 - Stacked Mode Memory Stacked Mode Support (Def = Disable) $EN_DIS.

- UINT8 StackModeChBit

  Offset 0x06D6 - Stacked Mode Ch Bit Channel hash bit used during Stacked Mode(Def= BIT28) 0:BIT28, 1:BIT29, 2:BIT30, 3:BIT31, 4:BIT32, 5:BIT33, 6:BIT34.

- UINT8 LowMemChannel

  Offset 0x06D7 - Low Memory Channel Selecting which Physical Channel is mapped to low memory.

- UINT8 Disable2CycleBypass

  Offset 0x06D8 - Cycle Bypass Support Enables/Disable Cycle Bypass Support(Def=Disable) $EN_DIS.

- UINT8 MCREGOFFSET

  Offset 0x06D9 - MC Register Offset Apply user offsets to select MC registers(Def=Disable) $EN_DIS.

- UINT8 CAVrefCtlOffset

  Offset 0x06DA - CA Vref Ctl Offset Offset to be applied to DDRDATA7CH1_CR_DDRCRVREFADJUST1.CAVref 0↩ :-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.

- UINT8 Ch0VrefCtlOffset

  Offset 0x06DB - Ch0 DQ Vref Ctrl Offset Offset to be applied to DDRDATA7CH1_CR_DDRCRVREFADJUST1.↩ Ch0VrefCtl 0:-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.

- UINT8 Ch1VrefCtlOffset

  Offset 0x06DC - Ch1 DQ Vref Ctrl Offset Offset to be applied to DDRDATA7CH1_CR_DDRCRVREFADJUST1.↩ Ch1VrefCtl 0:-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.

- UINT8 Ch0ClkPiCodeOffset

Offset 0x06DD - Ch0 Clk PI Code Offset Offset to be applied to DDRCLKCH0_CR_DDRCRCLKPICODE.PiSetting↩ Rank[0-3] 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.

- UINT8 Ch1ClkPiCodeOffset

  Offset 0x06DE - Ch1 Clk PI Code Offset Offset to be applied to DDRCLKCH1_CR_DDRCRCLKPICODE.PiSetting↩ Rank[0-3] 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.

- UINT8 Ch0RcvEnOffset

  Offset 0x06DF - Ch0 RcvEn Offset Offset to be applied to DDRDATACH0_CR_DDRCRDATAOFFSETTRAIN.RcvEn 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch1RcvEnOffset

  Offset 0x06E0 - Ch1 RcvEn Offset Offset to be applied to DDRDATACH1_CR_DDRCRDATAOFFSETTRAIN.RcvEn 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch0RxDqsOffset

  Offset 0x06E1 - Ch0 Rx Dqs Offset Offset to be applied to DDRDATACH0_CR_DDRCRDATAOFFSETTRAIN.Rx↩ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch1RxDqsOffset

  Offset 0x06E2 - Ch1 Rx Dqs Offset Offset to be applied to DDRDATACH1_CR_DDRCRDATAOFFSETTRAIN.Rx↩ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch0TxDqOffset

  Offset 0x06E3 - Ch0 Tx Dq Offset Offset to be applied to DDRDATACH0_CR_DDRCRDATAOFFSETTRAIN.TxDq↩ Offset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch1TxDqOffset

  Offset 0x06E4 - Ch1 Tx Dq Offset Offset to be applied to DDRDATACH1_CR_DDRCRDATAOFFSETTRAIN.TxDq↩ Offset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch0TxDqsOffset

  Offset 0x06E5 - Ch0 Tx Dqs Offset Offset to be applied to DDRDATACH0_CR_DDRCRDATAOFFSETTRAIN.Tx↩ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch1TxDqsOffset

  Offset 0x06E6 - Ch1 Tx Dqs Offset Offset to be applied to DDRDATACH1_CR_DDRCRDATAOFFSETTRAIN.Tx↩ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.

- UINT8 Ch0VrefOffset

  Offset 0x06E7 - Ch0 Vref Offset Offset to be applied to DDRDATACH0_CR_DDRCRDATAOFFSETTRAIN.VrefOffset 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.

- UINT8 Ch1VrefOffset

  Offset 0x06E8 - Ch1 Vref Offset Offset to be applied to DDRDATACH1_CR_DDRCRDATAOFFSETTRAIN.VrefOffset 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.

- UINT8 MrcRestrictedRsvd0x067F [16]

  Offset 0x06E9.

- UINT8 DcttTest

  Offset 0x06F9 - DCTT Test Select which test to run 0:Basic walking memory test, 1:Row Hammer test.

- UINT8 DcttRhIterationOnRow

  Offset 0x06FA - DCTT: Iterations on Row Number of repetitions on a Row.

- UINT8 DcttRhPageCloseDelay

  Offset 0x06FB - Page Close Delay Prompt SubSequence Delay value used to ensure the page closes (In DClks)

- UINT8 DcttRhRefreshEnable

  Offset 0x06FC - Row Hammer Refresh Enable/Disables refreshes during the Row Hammer Test $EN_DIS.

- UINT8 DcttDataBase

  Offset 0x06FD - Data Base Select which data pattern that is used as the base pattern 0:Zeros, 1:Ones, 2:Five, 3:A.

- UINT8 UnusedUpdSpace12 [2]

  Offset 0x06FE.

- UINT32 DcttRhHammerCount

  Offset 0x0700 - DCTT: Row Hammer Count Number of Hammers for a given Row.

- UINT8 DcttRowSwizzleType

Offset 0x0704 - Row swizzle Select which Row swizzle algorithm to use during Row Hammer test 0:No Swizzle, 1:3xOr1_3xOr2, 2:01234567EFCDAB89.

- UINT8 DcttRefreshMultiplier

  Offset 0x0705 - Refresh Multiplier Multiplier applied to tREFI.
- UINT8 DcttBankDisableMask

  Offset 0x0706 - Bank Disable Mask Bit Mask Bank Disable for per-Bank tests (Row Hammer)
- UINT8 ScramClockGateAB

  Offset 0x0707 - Clock Gate AB Clock Gate AB 0:Disable, 1:2 Cycles, 2:3 Cycles, 3:4 Cycles.
- UINT8 ScramClockGateC

  Offset 0x0708 - Clock Gate C Select which Row swizzle algorithm to use during Row Hammer test 0:Disable, 1:2 Cycles, 2:4 Cycles, 3:8 Cycles.
- UINT8 ScramEnableDbiAB

  Offset 0x0709 - Enable DBI AB Enable DBI AB $EN_DIS.
- UINT8 Interpreter

  Offset 0x070A - MRC Interpreter Select CMOS location match of DD01 or Ctrl-Break key or force entry 0:CMOS, 1:Break, 2:Force.
- UINT8 IoOdtMode

  Offset 0x070B - ODT mode ODT mode 0:Default, 1:Ctt, 2:Vtt, 3:Vddq, 4:Vss,5:Max.
- UINT8 TestMenuDprLock

  Offset 0x070C - Lock DPR register Lock DPR register.
- UINT8 PerBankRefresh

  Offset 0x070D - PerBankRefresh Control of Per Bank Refresh feature for LPDDR DRAMs $EN_DIS.
- UINT8 CmdTriStateDis

  Offset 0x070E - Command Tristate Enables/Disable Command Tristate $EN_DIS.
- UINT8 MrcRestrictedRsvd [1]

  Offset 0x070F.
- UINT8 PpvBtrEnable

  Offset 0x0710 - PPV Boot Time Reduction This option disable/enable PPV Boot Time Reduction functionality.
- UINT8 UnusedUpdSpace13 [5]

  Offset 0x0711.
- UINT8 ReservedFspmRestrictedUpd [26]

  Offset 0x0716.

13.34.1 Detailed Description

Fsp M Restricted Configuration.

Definition at line 3097 of file FspmUpd.h.

13.34.2 Member Data Documentation

13.34.2.1 HeciCommunication

```
UINT8 FSP_M_RESTRICTED_CONFIG::HeciCommunication
```

Offset 0x06AE - HECI Communication Test, 0: POR, 1: enable, 2: disable, Disables HECI communication causing ME to enter error state.

$EN_DIS

Definition at line 3538 of file FspmUpd.h.

13.34.2.2 HeciCommunication3

```
UINT8 FSP_M_RESTRICTED_CONFIG::HeciCommunication3
```

Offset 0x06AF - HECI3 Interface Communication Test, 0: POR, 1: enable, 2: disable, Adds or Removes HECI3 Device from PCI space.

$EN_DIS

Definition at line 3544 of file FspmUpd.h.

13.34.2.3 LowMemChannel

```
UINT8 FSP_M_RESTRICTED_CONFIG::LowMemChannel
```

Offset 0x06D7 - Low Memory Channel Selecting which Physical Channel is mapped to low memory.

0:Channel A, 1:Channel B, 0xFF:AUTO

Definition at line 3644 of file FspmUpd.h.

13.34.2.4 MsegSize

```
UINT64 FSP_M_RESTRICTED_CONFIG::MsegSize
```

Offset 0x0678 - MSEG Size MSEG Size.

Valid values 0 : 512K , 1 : 1M , 2 : 1.5M , 3 : 2M , 4 : 2.4M , 5 : 3M 0 : 512K , 1 : 1M , 2 : 1.5M , 3 : 2M , 4 : 2.4M , 5 : 3M

Definition at line 3365 of file FspmUpd.h.

13.34.2.5 PchHdaTestPowerClockGating

```
UINT8 FSP_M_RESTRICTED_CONFIG::PchHdaTestPowerClockGating
```

Offset 0x06AD - HDA Power/Clock Gating (PGD/CGD) POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE.

0: POR, 1: Force Enable, 2: Force Disable

Definition at line 3531 of file FspmUpd.h.

13.34.2.6 PchTestDmiMeUmaRootSpaceCheck

```
UINT8 FSP_M_RESTRICTED_CONFIG::PchTestDmiMeUmaRootSpaceCheck
```

Offset 0x06AA - DMI ME UMA Root Space Check DMI IOSF Root Space attribute check for RS3 for cycles targeting MEUMA.

0: POR, 1: enable, 2: disable

Definition at line 3515 of file FspmUpd.h.

13.34.2.7 PpvBtrEnable

```
UINT8 FSP_M_RESTRICTED_CONFIG::PpvBtrEnable
```

Offset 0x0710 - PPV Boot Time Reduction This option disable/enable PPV Boot Time Reduction functionality.

(Default==False) 0:Platform POR, 1: Enable Skip non-MRC Resets, 2: Enable Skip MRC Full Training, 3: Enable Skip Both MRC FT and Resets

Definition at line 3868 of file FspmUpd.h.

13.34.2.8 SrefCfgIdleTmr

```
UINT16 FSP_M_RESTRICTED_CONFIG::SrefCfgIdleTmr
```

Offset 0x06D0 - SelfRefresh IdleTimer Self Refresh idle timer in nCK units: 0 = Auto (default), or value in range [512
.

. 65535]

Definition at line 3608 of file FspmUpd.h.

13.34.2.9 StrongWkLeaker

```
UINT8 FSP_M_RESTRICTED_CONFIG::StrongWkLeaker
```

Offset 0x06D2 - Strong Weak Leaker Strong Weak Leaker value.

7=def

Definition at line 3613 of file FspmUpd.h.

13.34.2.10 TestMenuDprLock

```
UINT8 FSP_M_RESTRICTED_CONFIG::TestMenuDprLock
```

Offset 0x070C - Lock DPR register Lock DPR register.

0: Platform POR ; 1: Enable; 2: Disable 0:Platform POR, 1: Enable, 2: Disable

Definition at line 3845 of file FspmUpd.h.

The documentation for this struct was generated from the following file:

- FspmUpd.h

13.35 FSP_M_TEST_CONFIG Struct Reference

Fsp M Test Configuration.

```
#include <FspmUpd.h>
```

Public Attributes

- UINT32 Signature

  Offset 0x0558.
- UINT8 SkipExtGfxScan

  Offset 0x055C - Skip external display device scanning Enable: Do not scan for external display device, Disable (Default): Scan external display devices $EN_DIS.
- UINT8 BdatEnable

  Offset 0x055D - Generate BIOS Data ACPI Table Enable: Generate BDAT for MRC RMT or SA PCIe data.
- UINT8 ScanExtGfxForLegacyOpRom

  Offset 0x055E - Detect External Graphics device for LegacyOpROM Detect and report if external graphics device only support LegacyOpROM or not (to support CSM auto-enable).
- UINT8 LockPTMregs

  Offset 0x055F - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.
- UINT8 DmiMaxLinkSpeed

  Offset 0x0560 - DMI Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.
- UINT8 DmiGen3EqPh2Enable

  Offset 0x0561 - DMI Equalization Phase 2 DMI Equalization Phase 2.
- UINT8 DmiGen3EqPh3Method

  Offset 0x0562 - DMI Gen3 Equalization Phase3 DMI Gen3 Equalization Phase3.
- UINT8 Peg0Gen3EqPh2Enable

  Offset 0x0563 - Phase2 EQ enable on the PEG 0:1:0.
- UINT8 Peg1Gen3EqPh2Enable

  Offset 0x0564 - Phase2 EQ enable on the PEG 0:1:1.
- UINT8 Peg2Gen3EqPh2Enable

  Offset 0x0565 - Phase2 EQ enable on the PEG 0:1:2.
- UINT8 Peg3Gen3EqPh2Enable

  Offset 0x0566 - Phase2 EQ enable on the PEG 0:1:3.

- UINT8 Peg0Gen3EqPh3Method

  Offset 0x0567 - Phase3 EQ method on the PEG 0:1:0.
- UINT8 Peg1Gen3EqPh3Method

  Offset 0x0568 - Phase3 EQ method on the PEG 0:1:1.
- UINT8 Peg2Gen3EqPh3Method

  Offset 0x0569 - Phase3 EQ method on the PEG 0:1:2.
- UINT8 Peg3Gen3EqPh3Method

  Offset 0x056A - Phase3 EQ method on the PEG 0:1:3.
- UINT8 PegGen3ProgramStaticEq

  Offset 0x056B - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program PEG Gen3 EQ Phase1 Static Presets.
- UINT8 Gen3SwEqAlwaysAttempt

  Offset 0x056C - PEG Gen3 SwEq Always Attempt Gen3 Software Equalization will be executed every boot.
- UINT8 Gen3SwEqNumberOfPresets

  Offset 0x056D - Select number of TxEq presets to test in the PCIe/DMI SwEq Select number of TxEq presets to test in the PCIe/DMI SwEq.
- UINT8 Gen3SwEqEnableVocTest

  Offset 0x056E - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.
- UINT8 PegRxCemTestingMode

  Offset 0x056F - PCIe Rx Compliance Testing Mode Disabled(0x0)(Default): Normal Operation - Disable PCIe Rx Compliance testing, Enabled(0x1): PCIe Rx Compliance Test Mode - PEG controller is in Rx Compliance Testing Mode; it should only be set when doing PCIe compliance testing $EN_DIS.
- UINT8 PegRxCemLoopbackLane

  Offset 0x0570 - PCIe Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specificied Lane (0 - 15) will be used for RxCEMLoopback.
- UINT8 PegGenerateBdatMarginTable

  Offset 0x0571 - Generate PCIe BDAT Margin Table Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.
- UINT8 PegRxCemNonProtocolAwareness

  Offset 0x0572 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.
- UINT8 PegGen3RxCtleOverride

  Offset 0x0573 - PCIe Override RxCTLE Disable(0x0)(Default): Normal Operation - RxCTLE adaptive behavior enabled, Enable(0x1): Override RxCTLE - Disable RxCTLE adaptive behavior to keep the configured RxCTLE peak values unmodified $EN_DIS.
- UINT8 PegGen3Rsvd

  Offset 0x0574 - Rsvd Disable(0x0)(Default): Normal Operation - RxCTLE adaptive behavior enabled, Enable(0x1)↩ : Override RxCTLE - Disable RxCTLE adaptive behavior to keep the configured RxCTLE peak values unmodified $EN_DIS.
- UINT8 PegGen3RootPortPreset [20]

  Offset 0x0575 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.
- UINT8 PegGen3EndPointPreset [20]

  Offset 0x0589 - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.
- UINT8 PegGen3EndPointHint [20]

  Offset 0x059D - PEG Gen3 End port Hint values per lane Used for programming PEG Gen3 Hint values per lane.
- UINT8 UnusedUpdSpace8

  Offset 0x05B1.
- UINT16 Gen3SwEqJitterDwellTime

  Offset 0x05B2 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.
- UINT16 Gen3SwEqJitterErrorTarget

  Offset 0x05B4 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.

- UINT16 Gen3SwEqVocDwellTime

  Offset 0x05B6 - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.
- UINT16 Gen3SwEqVocErrorTarget

  Offset 0x05B8 - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.
- UINT8 PanelPowerEnable

  Offset 0x05BA - Panel Power Enable Control for enabling/disabling VDD force bit (Required only for early enabling of eDP panel).
- UINT8 BdatTestType

  Offset 0x05BB - BdatTestType Indicates the type of Memory Training data to populate into the BDAT ACPI table.
- UINT8 VtdDisable

  Offset 0x05BC - Disable VT-d 0=Enable/FALSE(VT-d enabled), 1=Disable/TRUE (VT-d disabled) $EN_DIS.
- UINT8 UnusedUpdSpace9

  Offset 0x05BD.
- UINT16 DeltaT12PowerCycleDelayPreMem

  Offset 0x05BE - Delta T12 Power Cycle Delay required in ms Select the value for delay required.
- UINT8 OemT12DelayOverride

  Offset 0x05C0 - Oem T12 Dealy Override Oem T12 Dealy Override.
- UINT8 DmaControlGuarantee

  Offset 0x05C1 - State of DMA_CONTROL_GUARANTEE bit in the DMAR table 0=Disable/Clear, 1=Enable/Set $↩ EN_DIS.
- UINT8 SaPreMemTestRsvd [8]

  Offset 0x05C2 - SaPreMemTestRsvd Reserved for SA Pre-Mem Test $EN_DIS.
- UINT16 TotalFlashSize

  Offset 0x05CA - TotalFlashSize Enable/Disable.
- UINT16 BiosSize

  Offset 0x05CC - BiosSize Enable/Disable.
- UINT8 TxtAcheckRequest

  Offset 0x05CE - TxtAcheckRequest Enable/Disable.
- UINT8 SecurityTestRsvd [3]

  Offset 0x05CF - SecurityTestRsvd Reserved for SA Pre-Mem Test $EN_DIS.
- UINT8 SmbusDynamicPowerGating

  Offset 0x05D2 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.
- UINT8 WdtDisableAndLock

  Offset 0x05D3 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.
- UINT8 SmbusSpdWriteDisable

  Offset 0x05D4 - SMBUS SPD Write Disable Set/Clear Smbus SPD Write Disable.
- UINT8 PerCoreRatioOverride

  Offset 0x05D5 - Per Core Max Ratio override Enable or disable Per Core PState OC supported by writing OCMB 0x1D to program new favored core ratio to each Core.
- UINT8 PerCoreRatio [10]

  Offset 0x05D6 - Per Core Current Max Ratio Array for the Per Core Max Ratio.
- UINT8 ReservedPchPreMemTest [5]

  Offset 0x05E0 - ReservedPchPreMemTest Reserved for Pch Pre-Mem Test $EN_DIS.
- UINT8 DidInitStat

  Offset 0x05E5 - Force ME DID Init Status Test, 0: disable, 1: Success, 2: No Memory in Channels, 3: Memory Init Error, Set ME DID init stat value $EN_DIS.
- UINT8 DisableCpuReplacedPolling

  Offset 0x05E6 - CPU Replaced Polling Disable Test, 0: disable, 1: enable, Setting this option disables CPU replacement polling loop $EN_DIS.
- UINT8 SendDidMsg

  Offset 0x05E7 - ME DID Message Test, 0: disable, 1: enable, Enable/Disable ME DID Message (disable will prevent the DID message from being sent) $EN_DIS.

- UINT8 DisableMessageCheck

    Offset 0x05E8 - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.
- UINT8 SkipMbpHob

    Offset 0x05E9 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.
- UINT8 HeciCommunication2

    Offset 0x05EA - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.
- UINT8 KtDeviceEnable

    Offset 0x05EB - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.
- UINT8 tRd2RdSG

    Offset 0x05EC - tRd2RdSG Delay between Read-to-Read commands in the same Bank Group.
- UINT8 tRd2RdDG

    Offset 0x05ED - tRd2RdDG Delay between Read-to-Read commands in different Bank Group for DDR4.
- UINT8 tRd2RdDR

    Offset 0x05EE - tRd2RdDR Delay between Read-to-Read commands in different Ranks.
- UINT8 tRd2RdDD

    Offset 0x05EF - tRd2RdDD Delay between Read-to-Read commands in different DIMMs.
- UINT8 tWr2RdSG

    Offset 0x05F0 - tWr2RdSG Delay between Write-to-Read commands in the same Bank Group.
- UINT8 tWr2RdDG

    Offset 0x05F1 - tWr2RdDG Delay between Write-to-Read commands in different Bank Group for DDR4.
- UINT8 tWr2RdDR

    Offset 0x05F2 - tWr2RdDR Delay between Write-to-Read commands in different Ranks.
- UINT8 tWr2RdDD

    Offset 0x05F3 - tWr2RdDD Delay between Write-to-Read commands in different DIMMs.
- UINT8 tWr2WrSG

    Offset 0x05F4 - tWr2WrSG Delay between Write-to-Write commands in the same Bank Group.
- UINT8 tWr2WrDG

    Offset 0x05F5 - tWr2WrDG Delay between Write-to-Write commands in different Bank Group for DDR4.
- UINT8 tWr2WrDR

    Offset 0x05F6 - tWr2WrDR Delay between Write-to-Write commands in different Ranks.
- UINT8 tWr2WrDD

    Offset 0x05F7 - tWr2WrDD Delay between Write-to-Write commands in different DIMMs.
- UINT8 tRd2WrSG

    Offset 0x05F8 - tRd2WrSG Delay between Read-to-Write commands in the same Bank Group.
- UINT8 tRd2WrDG

    Offset 0x05F9 - tRd2WrDG Delay between Read-to-Write commands in different Bank Group for DDR4.
- UINT8 tRd2WrDR

    Offset 0x05FA - tRd2WrDR Delay between Read-to-Write commands in different Ranks.
- UINT8 tRd2WrDD

    Offset 0x05FB - tRd2WrDD Delay between Read-to-Write commands in different DIMMs.
- UINT8 tRRD_L

    Offset 0x05FC - tRRD_L Min Row Active to Row Active Delay Time for Same Bank Group, DDR4 Only.
- UINT8 tRRD_S

    Offset 0x05FD - tRRD_S Min Row Active to Row Active Delay Time for Different Bank Group, DDR4 Only.
- UINT8 tWTR_L

    Offset 0x05FE - tWTR_L Min Internal Write to Read Command Delay Time for Same Bank Group, DDR4 Only.
- UINT8 tWTR_S

    Offset 0x05FF - tWTR_S Min Internal Write to Read Command Delay Time for Different Bank Group, DDR4 Only.
- UINT8 SkipCpuReplacementCheck

Offset 0x0600 - Skip CPU replacement check Test, 0: disable, 1: enable, Setting this option to skip CPU replacement check $EN_DIS.

- UINT8 PcieRpHotPlug [24]

  Offset 0x0601 - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.

- UINT8 ReservedFspmTestUpd [7]

  Offset 0x0619.

13.35.1 Detailed Description

Fsp M Test Configuration.

Definition at line 2579 of file FspmUpd.h.

13.35.2 Member Data Documentation

13.35.2.1 BdatEnable

`UINT8 FSP_M_TEST_CONFIG::BdatEnable`

Offset 0x055D - Generate BIOS Data ACPI Table Enable: Generate BDAT for MRC RMT or SA PCIe data.

Disable (Default): Do not generate it $EN_DIS

Definition at line 2596 of file FspmUpd.h.

13.35.2.2 BdatTestType

`UINT8 FSP_M_TEST_CONFIG::BdatTestType`

Offset 0x05BB - BdatTestType Indicates the type of Memory Training data to populate into the BDAT ACPI table.

0:Rank Margin Tool, 1:Margin2D

Definition at line 2832 of file FspmUpd.h.

13.35.2.3 BiosSize

`UINT16 FSP_M_TEST_CONFIG::BiosSize`

Offset 0x05CC - BiosSize Enable/Disable.

0: Disable, define default value of BiosSize , 1: enable

Definition at line 2877 of file FspmUpd.h.

13.35.2.4 DeltaT12PowerCycleDelayPreMem

```
UINT16 FSP_M_TEST_CONFIG::DeltaT12PowerCycleDelayPreMem
```

Offset 0x05BE - Delta T12 Power Cycle Delay required in ms Select the value for delay required.

0(Default)= No delay, 0xFFFF = Auto calculate T12 Delay to max 500ms 0 : No Delay, 0xFFFF : Auto Calulate T12 Delay

Definition at line 2849 of file FspmUpd.h.

13.35.2.5 DisableMessageCheck

```
UINT8 FSP_M_TEST_CONFIG::DisableMessageCheck
```

Offset 0x05E8 - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.

$EN_DIS

Definition at line 2952 of file FspmUpd.h.

13.35.2.6 DmiGen3EqPh2Enable

```
UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh2Enable
```

Offset 0x0561 - DMI Equalization Phase 2 DMI Equalization Phase 2.

(0x0): Disable phase 2, (0x1): Enable phase 2, (0x2)(Default): AUTO - Use the current default method 0:Disable phase2, 1:Enable phase2, 2:Auto

Definition at line 2623 of file FspmUpd.h.

13.35.2.7 DmiGen3EqPh3Method

```
UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh3Method
```

Offset 0x0562 - DMI Gen3 Equalization Phase3 DMI Gen3 Equalization Phase3.

Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, Sw↩Eq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2633 of file FspmUpd.h.

13.35.2.8 Gen3SwEqAlwaysAttempt

```
UINT8 FSP_M_TEST_CONFIG::Gen3SwEqAlwaysAttempt
```

Offset 0x056C - PEG Gen3 SwEq Always Attempt Gen3 Software Equalization will be executed every boot.

Disabled(0x0)(Default): Reuse EQ settings saved/restored from NVRAM whenever possible, Enabled(0x1): Re-test and generate new EQ values every boot, not recommended 0:Disable, 1:Enable

Definition at line 2716 of file FspmUpd.h.

13.35.2.9 Gen3SwEqEnableVocTest

```
UINT8 FSP_M_TEST_CONFIG::Gen3SwEqEnableVocTest
```

Offset 0x056E - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.

Disabled(0x0): Disable VOC Test, Enabled(0x1): Enable VOC Test, Auto(0x2)(Default): Use the current default 0:Disable, 1:Enable, 2:Auto

Definition at line 2734 of file FspmUpd.h.

13.35.2.10 Gen3SwEqJitterDwellTime

```
UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterDwellTime
```

Offset 0x05B2 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.

Warning

Do not change from the default

Definition at line 2804 of file FspmUpd.h.

13.35.2.11 Gen3SwEqJitterErrorTarget

```
UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterErrorTarget
```

Offset 0x05B4 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.

Warning

Do not change from the default

Definition at line 2809 of file FspmUpd.h.

13.35.2.12 Gen3SwEqNumberOfPresets

```
UINT8 FSP_M_TEST_CONFIG::Gen3SwEqNumberOfPresets
```

Offset 0x056D - Select number of TxEq presets to test in the PCIe/DMI SwEq Select number of TxEq presets to test in the PCIe/DMI SwEq.

P7,P3,P5(0x0): Test Presets 7, 3, and 5, P0-P9(0x1): Test Presets 0-9, Auto(0x2)(Default): Use the current default method (Default)Auto will test Presets 7, 3, and 5. It is possible for this default to change over time;using Auto will ensure Reference Code always uses the latest default settings 0:P7 P3 P5, 1:P0 to P9, 2:Auto

Definition at line 2726 of file FspmUpd.h.

13.35.2.13 Gen3SwEqVocDwellTime

```
UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocDwellTime
```

Offset 0x05B6 - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.

Warning

Do not change from the default

Definition at line 2814 of file FspmUpd.h.

13.35.2.14 Gen3SwEqVocErrorTarget

```
UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocErrorTarget
```

Offset 0x05B8 - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.

Warning

Do not change from the default

Definition at line 2819 of file FspmUpd.h.

13.35.2.15 HeciCommunication2

```
UINT8 FSP_M_TEST_CONFIG::HeciCommunication2
```

Offset 0x05EA - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.

$EN_DIS

Definition at line 2964 of file FspmUpd.h.

13.35.2.16 KtDeviceEnable

```
UINT8 FSP_M_TEST_CONFIG::KtDeviceEnable
```

Offset 0x05EB - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

$EN_DIS

Definition at line 2970 of file FspmUpd.h.

13.35.2.17 LockPTMregs

```
UINT8 FSP_M_TEST_CONFIG::LockPTMregs
```

Offset 0x055F - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.

Enable(Default)=1, Disable=0 $EN_DIS

Definition at line 2609 of file FspmUpd.h.

13.35.2.18 OemT12DelayOverride

```
UINT8 FSP_M_TEST_CONFIG::OemT12DelayOverride
```

Offset 0x05C0 - Oem T12 Dealy Override Oem T12 Dealy Override.

0(Default)=Disable 1=Enable $EN_DIS

Definition at line 2855 of file FspmUpd.h.

13.35.2.19 PanelPowerEnable

```
UINT8 FSP_M_TEST_CONFIG::PanelPowerEnable
```

Offset 0x05BA - Panel Power Enable Control for enabling/disabling VDD force bit (Required only for early enabling of eDP panel).

0=Disable, 1(Default)=Enable $EN_DIS

Definition at line 2826 of file FspmUpd.h.

13.35.2.20 Peg0Gen3EqPh2Enable

```
UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh2Enable
```

Offset 0x0563 - Phase2 EQ enable on the PEG 0:1:0.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2640 of file FspmUpd.h.

13.35.2.21 Peg0Gen3EqPh3Method

```
UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh3Method
```

Offset 0x0567 - Phase3 EQ method on the PEG 0:1:0.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2671 of file FspmUpd.h.

13.35.2.22 Peg1Gen3EqPh2Enable

```
UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh2Enable
```

Offset 0x0564 - Phase2 EQ enable on the PEG 0:1:1.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2647 of file FspmUpd.h.

13.35.2.23 Peg1Gen3EqPh3Method

```
UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh3Method
```

Offset 0x0568 - Phase3 EQ method on the PEG 0:1:1.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2681 of file FspmUpd.h.

13.35.2.24 Peg2Gen3EqPh2Enable

```
UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh2Enable
```

Offset 0x0565 - Phase2 EQ enable on the PEG 0:1:2.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2654 of file FspmUpd.h.

13.35.2.25 Peg2Gen3EqPh3Method

```
UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh3Method
```

Offset 0x0569 - Phase3 EQ method on the PEG 0:1:2.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2691 of file FspmUpd.h.

13.35.2.26 Peg3Gen3EqPh2Enable

```
UINT8 FSP_M_TEST_CONFIG::Peg3Gen3EqPh2Enable
```

Offset 0x0566 - Phase2 EQ enable on the PEG 0:1:3.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2661 of file FspmUpd.h.

13.35.2.27 Peg3Gen3EqPh3Method

```
UINT8 FSP_M_TEST_CONFIG::Peg3Gen3EqPh3Method
```

Offset 0x056A - Phase3 EQ method on the PEG 0:1:3.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2701 of file FspmUpd.h.

13.35.2.28 PegGen3EndPointHint

```
UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointHint[20]
```

Offset 0x059D - PEG Gen3 End port Hint values per lane Used for programming PEG Gen3 Hint values per lane.

Range: 0-6, 2 is default for each lane

Definition at line 2795 of file FspmUpd.h.

13.35.2.29 PegGen3EndPointPreset

```
UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointPreset[20]
```

Offset 0x0589 - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.

Range: 0-9, 7 is default for each lane

Definition at line 2790 of file FspmUpd.h.

13.35.2.30 PegGen3ProgramStaticEq

```
UINT8 FSP_M_TEST_CONFIG::PegGen3ProgramStaticEq
```

Offset 0x056B - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program PEG Gen3 EQ Phase1 Static Presets.

Disabled(0x0): Disable EQ Phase1 Static Presets Programming, Enabled(0x1)(Default): Enable EQ Phase1 Static Presets Programming $EN_DIS

Definition at line 2708 of file FspmUpd.h.

13.35.2.31 PegGen3RootPortPreset

```
UINT8 FSP_M_TEST_CONFIG::PegGen3RootPortPreset[20]
```

Offset 0x0575 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.

Range: 0-9, 8 is default for each lane

Definition at line 2785 of file FspmUpd.h.

13.35.2.32 PegGenerateBdatMarginTable

```
UINT8 FSP_M_TEST_CONFIG::PegGenerateBdatMarginTable
```

Offset 0x0571 - Generate PCIe BDAT Margin Table Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

Disabled(0x0)(Default): Normal Operation - Disable PCIe BDAT margin data generation, Enable(0x1): Generate PCIe BDAT margin data $EN_DIS

Definition at line 2755 of file FspmUpd.h.

13.35.2.33 PegRxCemLoopbackLane

```
UINT8 FSP_M_TEST_CONFIG::PegRxCemLoopbackLane
```

Offset 0x0570 - PCIe Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specificied Lane (0 - 15) will be used for RxCEMLoopback.

Default is Lane 0

Definition at line 2747 of file FspmUpd.h.

13.35.2.34 PegRxCemNonProtocolAwareness

```
UINT8 FSP_M_TEST_CONFIG::PegRxCemNonProtocolAwareness
```

Offset 0x0572 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

Disabled(0x0)(Default): Normal Operation - Disable non-protocol awareness, Enable(0x1): Non-Protocol Awareness Enabled - Enable non-protocol awareness for compliance testing $EN_DIS

Definition at line 2764 of file FspmUpd.h.

13.35.2.35 PerCoreRatioOverride

```
UINT8 FSP_M_TEST_CONFIG::PerCoreRatioOverride
```

Offset 0x05D5 - Per Core Max Ratio override Enable or disable Per Core PState OC supported by writing OCMB 0x1D to program new favored core ratio to each Core.

0: Disable, 1: enable $EN_DIS

Definition at line 2915 of file FspmUpd.h.

13.35.2.36 ScanExtGfxForLegacyOpRom

```
UINT8 FSP_M_TEST_CONFIG::ScanExtGfxForLegacyOpRom
```

Offset 0x055E - Detect External Graphics device for LegacyOpROM Detect and report if external graphics device only support LegacyOpROM or not (to support CSM auto-enable).

Enable(Default)=1, Disable=0 $EN_DIS

Definition at line 2603 of file FspmUpd.h.

13.35.2.37 SkipMbpHob

```
UINT8 FSP_M_TEST_CONFIG::SkipMbpHob
```

Offset 0x05E9 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.

$EN_DIS

Definition at line 2958 of file FspmUpd.h.

13.35.2.38 SmbusDynamicPowerGating

```
UINT8 FSP_M_TEST_CONFIG::SmbusDynamicPowerGating
```

Offset 0x05D2 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.

$EN_DIS

Definition at line 2895 of file FspmUpd.h.

13.35.2.39 SmbusSpdWriteDisable

```
UINT8 FSP_M_TEST_CONFIG::SmbusSpdWriteDisable
```

Offset 0x05D4 - SMBUS SPD Write Disable Set/Clear Smbus SPD Write Disable.

0: leave SPD Write Disable bit; 1: set SPD Write Disable bit. For security recommendations, SPD write disable bit must be set. $EN_DIS

Definition at line 2908 of file FspmUpd.h.

13.35.2.40 TotalFlashSize

```
UINT16 FSP_M_TEST_CONFIG::TotalFlashSize
```

Offset 0x05CA - TotalFlashSize Enable/Disable.

0: Disable, define default value of TotalFlashSize , 1: enable

Definition at line 2872 of file FspmUpd.h.

13.35.2.41 tRd2RdDD

```
UINT8 FSP_M_TEST_CONFIG::tRd2RdDD
```

Offset 0x05EF - tRd2RdDD Delay between Read-to-Read commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 2991 of file FspmUpd.h.

13.35.2.42 tRd2RdDG

```
UINT8 FSP_M_TEST_CONFIG::tRd2RdDG
```

Offset 0x05ED - tRd2RdDG Delay between Read-to-Read commands in different Bank Group for DDR4.

All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Definition at line 2981 of file FspmUpd.h.

13.35.2.43 tRd2RdDR

```
UINT8 FSP_M_TEST_CONFIG::tRd2RdDR
```

Offset 0x05EE - tRd2RdDR Delay between Read-to-Read commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 2986 of file FspmUpd.h.

13.35.2.44 tRd2RdSG

```
UINT8 FSP_M_TEST_CONFIG::tRd2RdSG
```

Offset 0x05EC - tRd2RdSG Delay between Read-to-Read commands in the same Bank Group.

0-Auto, Range 4-54.

Definition at line 2975 of file FspmUpd.h.

13.35.2.45 tRd2WrDD

```
UINT8 FSP_M_TEST_CONFIG::tRd2WrDD
```

Offset 0x05FB - tRd2WrDD Delay between Read-to-Write commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3054 of file FspmUpd.h.

13.35.2.46 tRd2WrDG

```
UINT8 FSP_M_TEST_CONFIG::tRd2WrDG
```

Offset 0x05F9 - tRd2WrDG Delay between Read-to-Write commands in different Bank Group for DDR4.

All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Definition at line 3044 of file FspmUpd.h.

13.35.2.47 tRd2WrDR

```
UINT8 FSP_M_TEST_CONFIG::tRd2WrDR
```

Offset 0x05FA - tRd2WrDR Delay between Read-to-Write commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3049 of file FspmUpd.h.

13.35.2.48 tRd2WrSG

```
UINT8 FSP_M_TEST_CONFIG::tRd2WrSG
```

Offset 0x05F8 - tRd2WrSG Delay between Read-to-Write commands in the same Bank Group.

0-Auto, Range 4-54.

Definition at line 3038 of file FspmUpd.h.

13.35.2.49 tRRD_L

```
UINT8 FSP_M_TEST_CONFIG::tRRD_L
```

Offset 0x05FC - tRRD_L Min Row Active to Row Active Delay Time for Same Bank Group, DDR4 Only.

0: AUTO, max: 31

Definition at line 3059 of file FspmUpd.h.

13.35.2.50 tRRD_S

```
UINT8 FSP_M_TEST_CONFIG::tRRD_S
```

Offset 0x05FD - tRRD_S Min Row Active to Row Active Delay Time for Different Bank Group, DDR4 Only.

0: AUTO, max: 31

Definition at line 3065 of file FspmUpd.h.

13.35.2.51 tWr2RdDD

```
UINT8 FSP_M_TEST_CONFIG::tWr2RdDD
```

Offset 0x05F3 - tWr2RdDD Delay between Write-to-Read commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3012 of file FspmUpd.h.

13.35.2.52 tWr2RdDG

```
UINT8 FSP_M_TEST_CONFIG::tWr2RdDG
```

Offset 0x05F1 - tWr2RdDG Delay between Write-to-Read commands in different Bank Group for DDR4.

All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Definition at line 3002 of file FspmUpd.h.

13.35.2.53 tWr2RdDR

```
UINT8 FSP_M_TEST_CONFIG::tWr2RdDR
```

Offset 0x05F2 - tWr2RdDR Delay between Write-to-Read commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3007 of file FspmUpd.h.

13.35.2.54 tWr2RdSG

```
UINT8 FSP_M_TEST_CONFIG::tWr2RdSG
```

Offset 0x05F0 - tWr2RdSG Delay between Write-to-Read commands in the same Bank Group.

0-Auto, Range 4-86.

Definition at line 2996 of file FspmUpd.h.

13.35.2.55 tWr2WrDD

```
UINT8 FSP_M_TEST_CONFIG::tWr2WrDD
```

Offset 0x05F7 - tWr2WrDD Delay between Write-to-Write commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3033 of file FspmUpd.h.

13.35.2.56 tWr2WrDG

```
UINT8 FSP_M_TEST_CONFIG::tWr2WrDG
```

Offset 0x05F5 - tWr2WrDG Delay between Write-to-Write commands in different Bank Group for DDR4.

All other DDR technologies should set this equal to SG. 0-Auto, Range 4-54.

Definition at line 3023 of file FspmUpd.h.

13.35.2.57 tWr2WrDR

```
UINT8 FSP_M_TEST_CONFIG::tWr2WrDR
```

Offset 0x05F6 - tWr2WrDR Delay between Write-to-Write commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3028 of file FspmUpd.h.

13.35.2.58 tWr2WrSG

```
UINT8 FSP_M_TEST_CONFIG::tWr2WrSG
```

Offset 0x05F4 - tWr2WrSG Delay between Write-to-Write commands in the same Bank Group.

0-Auto, Range 4-54.

Definition at line 3017 of file FspmUpd.h.

13.35.2.59 tWTR_L

```
UINT8 FSP_M_TEST_CONFIG::tWTR_L
```

Offset 0x05FE - tWTR_L Min Internal Write to Read Command Delay Time for Same Bank Group, DDR4 Only.

0: AUTO, max: 60

Definition at line 3071 of file FspmUpd.h.

13.35.2.60 tWTR_S

```
UINT8 FSP_M_TEST_CONFIG::tWTR_S
```

Offset 0x05FF - tWTR_S Min Internal Write to Read Command Delay Time for Different Bank Group, DDR4 Only.

0: AUTO, max: 28

Definition at line 3077 of file FspmUpd.h.

13.35.2.61 TxtAcheckRequest

```
UINT8 FSP_M_TEST_CONFIG::TxtAcheckRequest
```

Offset 0x05CE - TxtAcheckRequest Enable/Disable.

When Enabled, it will forcing calling TXT Acheck once. $EN_DIS

Definition at line 2883 of file FspmUpd.h.

13.35.2.62 WdtDisableAndLock

```
UINT8 FSP_M_TEST_CONFIG::WdtDisableAndLock
```

Offset 0x05D3 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.

$EN_DIS

Definition at line 2901 of file FspmUpd.h.

The documentation for this struct was generated from the following file:

- FspmUpd.h

13.36 FSP_S_CONFIG Struct Reference

Fsp S Configuration.

```
#include <FspsUpd.h>
```

Public Attributes

- UINT32 LogoPtr

  Offset 0x0020 - Logo Pointer Points to PEI Display Logo Image.
- UINT32 LogoSize

  Offset 0x0024 - Logo Size Size of PEI Display Logo Image.
- UINT32 GraphicsConfigPtr

  Offset 0x0028 - Graphics Configuration Ptr Points to VBT.
- UINT8 Device4Enable

  Offset 0x002C - Enable Device 4 Enable/disable Device 4 $EN_DIS.
- UINT8 UnusedUpdSpace0 [3]

  Offset 0x002D.
- UINT32 MicrocodeRegionBase

  Offset 0x0030 - MicrocodeRegionBase Memory Base of Microcode Updates.
- UINT32 MicrocodeRegionSize

  Offset 0x0034 - MicrocodeRegionSize Size of Microcode Updates.
- UINT8 TurboMode

  Offset 0x0038 - Turbo Mode Enable/Disable Turbo mode.
- UINT8 PchDmiCwbEnable

  Offset 0x0039 - PchDmiCwbEnable Central Write Buffer feature configurable and disabled by default $EN_DIS.
- UINT8 Heci3Enabled

  Offset 0x003A - HECI3 state The HECI3 state from Mbp for reference in S3 path or when MbpHob is not installed.
- UINT8 Heci1Disabled

  Offset 0x003B - HECI1 state Determine if HECI1 is hidden prior to boot to OS.
- UINT8 AmtEnabled

  Offset 0x003C - AMT Switch Enable/Disable.
- UINT8 WatchDogEnabled

  Offset 0x003D - WatchDog Timer Switch Enable/Disable.
- UINT8 ManageabilityMode

  Offset 0x003E - Manageability Mode set by Mebx Enable/Disable.
- UINT8 FwProgress

  Offset 0x003F - PET Progress Enable/Disable.
- UINT8 AmtSolEnabled

  Offset 0x0040 - SOL Switch Enable/Disable.
- UINT8 UnusedUpdSpace1

  Offset 0x0041.
- UINT16 WatchDogTimerOs

  Offset 0x0042 - OS Timer 16 bits Value, Set OS watchdog timer.
- UINT16 WatchDogTimerBios

  Offset 0x0044 - BIOS Timer 16 bits Value, Set BIOS watchdog timer.
- UINT8 RemoteAssistance

  Offset 0x0046 - Remote Assistance Trigger Availablilty Enable/Disable.
- UINT8 AmtKvmEnabled

  Offset 0x0047 - KVM Switch Enable/Disable.
- UINT8 ForcMebxSyncUp

  Offset 0x0048 - MEBX execution Enable/Disable.
- UINT8 CridEnable

  Offset 0x0049 - Enable/Disable SA CRID Enable: SA CRID, Disable (Default): SA CRID $EN_DIS.
- UINT8 DmiAspm

  Offset 0x004A - DMI ASPM 0=Disable, 1:L0s, 2:L1, 3(Default)=L0sL1 0:Disable, 1:L0s, 2:L1, 3:L0sL1.
- UINT8 PegDeEmphasis [4]

Offset 0x004B - PCIe DeEmphasis control per root port 0: -6dB, 1(Default): -3.5dB 0:-6dB, 1:-3.5dB.

- UINT8 PegSlotPowerLimitValue [4]

  Offset 0x004F - PCIe Slot Power Limit value per root port Slot power limit value per root port.
- UINT8 PegSlotPowerLimitScale [4]

  Offset 0x0053 - PCIe Slot Power Limit scale per root port Slot power limit scale per root port 0:1.0x, 1:0.1x, 2:0.01x, 3:0x001x.
- UINT8 UnusedUpdSpace2 [1]

  Offset 0x0057.
- UINT16 PegPhysicalSlotNumber [4]

  Offset 0x0058 - PCIe Physical Slot Number per root port Physical Slot Number per root port.
- UINT8 PavpEnable

  Offset 0x0060 - Enable/Disable PavpEnable Enable(Default): Enable PavpEnable, Disable: Disable PavpEnable $↩ EN_DIS.
- UINT8 CdClock

  Offset 0x0061 - CdClock Frequency selection 0=337.5 Mhz, 1=450 Mhz, 2=540 Mhz, 3(Default)=675 Mhz 0: 337.5 Mhz, 1: 450 Mhz, 2: 540 Mhz, 3: 675 Mhz.
- UINT8 PeiGraphicsPeimInit

  Offset 0x0062 - Enable/Disable PeiGraphicsPeimInit Enable: Enable PeiGraphicsPeimInit, Disable(Default): Disable PeiGraphicsPeimInit $EN_DIS.
- UINT8 GnaEnable

  Offset 0x0063 - Enable or disable GNA device 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 X2ApicOptOutDeprecated

  Offset 0x0064 - State of X2APIC_OPT_OUT bit in the DMAR table 0=Disable/Clear, 1=Enable/Set $EN_DIS.
- UINT8 UnusedUpdSpace3 [3]

  Offset 0x0065.
- UINT32 VtdBaseAddressDeprecated [3]

  Offset 0x0068 - Base addresses for VT-d function MMIO access Base addresses for VT-d MMIO access per VT-d engine.
- UINT8 DdiPortEdp

  Offset 0x0074 - Enable or disable eDP device 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortBHpd

  Offset 0x0075 - Enable or disable HPD of DDI port B 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortCHpd

  Offset 0x0076 - Enable or disable HPD of DDI port C 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortDHpd

  Offset 0x0077 - Enable or disable HPD of DDI port D 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortFHpd

  Offset 0x0078 - Enable or disable HPD of DDI port F 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortBDdc

  Offset 0x0079 - Enable or disable DDC of DDI port B 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortCDdc

  Offset 0x007A - Enable or disable DDC of DDI port C 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortDDdc

  Offset 0x007B - Enable or disable DDC of DDI port D 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DdiPortFDdc

  Offset 0x007C - Enable or disable DDC of DDI port F 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 SkipS3CdClockInit

  Offset 0x007D - Enable/Disable SkipS3CdClockInit Enable: Skip Full CD clock initializaton, Disable(Default): Initialize the full CD clock in S3 resume due to GOP absent $EN_DIS.
- UINT16 DeltaT12PowerCycleDelay

  Offset 0x007E - Delta T12 Power Cycle Delay required in ms DEPRECATED 0 : No Delay, 0xFFFF : Auto Calulate T12 Delay.

- UINT32 BltBufferAddress

  Offset 0x0080 - Blt Buffer Address Address of Blt buffer.

- UINT32 BltBufferSize

  Offset 0x0084 - Blt Buffer Size Size of Blt Buffer, is equal to PixelWidth ∗ PixelHeight ∗ 4 bytes (the size of EFI_G←RAPHICS_OUTPUT_BLT_PIXEL)

- UINT8 ProgramGtChickenBits

  Offset 0x0088 - Program GT Chicken bits Progarm the GT chicken bits in GTTMMADR + 0xD00 BITS [3:1].

- UINT8 SaPostMemProductionRsvd [34]

  Offset 0x0089 - SaPostMemProductionRsvd Reserved for SA Post-Mem Production $EN_DIS.

- UINT8 PcieRootPortGen2PllL1CgDisable [24]

  Offset 0x00AB - PCIE RP Disable Gen2PLL Shutdown and L1 Clock Gating Enable PCIE RP Disable Gen2PLL Shutdown and L1 Clock Gating Enable Workaround needed for Alpine ridge.

- UINT8 AesEnable

  Offset 0x00C3 - Advanced Encryption Standard (AES) feature Enable or Disable Advanced Encryption Standard (AES) feature; 0: Disable; ***1: Enable $EN_DIS.***

- UINT8 Psi3Enable [5]

  Offset 0x00C4 - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; ***1: Enable****.*

- UINT8 Psi4Enable [5]

  Offset 0x00C9 - Power State 4 enable/disable PCODE MMIO Mailbox: Power State 4 enable/disable; 0: Disable; ***1: Enable****.For all VR Indexes.*

- UINT8 ImonSlope [5]

  Offset 0x00CE - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.

- UINT8 ImonOffset [5]

  Offset 0x00D3 - Imon offset correction DEPRECATED.

- UINT8 VrConfigEnable [5]

  Offset 0x00D8 - Enable/Disable BIOS configuration of VR Enable/Disable BIOS configuration of VR; ***0: Disable****; 1: Enable.For all VR Indexes.*

- UINT8 TdcEnable [5]

  Offset 0x00DD - Thermal Design Current enable/disable PCODE MMIO Mailbox: Thermal Design Current enable/disable; ***0: Disable****; 1: Enable.For all VR Indexes.*

- UINT8 TdcTimeWindow [5]

  Offset 0x00E2 - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.

- UINT8 TdcLock [5]

  Offset 0x00E7 - Thermal Design Current Lock PCODE MMIO Mailbox: Thermal Design Current Lock; ***0: Disable****; 1: Enable.For all VR Indexes.*

- UINT8 PsysSlope

  Offset 0x00EC - Platform Psys slope correction PCODE MMIO Mailbox: Platform Psys slope correction.

- UINT8 PsysOffset

  Offset 0x00ED - Platform Psys offset correction PCODE MMIO Mailbox: Platform Psys offset correction.

- UINT8 AcousticNoiseMitigation

  Offset 0x00EE - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.

- UINT8 FastPkgCRampDisableIa

  Offset 0x00EF - Disable Fast Slew Rate for Deep Package C States for VR IA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

- UINT8 SlowSlewRateForIa

  Offset 0x00F0 - Slew Rate configuration for Deep Package C States for VR IA domain Slew Rate configuration for Deep Package C States for VR IA domain based on Acoustic Noise Mitigation feature enabled.

- UINT8 SlowSlewRateForGt

  Offset 0x00F1 - Slew Rate configuration for Deep Package C States for VR GT domain Slew Rate configuration for Deep Package C States for VR GT domain based on Acoustic Noise Mitigation feature enabled.

- UINT8 SlowSlewRateForSa

Offset 0x00F2 - Slew Rate configuration for Deep Package C States for VR SA domain Slew Rate configuration for Deep Package C States for VR SA domain based on Acoustic Noise Mitigation feature enabled.

- UINT8 UnusedUpdSpace4 [1]

  Offset 0x00F3.
- UINT16 TdcPowerLimit [5]

  Offset 0x00F4 - Thermal Design Current current limit PCODE MMIO Mailbox: Thermal Design Current current limit.
- UINT16 AcLoadline [5]

  Offset 0x00FE - AcLoadline PCODE MMIO Mailbox: AcLoadline in 1/100 mOhms (ie.
- UINT16 DcLoadline [5]

  Offset 0x0108 - DcLoadline PCODE MMIO Mailbox: DcLoadline in 1/100 mOhms (ie.
- UINT16 Psi1Threshold [5]

  Offset 0x0112 - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cuttof in 1/4 Amp increments.
- UINT16 Psi2Threshold [5]

  Offset 0x011C - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cuttof in 1/4 Amp increments.
- UINT16 Psi3Threshold [5]

  Offset 0x0126 - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cuttof in 1/4 Amp increments.
- UINT16 IccMax [5]

  Offset 0x0130 - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.
- UINT16 VrVoltageLimit [5]

  Offset 0x013A - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.
- UINT8 FastPkgCRampDisableGt

  Offset 0x0144 - Disable Fast Slew Rate for Deep Package C States for VR GT domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.
- UINT8 FastPkgCRampDisableSa

  Offset 0x0145 - Disable Fast Slew Rate for Deep Package C States for VR SA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.
- UINT8 SendVrMbxCmd

  Offset 0x0146 - Enable VR specific mailbox command VR specific mailbox commands.
- UINT8 Reserved2

  Offset 0x0147 - Reserved Reserved.
- UINT8 TxtEnable

  Offset 0x0148 - Enable or Disable TXT Enable or Disable TXT; 0: Disable; ***1: Enable****.*
- UINT8 SkipMpInitDeprecated

  Offset 0x0149 - Deprecated DO NOT USE Skip Multi-Processor Initialization.
- UINT8 McivrRfiFrequencyPrefix

  Offset 0x014A - McIVR RFI Frequency Prefix PCODE MMIO Mailbox: McIVR RFI Frequency Adjustment Prefix.
- UINT8 McivrRfiFrequencyAdjust

  Offset 0x014B - McIVR RFI Frequency Adjustment PCODE MMIO Mailbox: Adjust the RFI frequency relative to the nominal frequency in increments of 100KHz.
- UINT16 FivrRfiFrequency

  Offset 0x014C - FIVR RFI Frequency PCODE MMIO Mailbox: Set the desired RFI frequency, in increments of 100←KHz.
- UINT8 McivrSpreadSpectrum

  Offset 0x014E - McIVR RFI Spread Spectrum PCODE MMIO Mailbox: McIVR RFI Spread Spectrum.
- UINT8 FivrSpreadSpectrum

  Offset 0x014F - FIVR RFI Spread Spectrum PCODE MMIO Mailbox: FIVR RFI Spread Spectrum, in 0.1% increments.
- UINT8 FastPkgCRampDisableFivr

  Offset 0x0150 - Disable Fast Slew Rate for Deep Package C States for VR FIVR domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.
- UINT8 SlowSlewRateForFivr

Offset 0x0151 - Slew Rate configuration for Deep Package C States for VR FIVR domain Slew Rate configuration for Deep Package C States for VR FIVR domain based on Acoustic Noise Mitigation feature enabled.

- UINT8 UnusedUpdSpace5 [2]

  Offset 0x0152.

- UINT32 CpuBistData

  Offset 0x0154 - CpuBistData Pointer CPU BIST Data.

- UINT8 IslVrCmd

  Offset 0x0158 - Activates VR mailbox command for Intersil VR C-state issues.

- UINT8 UnusedUpdSpace6 [1]

  Offset 0x0159.

- UINT16 ImonSlope1 [5]

  Offset 0x015A - Imon slope1 correction PCODE MMIO Mailbox: Imon slope correction.

- UINT32 VrPowerDeliveryDesign

  Offset 0x0164 - CPU VR Power Delivery Design Used to communicate the power delivery design capability of the board.

- UINT8 PreWake

  Offset 0x0168 - Pre Wake Randomization time PCODE MMIO Mailbox: Acoustic Migitation Range.Defines the maximum pre-wake randomization time in micro ticks.This can be programmed only if AcousticNoiseMigitation is enabled.

- UINT8 RampUp

  Offset 0x0169 - Ramp Up Randomization time PCODE MMIO Mailbox: Acoustic Migitation Range.Defines the maximum Ramp Up randomization time in micro ticks.This can be programmed only if AcousticNoiseMigitation is enabled.Range 0-255 ***0****.*

- UINT8 RampDown

  Offset 0x016A - Ramp Down Randomization time PCODE MMIO Mailbox: Acoustic Migitation Range.Defines the maximum Ramp Down randomization time in micro ticks.This can be programmed only if AcousticNoiseMigitation is enabled.Range 0-255 ***0****.*

- UINT8 UnusedUpdSpace7

  Offset 0x016B.

- UINT32 CpuMpPpi

  Offset 0x016C - CpuMpPpi Pointer for CpuMpPpi.

- UINT32 CpuMpHob

  Offset 0x0170 - CpuMpHob Pointer for CpuMpHob.

- UINT8 DebugInterfaceEnable

  Offset 0x0174 - CPU Run Control Enable, Disable or Do not configure CPU Run Control; 0: Disable; 1: Enable ; ***2: No Change*** *0:Disabled, 1:Enabled, 2:No Change.*

- UINT8 UnusedUpdSpace8 [1]

  Offset 0x0175.

- UINT16 ImonOffset1 [5]

  Offset 0x0176 - Imon offset 1 correction PCODE MMIO Mailbox: Imon offset correction.

- UINT8 ReservedCpuPostMemProduction [8]

  Offset 0x0180 - ReservedCpuPostMemProduction Reserved for CPU Post-Mem Production $EN_DIS.

- UINT8 PchHdaDspEnable

  Offset 0x0188 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

- UINT8 SerialIoSpi0CsPolarity [2]

  Offset 0x0189 - SPI0 Chip Select Polarity Sets polarity for each chip Select.

- UINT8 SerialIoSpi1CsPolarity [2]

  Offset 0x018B - SPI1 Chip Select Polarity Sets polarity for each chip Select.

- UINT8 SerialIoSpi2CsPolarity [2]

  Offset 0x018D - SPI2 Chip Select Polarity Sets polarity for each chip Select.

- UINT8 SerialIoSpi0CsEnable [2]

  Offset 0x018F - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.

- UINT8 SerialIoSpi1CsEnable [2]

Offset 0x0191 - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.

- UINT8 SerialIoSpi2CsEnable [2]

  Offset 0x0193 - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.

- UINT8 SerialIoSpiMode [3]

  Offset 0x0195 - SPIn Device Mode Selects SPI operation mode.

- UINT8 SerialIoSpiDefaultCsOutput [3]

  Offset 0x0198 - SPIn Default Chip Select Output Sets Default CS as Output.

- UINT8 PchSerialIoI2cPadsTermination [6]

  Offset 0x019B - PCH SerialIo I2C Pads Termination 0x0: Hardware default, 0x1: None, 0x13: 1kOhm weak pull-up, 0x15: 5kOhm weak pull-up, 0x19: 20kOhm weak pull-up - Enable/disable SerialIo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5 pads termination respectively.

- UINT8 SerialIoI2cMode [6]

  Offset 0x01A1 - I2Cn Device Mode Selects I2c operation mode.

- UINT8 SerialIoUartMode [3]

  Offset 0x01A7 - UARTn Device Mode Selects Uart operation mode.

- UINT8 UnusedUpdSpace9 [2]

  Offset 0x01AA.

- UINT32 SerialIoUartBaudRate [3]

  Offset 0x01AC - Default BaudRate for each Serial IO UART Set default BaudRate Supported from 0 - default to 6000000.

- UINT8 SerialIoUartParity [3]

  Offset 0x01B8 - Default ParityType for each Serial IO UART Set default Parity.

- UINT8 SerialIoUartDataBits [3]

  Offset 0x01BB - Default DataBits for each Serial IO UART Set default word length.

- UINT8 SerialIoUartStopBits [3]

  Offset 0x01BE - Default StopBits for each Serial IO UART Set default stop bits.

- UINT8 SerialIoUartPowerGating [3]

  Offset 0x01C1 - Power Gating mode for each Serial IO UART that works in COM mode Set Power Gating.

- UINT8 SerialIoUartDmaEnable [3]

  Offset 0x01C4 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.

- UINT8 SerialIoUartAutoFlow [3]

  Offset 0x01C7 - Enables UART hardware flow control, CTS and RTS lines Enables UART hardware flow control, CTS and RTS lines.

- UINT8 SerialIoUartPinMux [3]

  *Offset 0x01CA - Serial IO UART Pin Mux Applies only to UART0 muxed with CNVI **0 = GPIO C8 to C11** 1 = GPIO F5 - F7 (PCH LP) J5 - J7 (PCH H)*

- UINT8 SerialIoDebugUartNumber

  Offset 0x01CD - UART Number For Debug Purpose UART number for debug purpose.

- UINT8 SerialIoUartDbg2 [3]

  *Offset 0x01CE - Serial IO UART DBG2 table Enable or disable Serial Io UART DBG2 table, default is Disable; **0: Disable;** 1: Enable.*

- UINT8 ScsEmmcEnabled

  Offset 0x01D1 - Enable eMMC Controller Enable/disable eMMC Controller.

- UINT8 ScsEmmcHs400Enabled

  Offset 0x01D2 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.

- UINT8 ScsSdCardEnabled

  Offset 0x01D3 - Enable SdCard Controller Enable/disable SD Card Controller.

- UINT8 ShowSpiController

  Offset 0x01D4 - Show SPI controller Enable/disable to show SPI controller.

- UINT8 SataSalpSupport

  Offset 0x01D5 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.

- UINT8 SataPortsEnable [8]

Offset 0x01D6 - Enable SATA ports Enable/disable SATA ports.

- UINT8 SataPortsDevSlp [8]

  Offset 0x01DE - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.
- UINT8 PortUsb20Enable [16]

  Offset 0x01E6 - Enable USB2 ports Enable/disable per USB2 ports.
- UINT8 PortUsb30Enable [10]

  Offset 0x01F6 - Enable USB3 ports Enable/disable per USB3 ports.
- UINT8 XdciEnable

  Offset 0x0200 - Enable xDCI controller Enable/disable to xDCI controller.
- UINT8 UnusedUpdSpace10 [3]

  Offset 0x0201.
- UINT32 DevIntConfigPtr

  Offset 0x0204 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.
- UINT8 NumOfDevIntConfig

  Offset 0x0208 - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.
- UINT8 PxRcConfig [8]

  Offset 0x0209 - PIRQx to IRQx Map Config PIRQx to IRQx mapping.
- UINT8 GpioIrqRoute

  Offset 0x0211 - Select GPIO IRQ Route GPIO IRQ Select.
- UINT8 SciIrqSelect

  Offset 0x0212 - Select SciIrqSelect SCI IRQ Select.
- UINT8 TcoIrqSelect

  Offset 0x0213 - Select TcoIrqSelect TCO IRQ Select.
- UINT8 TcoIrqEnable

  Offset 0x0214 - Enable/Disable Tco IRQ Enable/disable TCO IRQ $EN_DIS.
- UINT8 PchHdaVerbTableEntryNum

  Offset 0x0215 - PCH HDA Verb Table Entry Number Number of Entries in Verb Table.
- UINT8 UnusedUpdSpace11 [2]

  Offset 0x0216.
- UINT32 PchHdaVerbTablePtr

  Offset 0x0218 - PCH HDA Verb Table Pointer Pointer to Array of pointers to Verb Table.
- UINT8 PchHdaCodecSxWakeCapability

  Offset 0x021C - PCH HDA Codec Sx Wake Capability Capability to detect wake initiated by a codec in Sx.
- UINT8 SataEnable

  Offset 0x021D - Enable SATA Enable/disable SATA controller.
- UINT8 SataMode

  Offset 0x021E - SATA Mode Select SATA controller working mode.
- UINT8 Usb2AfePetxiset [16]

  Offset 0x021F - USB Per Port HS Preemphasis Bias USB Per Port HS Preemphasis Bias.
- UINT8 Usb2AfeTxiset [16]

  Offset 0x022F - USB Per Port HS Transmitter Bias USB Per Port HS Transmitter Bias.
- UINT8 Usb2AfePredeemp [16]

  Offset 0x023F - USB Per Port HS Transmitter Emphasis USB Per Port HS Transmitter Emphasis.
- UINT8 Usb2AfePehalfbit [16]

  Offset 0x024F - USB Per Port Half Bit Pre-emphasis USB Per Port Half Bit Pre-emphasis.
- UINT8 Usb3HsioTxDeEmphEnable [10]

  Offset 0x025F - Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment.
- UINT8 Usb3HsioTxDeEmph [10]

  *Offset 0x0269 - USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting, HSIO_TX_DWORD5[21:16], **Default = 29h** (approximately -3.5dB De-Emphasis).*

- UINT8 Usb3HsioTxDownscaleAmpEnable [10]

  Offset 0x0273 - Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment, Each value in arrary can be between 0-1.
- UINT8 Usb3HsioTxDownscaleAmp [10]

  *Offset 0x027D - USB 3.0 TX Output Downscale Amplitude Adjustment USB 3.0 TX Output Downscale Amplitude Adjustment, HSIO_TX_DWORD8[21:16], **Default = 00h**.*
- UINT8 PchUsbLtrOverrideEnable

  Offset 0x0287 - Enable xHCI LTR override Enables override of recommended LTR values for xHCI $EN_DIS.
- UINT32 PchUsbLtrHighIdleTimeOverride

  Offset 0x0288 - xHCI High Idle Time LTR override Value used for overriding LTR recommendation for xHCI High Idle Time LTR setting.
- UINT32 PchUsbLtrMediumIdleTimeOverride

  Offset 0x028C - xHCI Medium Idle Time LTR override Value used for overriding LTR recommendation for xHCI Medium Idle Time LTR setting.
- UINT32 PchUsbLtrLowIdleTimeOverride

  Offset 0x0290 - xHCI Low Idle Time LTR override Value used for overriding LTR recommendation for xHCI Low Idle Time LTR setting.
- UINT8 PchLanEnable

  Offset 0x0294 - Enable LAN Enable/disable LAN controller.
- UINT8 PchHdaAudioLinkHda

  Offset 0x0295 - Enable HD Audio Link Enable/disable HD Audio Link.
- UINT8 PchHdaAudioLinkDmic0

  Offset 0x0296 - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.
- UINT8 PchHdaAudioLinkDmic1

  Offset 0x0297 - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.
- UINT8 PchHdaAudioLinkSsp0

  Offset 0x0298 - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.
- UINT8 PchHdaAudioLinkSsp1

  Offset 0x0299 - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.
- UINT8 PchHdaAudioLinkSsp2

  Offset 0x029A - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.
- UINT8 PchHdaAudioLinkSndw1

  Offset 0x029B - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.
- UINT8 PchHdaAudioLinkSndw2

  Offset 0x029C - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.
- UINT8 PchHdaAudioLinkSndw3

  Offset 0x029D - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.
- UINT8 PchHdaAudioLinkSndw4

  Offset 0x029E - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.
- UINT8 PchHdaSndwBufferRcomp

  Offset 0x029F - Soundwire Clock Buffer GPIO RCOMP Setting 0: non-ACT - 50 Ohm driver impedance, 1: ACT - 8 Ohm driver impedance.
- UINT32 PcieRpPtmMask

  Offset 0x02A0 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.
- UINT32 PcieRpDpcMask

  Offset 0x02A4 - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.
- UINT32 PcieRpDpcExtensionsMask

  Offset 0x02A8 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.
- UINT8 UsbPdoProgramming

  Offset 0x02AC - USB PDO Programming Enable/disable PDO programming for USB in PEI phase.
- UINT8 UnusedUpdSpace12 [3]

  Offset 0x02AD.

- UINT32 PmcPowerButtonDebounce

  Offset 0x02B0 - Power button debounce configuration Debounce time for PWRBTN in microseconds.
- UINT8 PchEspiBmeMasterSlaveEnabled

  Offset 0x02B4 - PCH eSPI Master and Slave BME enabled PCH eSPI Master and Slave BME enabled $EN_DIS.
- UINT8 SataRstLegacyOrom

  Offset 0x02B5 - PCH SATA use RST Legacy OROM Use PCH SATA RST Legacy OROM when CSM is Enabled $EN_DIS.
- UINT8 UnusedUpdSpace13 [2]

  Offset 0x02B6.
- UINT32 TraceHubMemBase

  Offset 0x02B8 - Trace Hub Memory Base If Trace Hub is enabled and trace to memory is desired, BootLoader needs to allocate trace hub memory as reserved and uncacheable, set the base to ensure Trace Hub memory is configured properly.
- UINT8 PmcDbgMsgEn

  Offset 0x02BC - PMC Debug Message Enable When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug meesages to trace hub.
- UINT8 UnusedUpdSpace14 [3]

  Offset 0x02BD.
- UINT32 ChipsetInitBinPtr

  Offset 0x02C0 - Pointer of ChipsetInit Binary ChipsetInit Binary Pointer.
- UINT32 ChipsetInitBinLen

  Offset 0x02C4 - Length of ChipsetInit Binary ChipsetInit Binary Length.
- UINT8 ScsUfsEnabled

  Offset 0x02C8 - Enable Ufs Controller Enable/disable Ufs 2.0 Controller.
- UINT8 CnviMode

  Offset 0x02C9 - CNVi Configuration This option allows for automatic detection of Connectivity Solution.
- UINT8 CnviBtCore

  Offset 0x02CA - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.
- UINT8 CnviBtAudioOffload

  Offset 0x02CB - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.
- UINT8 SdCardPowerEnableActiveHigh

  Offset 0x02CC - SdCard power enable polarity Choose SD_PWREN# polarity 0: Active low, 1: Active high.
- UINT8 PchUsb2PhySusPgEnable

  Offset 0x02CD - PCH USB2 PHY Power Gating enable 1: Will enable USB2 PHY SUS Well Power Gating, 0: Will not enable PG of USB2 PHY Sus Well PG $EN_DIS.
- UINT8 PchUsbOverCurrentEnable

  Offset 0x02CE - PCH USB OverCurrent mapping enable 1: Will program USB OC pin mapping in xHCI controller memory, 0: Will clear OC pin mapping allow for NOA usage of OC pins $EN_DIS.
- UINT8 PchEspiLgmrEnable

  Offset 0x02CF - Espi Lgmr Memory Range decode This option enables or disables espi lgmr $EN_DIS.
- UINT8 PchHotEnable

  Offset 0x02D0 - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.
- UINT8 SataLedEnable

  Offset 0x02D1 - SATA LED SATA LED indicating SATA controller activity.
- UINT8 PchPmVrAlert

  Offset 0x02D2 - VRAlert# Pin When VRAlert# feature pin is enabled and its state is '0', the PMC requests throttling to a T3 Tstate to the PCH throttling unit.
- UINT8 PchPmSlpS0VmRuntimeControl

  Offset 0x02D3 - SLP_S0 VM Dynamic Control SLP_S0 Voltage Margining Runtime Control Policy.
- UINT8 PchPmSlpS0Vm070VSupport

  Offset 0x02D4 - SLP_S0 VM 0.70V Support SLP_S0 Voltage Margining 0.70V Support Policy.
- UINT8 PchPmSlpS0Vm075VSupport

Offset 0x02D5 - SLP_S0 VM 0.75V Support SLP_S0 Voltage Margining 0.75V Support Policy.

- UINT8 PcieRpSlotImplemented [24]

  Offset 0x02D6 - PCH PCIe root port connection type 0: built-in device, 1:slot.
- UINT8 PcieClkSrcUsage [16]

  Offset 0x02EE - Usage type for ClkSrc 0-23: PCH rootport, 0x40-0x43: PEG port, 0x70:LAN, 0x80: unspecified but in use (free running), 0xFF: not used.
- UINT8 PcieClkSrcClkReq [16]

  Offset 0x02FE - ClkReq-to-ClkSrc mapping Number of ClkReq signal assigned to ClkSrc.
- UINT8 PcieRpAcsEnabled [24]

  Offset 0x030E - PCIE RP Access Control Services Extended Capability Enable/Disable PCIE RP Access Control Services Extended Capability.
- UINT8 PcieRpEnableCpm [24]

  Offset 0x0326 - PCIE RP Clock Power Management Enable/Disable PCIE RP Clock Power Management, even if disabled, CLKREQ# signal can still be controlled by L1 PM substates mechanism.
- UINT16 PcieRpDetectTimeoutMs [24]

  Offset 0x033E - PCIE RP Detect Timeout Ms The number of milliseconds within 0∼65535 in reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
- UINT8 PmcModPhySusPgEnable

  Offset 0x036E - ModPHY SUS Power Domain Dynamic Gating Enable/Disable ModPHY SUS Power Domain Dynamic Gating.
- UINT8 SlpS0WithGbeSupport

  Offset 0x036F - SlpS0WithGbeSupport Enable/Disable SLP_S0 with GBE Support.
- UINT8 PchPwrOptEnable

  Offset 0x0370 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.
- UINT8 PchWriteProtectionEnable [5]

  Offset 0x0371 - PCH Flash Protection Ranges Write Enble Write or erase is blocked by hardware.
- UINT8 PchReadProtectionEnable [5]

  Offset 0x0376 - PCH Flash Protection Ranges Read Enble Read is blocked by hardware.
- UINT8 UnusedUpdSpace15 [1]

  Offset 0x037B.
- UINT16 PchProtectedRangeLimit [5]

  Offset 0x037C - PCH Protect Range Limit Left shifted address by 12 bits with address bits 11:0 are assumed to be FFFh for limit comparison.
- UINT16 PchProtectedRangeBase [5]

  Offset 0x0386 - PCH Protect Range Base Left shifted address by 12 bits with address bits 11:0 are assumed to be 0.
- UINT8 PchHdaPme

  Offset 0x0390 - Enable Pme Enable Azalia wake-on-ring.
- UINT8 PchHdaVcType

  Offset 0x0391 - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.
- UINT8 PchHdaLinkFrequency

  Offset 0x0392 - HD Audio Link Frequency HDA Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 0: 6MHz, 1: 12MHz, 2: 24MHz.
- UINT8 PchHdaIDispLinkFrequency

  Offset 0x0393 - iDisp-Link Frequency iDisp-Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 4: 96MHz, 3: 48MHz.
- UINT8 PchHdaIDispLinkTmode

  Offset 0x0394 - iDisp-Link T-mode iDisp-Link T-Mode (PCH_HDAUDIO_IDISP_TMODE enum): 0: 2T, 1: 1T.
- UINT8 PchHdaDspUaaCompliance

  Offset 0x0395 - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).
- UINT8 PchHdaIDispCodecDisconnect

  Offset 0x0396 - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.

- UINT8 PchUsbHsioFilterSel [10]

  Offset 0x0397 - USB LFPS Filter selection For each byte bits 2:0 are for p, bits 4:6 are for n.
- UINT8 PchIoApicEntry24_119

  Offset 0x03A1 - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.
- UINT8 PchIoApicId

  Offset 0x03A2 - PCH Io Apic ID This member determines IOAPIC ID.
- UINT8 PchIshSpiGpioAssign

  Offset 0x03A3 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshUart0GpioAssign

  Offset 0x03A4 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshUart1GpioAssign

  Offset 0x03A5 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c0GpioAssign

  Offset 0x03A6 - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c1GpioAssign

  Offset 0x03A7 - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c2GpioAssign

  Offset 0x03A8 - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp0GpioAssign

  Offset 0x03A9 - Enable PCH ISH GP_0 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp1GpioAssign

  Offset 0x03AA - Enable PCH ISH GP_1 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp2GpioAssign

  Offset 0x03AB - Enable PCH ISH GP_2 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp3GpioAssign

  Offset 0x03AC - Enable PCH ISH GP_3 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp4GpioAssign

  Offset 0x03AD - Enable PCH ISH GP_4 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp5GpioAssign

  Offset 0x03AE - Enable PCH ISH GP_5 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp6GpioAssign

  Offset 0x03AF - Enable PCH ISH GP_6 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp7GpioAssign

  Offset 0x03B0 - Enable PCH ISH GP_7 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshPdtUnlock

  Offset 0x03B1 - PCH ISH PDT Unlock Msg 0: False; 1: True.
- UINT8 PchLanLtrEnable

  Offset 0x03B2 - Enable PCH Lan LTR capabilty of PCH internal LAN 0: Disable; 1: Enable.
- UINT8 PchLockDownBiosLock

  Offset 0x03B3 - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:RegD↵ Ch[5]) for the BIOS region protection.
- UINT8 PchCrid

  Offset 0x03B4 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.
- UINT8 PchLockDownRtcMemoryLock

  Offset 0x03B5 - RTC CMOS MEMORY LOCK Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.
- UINT8 PcieRpHotPlug [24]

  Offset 0x03B6 - Enable PCIE RP HotPlug DEPRECATED.
- UINT8 PcieRpPmSci [24]

  Offset 0x03CE - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.

- UINT8 PcieRpExtSync [24]

  Offset 0x03E6 - Enable PCIE RP Ext Sync Indicate whether the extended synch is enabled.
- UINT8 PcieRpTransmitterHalfSwing [24]

  Offset 0x03FE - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.
- UINT8 PcieRpClkReqDetect [24]

  Offset 0x0416 - Enable PCIE RP Clk Req Detect Probe CLKREQ# signal before enabling CLKREQ# based power management.
- UINT8 PcieRpAdvancedErrorReporting [24]

  Offset 0x042E - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.
- UINT8 PcieRpUnsupportedRequestReport [24]

  Offset 0x0446 - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.
- UINT8 PcieRpFatalErrorReport [24]

  Offset 0x045E - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.
- UINT8 PcieRpNoFatalErrorReport [24]

  Offset 0x0476 - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.
- UINT8 PcieRpCorrectableErrorReport [24]

  Offset 0x048E - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.
- UINT8 PcieRpSystemErrorOnFatalError [24]

  Offset 0x04A6 - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.
- UINT8 PcieRpSystemErrorOnNonFatalError [24]

  Offset 0x04BE - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.
- UINT8 PcieRpSystemErrorOnCorrectableError [24]

  Offset 0x04D6 - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.
- UINT8 PcieRpMaxPayload [24]

  Offset 0x04EE - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH_PCIE_MAX_↩ PAYLOAD.
- UINT8 PchUsbHsioRxTuningParameters [10]

  Offset 0x0506 - PCH USB3 RX HSIO Tuning parameters Bits 7:3 are for Signed Magnatude number added to the CTLE code, Bits 2:0 are for controlling the input offset.
- UINT8 PchUsbHsioRxTuningEnable [10]

  Offset 0x0510 - PCH USB3 HSIO Rx Tuning Enable Mask for enabling tuning of HSIO Rx signals of USB3 ports.
- UINT8 PcieRpPcieSpeed [24]

  Offset 0x051A - PCIE RP Pcie Speed Determines each PCIE Port speed capability.
- UINT8 PcieRpGen3EqPh3Method [24]

  Offset 0x0532 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_ME↩ THOD).
- UINT8 PcieRpPhysicalSlotNumber [24]

  Offset 0x054A - PCIE RP Physical Slot Number Indicates the slot number for the root port.
- UINT8 PcieRpCompletionTimeout [24]

  Offset 0x0562 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_↩ TIMEOUT).
- UINT8 PcieRpAspm [24]

  Offset 0x057A - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).
- UINT8 PcieRpL1Substates [24]

  Offset 0x0592 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUBS↩ TATES_CONTROL).
- UINT8 PcieRpLtrEnable [24]

  Offset 0x05AA - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.
- UINT8 PcieRpLtrConfigLock [24]

  Offset 0x05C2 - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.

- UINT8 PcieEqPh3LaneParamCm [24]

  Offset 0x05DA - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.
- UINT8 PcieEqPh3LaneParamCp [24]

  Offset 0x05F2 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.
- UINT8 PcieSwEqCoeffListCm [5]

  Offset 0x060A - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.
- UINT8 PcieSwEqCoeffListCp [5]

  Offset 0x060F - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.
- UINT8 PcieDisableRootPortClockGating

  Offset 0x0614 - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.
- UINT8 PcieEnablePeerMemoryWrite

  Offset 0x0615 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.
- UINT8 PcieComplianceTestMode

  Offset 0x0616 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.
- UINT8 PcieRpFunctionSwap

  Offset 0x0617 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.
- UINT8 TetonGlacierCR

  Offset 0x0618 - Teton Glacier Cycle Router Specify to which cycle router Teton Glacier is connected, it is valid only when Teton Glacier support is enabled.
- UINT8 PchPmPmeB0S5Dis

  Offset 0x0619 - PCH Pm PME_B0_S5_DIS When cleared (default), wake events from PME_B0_STS are allowed in S5 if PME_B0_EN = 1.
- UINT8 PcieRpImrEnabled

  Offset 0x061A - PCIE IMR Enables Isolated Memory Region for PCIe.
- UINT8 PcieRpImrSelection

  Offset 0x061B - PCIE IMR port number Selects PCIE root port number for IMR feature.
- UINT8 TetonGlacierMode

  Offset 0x061C - Teton Glacier Detection and Configuration Mode Enables support for Teton Glacier hybrid storage device.
- UINT8 PchPmWolEnableOverride

  Offset 0x061D - PCH Pm Wol Enable Override Corresponds to the WOL Enable Override bit in the General PM Configuration B (GEN_PMCON_B) register.
- UINT8 PchPmPcieWakeFromDeepSx

  Offset 0x061E - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.
- UINT8 PchPmWoWlanEnable

  Offset 0x061F - PCH Pm WoW lan Enable Determine if WLAN wake from Sx, corresponds to the HOST_WLAN_↩ PP_EN bit in the PWRM_CFG3 register.
- UINT8 PchPmWoWlanDeepSxEnable

  Offset 0x0620 - PCH Pm WoW lan DeepSx Enable Determine if WLAN wake from DeepSx, corresponds to the DSX_WLAN_PP_EN bit in the PWRM_CFG3 register.
- UINT8 PchPmLanWakeFromDeepSx

  Offset 0x0621 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.
- UINT8 PchPmDeepSxPol

  Offset 0x0622 - PCH Pm Deep Sx Pol Deep Sx Policy.
- UINT8 PchPmSlpS3MinAssert

  Offset 0x0623 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.
- UINT8 PchPmSlpS4MinAssert

  Offset 0x0624 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.
- UINT8 PchPmSlpSusMinAssert

Offset 0x0625 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.

- UINT8 PchPmSlpAMinAssert

  Offset 0x0626 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.

- UINT8 SlpS0Override

  Offset 0x0627 - SLP_S0# Override Select 'Auto', it will be auto-configured according to probe type.

- UINT8 SlpS0DisQForDebug

  Offset 0x0628 - S0ix Override Settings Select 'Auto', it will be auto-configured according to probe type.

- UINT8 PchEnableDbcObs

  Offset 0x0629 - USB Overcurrent Override for DbC This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option.

- UINT8 PchLegacyIoLowLatency

  Offset 0x062A - PCH Legacy IO Low Latency Enable Set to enable low latency of legacy IO.

- UINT8 PchPmLpcClockRun

  Offset 0x062B - PCH Pm Lpc Clock Run This member describes whether or not the LPC ClockRun feature of PCH should be enabled.

- UINT8 PchPmSlpStrchSusUp

  Offset 0x062C - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.

- UINT8 PchPmSlpLanLowDc

  Offset 0x062D - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.

- UINT8 PchPmPwrBtnOverridePeriod

  Offset 0x062E - PCH Pm Pwr Btn Override Period PCH power button override period.

- UINT8 PchPmDisableDsxAcPresentPulldown

  Offset 0x062F - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRESENT in deep SX and during G3 exit.

- UINT8 PchPmDisableNativePowerButton

  Offset 0x0630 - PCH Pm Disable Native Power Button Power button native mode disable.

- UINT8 PchPmSlpS0Enable

  Offset 0x0631 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.

- UINT8 PchPmMeWakeSts

  Offset 0x0632 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS) register.

- UINT8 PchPmWolOvrWkSts

  Offset 0x0633 - PCH Pm WOL_OVR_WK_STS Clear the WOL_OVR_WK_STS bit in the Power and Reset Status (PRSTS) register.

- UINT8 PchPmPwrCycDur

  Offset 0x0634 - PCH Pm Reset Power Cycle Duration Could be customized in the unit of second.

- UINT8 PchPmPciePllSsc

  Offset 0x0635 - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.

- UINT8 SataPwrOptEnable

  Offset 0x0636 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.

- UINT8 EsataSpeedLimit

  Offset 0x0637 - PCH Sata eSATA Speed Limit When enabled, BIOS will configure the PxSCTL.SPD to 2 to limit the eSATA port speed.

- UINT8 SataSpeedLimit

  Offset 0x0638 - PCH Sata Speed Limit Indicates the maximum speed the SATA controller can support 0h: Pch↩ SataSpeedDefault.

- UINT8 SataPortsHotPlug [8]

  Offset 0x0639 - Enable SATA Port HotPlug Enable SATA Port HotPlug.

- UINT8 SataPortsInterlockSw [8]

  Offset 0x0641 - Enable SATA Port Interlock Sw Enable SATA Port Interlock Sw.

- UINT8 SataPortsExternal [8]

  Offset 0x0649 - Enable SATA Port External Enable SATA Port External.

- UINT8 SataPortsSpinUp [8]

  Offset 0x0651 - Enable SATA Port SpinUp Enable the COMRESET initialization Sequence to the device.
- UINT8 SataPortsSolidStateDrive [8]

  Offset 0x0659 - Enable SATA Port Solid State Drive 0: HDD; 1: SSD.
- UINT8 SataPortsEnableDitoConfig [8]

  Offset 0x0661 - Enable SATA Port Enable Dito Config Enable DEVSLP Idle Timeout settings (DmVal, DitoVal).
- UINT8 SataPortsDmVal [8]

  Offset 0x0669 - Enable SATA Port DmVal DITO multiplier.
- UINT8 UnusedUpdSpace16 [1]

  Offset 0x0671.
- UINT16 SataPortsDitoVal [8]

  Offset 0x0672 - Enable SATA Port DmVal DEVSLP Idle Timeout (DITO), Default is 625.
- UINT8 SataPortsZpOdd [8]

  Offset 0x0682 - Enable SATA Port ZpOdd Support zero power ODD.
- UINT8 SataRstRaidDeviceId

  Offset 0x068A - PCH Sata Rst Raid Device Id Enable RAID Alternate ID.
- UINT8 SataRstRaid0

  Offset 0x068B - PCH Sata Rst Raid0 RAID0.
- UINT8 SataRstRaid1

  Offset 0x068C - PCH Sata Rst Raid1 RAID1.
- UINT8 SataRstRaid10

  Offset 0x068D - PCH Sata Rst Raid10 RAID10.
- UINT8 SataRstRaid5

  Offset 0x068E - PCH Sata Rst Raid5 RAID5.
- UINT8 SataRstIrrt

  Offset 0x068F - PCH Sata Rst Irrt Intel Rapid Recovery Technology.
- UINT8 SataRstOromUiBanner

  Offset 0x0690 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.
- UINT8 SataRstOromUiDelay

  Offset 0x0691 - PCH Sata Rst Orom Ui Delay 00b: 2 secs; 01b: 4 secs; 10b: 6 secs; 11: 8 secs (see: PCH_SATA↩_OROM_DELAY).
- UINT8 SataRstHddUnlock

  Offset 0x0692 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.
- UINT8 SataRstLedLocate

  Offset 0x0693 - PCH Sata Rst Led Locate Indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.
- UINT8 SataRstIrrtOnly

  Offset 0x0694 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.
- UINT8 SataRstSmartStorage

  Offset 0x0695 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.
- UINT8 SataRstPcieEnable [3]

  Offset 0x0696 - PCH Sata Rst Pcie Storage Remap enable Enable Intel RST for PCIe Storage remapping.
- UINT8 SataRstPcieStoragePort [3]

  Offset 0x0699 - PCH Sata Rst Pcie Storage Port Intel RST for PCIe Storage remapping - PCIe Port Selection (1-based, 0 = autodetect).
- UINT8 SataRstPcieDeviceResetDelay [3]

  Offset 0x069C - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.
- UINT8 PchScsEmmcHs400TuningRequired

  Offset 0x069F - Enable eMMC HS400 Training Deprecated.
- UINT8 PchScsEmmcHs400DllDataValid

  Offset 0x06A0 - Set HS400 Tuning Data Valid Deprecated $EN_DIS.

- UINT8 PchScsEmmcHs400RxStrobeDll1

  Offset 0x06A1 - Rx Strobe Delay Control Deprecated.
- UINT8 PchScsEmmcHs400TxDataDll

  Offset 0x06A2 - Tx Data Delay Control Deprecated.
- UINT8 PchScsEmmcHs400DriverStrength

  Offset 0x06A3 - I/O Driver Strength Deprecated 0:33 Ohm, 1:40 Ohm, 2:50 Ohm.
- UINT8 PchSirqEnable

  Offset 0x06A4 - Enable Serial IRQ Determines if enable Serial IRQ.
- UINT8 PchSirqMode

  Offset 0x06A5 - Serial IRQ Mode Select Serial IRQ Mode Select, 0: quiet mode, 1: continuous mode.
- UINT8 PchStartFramePulse

  Offset 0x06A6 - Start Frame Pulse Width Start Frame Pulse Width, 0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: PchSfpw8↩ Clk.
- UINT8 PchEspiLockLinkConfiguration

  Offset 0x06A7 - PCH eSPI Link Configuration Lock (SBLCL) Enable/Disable lock of communication through SET_↩ CONFIG/GET_CONFIG to eSPI slaves addresseses from range 0x0 - 0x7FF $EN_DIS.
- UINT8 PchTsmicLock

  Offset 0x06A8 - Thermal Device SMI Enable This locks down SMI Enable on Alert Thermal Sensor Trip.
- UINT8 UnusedUpdSpace17

  Offset 0x06A9.
- UINT16 PchT0Level

  Offset 0x06AA - Thermal Throttling Custimized T0Level Value Custimized T0Level value.
- UINT16 PchT1Level

  Offset 0x06AC - Thermal Throttling Custimized T1Level Value Custimized T1Level value.
- UINT16 PchT2Level

  Offset 0x06AE - Thermal Throttling Custimized T2Level Value Custimized T2Level value.
- UINT8 PchTTEnable

  Offset 0x06B0 - Enable The Thermal Throttle Enable the thermal throttle function.
- UINT8 PchTTState13Enable

  Offset 0x06B1 - PMSync State 13 When set to 1 and the programmed GPIO pin is a 1, then PMSync state 13 will force at least T2 state.
- UINT8 PchTTLock

  Offset 0x06B2 - Thermal Throttle Lock Thermal Throttle Lock.
- UINT8 TTSuggestedSetting

  Offset 0x06B3 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.
- UINT8 TTCrossThrottling

  Offset 0x06B4 - Enable PCH Cross Throttling Enable/Disable PCH Cross Throttling $EN_DIS.
- UINT8 PchDmiTsawEn

  Offset 0x06B5 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.
- UINT8 DmiSuggestedSetting

  Offset 0x06B6 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.
- UINT8 DmiTS0TW

  Offset 0x06B7 - Thermal Sensor 0 Target Width DMT thermal sensor suggested representative values.
- UINT8 DmiTS1TW

  Offset 0x06B8 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.
- UINT8 DmiTS2TW

  Offset 0x06B9 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.
- UINT8 DmiTS3TW

  Offset 0x06BA - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.
- UINT8 SataP0T1M

  Offset 0x06BB - Port 0 T1 Multipler Port 0 T1 Multipler.

- UINT8 SataP0T2M

  Offset 0x06BC - Port 0 T2 Multipler Port 0 T2 Multipler.
- UINT8 SataP0T3M

  Offset 0x06BD - Port 0 T3 Multipler Port 0 T3 Multipler.
- UINT8 SataP0TDisp

  Offset 0x06BE - Port 0 Tdispatch Port 0 Tdispatch.
- UINT8 SataP1T1M

  Offset 0x06BF - Port 1 T1 Multipler Port 1 T1 Multipler.
- UINT8 SataP1T2M

  Offset 0x06C0 - Port 1 T2 Multipler Port 1 T2 Multipler.
- UINT8 SataP1T3M

  Offset 0x06C1 - Port 1 T3 Multipler Port 1 T3 Multipler.
- UINT8 SataP1TDisp

  Offset 0x06C2 - Port 1 Tdispatch Port 1 Tdispatch.
- UINT8 SataP0Tinact

  Offset 0x06C3 - Port 0 Tinactive Port 0 Tinactive.
- UINT8 SataP0TDispFinit

  Offset 0x06C4 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.
- UINT8 SataP1Tinact

  Offset 0x06C5 - Port 1 Tinactive Port 1 Tinactive.
- UINT8 SataP1TDispFinit

  Offset 0x06C6 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.
- UINT8 SataThermalSuggestedSetting

  Offset 0x06C7 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.
- UINT8 PchMemoryThrottlingEnable

  Offset 0x06C8 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryPmsyncEnable [2]

  Offset 0x06C9 - Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryC0TransmitEnable [2]

  Offset 0x06CB - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryPinSelection [2]

  Offset 0x06CD - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 UnusedUpdSpace18

  Offset 0x06CF.
- UINT16 PchTemperatureHotLevel

  Offset 0x06D0 - Thermal Device Temperature Decides the temperature.
- UINT8 PchEnableComplianceMode

  Offset 0x06D2 - Enable xHCI Compliance Mode Compliance Mode can be enabled for testing through this option but this is disabled by default.
- UINT8 Usb2OverCurrentPin [16]

  Offset 0x06D3 - USB2 Port Over Current Pin Describe the specific over current pin number of USB 2.0 Port N.
- UINT8 Usb3OverCurrentPin [10]

  Offset 0x06E3 - USB3 Port Over Current Pin Describe the specific over current pin number of USB 3.0 Port N.
- UINT8 Enable8254ClockGating

  Offset 0x06ED - Enable 8254 Static Clock Gating Set 8254CGE=1 is required for SLP_S0 support.
- UINT8 SataRstOptaneMemory

  Offset 0x06EE - PCH Sata Rst Optane Memory Optane Memory $EN_DIS.
- UINT8 SataRstCpuAttachedStorage

  Offset 0x06EF - PCH Sata Rst CPU Attached Storage CPU Attached Storage $EN_DIS.
- UINT8 Enable8254ClockGatingOnS3

Offset 0x06F0 - Enable 8254 Static Clock Gating On S3 This is only applicable when Enable8254ClockGating is disabled.

- UINT8 UnusedUpdSpace19 [3]

  Offset 0x06F1.

- UINT32 PchPcieDeviceOverrideTablePtr

  Offset 0x06F4 - Pch PCIE device override table pointer The PCIe device table is being used to override PCIe device ASPM settings.

- UINT8 EnableTcoTimer

  Offset 0x06F8 - Enable TCO timer.

- UINT8 PsOnEnable

  Offset 0x06F9 - Enable PS_ON.

- UINT8 PmcCpuC10GatePinEnable

  Offset 0x06FA - Pmc Cpu C10 Gate Pin Enable Enable/Disable platform support for CPU_C10_GATE# pin to control gating of CPU VccIO and VccSTG rails instead of SLP_S0# pin.

- UINT8 PchDmiAspmCtrl

  Offset 0x06FB - Pch Dmi Aspm Ctrl ASPM configuration on the PCH side of the DMI/OPI Link.

- UINT8 Usb3HsioTxRate3UniqTranEnable [10]

  Offset 0x06FC - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 3 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 3, Each value in array can be between 0-1.

- UINT8 Usb3HsioTxRate3UniqTran [10]

  *Offset 0x0706 - USB 3.0 TX Output Unique Transition Bit Scale for rate 3 USB 3.0 TX Output Unique Transition Bit Scale for rate 3, HSIO_TX_DWORD9[6:0], **Default = 4Ch**.*

- UINT8 Usb3HsioTxRate2UniqTranEnable [10]

  Offset 0x0710 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 2 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 2, Each value in array can be between 0-1.

- UINT8 Usb3HsioTxRate2UniqTran [10]

  *Offset 0x071A - USB 3.0 TX Output Unique Transition Bit Scale for rate 2 USB 3.0 TX Output Unique Transition Bit Scale for rate 2, HSIO_TX_DWORD9[14:8], **Default = 4Ch**.*

- UINT8 Usb3HsioTxRate1UniqTranEnable [10]

  Offset 0x0724 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 1 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 1, Each value in array can be between 0-1.

- UINT8 Usb3HsioTxRate1UniqTran [10]

  *Offset 0x072E - USB 3.0 TX Output Unique Transition Bit Scale for rate 1 USB 3.0 TX Output Unique Transition Bit Scale for rate 1, HSIO_TX_DWORD9[22:16], **Default = 4Ch**.*

- UINT8 Usb3HsioTxRate0UniqTranEnable [10]

  Offset 0x0738 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 0 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 0, Each value in array can be between 0-1.

- UINT8 Usb3HsioTxRate0UniqTran [10]

  *Offset 0x0742 - USB 3.0 TX Output Unique Transition Bit Scale for rate 0 USB 3.0 TX Output Unique Transition Bit Scale for rate 0, HSIO_TX_DWORD9[30:24], **Default = 4Ch**.*

- UINT8 PcieNumOfCoefficients

  Offset 0x074C - Number of Coefficients to be used The number of coefficients to be used for equalization, default value is 3.

- UINT8 GpioPmRcompCommunityLocalClockGating

  Offset 0x074D - GPIO RCOMP Community Clock Gating 0 = Disable dynamic RCOMP clock local clock gating, 1 = Enable dynamic RCOMP clock local clock gating, default value is 1 $EN_DIS.

- UINT8 ScsSdCardWpPinEnabled

  Offset 0x074E - Enable SD Card Write Protect Pin Enable/disable SD Card Write Protect Pin.

- UINT8 SataPortsDevSlpResetConfig [8]

  Offset 0x074F - Set SATA DEVSLP GPIO Reset Config Set SATA DEVSLP GPIO Reset Config per port.

- UINT8 SpiFlashCfgLockDown

  Offset 0x0757 - Flash Configuration Lock Down Enable/disable flash lock down.

- UINT8 PchHdaSndwLinkIoControlEnabled [4]

Offset 0x0758 - Enable HD Audio Sndw Link IO Control 0:Disabled, 1:Enabled.

- UINT8 ReservedPchPostMem [3]

  Offset 0x075C - ReservedPchPostMem Reserved for Pch Post-Mem $EN_DIS.
- UINT8 UnusedUpdSpace20 [1]

  Offset 0x075F.
- UINT64 BgpdtHash [4]

  Offset 0x0760 - BgpdtHash[4] BgpdtHash values.
- UINT32 BiosGuardAttr

  Offset 0x0780 - BiosGuardAttr BiosGuardAttr default values.
- UINT8 UnusedUpdSpace21 [4]

  Offset 0x0784.
- UINT64 BiosGuardModulePtr

  Offset 0x0788 - BiosGuardModulePtr BiosGuardModulePtr default values.
- UINT64 SendEcCmd

  Offset 0x0790 - SendEcCmd SendEcCmd function pointer.
- UINT8 EcCmdProvisionEav

  Offset 0x0798 - EcCmdProvisionEav Ephemeral Authorization Value default values.
- UINT8 EcCmdLock

  Offset 0x0799 - EcCmdLock EcCmdLock default values.
- UINT8 UnusedUpdSpace22 [6]

  Offset 0x079A.
- UINT64 SgxEpoch0

  Offset 0x07A0 - SgxEpoch0 SgxEpoch0 default values.
- UINT64 SgxEpoch1

  Offset 0x07A8 - SgxEpoch1 SgxEpoch1 default values.
- UINT8 SgxSinitNvsData

  Offset 0x07B0 - SgxSinitNvsData SgxSinitNvsData default values.
- UINT8 SiCsmFlag

  Offset 0x07B1 - Si Config CSM Flag.
- UINT8 UnusedUpdSpace23 [2]

  Offset 0x07B2.
- UINT32 SiSsidTablePtr

  Offset 0x07B4 - SVID SDID table Poniter.
- UINT16 SiNumberOfSsidTableEntry

  Offset 0x07B8 - Number of ssid table.
- UINT8 SataRstInterrupt

  Offset 0x07BA - SATA RST Interrupt Mode Allowes to choose which interrupts will be implemented by SATA controller in RAID mode.
- UINT8 MeUnconfigOnRtcClear

  Offset 0x07BB - ME Unconfig on RTC clear 0: Disable ME Unconfig On Rtc Clear.
- UINT8 UnusedUpdSpace24 [3]

  Offset 0x07BC.
- UINT8 ReservedFspsUpd [1]

  Offset 0x07BF.

13.36.1 Detailed Description

Fsp S Configuration.

Definition at line 86 of file FspsUpd.h.

13.36.2 Member Data Documentation

13.36.2.1 AcLoadline

```
UINT16 FSP_S_CONFIG::AcLoadline[5]
```

Offset 0x00FE - AcLoadline PCODE MMIO Mailbox: AcLoadline in 1/100 mOhms (ie.

1250 = 12.50 mOhm); Range is 0-6249. **Intel Recommended Defaults vary by domain and SKU.**

Definition at line 501 of file FspsUpd.h.

13.36.2.2 AcousticNoiseMitigation

```
UINT8 FSP_S_CONFIG::AcousticNoiseMitigation
```

Offset 0x00EE - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.

This has to be enabled to program slew rate configuration for all VR domains, Pre Wake, Ramp Up and, Ramp Down times.**0: Disabled**; 1: Enabled $EN_DIS

Definition at line 457 of file FspsUpd.h.

13.36.2.3 AmtEnabled

```
UINT8 FSP_S_CONFIG::AmtEnabled
```

Offset 0x003C - AMT Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable AMT functionality. $EN_DIS

Definition at line 152 of file FspsUpd.h.

13.36.2.4 AmtKvmEnabled

```
UINT8 FSP_S_CONFIG::AmtKvmEnabled
```

Offset 0x0047 - KVM Switch Enable/Disable.

0: Disable, 1: enable, KVM enable/disable state by Mebx. Setting is invalid if AmtEnabled is 0. $EN_DIS

Definition at line 206 of file FspsUpd.h.

13.36.2.5 AmtSolEnabled

```
UINT8 FSP_S_CONFIG::AmtSolEnabled
```

Offset 0x0040 - SOL Switch Enable/Disable.

0: Disable, 1: enable, Serial Over Lan enable/disable state by Mebx. Setting is invalid if AmtEnabled is 0. $EN_DIS

Definition at line 179 of file FspsUpd.h.

13.36.2.6 CnviBtAudioOffload

```
UINT8 FSP_S_CONFIG::CnviBtAudioOffload
```

Offset 0x02CB - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.

0: DISABLE, 1: ENABLE $EN_DIS

Definition at line 1216 of file FspsUpd.h.

13.36.2.7 CnviBtCore

```
UINT8 FSP_S_CONFIG::CnviBtCore
```

Offset 0x02CA - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.

0: DISABLE, 1: ENABLE $EN_DIS

Definition at line 1210 of file FspsUpd.h.

13.36.2.8 CnviMode

```
UINT8 FSP_S_CONFIG::CnviMode
```

Offset 0x02C9 - CNVi Configuration This option allows for automatic detection of Connectivity Solution.

[Auto Detection] assumes that CNVi will be enabled when available, [Disable] allows for disabling CNVi. 0:Disable, 1:Auto

Definition at line 1204 of file FspsUpd.h.

13.36.2.9 CpuMpHob

```
UINT32 FSP_S_CONFIG::CpuMpHob
```

Offset 0x0170 - CpuMpHob Pointer for CpuMpHob.

This is optional data buffer for CpuMpPpi usage.

Definition at line 683 of file FspsUpd.h.

13.36.2.10 DcLoadline

```
UINT16 FSP_S_CONFIG::DcLoadline[5]
```

Offset 0x0108 - DcLoadline PCODE MMIO Mailbox: DcLoadline in 1/100 mOhms (ie.

1250 = 12.50 mOhm); Range is 0-6249.**Intel Recommended Defaults vary by domain and SKU.**

Definition at line 507 of file FspsUpd.h.

13.36.2.11 DevIntConfigPtr

```
UINT32 FSP_S_CONFIG::DevIntConfigPtr
```

Offset 0x0204 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.

The address of the table of PCH_DEVICE_INTERRUPT_CONFIG.

Definition at line 906 of file FspsUpd.h.

13.36.2.12 DmiSuggestedSetting

```
UINT8 FSP_S_CONFIG::DmiSuggestedSetting
```

Offset 0x06B6 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.

$EN_DIS

Definition at line 2170 of file FspsUpd.h.

13.36.2.13 DmiTS0TW

```
UINT8 FSP_S_CONFIG::DmiTS0TW
```

Offset 0x06B7 - Thermal Sensor 0 Target Width DMT thermal sensor suggested representative values.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2176 of file FspsUpd.h.

13.36.2.14 DmiTS1TW

```
UINT8 FSP_S_CONFIG::DmiTS1TW
```

Offset 0x06B8 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2182 of file FspsUpd.h.

13.36.2.15 DmiTS2TW

```
UINT8 FSP_S_CONFIG::DmiTS2TW
```

Offset 0x06B9 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2188 of file FspsUpd.h.

13.36.2.16 DmiTS3TW

```
UINT8 FSP_S_CONFIG::DmiTS3TW
```

Offset 0x06BA - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2194 of file FspsUpd.h.

13.36.2.17 EcCmdLock

```
UINT8 FSP_S_CONFIG::EcCmdLock
```

Offset 0x0799 - EcCmdLock EcCmdLock default values.

Locks Ephemeral Authorization Value sent previously

Definition at line 2509 of file FspsUpd.h.

13.36.2.18 EcCmdProvisionEav

```
UINT8 FSP_S_CONFIG::EcCmdProvisionEav
```

Offset 0x0798 - EcCmdProvisionEav Ephemeral Authorization Value default values.

Provisions an ephemeral shared secret to the EC

Definition at line 2504 of file FspsUpd.h.

13.36.2.19 Enable8254ClockGating

```
UINT8 FSP_S_CONFIG::Enable8254ClockGating
```

Offset 0x06ED - Enable 8254 Static Clock Gating Set 8254CGE=1 is required for SLP_S0 support.

However, set 8254CGE=1 in POST time might fail to boot legacy OS using 8254 timer. Make sure it is disabled to support boot legacy OS using 8254 timer. Also enable this while S0ix is enabled. $EN_DIS

Definition at line 2317 of file FspsUpd.h.

13.36.2.20 Enable8254ClockGatingOnS3

```
UINT8 FSP_S_CONFIG::Enable8254ClockGatingOnS3
```

Offset 0x06F0 - Enable 8254 Static Clock Gating On S3 This is only applicable when Enable8254ClockGating is disabled.

FSP will do the 8254 CGE programming on S3 resume when Enable8254ClockGatingOnS3 is enabled. This avoids the SMI requirement for the programming. $EN_DIS

Definition at line 2337 of file FspsUpd.h.

13.36.2.21 EnableTcoTimer

```
UINT8 FSP_S_CONFIG::EnableTcoTimer
```

Offset 0x06F8 - Enable TCO timer.

When FALSE, it disables PCH ACPI timer, and stops TCO timer. NOTE: This will have huge power impact when it's enabled. If TCO timer is disabled, uCode ACPI timer emulation must be enabled, and WDAT table must not be exposed to the OS. $EN_DIS

Definition at line 2357 of file FspsUpd.h.

13.36.2.22 EsataSpeedLimit

```
UINT8 FSP_S_CONFIG::EsataSpeedLimit
```

Offset 0x0637 - PCH Sata eSATA Speed Limit When enabled, BIOS will configure the PxSCTL.SPD to 2 to limit the eSATA port speed.

$EN_DIS

Definition at line 1908 of file FspsUpd.h.

13.36.2.23 FastPkgCRampDisableFivr

```
UINT8 FSP_S_CONFIG::FastPkgCRampDisableFivr
```

Offset 0x0150 - Disable Fast Slew Rate for Deep Package C States for VR FIVR domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True $EN_DIS

Definition at line 609 of file FspsUpd.h.

13.36.2.24 FastPkgCRampDisableGt

```
UINT8 FSP_S_CONFIG::FastPkgCRampDisableGt
```

Offset 0x0144 - Disable Fast Slew Rate for Deep Package C States for VR GT domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True $EN_DIS

Definition at line 539 of file FspsUpd.h.

13.36.2.25 FastPkgCRampDisableIa

```
UINT8 FSP_S_CONFIG::FastPkgCRampDisableIa
```

Offset 0x00EF - Disable Fast Slew Rate for Deep Package C States for VR IA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True $EN_DIS

Definition at line 464 of file FspsUpd.h.

13.36.2.26 FastPkgCRampDisableSa

```
UINT8 FSP_S_CONFIG::FastPkgCRampDisableSa
```

Offset 0x0145 - Disable Fast Slew Rate for Deep Package C States for VR SA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True $EN_DIS

Definition at line 546 of file FspsUpd.h.

13.36.2.27 FivrRfiFrequency

```
UINT16 FSP_S_CONFIG::FivrRfiFrequency
```

Offset 0x014C - FIVR RFI Frequency PCODE MMIO Mailbox: Set the desired RFI frequency, in increments of 100KHz.

0: Auto. Range varies based on XTAL clock: 0-1918 (Up to 191.8HMz) for 24MHz clock; 0-1535 (Up to 153.5MHz) for 19MHz clock.

Definition at line 590 of file FspsUpd.h.

13.36.2.28 FivrSpreadSpectrum

```
UINT8 FSP_S_CONFIG::FivrSpreadSpectrum
```

Offset 0x014F - FIVR RFI Spread Spectrum PCODE MMIO Mailbox: FIVR RFI Spread Spectrum, in 0.1% increments.

0: 0%; Range: 0.0% to 10.0% (0-100).

Definition at line 602 of file FspsUpd.h.

13.36.2.29 ForcMebxSyncUp

```
UINT8 FSP_S_CONFIG::ForcMebxSyncUp
```

Offset 0x0048 - MEBX execution Enable/Disable.

0: Disable, 1: enable, Force MEBX execution. $EN_DIS

Definition at line 212 of file FspsUpd.h.

13.36.2.30 FwProgress

```
UINT8 FSP_S_CONFIG::FwProgress
```

Offset 0x003F - PET Progress Enable/Disable.

0: Disable, 1: enable, Enable/Disable PET Events Progress to receive PET Events. Setting is invalid if AmtEnabled is 0. $EN_DIS

Definition at line 172 of file FspsUpd.h.

13.36.2.31 GpioIrqRoute

```
UINT8 FSP_S_CONFIG::GpioIrqRoute
```

Offset 0x0211 - Select GPIO IRQ Route GPIO IRQ Select.

The valid value is 14 or 15.

Definition at line 924 of file FspsUpd.h.

13.36.2.32 Heci1Disabled

```
UINT8 FSP_S_CONFIG::Heci1Disabled
```

Offset 0x003B - HECI1 state Determine if HECI1 is hidden prior to boot to OS.

0: Disable; 1: Enable. $EN_DIS

Definition at line 146 of file FspsUpd.h.

13.36.2.33 Heci3Enabled

```
UINT8 FSP_S_CONFIG::Heci3Enabled
```

Offset 0x003A - HECI3 state The HECI3 state from Mbp for reference in S3 path or when MbpHob is not installed.

0: disable, 1: enable $EN_DIS

Definition at line 140 of file FspsUpd.h.

13.36.2.34 IccMax

```
UINT16 FSP_S_CONFIG::IccMax[5]
```

Offset 0x0130 - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.

0-255A in 1/4 A units. 400 = 100A

Definition at line 527 of file FspsUpd.h.

13.36.2.35 ImonOffset1

```
UINT16 FSP_S_CONFIG::ImonOffset1[5]
```

Offset 0x0176 - Imon offset 1 correction PCODE MMIO Mailbox: Imon offset correction.

Value is a 2's complement signed integer. Units 1/1000, Range 0-63999. For an offset = 12.580, use 12580. **0: Auto**

Definition at line 700 of file FspsUpd.h.

13.36.2.36 ImonSlope

```
UINT8 FSP_S_CONFIG::ImonSlope[5]
```

Offset 0x00CE - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.

Specified in 1/100 increment values. Range is 0-200. 125 = 1.25. **0: Auto**.For all VR Indexes

Definition at line 408 of file FspsUpd.h.

13.36.2.37 ImonSlope1

```
UINT16 FSP_S_CONFIG::ImonSlope1[5]
```

Offset 0x015A - Imon slope1 correction PCODE MMIO Mailbox: Imon slope correction.

Specified in 1/100 increment values. Range is 0-200. 125 = 1.25. **0: Auto**.For all VR Indexes

Definition at line 641 of file FspsUpd.h.

13.36.2.38 IslVrCmd

```
UINT8 FSP_S_CONFIG::IslVrCmd
```

Offset 0x0158 - Activates VR mailbox command for Intersil VR C-state issues.

Intersil VR mailbox command. **0 - no mailbox command sent.** 1 - VR mailbox command sent for IA/GT rails only. 2 - VR mailbox command sent for IA/GT/SA rails.

Definition at line 631 of file FspsUpd.h.

13.36.2.39 ManageabilityMode

```
UINT8 FSP_S_CONFIG::ManageabilityMode
```

Offset 0x003E - Manageability Mode set by Mebx Enable/Disable.

0: Disable, 1: enable, Enable or disable Manageability Mode. $EN_DIS

Definition at line 165 of file FspsUpd.h.

13.36.2.40 McivrRfiFrequencyAdjust

```
UINT8 FSP_S_CONFIG::McivrRfiFrequencyAdjust
```

Offset 0x014B - McIVR RFI Frequency Adjustment PCODE MMIO Mailbox: Adjust the RFI frequency relative to the nominal frequency in increments of 100KHz.

For subtraction, change McivrRfiFrequencyPrefix. **0: Auto**.

Definition at line 583 of file FspsUpd.h.

13.36.2.41 McivrRfiFrequencyPrefix

```
UINT8 FSP_S_CONFIG::McivrRfiFrequencyPrefix
```

Offset 0x014A - McIVR RFI Frequency Prefix PCODE MMIO Mailbox: McIVR RFI Frequency Adjustment Prefix.

0: Plus (+); 1: Minus (-).

Definition at line 577 of file FspsUpd.h.

13.36.2.42 McivrSpreadSpectrum

```
UINT8 FSP_S_CONFIG::McivrSpreadSpectrum
```

Offset 0x014E - McIVR RFI Spread Spectrum PCODE MMIO Mailbox: McIVR RFI Spread Spectrum.

0: 0%; 1: +/- 0.5%; 2: +/- 1%; 3: +/- 1.5%; 4: +/- 2%; 5: +/- 3%; 6: +/- 4%; 7: +/- 5%; 8: +/- 6%.

Definition at line 596 of file FspsUpd.h.

13.36.2.43 MeUnconfigOnRtcClear

```
UINT8 FSP_S_CONFIG::MeUnconfigOnRtcClear
```

Offset 0x07BB - ME Unconfig on RTC clear 0: Disable ME Unconfig On Rtc Clear.

1: Enable ME Unconfig On Rtc Clear. 2: Cmos is clear, status unkonwn. 3: Reserved 0: Disable ME Unconfig On Rtc Clear, 1: Enable ME Unconfig On Rtc Clear, 2: Cmos is clear, 3: Reserved

Definition at line 2562 of file FspsUpd.h.

13.36.2.44 NumOfDevIntConfig

```
UINT8 FSP_S_CONFIG::NumOfDevIntConfig
```

Offset 0x0208 - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.

If this is not zero, the DevIntConfigPtr must not be NULL.

Definition at line 912 of file FspsUpd.h.

13.36.2.45 PchCrid

```
UINT8 FSP_S_CONFIG::PchCrid
```

Offset 0x03B4 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.

$EN_DIS

Definition at line 1527 of file FspsUpd.h.

13.36.2.46 PchDmiAspmCtrl

```
UINT8 FSP_S_CONFIG::PchDmiAspmCtrl
```

Offset 0x06FB - Pch Dmi Aspm Ctrl ASPM configuration on the PCH side of the DMI/OPI Link.

Default is **PchPcieAspmAutoConfig** 0:Disabled, 1:L0s, 2:L1, 3:L0sL1, 4:Auto

Definition at line 2378 of file FspsUpd.h.

13.36.2.47 PchDmiTsawEn

```
UINT8 FSP_S_CONFIG::PchDmiTsawEn
```

Offset 0x06B5 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.

$EN_DIS

Definition at line 2164 of file FspsUpd.h.

13.36.2.48 PchEnableComplianceMode

```
UINT8 FSP_S_CONFIG::PchEnableComplianceMode
```

Offset 0x06D2 - Enable xHCI Compliance Mode Compliance Mode can be enabled for testing through this option but this is disabled by default.

$EN_DIS

Definition at line 2299 of file FspsUpd.h.

13.36.2.49 PchEnableDbcObs

```
UINT8 FSP_S_CONFIG::PchEnableDbcObs
```

Offset 0x0629 - USB Overcurrent Override for DbC This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option.

Enable when DbC is used to avoid signaling conflicts. $EN_DIS

Definition at line 1824 of file FspsUpd.h.

13.36.2.50 PchHdaAudioLinkDmic0

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkDmic0
```

Offset 0x0296 - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.

Muxed with SNDW4. $EN_DIS

Definition at line 1058 of file FspsUpd.h.

13.36.2.51 PchHdaAudioLinkDmic1

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkDmic1
```

Offset 0x0297 - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.

Muxed with SNDW3. $EN_DIS

Definition at line 1064 of file FspsUpd.h.

13.36.2.52 PchHdaAudioLinkHda

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkHda
```

Offset 0x0295 - Enable HD Audio Link Enable/disable HD Audio Link.

Muxed with SSP0/SSP1/SNDW1. $EN_DIS

Definition at line 1052 of file FspsUpd.h.

13.36.2.53 PchHdaAudioLinkSndw1

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw1
```

Offset 0x029B - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.

Muxed with HDA. $EN_DIS

Definition at line 1088 of file FspsUpd.h.

13.36.2.54 PchHdaAudioLinkSndw2

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw2
```

Offset 0x029C - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.

Muxed with SSP1. $EN_DIS

Definition at line 1094 of file FspsUpd.h.

13.36.2.55 PchHdaAudioLinkSndw3

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw3
```

Offset 0x029D - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.

Muxed with DMIC1. $EN_DIS

Definition at line 1100 of file FspsUpd.h.

13.36.2.56 PchHdaAudioLinkSndw4

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw4
```

Offset 0x029E - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.

Muxed with DMIC0. $EN_DIS

Definition at line 1106 of file FspsUpd.h.

13.36.2.57 PchHdaAudioLinkSsp0

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp0
```

Offset 0x0298 - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.

Muxed with HDA. $EN_DIS

Definition at line 1070 of file FspsUpd.h.

13.36.2.58 PchHdaAudioLinkSsp1

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp1
```

Offset 0x0299 - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.

Muxed with HDA/SNDW2. $EN_DIS

Definition at line 1076 of file FspsUpd.h.

13.36.2.59 PchHdaAudioLinkSsp2

```
UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp2
```

Offset 0x029A - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.

$EN_DIS

Definition at line 1082 of file FspsUpd.h.

13.36.2.60 PchHdaDspEnable

```
UINT8 FSP_S_CONFIG::PchHdaDspEnable
```

Offset 0x0188 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

$EN_DIS

Definition at line 712 of file FspsUpd.h.

13.36.2.61 PchHdaDspUaaCompliance

```
UINT8 FSP_S_CONFIG::PchHdaDspUaaCompliance
```

Offset 0x0395 - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).

$EN_DIS

Definition at line 1395 of file FspsUpd.h.

13.36.2.62 PchHdaIDispCodecDisconnect

```
UINT8 FSP_S_CONFIG::PchHdaIDispCodecDisconnect
```

Offset 0x0396 - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.

$EN_DIS

Definition at line 1401 of file FspsUpd.h.

13.36.2.63 PchHdaIDispLinkFrequency

```
UINT8 FSP_S_CONFIG::PchHdaIDispLinkFrequency
```

Offset 0x0393 - iDisp-Link Frequency iDisp-Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 4: 96MHz, 3: 48MHz.

4: 96MHz, 3: 48MHz

Definition at line 1382 of file FspsUpd.h.

13.36.2.64 PchHdaIDispLinkTmode

```
UINT8 FSP_S_CONFIG::PchHdaIDispLinkTmode
```

Offset 0x0394 - iDisp-Link T-mode iDisp-Link T-Mode (PCH_HDAUDIO_IDISP_TMODE enum): 0: 2T, 1: 1T.

0: 2T, 1: 1T

Definition at line 1388 of file FspsUpd.h.

13.36.2.65 PchHdaLinkFrequency

```
UINT8 FSP_S_CONFIG::PchHdaLinkFrequency
```

Offset 0x0392 - HD Audio Link Frequency HDA Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 0: 6MHz, 1: 12MHz, 2: 24MHz.

0: 6MHz, 1: 12MHz, 2: 24MHz

Definition at line 1376 of file FspsUpd.h.

13.36.2.66 PchHdaPme

```
UINT8 FSP_S_CONFIG::PchHdaPme
```

Offset 0x0390 - Enable Pme Enable Azalia wake-on-ring.

$EN_DIS

Definition at line 1364 of file FspsUpd.h.

13.36.2.67 PchHdaSndwBufferRcomp

```
UINT8 FSP_S_CONFIG::PchHdaSndwBufferRcomp
```

Offset 0x029F - Soundwire Clock Buffer GPIO RCOMP Setting 0: non-ACT - 50 Ohm driver impedance, 1: ACT - 8 Ohm driver impedance.

$EN_DIS

Definition at line 1112 of file FspsUpd.h.

13.36.2.68 PchHdaSndwLinkIoControlEnabled

```
UINT8 FSP_S_CONFIG::PchHdaSndwLinkIoControlEnabled[4]
```

Offset 0x0758 - Enable HD Audio Sndw Link IO Control 0:Disabled, 1:Enabled.

Enables IO Control to Sndw link if it is Enabled

Definition at line 2463 of file FspsUpd.h.

13.36.2.69 PchHdaVcType

```
UINT8 FSP_S_CONFIG::PchHdaVcType
```

Offset 0x0391 - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.

0: VC0, 1: VC1

Definition at line 1370 of file FspsUpd.h.

13.36.2.70 PchHotEnable

```
UINT8 FSP_S_CONFIG::PchHotEnable
```

Offset 0x02D0 - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.

0: disable, 1: enable $EN_DIS

Definition at line 1248 of file FspsUpd.h.

13.36.2.71 PchIoApicEntry24_119

```
UINT8 FSP_S_CONFIG::PchIoApicEntry24_119
```

Offset 0x03A1 - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1413 of file FspsUpd.h.

13.36.2.72 PchIoApicId

```
UINT8 FSP_S_CONFIG::PchIoApicId
```

Offset 0x03A2 - PCH Io Apic ID This member determines IOAPIC ID.

Default is 0x02.

Definition at line 1418 of file FspsUpd.h.

13.36.2.73 PchIshGp0GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp0GpioAssign
```

Offset 0x03A9 - Enable PCH ISH GP_0 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1460 of file FspsUpd.h.

13.36.2.74 PchIshGp1GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp1GpioAssign
```

Offset 0x03AA - Enable PCH ISH GP_1 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1466 of file FspsUpd.h.

13.36.2.75 PchIshGp2GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp2GpioAssign
```

Offset 0x03AB - Enable PCH ISH GP_2 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1472 of file FspsUpd.h.

13.36.2.76 PchIshGp3GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp3GpioAssign
```

Offset 0x03AC - Enable PCH ISH GP_3 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1478 of file FspsUpd.h.

13.36.2.77 PchIshGp4GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp4GpioAssign
```

Offset 0x03AD - Enable PCH ISH GP_4 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1484 of file FspsUpd.h.

13.36.2.78 PchIshGp5GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp5GpioAssign
```

Offset 0x03AE - Enable PCH ISH GP_5 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1490 of file FspsUpd.h.

13.36.2.79 PchIshGp6GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp6GpioAssign
```

Offset 0x03AF - Enable PCH ISH GP_6 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1496 of file FspsUpd.h.

13.36.2.80 PchIshGp7GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshGp7GpioAssign
```

Offset 0x03B0 - Enable PCH ISH GP_7 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1502 of file FspsUpd.h.

13.36.2.81 PchIshI2c0GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshI2c0GpioAssign
```

Offset 0x03A6 - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1442 of file FspsUpd.h.

13.36.2.82 PchIshI2c1GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshI2c1GpioAssign
```

Offset 0x03A7 - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1448 of file FspsUpd.h.

13.36.2.83 PchIshI2c2GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshI2c2GpioAssign
```

Offset 0x03A8 - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1454 of file FspsUpd.h.

13.36.2.84 PchIshPdtUnlock

```
UINT8 FSP_S_CONFIG::PchIshPdtUnlock
```

Offset 0x03B1 - PCH ISH PDT Unlock Msg 0: False; 1: True.

$EN_DIS

Definition at line 1508 of file FspsUpd.h.

13.36.2.85 PchIshSpiGpioAssign

```
UINT8 FSP_S_CONFIG::PchIshSpiGpioAssign
```

Offset 0x03A3 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1424 of file FspsUpd.h.

13.36.2.86 PchIshUart0GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshUart0GpioAssign
```

Offset 0x03A4 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1430 of file FspsUpd.h.

13.36.2.87 PchIshUart1GpioAssign

```
UINT8 FSP_S_CONFIG::PchIshUart1GpioAssign
```

Offset 0x03A5 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1436 of file FspsUpd.h.

13.36.2.88 PchLanEnable

```
UINT8 FSP_S_CONFIG::PchLanEnable
```

Offset 0x0294 - Enable LAN Enable/disable LAN controller.

$EN_DIS

Definition at line 1046 of file FspsUpd.h.

13.36.2.89 PchLanLtrEnable

```
UINT8 FSP_S_CONFIG::PchLanLtrEnable
```

Offset 0x03B2 - Enable PCH Lan LTR capabilty of PCH internal LAN 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1514 of file FspsUpd.h.

13.36.2.90 PchLegacyIoLowLatency

```
UINT8 FSP_S_CONFIG::PchLegacyIoLowLatency
```

Offset 0x062A - PCH Legacy IO Low Latency Enable Set to enable low latency of legacy IO.

0: Disable, 1: Enable $EN_DIS

Definition at line 1830 of file FspsUpd.h.

13.36.2.91 PchLockDownBiosLock

```
UINT8 FSP_S_CONFIG::PchLockDownBiosLock
```

Offset 0x03B3 - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:RegD↩ Ch[5]) for the BIOS region protection.

$EN_DIS

Definition at line 1521 of file FspsUpd.h.

13.36.2.92 PchLockDownRtcMemoryLock

```
UINT8 FSP_S_CONFIG::PchLockDownRtcMemoryLock
```

Offset 0x03B5 - RTC CMOS MEMORY LOCK Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.

$EN_DIS

Definition at line 1534 of file FspsUpd.h.

13.36.2.93 PchMemoryThrottlingEnable

```
UINT8 FSP_S_CONFIG::PchMemoryThrottlingEnable
```

Offset 0x06C8 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.

$EN_DIS

Definition at line 2268 of file FspsUpd.h.

13.36.2.94 PchPcieDeviceOverrideTablePtr

```
UINT32 FSP_S_CONFIG::PchPcieDeviceOverrideTablePtr
```

Offset 0x06F4 - Pch PCIE device override table pointer The PCIe device table is being used to override PCIe device ASPM settings.

This is a pointer points to a 32bit address. And it's only used in PostMem phase. Please refer to PCH_PCIE_DEVICE_OVERRIDE structure for the table. Last entry VendorId must be 0.

Definition at line 2349 of file FspsUpd.h.

13.36.2.95 PchPmDeepSxPol

```
UINT8 FSP_S_CONFIG::PchPmDeepSxPol
```

Offset 0x0622 - PCH Pm Deep Sx Pol Deep Sx Policy.

$EN_DIS

Definition at line 1776 of file FspsUpd.h.

13.36.2.96 PchPmDisableDsxAcPresentPulldown

```
UINT8 FSP_S_CONFIG::PchPmDisableDsxAcPresentPulldown
```

Offset 0x062F - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRESENT in deep SX and during G3 exit.

$EN_DIS

Definition at line 1860 of file FspsUpd.h.

13.36.2.97 PchPmDisableNativePowerButton

```
UINT8 FSP_S_CONFIG::PchPmDisableNativePowerButton
```

Offset 0x0630 - PCH Pm Disable Native Power Button Power button native mode disable.

$EN_DIS

Definition at line 1866 of file FspsUpd.h.

13.36.2.98 PchPmLanWakeFromDeepSx

```
UINT8 FSP_S_CONFIG::PchPmLanWakeFromDeepSx
```

Offset 0x0621 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.

$EN_DIS

Definition at line 1770 of file FspsUpd.h.

13.36.2.99 PchPmLpcClockRun

```
UINT8 FSP_S_CONFIG::PchPmLpcClockRun
```

Offset 0x062B - PCH Pm Lpc Clock Run This member describes whether or not the LPC ClockRun feature of PCH should be enabled.

Default value is Disabled $EN_DIS

Definition at line 1837 of file FspsUpd.h.

13.36.2.100 PchPmMeWakeSts

```
UINT8 FSP_S_CONFIG::PchPmMeWakeSts
```

Offset 0x0632 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS) register.

$EN_DIS

Definition at line 1878 of file FspsUpd.h.

13.36.2.101 PchPmPciePllSsc

```
UINT8 FSP_S_CONFIG::PchPmPciePllSsc
```

Offset 0x0635 - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.

The default is 0xFF: AUTO - No BIOS override.

Definition at line 1896 of file FspsUpd.h.

13.36.2.102 PchPmPcieWakeFromDeepSx

```
UINT8 FSP_S_CONFIG::PchPmPcieWakeFromDeepSx
```

Offset 0x061E - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.

$EN_DIS

Definition at line 1751 of file FspsUpd.h.

13.36.2.103 PchPmPmeB0S5Dis

```
UINT8 FSP_S_CONFIG::PchPmPmeB0S5Dis
```

Offset 0x0619 - PCH Pm PME_B0_S5_DIS When cleared (default), wake events from PME_B0_STS are allowed in S5 if PME_B0_EN = 1.

$EN_DIS

Definition at line 1721 of file FspsUpd.h.

13.36.2.104 PchPmPwrBtnOverridePeriod

```
UINT8 FSP_S_CONFIG::PchPmPwrBtnOverridePeriod
```

Offset 0x062E - PCH Pm Pwr Btn Override Period PCH power button override period.

000b-4s, 001b-6s, 010b-8s, 011b-10s, 100b-12s, 101b-14s.

Definition at line 1854 of file FspsUpd.h.

13.36.2.105 PchPmPwrCycDur

```
UINT8 FSP_S_CONFIG::PchPmPwrCycDur
```

Offset 0x0634 - PCH Pm Reset Power Cycle Duration Could be customized in the unit of second.

Please refer to EDS for all support settings. 0 is default, 1 is 1 second, 2 is 2 seconds, ...

Definition at line 1890 of file FspsUpd.h.

13.36.2.106 PchPmSlpAMinAssert

```
UINT8 FSP_S_CONFIG::PchPmSlpAMinAssert
```

Offset 0x0626 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.

Default is PchSlpA2s.

Definition at line 1796 of file FspsUpd.h.

13.36.2.107 PchPmSlpLanLowDc

```
UINT8 FSP_S_CONFIG::PchPmSlpLanLowDc
```

Offset 0x062D - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.

$EN_DIS

Definition at line 1849 of file FspsUpd.h.

13.36.2.108 PchPmSlpS0Enable

```
UINT8 FSP_S_CONFIG::PchPmSlpS0Enable
```

Offset 0x0631 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.

$EN_DIS

Definition at line 1872 of file FspsUpd.h.

13.36.2.109 PchPmSlpS0Vm070VSupport

```
UINT8 FSP_S_CONFIG::PchPmSlpS0Vm070VSupport
```

Offset 0x02D4 - SLP_S0 VM 0.70V Support SLP_S0 Voltage Margining 0.70V Support Policy.

0: disable, 1: enable $EN_DIS

Definition at line 1273 of file FspsUpd.h.

13.36.2.110 PchPmSlpS0Vm075VSupport

```
UINT8 FSP_S_CONFIG::PchPmSlpS0Vm075VSupport
```

Offset 0x02D5 - SLP_S0 VM 0.75V Support SLP_S0 Voltage Margining 0.75V Support Policy.

0: disable, 1: enable $EN_DIS

Definition at line 1279 of file FspsUpd.h.

13.36.2.111 PchPmSlpS0VmRuntimeControl

```
UINT8 FSP_S_CONFIG::PchPmSlpS0VmRuntimeControl
```

Offset 0x02D3 - SLP_S0 VM Dynamic Control SLP_S0 Voltage Margining Runtime Control Policy.

0: disable, 1: enable $EN_DIS

Definition at line 1267 of file FspsUpd.h.

13.36.2.112 PchPmSlpS3MinAssert

```
UINT8 FSP_S_CONFIG::PchPmSlpS3MinAssert
```

Offset 0x0623 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.

Default is PchSlpS350ms.

Definition at line 1781 of file FspsUpd.h.

13.36.2.113 PchPmSlpS4MinAssert

```
UINT8 FSP_S_CONFIG::PchPmSlpS4MinAssert
```

Offset 0x0624 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.

Default is PchSlpS44s.

Definition at line 1786 of file FspsUpd.h.

13.36.2.114 PchPmSlpStrchSusUp

```
UINT8 FSP_S_CONFIG::PchPmSlpStrchSusUp
```

Offset 0x062C - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.

$EN_DIS

Definition at line 1843 of file FspsUpd.h.

13.36.2.115 PchPmSlpSusMinAssert

```
UINT8 FSP_S_CONFIG::PchPmSlpSusMinAssert
```

Offset 0x0625 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.

Default is PchSlpSus4s.

Definition at line 1791 of file FspsUpd.h.

13.36.2.116 PchPmVrAlert

```
UINT8 FSP_S_CONFIG::PchPmVrAlert
```

Offset 0x02D2 - VRAlert# Pin When VRAlert# feature pin is enabled and its state is '0', the PMC requests throttling to a T3 Tstate to the PCH throttling unit.

. 0: disable, 1: enable $EN_DIS

Definition at line 1261 of file FspsUpd.h.

13.36.2.117 PchPmWolEnableOverride

```
UINT8 FSP_S_CONFIG::PchPmWolEnableOverride
```

Offset 0x061D - PCH Pm Wol Enable Override Corresponds to the WOL Enable Override bit in the General PM Configuration B (GEN_PMCON_B) register.

$EN_DIS

Definition at line 1745 of file FspsUpd.h.

13.36.2.118 PchPmWolOvrWkSts

```
UINT8 FSP_S_CONFIG::PchPmWolOvrWkSts
```

Offset 0x0633 - PCH Pm WOL_OVR_WK_STS Clear the WOL_OVR_WK_STS bit in the Power and Reset Status (PRSTS) register.

$EN_DIS

Definition at line 1884 of file FspsUpd.h.

13.36.2.119 PchPmWoWlanDeepSxEnable

```
UINT8 FSP_S_CONFIG::PchPmWoWlanDeepSxEnable
```

Offset 0x0620 - PCH Pm WoW lan DeepSx Enable Determine if WLAN wake from DeepSx, corresponds to the DSX_WLAN_PP_EN bit in the PWRM_CFG3 register.

$EN_DIS

Definition at line 1764 of file FspsUpd.h.

13.36.2.120 PchPmWoWlanEnable

```
UINT8 FSP_S_CONFIG::PchPmWoWlanEnable
```

Offset 0x061F - PCH Pm WoW lan Enable Determine if WLAN wake from Sx, corresponds to the HOST_WLAN↩
_PP_EN bit in the PWRM_CFG3 register.

$EN_DIS

Definition at line 1757 of file FspsUpd.h.

13.36.2.121 PchPwrOptEnable

```
UINT8 FSP_S_CONFIG::PchPwrOptEnable
```

Offset 0x0370 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.

$EN_DIS

Definition at line 1333 of file FspsUpd.h.

13.36.2.122 PchScsEmmcHs400TuningRequired

```
UINT8 FSP_S_CONFIG::PchScsEmmcHs400TuningRequired
```

Offset 0x069F - Enable eMMC HS400 Training Deprecated.

$EN_DIS

Definition at line 2055 of file FspsUpd.h.

13.36.2.123 PchSerialIoI2cPadsTermination

```
UINT8 FSP_S_CONFIG::PchSerialIoI2cPadsTermination[6]
```

Offset 0x019B - PCH SerialIo I2C Pads Termination 0x0: Hardware default, 0x1: None, 0x13: 1kOhm weak pull-up, 0x15: 5kOhm weak pull-up, 0x19: 20kOhm weak pull-up - Enable/disable SerialIo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5 pads termination respectively.

One byte for each controller, byte0 for I2C0, byte1 for I2C1, and so on.

Definition at line 765 of file FspsUpd.h.

13.36.2.124 PchSirqEnable

```
UINT8 FSP_S_CONFIG::PchSirqEnable
```

Offset 0x06A4 - Enable Serial IRQ Determines if enable Serial IRQ.

$EN_DIS

Definition at line 2083 of file FspsUpd.h.

13.36.2.125 PchSirqMode

```
UINT8 FSP_S_CONFIG::PchSirqMode
```

Offset 0x06A5 - Serial IRQ Mode Select Serial IRQ Mode Select, 0: quiet mode, 1: continuous mode.

$EN_DIS

Definition at line 2089 of file FspsUpd.h.

13.36.2.126 PchStartFramePulse

```
UINT8 FSP_S_CONFIG::PchStartFramePulse
```

Offset 0x06A6 - Start Frame Pulse Width Start Frame Pulse Width, 0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: Pch←Sfpw8Clk.

0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: PchSfpw8Clk

Definition at line 2095 of file FspsUpd.h.

13.36.2.127 PchTsmicLock

```
UINT8 FSP_S_CONFIG::PchTsmicLock
```

Offset 0x06A8 - Thermal Device SMI Enable This locks down SMI Enable on Alert Thermal Sensor Trip.

$EN_DIS

Definition at line 2108 of file FspsUpd.h.

13.36.2.128 PchTTEnable

```
UINT8 FSP_S_CONFIG::PchTTEnable
```

Offset 0x06B0 - Enable The Thermal Throttle Enable the thermal throttle function.

$EN_DIS

Definition at line 2133 of file FspsUpd.h.

13.36.2.129 PchTTLock

```
UINT8 FSP_S_CONFIG::PchTTLock
```

Offset 0x06B2 - Thermal Throttle Lock Thermal Throttle Lock.

$EN_DIS

Definition at line 2146 of file FspsUpd.h.

13.36.2.130 PchTTState13Enable

```
UINT8 FSP_S_CONFIG::PchTTState13Enable
```

Offset 0x06B1 - PMSync State 13 When set to 1 and the programmed GPIO pin is a 1, then PMSync state 13 will force at least T2 state.

$EN_DIS

Definition at line 2140 of file FspsUpd.h.

13.36.2.131 PchUsbHsioFilterSel

```
UINT8 FSP_S_CONFIG::PchUsbHsioFilterSel[10]
```

Offset 0x0397 - USB LFPS Filter selection For each byte bits 2:0 are for p, bits 4:6 are for n.

0h:1.6ns, 1h:2.4ns, 2h:3.2ns, 3h:4.0ns, 4h:4.8ns, 5h:5.6ns, 6h:6.4ns.

Definition at line 1407 of file FspsUpd.h.

13.36.2.132 PchUsbHsioRxTuningEnable

```
UINT8 FSP_S_CONFIG::PchUsbHsioRxTuningEnable[10]
```

Offset 0x0510 - PCH USB3 HSIO Rx Tuning Enable Mask for enabling tuning of HSIO Rx signals of USB3 ports.

Bits: 0 - HsioCtrlAdaptOffsetCfgEnable, 1 - HsioFilterSelNEnable, 2 - HsioFilterSelPEnable, 3 - HsioOlfpsCfgPull↩UpDwnResEnable, 4 - HsioCtrlCompMultEnable

Definition at line 1617 of file FspsUpd.h.

13.36.2.133 PcieComplianceTestMode

```
UINT8 FSP_S_CONFIG::PcieComplianceTestMode
```

Offset 0x0616 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

$EN_DIS

Definition at line 1702 of file FspsUpd.h.

13.36.2.134 PcieDisableRootPortClockGating

```
UINT8 FSP_S_CONFIG::PcieDisableRootPortClockGating
```

Offset 0x0614 - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.

0: Disable; 1: Enable. $EN_DIS

Definition at line 1690 of file FspsUpd.h.

13.36.2.135 PcieEnablePeerMemoryWrite

```
UINT8 FSP_S_CONFIG::PcieEnablePeerMemoryWrite
```

Offset 0x0615 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

$EN_DIS

Definition at line 1696 of file FspsUpd.h.

13.36.2.136 PcieEqPh3LaneParamCm

```
UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCm[24]
```

Offset 0x05DA - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.

Coefficient C-1.

Definition at line 1666 of file FspsUpd.h.

13.36.2.137 PcieEqPh3LaneParamCp

```
UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCp[24]
```

Offset 0x05F2 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.

Coefficient C+1.

Definition at line 1671 of file FspsUpd.h.

13.36.2.138 PcieRpAspm

```
UINT8 FSP_S_CONFIG::PcieRpAspm[24]
```

Offset 0x057A - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 1645 of file FspsUpd.h.

13.36.2.139 PcieRpCompletionTimeout

```
UINT8 FSP_S_CONFIG::PcieRpCompletionTimeout[24]
```

Offset 0x0562 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_TIMEOUT).

Default is PchPcieCompletionTO_Default.

Definition at line 1639 of file FspsUpd.h.

13.36.2.140 PcieRpDpcExtensionsMask

```
UINT32 FSP_S_CONFIG::PcieRpDpcExtensionsMask
```

Offset 0x02A8 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 1130 of file FspsUpd.h.

13.36.2.141 PcieRpDpcMask

```
UINT32 FSP_S_CONFIG::PcieRpDpcMask
```

Offset 0x02A4 - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 1124 of file FspsUpd.h.

13.36.2.142 PcieRpFunctionSwap

```
UINT8 FSP_S_CONFIG::PcieRpFunctionSwap
```

Offset 0x0617 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.

$EN_DIS

Definition at line 1709 of file FspsUpd.h.

13.36.2.143 PcieRpGen3EqPh3Method

```
UINT8 FSP_S_CONFIG::PcieRpGen3EqPh3Method[24]
```

Offset 0x0532 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_M↩ETHOD).

0: DEPRECATED, hardware equalization; 1: hardware equalization; 4: Fixed Coeficients.

Definition at line 1629 of file FspsUpd.h.

13.36.2.144 PcieRpImrEnabled

```
UINT8 FSP_S_CONFIG::PcieRpImrEnabled
```

Offset 0x061A - PCIE IMR Enables Isolated Memory Region for PCIe.

$EN_DIS

Definition at line 1727 of file FspsUpd.h.

13.36.2.145 PcieRpL1Substates

```
UINT8 FSP_S_CONFIG::PcieRpL1Substates[24]
```

Offset 0x0592 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUBSTATES_CONTROL).

Default is PchPcieL1SubstatesL1_1_2.

Definition at line 1651 of file FspsUpd.h.

13.36.2.146 PcieRpPcieSpeed

```
UINT8 FSP_S_CONFIG::PcieRpPcieSpeed[24]
```

Offset 0x051A - PCIE RP Pcie Speed Determines each PCIE Port speed capability.

0: Auto; 1: Gen1; 2: Gen2; 3: Gen3 (see: PCH_PCIE_SPEED).

Definition at line 1623 of file FspsUpd.h.

13.36.2.147 PcieRpPhysicalSlotNumber

```
UINT8 FSP_S_CONFIG::PcieRpPhysicalSlotNumber[24]
```

Offset 0x054A - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 1634 of file FspsUpd.h.

13.36.2.148 PcieRpPtmMask

```
UINT32 FSP_S_CONFIG::PcieRpPtmMask
```

Offset 0x02A0 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 1118 of file FspsUpd.h.

13.36.2.149 PcieSwEqCoeffListCm

```
UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCm[5]
```

Offset 0x060A - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.

Coefficient C-1. The values depend on PcieNumOfCoefficients, the default value of PcieNumOfCoefficients is 3 hence only first 3 values are considered.

Definition at line 1677 of file FspsUpd.h.

13.36.2.150 PcieSwEqCoeffListCp

```
UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCp[5]
```

Offset 0x060F - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

Coefficient C+1.The values depend on PcieNumOfCoefficients, the default value of PcieNumOfCoefficients is 3 hence only first 3 values are considered.

Definition at line 1683 of file FspsUpd.h.

13.36.2.151 PmcCpuC10GatePinEnable

```
UINT8 FSP_S_CONFIG::PmcCpuC10GatePinEnable
```

Offset 0x06FA - Pmc Cpu C10 Gate Pin Enable Enable/Disable platform support for CPU_C10_GATE# pin to control gating of CPU VccIO and VccSTG rails instead of SLP_S0# pin.

$EN_DIS

Definition at line 2372 of file FspsUpd.h.

13.36.2.152 PmcDbgMsgEn

```
UINT8 FSP_S_CONFIG::PmcDbgMsgEn
```

Offset 0x02BC - PMC Debug Message Enable When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug meesages to trace hub.

Noted: When Enabled, may not enter S0ix $EN_DIS

Definition at line 1177 of file FspsUpd.h.

13.36.2.153 PmcModPhySusPgEnable

```
UINT8 FSP_S_CONFIG::PmcModPhySusPgEnable
```

Offset 0x036E - ModPHY SUS Power Domain Dynamic Gating Enable/Disable ModPHY SUS Power Domain Dynamic Gating.

Setting not supported on PCH-H. 0: disable, 1: enable $EN_DIS

Definition at line 1320 of file FspsUpd.h.

13.36.2.154 PmcPowerButtonDebounce

```
UINT32 FSP_S_CONFIG::PmcPowerButtonDebounce
```

Offset 0x02B0 - Power button debounce configuration Debounce time for PWRBTN in microseconds.

For values not supported by HW, they will be rounded down to closest supported on. 0: disable, 250-1024000us: supported range

Definition at line 1147 of file FspsUpd.h.

13.36.2.155 PortUsb20Enable

```
UINT8 FSP_S_CONFIG::PortUsb20Enable[16]
```

Offset 0x01E6 - Enable USB2 ports Enable/disable per USB2 ports.

One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 885 of file FspsUpd.h.

13.36.2.156 PortUsb30Enable

```
UINT8 FSP_S_CONFIG::PortUsb30Enable[10]
```

Offset 0x01F6 - Enable USB3 ports Enable/disable per USB3 ports.

One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 891 of file FspsUpd.h.

13.36.2.157 PreWake

```
UINT8 FSP_S_CONFIG::PreWake
```

Offset 0x0168 - Pre Wake Randomization time PCODE MMIO Mailbox: Acoustic Migitation Range.Defines the maximum pre-wake randomization time in micro ticks.This can be programmed only if AcousticNoiseMigitation is enabled.

Range 0-255 **0**.

Definition at line 655 of file FspsUpd.h.

13.36.2.158 Psi1Threshold

```
UINT16 FSP_S_CONFIG::Psi1Threshold[5]
```

Offset 0x0112 - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cuttof in 1/4 Amp increments.

Range is 0-128A.

Definition at line 512 of file FspsUpd.h.

13.36.2.159 Psi2Threshold

```
UINT16 FSP_S_CONFIG::Psi2Threshold[5]
```

Offset 0x011C - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cuttof in 1/4 Amp increments.

Range is 0-128A.

Definition at line 517 of file FspsUpd.h.

13.36.2.160 Psi3Enable

```
UINT8 FSP_S_CONFIG::Psi3Enable[5]
```

Offset 0x00C4 - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; **1: Enable**.

For all VR Indexes

Definition at line 396 of file FspsUpd.h.

13.36.2.161 Psi3Threshold

```
UINT16 FSP_S_CONFIG::Psi3Threshold[5]
```

Offset 0x0126 - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cuttof in 1/4 Amp increments.

Range is 0-128A.

Definition at line 522 of file FspsUpd.h.

13.36.2.162 PsOnEnable

```
UINT8 FSP_S_CONFIG::PsOnEnable
```

Offset 0x06F9 - Enable PS_ON.

PS_ON is a new C10 state from the CPU on desktop SKUs that enables a lower power target that will be required by the California Energy Commission (CEC). When FALSE, PS_ON is to be disabled. $EN_DIS

Definition at line 2365 of file FspsUpd.h.

13.36.2.163 PsysOffset

```
UINT8 FSP_S_CONFIG::PsysOffset
```

Offset 0x00ED - Platform Psys offset correction PCODE MMIO Mailbox: Platform Psys offset correction.

0 - Auto Units 1/4, Range 0-255. Value of 100 = 100/4 = 25 offset

Definition at line 449 of file FspsUpd.h.

13.36.2.164 PsysSlope

```
UINT8 FSP_S_CONFIG::PsysSlope
```

Offset 0x00EC - Platform Psys slope correction PCODE MMIO Mailbox: Platform Psys slope correction.

0 - Auto Specified in 1/100 increment values. Range is 0-200. 125 = 1.25

Definition at line 443 of file FspsUpd.h.

13.36.2.165 PxRcConfig

```
UINT8 FSP_S_CONFIG::PxRcConfig[8]
```

Offset 0x0209 - PIRQx to IRQx Map Config PIRQx to IRQx mapping.

The valid value is 0x00 to 0x0F for each. First byte is for PIRQA, second byte is for PIRQB, and so on. The setting is only available in Legacy 8259 PCI mode.

Definition at line 919 of file FspsUpd.h.

13.36.2.166 RemoteAssistance

```
UINT8 FSP_S_CONFIG::RemoteAssistance
```

Offset 0x0046 - Remote Assistance Trigger Availablilty Enable/Disable.

0: Disable, 1: enable, Remote Assistance enable/disable state by Mebx. $EN_DIS

Definition at line 199 of file FspsUpd.h.

13.36.2.167 SataEnable

```
UINT8 FSP_S_CONFIG::SataEnable
```

Offset 0x021D - Enable SATA Enable/disable SATA controller.

$EN_DIS

Definition at line 965 of file FspsUpd.h.

13.36.2.168 SataLedEnable

```
UINT8 FSP_S_CONFIG::SataLedEnable
```

Offset 0x02D1 - SATA LED SATA LED indicating SATA controller activity.

0: disable, 1: enable $EN_DIS

Definition at line 1254 of file FspsUpd.h.

13.36.2.169 SataMode

```
UINT8 FSP_S_CONFIG::SataMode
```

Offset 0x021E - SATA Mode Select SATA controller working mode.

0:AHCI, 1:RAID

Definition at line 971 of file FspsUpd.h.

13.36.2.170 SataP0TDispFinit

```
UINT8 FSP_S_CONFIG::SataP0TDispFinit
```

Offset 0x06C4 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.

$EN_DIS

Definition at line 2245 of file FspsUpd.h.

13.36.2.171 SataP1TDispFinit

```
UINT8 FSP_S_CONFIG::SataP1TDispFinit
```

Offset 0x06C6 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.

$EN_DIS

Definition at line 2256 of file FspsUpd.h.

13.36.2.172 SataPortsDevSlp

```
UINT8 FSP_S_CONFIG::SataPortsDevSlp[8]
```

Offset 0x01DE - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.

0 is disable, 1 is enable. One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 879 of file FspsUpd.h.

13.36.2.173 SataPortsDevSlpResetConfig

```
UINT8 FSP_S_CONFIG::SataPortsDevSlpResetConfig[8]
```

Offset 0x074F - Set SATA DEVSLP GPIO Reset Config Set SATA DEVSLP GPIO Reset Config per port.

0x00 - GpioResetDefault, 0x01 - GpioResumeReset, 0x03 - GpioHostDeepReset, 0x05 - GpioPlatformReset, 0x07 - GpioDswReset. One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 2451 of file FspsUpd.h.

13.36.2.174 SataPortsDmVal

```
UINT8 FSP_S_CONFIG::SataPortsDmVal[8]
```

Offset 0x0669 - Enable SATA Port DmVal DITO multiplier.

Default is 15.

Definition at line 1948 of file FspsUpd.h.

13.36.2.175 SataPortsEnable

```
UINT8 FSP_S_CONFIG::SataPortsEnable[8]
```

Offset 0x01D6 - Enable SATA ports Enable/disable SATA ports.

One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 873 of file FspsUpd.h.

13.36.2.176 SataPwrOptEnable

```
UINT8 FSP_S_CONFIG::SataPwrOptEnable
```

Offset 0x0636 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.

$EN_DIS

Definition at line 1902 of file FspsUpd.h.

13.36.2.177 SataRstHddUnlock

```
UINT8 FSP_S_CONFIG::SataRstHddUnlock
```

Offset 0x0692 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.

$EN_DIS

Definition at line 2015 of file FspsUpd.h.

13.36.2.178 SataRstInterrupt

```
UINT8 FSP_S_CONFIG::SataRstInterrupt
```

Offset 0x07BA - SATA RST Interrupt Mode Allowes to choose which interrupts will be implemented by SATA controller in RAID mode.

0:Msix, 1:Msi, 2:Legacy

Definition at line 2554 of file FspsUpd.h.

13.36.2.179 SataRstIrrt

```
UINT8 FSP_S_CONFIG::SataRstIrrt
```

Offset 0x068F - PCH Sata Rst Irrt Intel Rapid Recovery Technology.

$EN_DIS

Definition at line 1998 of file FspsUpd.h.

13.36.2.180 SataRstIrrtOnly

```
UINT8 FSP_S_CONFIG::SataRstIrrtOnly
```

Offset 0x0694 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.

$EN_DIS

Definition at line 2028 of file FspsUpd.h.

13.36.2.181 SataRstLedLocate

```
UINT8 FSP_S_CONFIG::SataRstLedLocate
```

Offset 0x0693 - PCH Sata Rst Led Locate Indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

$EN_DIS

Definition at line 2022 of file FspsUpd.h.

13.36.2.182 SataRstOromUiBanner

```
UINT8 FSP_S_CONFIG::SataRstOromUiBanner
```

Offset 0x0690 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.

$EN_DIS

Definition at line 2004 of file FspsUpd.h.

13.36.2.183 SataRstPcieDeviceResetDelay

```
UINT8 FSP_S_CONFIG::SataRstPcieDeviceResetDelay[3]
```

Offset 0x069C - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.

Default value is 100ms

Definition at line 2049 of file FspsUpd.h.

13.36.2.184 SataRstRaid0

```
UINT8 FSP_S_CONFIG::SataRstRaid0
```

Offset 0x068B - PCH Sata Rst Raid0 RAID0.

$EN_DIS

Definition at line 1974 of file FspsUpd.h.

13.36.2.185 SataRstRaid1

```
UINT8 FSP_S_CONFIG::SataRstRaid1
```

Offset 0x068C - PCH Sata Rst Raid1 RAID1.

$EN_DIS

Definition at line 1980 of file FspsUpd.h.

13.36.2.186 SataRstRaid10

```
UINT8 FSP_S_CONFIG::SataRstRaid10
```

Offset 0x068D - PCH Sata Rst Raid10 RAID10.

$EN_DIS

Definition at line 1986 of file FspsUpd.h.

13.36.2.187 SataRstRaid5

```
UINT8 FSP_S_CONFIG::SataRstRaid5
```

Offset 0x068E - PCH Sata Rst Raid5 RAID5.

$EN_DIS

Definition at line 1992 of file FspsUpd.h.

13.36.2.188 SataRstRaidDeviceId

```
UINT8 FSP_S_CONFIG::SataRstRaidDeviceId
```

Offset 0x068A - PCH Sata Rst Raid Device Id Enable RAID Alternate ID.

0:Client, 1:Alternate, 2:Server

Definition at line 1968 of file FspsUpd.h.

13.36.2.189 SataRstSmartStorage

```
UINT8 FSP_S_CONFIG::SataRstSmartStorage
```

Offset 0x0695 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.

$EN_DIS

Definition at line 2034 of file FspsUpd.h.

13.36.2.190 SataSalpSupport

```
UINT8 FSP_S_CONFIG::SataSalpSupport
```

Offset 0x01D5 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.

$EN_DIS

Definition at line 867 of file FspsUpd.h.

13.36.2.191 SataThermalSuggestedSetting

```
UINT8 FSP_S_CONFIG::SataThermalSuggestedSetting
```

Offset 0x06C7 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.

$EN_DIS

Definition at line 2262 of file FspsUpd.h.

13.36.2.192 SciIrqSelect

```
UINT8 FSP_S_CONFIG::SciIrqSelect
```

Offset 0x0212 - Select SciIrqSelect SCI IRQ Select.

The valid value is 9, 10, 11, and 20, 21, 22, 23 for APIC only.

Definition at line 929 of file FspsUpd.h.

13.36.2.193 ScsEmmcEnabled

```
UINT8 FSP_S_CONFIG::ScsEmmcEnabled
```

Offset 0x01D1 - Enable eMMC Controller Enable/disable eMMC Controller.

$EN_DIS

Definition at line 843 of file FspsUpd.h.

13.36.2.194 ScsEmmcHs400Enabled

```
UINT8 FSP_S_CONFIG::ScsEmmcHs400Enabled
```

Offset 0x01D2 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.

$EN_DIS

Definition at line 849 of file FspsUpd.h.

13.36.2.195 ScsSdCardEnabled

```
UINT8 FSP_S_CONFIG::ScsSdCardEnabled
```

Offset 0x01D3 - Enable SdCard Controller Enable/disable SD Card Controller.

$EN_DIS

Definition at line 855 of file FspsUpd.h.

13.36.2.196 ScsSdCardWpPinEnabled

```
UINT8 FSP_S_CONFIG::ScsSdCardWpPinEnabled
```

Offset 0x074E - Enable SD Card Write Protect Pin Enable/disable SD Card Write Protect Pin.

$EN_DIS

Definition at line 2444 of file FspsUpd.h.

13.36.2.197 ScsUfsEnabled

```
UINT8 FSP_S_CONFIG::ScsUfsEnabled
```

Offset 0x02C8 - Enable Ufs Controller Enable/disable Ufs 2.0 Controller.

$EN_DIS

Definition at line 1197 of file FspsUpd.h.

13.36.2.198 SendEcCmd

```
UINT64 FSP_S_CONFIG::SendEcCmd
```

Offset 0x0790 - SendEcCmd SendEcCmd function pointer.

```
 typedef EFI_STATUS (EFIAPI *PLATFORM_SEND_EC_COMMAND) (IN EC_COMMAND_TYPE
EcCmdType, IN UINT8  EcCmd, IN UINT8  SendData, IN OUT UINT8  *ReceiveData);
```

Definition at line 2499 of file FspsUpd.h.

13.36.2.199 SendVrMbxCmd

```
UINT8 FSP_S_CONFIG::SendVrMbxCmd
```

Offset 0x0146 - Enable VR specific mailbox command VR specific mailbox commands.

00b - no VR specific command sent. 01b - A VR mailbox command specifically for the MPS IMPV8 VR will be sent. 10b - VR specific command sent for PS4 exit issue. 11b - Reserved. $EN_DIS

Definition at line 554 of file FspsUpd.h.

13.36.2.200 SerialIoDebugUartNumber

```
UINT8 FSP_S_CONFIG::SerialIoDebugUartNumber
```

Offset 0x01CD - UART Number For Debug Purpose UART number for debug purpose.

0:UART0, 1: UART1, 2:UART2. Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:UART0, 1:UART1, 2:UART2

Definition at line 831 of file FspsUpd.h.

13.36.2.201 SerialIoI2cMode

```
UINT8 FSP_S_CONFIG::SerialIoI2cMode[6]
```

Offset 0x01A1 - I2Cn Device Mode Selects I2c operation mode.

N represents controller index: I2c0, I2c1, ... Available modes: 0:SerialIoI2cDisabled, 1:SerialIoI2cPci, 2:SerialIo↩ I2cHidden

Definition at line 771 of file FspsUpd.h.

13.36.2.202 SerialIoSpi0CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi0CsEnable[2]
```

Offset 0x018F - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 735 of file FspsUpd.h.

13.36.2.203 SerialIoSpi0CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi0CsPolarity[2]
```

Offset 0x0189 - SPI0 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 718 of file FspsUpd.h.

13.36.2.204 SerialIoSpi1CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsEnable[2]
```

Offset 0x0191 - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 740 of file FspsUpd.h.

13.36.2.205 SerialIoSpi1CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsPolarity[2]
```

Offset 0x018B - SPI1 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 724 of file FspsUpd.h.

13.36.2.206 SerialIoSpi2CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi2CsEnable[2]
```

Offset 0x0193 - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 745 of file FspsUpd.h.

13.36.2.207 SerialIoSpi2CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi2CsPolarity[2]
```

Offset 0x018D - SPI2 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 730 of file FspsUpd.h.

13.36.2.208 SerialIoSpiDefaultCsOutput

```
UINT8 FSP_S_CONFIG::SerialIoSpiDefaultCsOutput[3]
```

Offset 0x0198 - SPIn Default Chip Select Output Sets Default CS as Output.

N represents controller index: SPI0, SPI1, ... Available options: 0:CS0, 1:CS1

Definition at line 757 of file FspsUpd.h.

13.36.2.209 SerialIoSpiMode

```
UINT8 FSP_S_CONFIG::SerialIoSpiMode[3]
```

Offset 0x0195 - SPIn Device Mode Selects SPI operation mode.

N represents controller index: SPI0, SPI1, ... Available modes: 0:SerialIoSpiDisabled, 1:SerialIoSpiPci, 2:Serial↩ IoSpiHidden

Definition at line 751 of file FspsUpd.h.

13.36.2.210 SerialIoUartDataBits

```
UINT8 FSP_S_CONFIG::SerialIoUartDataBits[3]
```

Offset 0x01BB - Default DataBits for each Serial IO UART Set default word length.

0: Default, 5,6,7,8

Definition at line 797 of file FspsUpd.h.

13.36.2.211 SerialIoUartDmaEnable

```
UINT8 FSP_S_CONFIG::SerialIoUartDmaEnable[3]
```

Offset 0x01C4 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.

0: Disabled, 1: Enabled

Definition at line 813 of file FspsUpd.h.

13.36.2.212 SerialIoUartMode

```
UINT8 FSP_S_CONFIG::SerialIoUartMode[3]
```

Offset 0x01A7 - UARTn Device Mode Selects Uart operation mode.

N represents controller index: Uart0, Uart1, ... Available modes: 0:SerialIoUartDisabled, 1:SerialIoUartPci, 2↩ :SerialIoUartHidden, 3:SerialIoUartCom, 4:SerialIoUartSkipInit

Definition at line 778 of file FspsUpd.h.

13.36.2.213 SerialIoUartParity

```
UINT8 FSP_S_CONFIG::SerialIoUartParity[3]
```

Offset 0x01B8 - Default ParityType for each Serial IO UART Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 792 of file FspsUpd.h.

13.36.2.214 SerialIoUartPowerGating

```
UINT8 FSP_S_CONFIG::SerialIoUartPowerGating[3]
```

Offset 0x01C1 - Power Gating mode for each Serial IO UART that works in COM mode Set Power Gating.

0: Disabled, 1: Enabled, 2: Auto

Definition at line 808 of file FspsUpd.h.

13.36.2.215 SerialIoUartStopBits

```
UINT8 FSP_S_CONFIG::SerialIoUartStopBits[3]
```

Offset 0x01BE - Default StopBits for each Serial IO UART Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 803 of file FspsUpd.h.

13.36.2.216 ShowSpiController

```
UINT8 FSP_S_CONFIG::ShowSpiController
```

Offset 0x01D4 - Show SPI controller Enable/disable to show SPI controller.

$EN_DIS

Definition at line 861 of file FspsUpd.h.

13.36.2.217 SiCsmFlag

```
UINT8 FSP_S_CONFIG::SiCsmFlag
```

Offset 0x07B1 - Si Config CSM Flag.

Platform specific common policies that used by several silicon components. CSM status flag. $EN_DIS

Definition at line 2534 of file FspsUpd.h.

13.36.2.218 SiNumberOfSsidTableEntry

```
UINT16 FSP_S_CONFIG::SiNumberOfSsidTableEntry
```

Offset 0x07B8 - Number of ssid table.

SiNumberOfSsidTableEntry should match the table entries created in SiSsidTablePtr.

Definition at line 2548 of file FspsUpd.h.

13.36.2.219 SiSsidTablePtr

```
UINT32 FSP_S_CONFIG::SiSsidTablePtr
```

Offset 0x07B4 - SVID SDID table Poniter.

The address of the table of SVID SDID to customize each SVID SDID entry.

Definition at line 2543 of file FspsUpd.h.

13.36.2.220 SkipMpInitDeprecated

```
UINT8 FSP_S_CONFIG::SkipMpInitDeprecated
```

Offset 0x0149 - Deprecated DO NOT USE Skip Multi-Processor Initialization.

Deprecated SkipMpInit has been moved to FspmUpd $EN_DIS

Definition at line 571 of file FspsUpd.h.

13.36.2.221 SlowSlewRateForFivr

```
UINT8 FSP_S_CONFIG::SlowSlewRateForFivr
```

Offset 0x0151 - Slew Rate configuration for Deep Package C States for VR FIVR domain Slew Rate configuration for Deep Package C States for VR FIVR domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 616 of file FspsUpd.h.

13.36.2.222 SlowSlewRateForGt

```
UINT8 FSP_S_CONFIG::SlowSlewRateForGt
```

Offset 0x00F1 - Slew Rate configuration for Deep Package C States for VR GT domain Slew Rate configuration for Deep Package C States for VR GT domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 478 of file FspsUpd.h.

13.36.2.223 SlowSlewRateForIa

```
UINT8 FSP_S_CONFIG::SlowSlewRateForIa
```

Offset 0x00F0 - Slew Rate configuration for Deep Package C States for VR IA domain Slew Rate configuration for Deep Package C States for VR IA domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 471 of file FspsUpd.h.

13.36.2.224 SlowSlewRateForSa

```
UINT8 FSP_S_CONFIG::SlowSlewRateForSa
```

Offset 0x00F2 - Slew Rate configuration for Deep Package C States for VR SA domain Slew Rate configuration for Deep Package C States for VR SA domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 485 of file FspsUpd.h.

13.36.2.225 SlpS0DisQForDebug

```
UINT8 FSP_S_CONFIG::SlpS0DisQForDebug
```

Offset 0x0628 - S0ix Override Settings Select 'Auto', it will be auto-configured according to probe type.

'No Change' will keep PMC default settings. Or select the desired debug probe type for S0ix Override settings.
Reminder: DCI OOB (aka BSSB) uses CCA probe.
Note: This BIOS option should keep 'Auto', other options are intended for advanced configuration only. 0:No Change, 1:DCI OOB, 2:USB2 DbC, 3:Auto

Definition at line 1817 of file FspsUpd.h.

13.36.2.226 SlpS0Override

```
UINT8 FSP_S_CONFIG::SlpS0Override
```

Offset 0x0627 - SLP_S0# Override Select 'Auto', it will be auto-configured according to probe type.

Select 'Enabled' will disable SLP_S0# assertion whereas 'Disabled' will enable SLP_S0# assertion when debug is enabled.
Note: This BIOS option should keep 'Auto', other options are intended for advanced configuration only. 0:Disabled, 1:Enabled, 2:Auto

Definition at line 1806 of file FspsUpd.h.

13.36.2.227 SlpS0WithGbeSupport

```
UINT8 FSP_S_CONFIG::SlpS0WithGbeSupport
```

Offset 0x036F - SlpS0WithGbeSupport Enable/Disable SLP_S0 with GBE Support.

Default is 0 for PCH-LP, WHL V0 Stepping CPU and 1 for PCH-H Series. 0: Disable, 1: Enable $EN_DIS

Definition at line 1327 of file FspsUpd.h.

13.36.2.228 SpiFlashCfgLockDown

```
UINT8 FSP_S_CONFIG::SpiFlashCfgLockDown
```

Offset 0x0757 - Flash Configuration Lock Down Enable/disable flash lock down.

If platform decides to skip this programming, it must lock SPI flash register DLOCK, FLOCKDN, and WRSDIS before end of post. $EN_DIS

Definition at line 2458 of file FspsUpd.h.

13.36.2.229 TcoIrqSelect

```
UINT8 FSP_S_CONFIG::TcoIrqSelect
```

Offset 0x0213 - Select TcoIrqSelect TCO IRQ Select.

The valid value is 9, 10, 11, 20, 21, 22, 23.

Definition at line 934 of file FspsUpd.h.

13.36.2.230 TdcPowerLimit

```
UINT16 FSP_S_CONFIG::TdcPowerLimit[5]
```

Offset 0x00F4 - Thermal Design Current current limit PCODE MMIO Mailbox: Thermal Design Current current limit.

Specified in 1/8A units. Range is 0-4095. 1000 = 125A. **0: Auto**. For all VR Indexes

Definition at line 495 of file FspsUpd.h.

13.36.2.231 TdcTimeWindow

```
UINT8 FSP_S_CONFIG::TdcTimeWindow[5]
```

Offset 0x00E2 - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.

Defined in milli seconds. Valid Values 1 - 1ms , 2 - 2ms , 3 - 3ms , 4 - 4ms , 5 - 5ms , 6 - 6ms , 7 - 7ms , 8 - 8ms , 10 - 10ms.For all VR Indexe

Definition at line 431 of file FspsUpd.h.

13.36.2.232 TetonGlacierCR

```
UINT8 FSP_S_CONFIG::TetonGlacierCR
```

Offset 0x0618 - Teton Glacier Cycle Router Specify to which cycle router Teton Glacier is connected, it is valid only when Teton Glacier support is enabled.

Default is 0 for CNP-H system and 1 for CNP-LP system

Definition at line 1715 of file FspsUpd.h.

13.36.2.233 TetonGlacierMode

```
UINT8 FSP_S_CONFIG::TetonGlacierMode
```

Offset 0x061C - Teton Glacier Detection and Configuration Mode Enables support for Teton Glacier hybrid storage device.

0: Disabled; 1: Dynamic Configuration. Default is 0: Disabled 0: Disabled, 1: Dynamic Configuration

Definition at line 1739 of file FspsUpd.h.

13.36.2.234 TTSuggestedSetting

```
UINT8 FSP_S_CONFIG::TTSuggestedSetting
```

Offset 0x06B3 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.

$EN_DIS

Definition at line 2152 of file FspsUpd.h.

13.36.2.235 TurboMode

```
UINT8 FSP_S_CONFIG::TurboMode
```

Offset 0x0038 - Turbo Mode Enable/Disable Turbo mode.

0: disable, 1: enable $EN_DIS

Definition at line 127 of file FspsUpd.h.

13.36.2.236 TxtEnable

```
UINT8 FSP_S_CONFIG::TxtEnable
```

Offset 0x0148 - Enable or Disable TXT Enable or Disable TXT; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 565 of file FspsUpd.h.

13.36.2.237 Usb2AfePehalfbit

```
UINT8 FSP_S_CONFIG::Usb2AfePehalfbit[16]
```

Offset 0x024F - USB Per Port Half Bit Pre-emphasis USB Per Port Half Bit Pre-emphasis.

1b - half-bit pre-emphasis, 0b - full-bit pre-emphasis. One byte for each port.

Definition at line 995 of file FspsUpd.h.

13.36.2.238 Usb2AfePetxiset

```
UINT8 FSP_S_CONFIG::Usb2AfePetxiset[16]
```

Offset 0x021F - USB Per Port HS Preemphasis Bias USB Per Port HS Preemphasis Bias.

000b-0mV, 001b-11.25mV, 010b-16.9mV, 011b-28.15mV, 100b-28.15mV, 101b-39.35mV, 110b-45mV, 111b-56.3mV. One byte for each port.

Definition at line 977 of file FspsUpd.h.

13.36.2.239 Usb2AfePredeemp

```
UINT8 FSP_S_CONFIG::Usb2AfePredeemp[16]
```

Offset 0x023F - USB Per Port HS Transmitter Emphasis USB Per Port HS Transmitter Emphasis.

00b - Emphasis OFF, 01b - De-emphasis ON, 10b - Pre-emphasis ON, 11b - Pre-emphasis & De-emphasis ON. One byte for each port.

Definition at line 989 of file FspsUpd.h.

13.36.2.240 Usb2AfeTxiset

```
UINT8 FSP_S_CONFIG::Usb2AfeTxiset[16]
```

Offset 0x022F - USB Per Port HS Transmitter Bias USB Per Port HS Transmitter Bias.

000b-0mV, 001b-11.25mV, 010b-16.9mV, 011b-28.15mV, 100b-28.15mV, 101b-39.35mV, 110b-45mV, 111b-56.3mV, One byte for each port.

Definition at line 983 of file FspsUpd.h.

13.36.2.241 Usb3HsioTxDeEmph

```
UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmph[10]
```

Offset 0x0269 - USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting USB 3.0 TX Output -3.5dB De-↩ Emphasis Adjustment Setting, HSIO_TX_DWORD5[21:16], **Default = 29h** (approximately -3.5dB De-Emphasis).

One byte for each port.

Definition at line 1007 of file FspsUpd.h.

13.36.2.242 Usb3HsioTxDeEmphEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmphEnable[10]
```

Offset 0x025F - Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment.

Each value in arrary can be between 0-1. One byte for each port.

Definition at line 1001 of file FspsUpd.h.

13.36.2.243 Usb3HsioTxDownscaleAmp

```
UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmp[10]
```

Offset 0x027D - USB 3.0 TX Output Downscale Amplitude Adjustment USB 3.0 TX Output Downscale Amplitude Adjustment, HSIO_TX_DWORD8[21:16], **Default = 00h**.

One byte for each port.

Definition at line 1019 of file FspsUpd.h.

13.36.2.244 Usb3HsioTxDownscaleAmpEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmpEnable[10]
```

Offset 0x0273 - Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment, Each value in arrary can be between 0-1.

One byte for each port.

Definition at line 1013 of file FspsUpd.h.

13.36.2.245 Usb3HsioTxRate0UniqTran

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate0UniqTran[10]
```

Offset 0x0742 - USB 3.0 TX Output Unique Transition Bit Scale for rate 0 USB 3.0 TX Output Unique Transition Bit Scale for rate 0, HSIO_TX_DWORD9[30:24], **Default = 4Ch**.

One byte for each port.

Definition at line 2426 of file FspsUpd.h.

13.36.2.246 Usb3HsioTxRate0UniqTranEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate0UniqTranEnable[10]
```

Offset 0x0738 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 0 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 0, Each value in array can be between 0-1.

One byte for each port.

Definition at line 2420 of file FspsUpd.h.

13.36.2.247 Usb3HsioTxRate1UniqTran

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate1UniqTran[10]
```

Offset 0x072E - USB 3.0 TX Output Unique Transition Bit Scale for rate 1 USB 3.0 TX Output Unique Transition Bit Scale for rate 1, HSIO_TX_DWORD9[22:16], **Default = 4Ch**.

One byte for each port.

Definition at line 2414 of file FspsUpd.h.

13.36.2.248 Usb3HsioTxRate1UniqTranEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate1UniqTranEnable[10]
```

Offset 0x0724 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 1 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 1, Each value in array can be between 0-1.

One byte for each port.

Definition at line 2408 of file FspsUpd.h.

13.36.2.249 Usb3HsioTxRate2UniqTran

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate2UniqTran[10]
```

Offset 0x071A - USB 3.0 TX Output Unique Transition Bit Scale for rate 2 USB 3.0 TX Output Unique Transition Bit Scale for rate 2, HSIO_TX_DWORD9[14:8], **Default = 4Ch**.

One byte for each port.

Definition at line 2402 of file FspsUpd.h.

13.36.2.250 Usb3HsioTxRate2UniqTranEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate2UniqTranEnable[10]
```

Offset 0x0710 - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 2 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 2, Each value in array can be between 0-1.

One byte for each port.

Definition at line 2396 of file FspsUpd.h.

13.36.2.251 Usb3HsioTxRate3UniqTran

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate3UniqTran[10]
```

Offset 0x0706 - USB 3.0 TX Output Unique Transition Bit Scale for rate 3 USB 3.0 TX Output Unique Transition Bit Scale for rate 3, HSIO_TX_DWORD9[6:0], **Default = 4Ch**.

One byte for each port.

Definition at line 2390 of file FspsUpd.h.

13.36.2.252 Usb3HsioTxRate3UniqTranEnable

```
UINT8 FSP_S_CONFIG::Usb3HsioTxRate3UniqTranEnable[10]
```

Offset 0x06FC - Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 3 Enable the write to USB 3.0 TX Output Unique Transition Bit Mode for rate 3, Each value in array can be between 0-1.

One byte for each port.

Definition at line 2384 of file FspsUpd.h.

13.36.2.253 UsbPdoProgramming

```
UINT8 FSP_S_CONFIG::UsbPdoProgramming
```

Offset 0x02AC - USB PDO Programming Enable/disable PDO programming for USB in PEI phase.

Disabling will allow for programming during later phase. 1: enable, 0: disable $EN_DIS

Definition at line 1137 of file FspsUpd.h.

13.36.2.254 VrPowerDeliveryDesign

```
UINT32 FSP_S_CONFIG::VrPowerDeliveryDesign
```

Offset 0x0164 - CPU VR Power Delivery Design Used to communicate the power delivery design capability of the board.

This value is an enum of the available power delivery segments that are defined in the Platform Design Guide.

Definition at line 648 of file FspsUpd.h.

13.36.2.255 VrVoltageLimit

```
UINT16 FSP_S_CONFIG::VrVoltageLimit[5]
```

Offset 0x013A - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.

Range is 0-7999mV.

Definition at line 532 of file FspsUpd.h.

13.36.2.256 WatchDogEnabled

```
UINT8 FSP_S_CONFIG::WatchDogEnabled
```

Offset 0x003D - WatchDog Timer Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable WatchDog timer. Setting is invalid if AmtEnabled is 0. $EN_DIS

Definition at line 159 of file FspsUpd.h.

13.36.2.257 WatchDogTimerBios

```
UINT16 FSP_S_CONFIG::WatchDogTimerBios
```

Offset 0x0044 - BIOS Timer 16 bits Value, Set BIOS watchdog timer.

Setting is invalid if AmtEnabled is 0.

Definition at line 193 of file FspsUpd.h.

13.36.2.258 WatchDogTimerOs

```
UINT16 FSP_S_CONFIG::WatchDogTimerOs
```

Offset 0x0042 - OS Timer 16 bits Value, Set OS watchdog timer.

Setting is invalid if AmtEnabled is 0.

Definition at line 188 of file FspsUpd.h.

13.36.2.259 XdciEnable

```
UINT8 FSP_S_CONFIG::XdciEnable
```

Offset 0x0200 - Enable xDCI controller Enable/disable to xDCI controller.

$EN_DIS

Definition at line 897 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.37 FSP_S_RESTRICTED_CONFIG Struct Reference

Fsp S Restricted Configuration.

```
#include <FspsUpd.h>
```

Public Attributes

- UINT32 Signature

    Offset 0x0AD0.
- UINT8 TestGnaErrorCheckDis

    Offset 0x0AD4 - Enable or disable GNA Error Check Disable Bit 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 DmaPassThroughDeprecated

    Offset 0x0AD5 - Enable or disable VT-d DmaPassThrough 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 CCHit2pendDeprecated

    Offset 0x0AD6 - Enable or disable VT-d CCHit2pend 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 ContextInvalidationDeprecated

    Offset 0x0AD7 - Enable or disable VT-d ContextInvalidation 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 IotlbInvalidationDeprecated

    Offset 0x0AD8 - Enable or disable VT-d IotlbInvalidation 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 ContextCacheDisDeprecated

    Offset 0x0AD9 - Enable or disable VT-d ContextCacheDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L1DisableDeprecated

    Offset 0x0ADA - Enable or disable VT-d L1Disable 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L2DisableDeprecated

    Offset 0x0ADB - Enable or disable VT-d L2Disable 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L3DisableDeprecated

    Offset 0x0ADC - Enable or disable VT-d L3Disable 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L1Hit2PendDisDeprecated

    Offset 0x0ADD - Enable or disable VT-d L1Hit2PendDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 L3Hit2PendDisDeprecated

    Offset 0x0ADE - Enable or disable VT-d L3Hit2PendDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 InvQueueCohDisDeprecated

    Offset 0x0ADF - Enable or disable VT-d InvQueueCohDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 SuperPageCapDeprecated

    Offset 0x0AE0 - Enable or disable VT-d SuperPageCap 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 QueueInvCapDisDeprecated

    Offset 0x0AE1 - Enable or disable VT-d QueueInvCapDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 TestIntrRemapCapDisDeprecated

    Offset 0x0AE2 - Enable or disable VT-d IntrRemapCapDis 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 SnoopControlDeprecated

    Offset 0x0AE3 - Enable or disable VT-d SnoopControl 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 RemapReverseCtrlDeprecated

    Offset 0x0AE4 - Enable or disable VT-d RemapReverseCtrl 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 VtdSvPolicyEnable

    Offset 0x0AE5 - Enable or disable VT-d SvPolicyEnable 0(Default)=Disable, 1=Enable $EN_DIS.
- UINT8 SaTestForceWake

    Offset 0x0AE6 - Sa Graphics Pei Test Force Wake Test Force Wake.
- UINT8 SaTestGfxPause

    Offset 0x0AE7 - Sa Graphics Pei Test Gfx Pause Test Gfx Pause.
- UINT8 SaTestGraphicsFreqModify

    Offset 0x0AE8 - Sa Graphics Pei Test Graphics Freq Modify Test Graphics Freq Modify.
- UINT8 SaTestPmLock

    Offset 0x0AE9 - Sa Graphics Pei Test PmLock Test PmLock.
- UINT8 SaTestPavpHeavyMode

    Offset 0x0AEA - Sa Graphics Pei Test Pavp Heavy Mode Test Pavp Heavy Mode.
- UINT8 SaTestDopClockGating

Offset 0x0AEB - Sa Graphics Pei Test Dop ClockGating Test Dop ClockGating.

- UINT8 SaTestUnsolicitedAttackOverride

  Offset 0x0AEC - Sa Graphics Pei Test Unsolicited Attack Override Test Unsolicited Attack Override.
- UINT8 SaTestWOPCMSupport

  Offset 0x0AED - Sa Graphics Pei Test WOPCM Support Test WOPCM Support.
- UINT8 SaTestPavpAsmf

  Offset 0x0AEE - Sa Graphics Pei Test Pavp Asmf Test Pavp Asmf.
- UINT8 SaTestPowerGating

  Offset 0x0AEF - Sa Graphics Pei Test Power Gating Test Power Gating.
- UINT8 SaTestUnitLevelClockGating

  Offset 0x0AF0 - Sa Graphics Pei Test Unit Level ClockGating Test Unit Level ClockGating.
- UINT8 SaTestAutoTearDown

  Offset 0x0AF1 - Sa Graphics Pei Test Auto TearDown Test Auto TearDown.
- UINT8 SaTestGraphicsVideoFreq

  Offset 0x0AF2 - Sa Graphics Pei Test Graphics Video Freq Test Graphics Video Freq.
- UINT8 SaTestWOPCMSize

  Offset 0x0AF3 - Sa Graphics Pei Test WOPCM Size Test WOPCM Size.
- UINT8 SaTestGraphicsFreqReq

  Offset 0x0AF4 - Sa Graphics Pei Test Graphics Freq Req Test Graphics Freq Req.
- UINT8 SaTestPegAspmL0sAggression [4]

  Offset 0x0AF5 - Sa Test Peg Aspm L0s Aggression Test Peg Aspm L0s Aggression.
- UINT8 SaClearCorrUnCorrErrEnable

  Offset 0x0AF9 - Sa Clear CorrUnCorrErr Enable Clear CorrUnCorrErr Enable $EN_DIS.
- UINT8 SaSvPegArifen [4]

  Offset 0x0AFA - Sa SvPegArifen SvPegArifen.
- UINT8 SaPeg0CompletionTimeout

  Offset 0x0AFE - Sa Peg0 Completion Timeout Peg0 Completion Timeout.
- UINT8 SaPeg1CompletionTimeout

  Offset 0x0AFF - Sa Peg1 Completion Timeout Peg1 Completion Timeout.
- UINT8 SaPeg2CompletionTimeout

  Offset 0x0B00 - Sa Peg2 Completion Timeout Peg2 Completion Timeout.
- UINT8 SaPeg3CompletionTimeout

  Offset 0x0B01 - Sa Peg3 Completion Timeout Peg3 Completion Timeout.
- UINT8 SaSvPegComplianceDeemphasis [4]

  Offset 0x0B02 - Sa Sv Peg Compliance Deemphasis SvPegComplianceDeemphasis.
- UINT8 SaSvPegTxLnStaggeringMode [4]

  Offset 0x0B06 - Sa Sv Peg TxLn Staggering Mode SvPegTxLnStaggeringMode.
- UINT8 SaSvPegTxLaneStaggeringInterval [4]

  Offset 0x0B0A - Sa Sv Peg TxLane Staggering Interval SvPegTxLaneStaggeringInterval.
- UINT8 SaSvPegRxLnStaggeringMode [4]

  Offset 0x0B0E - Sa Sv Peg RxLn Staggering Mode SvPegRxLnStaggeringMode.
- UINT8 SaSvPegRxLaneStaggeringInterval [4]

  Offset 0x0B12 - Sa Sv Peg RxLane Staggering Interval SvPegRxLaneStaggeringInterval.
- UINT8 SaTestMpllOffSen

  Offset 0x0B16 - Sa Test MpllOffSen TestMpllOffSen.
- UINT8 SaTestMdllOffSen

  Offset 0x0B17 - Sa Test MdllOffSen TestMdllOffSen.
- UINT8 SaTestModeEdramInternal

  Offset 0x0B18 - Sa Test Mode Edram Internal Edram Enable Option.
- UINT8 SaTestSecurityLock

  Offset 0x0B19 - Sa Test Security Lock Enable/Disable Security lock.

- UINT8 SaTestSpcLock

  Offset 0x0B1A - Sa Graphics Pei Test SPC Lock Test Spc Lock 0: POR (Enable), 1: Enable, 2: Disable.
- UINT8 SaTestTouchLock

  Offset 0x0B1B - Sa Itouch Doorbell Lock Enable Sa Itouch Doorbell Lock $EN_DIS.
- UINT8 SaPostMemRestrictedRsvd [21]

  Offset 0x0B1C - SaPostMemRestrictedRsvd Reserved for SA Post-Mem Restricted $EN_DIS.
- UINT8 CpuPostMemRestrictedRsvd [15]

  Offset 0x0B31 - CpuPostMemRestrictedRsvd Reserved for CPU Post-Mem Restricted $EN_DIS.
- UINT8 SkipAcpiNvs

  Offset 0x0B40 - SkipAcpiNvs SkipAcpiNvs default values.
- UINT8 EnableSgx7a

  Offset 0x0B41 - EnableSgx7a EnableSgx7a default values.
- UINT8 SgxDebugMode

  Offset 0x0B42 - SgxDebugMode SgxDebugMode default values.
- UINT8 SvLtEnable

  Offset 0x0B43 - SvLtEnable SvLtEnable default values.
- UINT16 SelectiveEnableSgx

  Offset 0x0B44 - SelectiveEnableSgx Deprecated.
- UINT8 UnusedUpdSpace33 [2]

  Offset 0x0B46.
- UINT64 EpcOffset

  Offset 0x0B48 - EpcOffset EpcOffset default values.
- UINT64 EpcLength

  Offset 0x0B50 - EpcLength EpcLength default values.
- UINT8 SgxLCP

  Offset 0x0B58 - SgxLCP SgxLCP default values.
- UINT8 UnusedUpdSpace34 [7]

  Offset 0x0B59.
- UINT64 SgxLEPubKeyHash0

  Offset 0x0B60 - EpcLength EpcLength default values.
- UINT64 SgxLEPubKeyHash1

  Offset 0x0B68 - EpcLength EpcLength default values.
- UINT64 SgxLEPubKeyHash2

  Offset 0x0B70 - EpcLength EpcLength default values.
- UINT64 SgxLEPubKeyHash3

  Offset 0x0B78 - EpcLength EpcLength default values.
- UINT32 SelectiveEnableSgx1

  Offset 0x0B80 - SelectiveEnableSgx1 SelectiveEnableSgx1 default values.
- UINT8 PchDmiTestMemCloseStateEn

  Offset 0x0B84 - MEM CLOSED State on PCH side Enable/Disable MEM CLOSED State on PCH side.
- UINT8 PchDmiTestInternalObffEn

  Offset 0x0B85 - Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side enable/disable Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side.
- UINT8 PchDmiTestDmiExtSync

  Offset 0x0B86 - Determines if force extended transmission of FTS ordered sets Determines if force extended transmission of FTS ordered sets when exiting L0s prior to entering L0.
- UINT8 PchDmiTestExternalObffEn

  Offset 0x0B87 - Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side Enable/Disable Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side.
- UINT8 PchDmiTestClientObffEn

  Offset 0x0B88 - Client Obff Enable Client Obff Enable.

- UINT8 PchDmiTestCxObffEntryDelay

  Offset 0x0B89 - CxObff Entry Delay CxObff Entry Delay.
- UINT8 PchDmiTestPchTcLockDown

  Offset 0x0B8A - Pch Tc Lock Down Pch Tc Lock Down.
- UINT8 PchDmiTestDelayEnDmiAspm

  Offset 0x0B8B - Enable DMI ASPM after booting to OS Enable DMI ASPM after booting to OS.
- UINT8 PchDmiTestDmiSecureRegLock

  Offset 0x0B8C - DMI Secure Reg Lock DMI Secure Reg Lock.
- UINT8 PchHdaTestConfigLockdown

  Offset 0x0B8D - Configuration Lockdown (BCLD) 0: POR (Enable), 1: Enable, 2: Disable.
- UINT8 PchHdaTestLowFreqLinkClkSrc

  Offset 0x0B8E - Low Frequency Link Clock Source (LFLCS) 0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL).
- UINT8 PchLanTestPchWOLFastSupport

  Offset 0x0B8F - PCH Lan Test WOL Fast Support Enables bit B_PCH_ACPI_GPE0_EN_127_96_PME_B0 during PchLanSxCallback in PchLanSxSmm.
- UINT8 PchLockDownTestSmiUnlock

  Offset 0x0B90 - Smi Unlock bit for SV policy 0: Lock; 1: Unlock.
- UINT8 PchPostMemRestrictedRsvd [24]

  Offset 0x0B91 - PchPostMemRestrictedRsvd Reserved for PCH Post-Mem Restricted Reserved $EN_DIS.
- UINT8 PcieRpTestEqPh2Override [24]

  Offset 0x0BA9 - Gen3 EQ Phase2 Tx override Coefficient requested by the remote device is ignored.
- UINT8 PcieRpTestEqPh2Preset [24]

  Offset 0x0BC1 - Tx preset to use when TestEqPh2Override is set Tx preset to use when TestEqPh2Override is set.
- UINT8 PcieRpTestAspmOc [24]

  Offset 0x0BD9 - Enable/Disable ASPM Optionality Compliance Enable/Disable ASPM Optionality Compliance.
- UINT8 PcieRpTestForceLtrOverride [24]

  Offset 0x0BF1 - Force LTR Override Force LTR Override.
- UINT8 PcieTestPchPciebem

  Offset 0x0C09 - PCH Pcie bem PCH Pcie bem.
- UINT8 PcieTestPchPciebemPortIndex

  Offset 0x0C0A - PCH Pcie Test bem Port Index PCH Pcie Test bem Port Index.
- UINT8 PcieTestPchPcieRpdbcgen

  Offset 0x0C0B - PCH Test PcieRp dbc gen PCH Test PcieRp dbc gen.
- UINT8 PcieTestPchPcieRpdlcgen

  Offset 0x0C0C - PCH Test PcieRp dlc gen PCH Test PcieRp dlc gen.
- UINT8 PcieTestPchPcieDcgeisma

  Offset 0x0C0D - PCH Test Pcie Dcgeisma PCH Test Pcie Dcgeisma.
- UINT8 PcieTestPchPcieRpscgen

  Offset 0x0C0E - PCH Test PcieRp scgen PCH Test PcieRp scgen.
- UINT8 PcieTestPchPcieSrdbcgen

  Offset 0x0C0F - PCH Test Pcie Srdbcgen PCH Test Pcie Srdbcgen.
- UINT8 PcieTestPchPcieScptcge

  Offset 0x0C10 - PCH Test Pcie Scptcge PCH Test Pcie Scptcge.
- UINT8 PcieTestPchPcieFdppge

  Offset 0x0C11 - PCH Test Pcie Fdppge PCH Test Pcie Fdppge.
- UINT8 PcieTestPchPciePhyclpge

  Offset 0x0C12 - PCH Test Pcie Phyclpge PCH Test Pcie Phyclpge.
- UINT8 PcieTestPchPcieFdcpge

  Offset 0x0C13 - PCH Test Pcie Fdcpge PCH Test Pcie Fdcpge.
- UINT8 PcieTestPchPcieDetscpge

Offset 0x0C14 - PCH Test Pcie Detscpge PCH Test Pcie Detscpge.

- UINT8 PcieTestPchPcieL23rdyscpge

  Offset 0x0C15 - PCH Test Pcie L23 rdyscpge PCH Test Pcie L23 rdyscpge.
- UINT8 PcieTestPchPcieDisscpge

  Offset 0x0C16 - PCH Test Pcie Disscpge PCH Test Pcie Disscpge.
- UINT8 PcieTestPchPcieL1scpge

  Offset 0x0C17 - PCH Test Pcie L1 scpge PCH Test Pcie L1 scpge.
- UINT8 PcieTestLaneEqEn

  Offset 0x0C18 - PCH Pcie Test Lane Eq En PCH PcieTest Lane Eq En.
- UINT8 PchPmTestPchPmRegisterLock

  Offset 0x0C19 - PCH Pm Register Lock PCH Pm Register Lock.
- UINT8 PchPmTestSlpS0CsMePgQDis

  Offset 0x0C1A - PCH Pm Test SlpS0 CsMe PgQDis CPPM VRIC CSME Power Gated Qualification Disable.
- UINT8 PchPmTestSlpS0GbeDiscQDis

  Offset 0x0C1B - PCH Pm Test Slp S0 Gbe Disc QDis CPPM VRIC GbE Disconnected Qualification Disable.
- UINT8 PchPmTestSlpS0ADspD3QDis

  Offset 0x0C1C - PCH Pm Test Slp S0A Dsp D3 QDis CPPM VRIC Audio DSP is in D3 Qualification Disable.
- UINT8 PchPmTestSlpS0XhciD3QDis

  Offset 0x0C1D - PCH Pm Test Slp S0 Xhci D3QDis CPPM VRIC XHCI is in D3 Qualification Disable.
- UINT8 PchPmTestSlpS0LpioD3QDis

  Offset 0x0C1E - PCH Pm Test Slp S0 Lpio D3QDis CPPM VRIC LPIO is in D3 Qualification Disable.
- UINT8 PchPmTestSlpS0IccPllWBEn

  Offset 0x0C1F - PCH Pm Test Slp S0 Icc Pll W BEn CPPM VRIC ICC PLL Wake Block Enable.
- UINT8 PchPmTestSlpS0PUGBEn

  Offset 0x0C20 - PCH Pm Test Slp S0 PUGB En PCH Pm CPPM VRIC Power Ungate Block Enable.
- UINT8 PchPmTestPchClearPowerSts

  Offset 0x0C21 - PCH Pm Test Clear Power Sts.
- UINT8 SataTestRstPcieStorageTestMode [3]

  Offset 0x0C22 - PCH Sata Test Rst Pcie Storage Test Mode PCIe Storage remapping Test Mode to override existing PCIe Storage remapping POR setting for development purpose.
- UINT8 SataTestRstPcieStoragePortConfigCheck [3]

  Offset 0x0C25 - PCH Sata Test Rst Pcie Storage Port Config Check Enable/Disable Port Configuration Check for RST PCIe Storage Remapping.
- UINT8 SataTestRstPcieStorageDeviceInterface [3]

  Offset 0x0C28 - PCH Sata Test Rst Pcie Storage Device Interface Select the device interface (AHCI/NVME) for remapped device.
- UINT8 SataTestRstPcieStorageDeviceBarSizeCheck [3]

  Offset 0x0C2B - PCH Sata Test Rst Pcie Storage Device Bar Size Check Enable/Disable Device BAR Size Check for remapped device.
- UINT8 SataTestRstPcieStorageDeviceBarSelect [3]

  Offset 0x0C2E - PCH Sata Test Rst Pcie Storage Device Bar Select Select the device BAR (BAR0-BAR5) that will be used for Remapping.
- UINT8 SataTestRstPcieStorageDeviceInterrupt [3]

  Offset 0x0C31 - PCH Sata Test Rst Pcie Storage Device Interrupt Select the device interrupt (Legacy/MSIX) for remapped device.
- UINT8 SataTestRstPcieStorageAspmProgramming [3]

  Offset 0x0C34 - PCH Sata Test Rst Pcie Storage Aspm Programming Enable/Disable ASPM Programming for remapped device.
- UINT8 SataTestRstPcieStorageSaveRestore [3]

  Offset 0x0C37 - PCH Sata Test Rst Pcie Storage Save Restore Enable/Disable ASPM Programming for remapped device.
- UINT8 SataTestLtrEnable

Offset 0x0C3A - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.

- UINT8 SataTestLtrConfigLock

  Offset 0x0C3B - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.
- UINT8 SataTestLtrOverride

  Offset 0x0C3C - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.
- UINT8 SataTestSnoopLatencyOverrideMultiplier

  Offset 0x0C3D - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.
- UINT16 SataTestSnoopLatencyOverrideValue

  Offset 0x0C3E - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.
- UINT8 SataTestSataAssel

  Offset 0x0C40 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.
- UINT8 PchTestTselLock

  Offset 0x0C41 - This locks down Enables the thermal sensor 0: Disabled, 1: Enabled.
- UINT8 PchTestTscLock

  Offset 0x0C42 - This locks down Catastrophic Power-Down Enable and Catastrophic Trip Point Register 0: Disabled, 1: Enabled.
- UINT8 PchTestPhlcLock

  Offset 0x0C43 - This locks down PHL and PHLC 0: Disabled, 1: Enabled.
- UINT32 PchTestEPTypeLockPolicy

  Offset 0x0C44 - USB EP Type Lock Policy USB EP Type Lock Policy.
- UINT32 PchTestEPTypeLockPolicyPortControl1

  Offset 0x0C48 - USB EP Type Lock Policy Control 1 USB EP Type Lock Policy Control 1.
- UINT32 PchTestEPTypeLockPolicyPortControl2

  Offset 0x0C4C - USB EP Type Lock Policy Control 2 USB EP Type Lock Policy Control 2.
- UINT8 PchTestControllerEnabled

  Offset 0x0C50 - Xhci Controller Enable 0: Disable; 1: Enable.
- UINT8 PchTestUnlockUsbForSvNoa

  Offset 0x0C51 - Unlock to enable NOA for SV usage 1: Unlock to enable NOA usage.
- UINT8 PchTestClkGatingXhci

  Offset 0x0C52 - Enable XHCI Clock Gating for SV usage 1: Enable XHCI Clock Gating.
- UINT8 PchTestCyclonePcieSwitchWA

  Offset 0x0C53 - Restricted Cyclone Pcie Switch WA Restricted Cyclone Pcie Switch WA.
- UINT8 PchTestPchRootPort

  Offset 0x0C54 - Restricted Pch Root Port Restricted Pch Root Port.
- UINT8 TestPchPmErDebugMode

  Offset 0x0C55 - PCH PMC ER Debug mode Disable/Enable Energy Reporting Debug Mode.
- UINT8 TestUsbTsLdoShutdown

  Offset 0x0C56 - USB2/TS LDO Dynamic Shutdown Enable/Disable USB2/TS LDO Dynamic Shutdown 0: POR, 1: force enable, 2: force disable.
- UINT8 PchDmiTestOpiPllPowerGating

  Offset 0x0C57 - OPI PLL Power Gating OPI PLL Power Gating.
- UINT8 PchHdaTestPowerClockGating

  Offset 0x0C58 - HDA Power/Clock Gating (PGD/CGD) Enable/Disable HD Audio Power and Clock Gating(POR↩ : Enable).
- UINT8 TestCnviWifiLtrEn

  Offset 0x0C59 - CNVi WiFi LTR Enable/Disable CNVi WiFi LTR.
- UINT8 TestPchPmLatchEventsC10Exit

  Offset 0x0C5A - PCH Pm Latch events C10 exit PCH Pm Latch events C10 exit Enable.
- UINT8 TestCnviLteCoex

  Offset 0x0C5B - CNVi LTE Coexistence Enable/Disable MFUART2 connection for coexistence between LTE and Wi-Fi/BT.

- UINT8 TestCnviBtInterface

  Offset 0x0C5C - CNVi BT Interface This option configures BT device interface to either USB or UART 0:UART, 1:USB.

- UINT8 TestCnviBtUartType

  Offset 0x0C5D - CNVi BT Uart Type This is a test option which allows configuration of UART type for BT communication 0:Serial IO Uart0, 1:ISH Uart0, 2:Uart over external pads.

- UINT8 TestCnviSharedXtalClocking

  Offset 0x0C5E - CNVi Shared XTAL Clocking This option is used to tell CNVi that XTAL is being shared.

- UINT8 PcieRpTestDmiL1Edm [24]

  Offset 0x0C5F - Enable/Disable DMI L1 entry disable mode Enable/Disable DMI L1 entry disable mode.

- UINT8 TestPcieMpcSecureRegisterLock

  Offset 0x0C77 - MPC Secure Register Lock Enable/Disable Secure Register Lock, 0: PLATFORM_POR, 1: FOR↩ CE_ENABLE, 2: FORCE_DISABLE.

- UINT8 SiSvPolicyEnable

  Offset 0x0C78 - Si Config SvPolicyEnable.

- UINT8 HsleWorkaround

  Offset 0x0C79 - Si Config HsleWorkaround Enable/Disable HSLE model specific workarounds $EN_DIS.

- UINT8 TestSkipPostBootSai

  Offset 0x0C7A - Skip POSTBOOT SAI This skips the Post Boot Sai programming.

- UINT8 UnusedUpdSpace35 [2]

  Offset 0x0C7B.

- UINT8 ReservedFspsRestrictedUpd [3]

  Offset 0x0C7D.

13.37.1 Detailed Description

Fsp S Restricted Configuration.

Definition at line 3679 of file FspsUpd.h.

13.37.2 Member Data Documentation

13.37.2.1 PchDmiTestClientObffEn

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestClientObffEn
```

Offset 0x0B88 - Client Obff Enable Client Obff Enable.

$EN_DIS

Definition at line 4074 of file FspsUpd.h.

13.37.2.2 PchDmiTestDelayEnDmiAspm

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestDelayEnDmiAspm
```

Offset 0x0B8B - Enable DMI ASPM after booting to OS Enable DMI ASPM after booting to OS.

$EN_DIS

Definition at line 4091 of file FspsUpd.h.

13.37.2.3 PchDmiTestDmiSecureRegLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestDmiSecureRegLock
```

Offset 0x0B8C - DMI Secure Reg Lock DMI Secure Reg Lock.

0: POR (Enable), 1: Enable, 2: Disable

Definition at line 4097 of file FspsUpd.h.

13.37.2.4 PchDmiTestExternalObffEn

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestExternalObffEn
```

Offset 0x0B87 - Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side Enable/Disable Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side.

$EN_DIS

Definition at line 4068 of file FspsUpd.h.

13.37.2.5 PchDmiTestInternalObffEn

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestInternalObffEn
```

Offset 0x0B85 - Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side enable/disable Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side.

$EN_DIS

Definition at line 4056 of file FspsUpd.h.

13.37.2.6 PchDmiTestMemCloseStateEn

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestMemCloseStateEn
```

Offset 0x0B84 - MEM CLOSED State on PCH side Enable/Disable MEM CLOSED State on PCH side.

$EN_DIS

Definition at line 4050 of file FspsUpd.h.

13.37.2.7 PchDmiTestOpiPllPowerGating

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestOpiPllPowerGating
```

Offset 0x0C57 - OPI PLL Power Gating OPI PLL Power Gating.

0: POR, 1: force enable, 2: force disable

Definition at line 4422 of file FspsUpd.h.

13.37.2.8 PchDmiTestPchTcLockDown

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchDmiTestPchTcLockDown
```

Offset 0x0B8A - Pch Tc Lock Down Pch Tc Lock Down.

$EN_DIS

Definition at line 4085 of file FspsUpd.h.

13.37.2.9 PchHdaTestConfigLockdown

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchHdaTestConfigLockdown
```

Offset 0x0B8D - Configuration Lockdown (BCLD) 0: POR (Enable), 1: Enable, 2: Disable.

0: POR (Enable), 1: Enable, 2: Disable

Definition at line 4103 of file FspsUpd.h.

13.37.2.10 PchHdaTestLowFreqLinkClkSrc

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchHdaTestLowFreqLinkClkSrc
```

Offset 0x0B8E - Low Frequency Link Clock Source (LFLCS) 0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL).

0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL)

Definition at line 4109 of file FspsUpd.h.

13.37.2.11 PchHdaTestPowerClockGating

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchHdaTestPowerClockGating
```

Offset 0x0C58 - HDA Power/Clock Gating (PGD/CGD) Enable/Disable HD Audio Power and Clock Gating(POR: Enable).

0: PLATFORM_POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4429 of file FspsUpd.h.

13.37.2.12 PchLanTestPchWOLFastSupport

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchLanTestPchWOLFastSupport
```

Offset 0x0B8F - PCH Lan Test WOL Fast Support Enables bit B_PCH_ACPI_GPE0_EN_127_96_PME_B0 during PchLanSxCallback in PchLanSxSmm.

$EN_DIS

Definition at line 4115 of file FspsUpd.h.

13.37.2.13 PchLockDownTestSmiUnlock

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchLockDownTestSmiUnlock
```

Offset 0x0B90 - Smi Unlock bit for SV policy 0: Lock; 1: Unlock.

$EN_DIS

Definition at line 4121 of file FspsUpd.h.

13.37.2.14 PchPmTestPchClearPowerSts

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchPmTestPchClearPowerSts
```

Offset 0x0C21 - PCH Pm Test Clear Power Sts.

Todo ADD DESCRIPTION.

Policy for SV usage. NO USE..

Definition at line 4272 of file FspsUpd.h.

13.37.2.15 PchTestClkGatingXhci

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchTestClkGatingXhci
```

Offset 0x0C52 - Enable XHCI Clock Gating for SV usage 1: Enable XHCI Clock Gating.

0: Disable XHCI Clock Gating. Policy for SV usage. $EN_DIS

Definition at line 4394 of file FspsUpd.h.

13.37.2.16 PchTestPhlcLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchTestPhlcLock
```

Offset 0x0C43 - This locks down PHL and PHLC 0: Disabled, 1: Enabled.

$EN_DIS

Definition at line 4361 of file FspsUpd.h.

13.37.2.17 PchTestTscLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchTestTscLock
```

Offset 0x0C42 - This locks down Catastrophic Power-Down Enable and Catastrophic Trip Point Register 0: Disabled, 1: Enabled.

$EN_DIS

Definition at line 4355 of file FspsUpd.h.

13.37.2.18 PchTestTselLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchTestTselLock
```

Offset 0x0C41 - This locks down Enables the thermal sensor 0: Disabled, 1: Enabled.

$EN_DIS

Definition at line 4349 of file FspsUpd.h.

13.37.2.19 PchTestUnlockUsbForSvNoa

```
UINT8 FSP_S_RESTRICTED_CONFIG::PchTestUnlockUsbForSvNoa
```

Offset 0x0C51 - Unlock to enable NOA for SV usage 1: Unlock to enable NOA usage.

0: Set Xhci OC registers, Set Xhci OCCDone bit, XHCI Access Control Bit. $EN_DIS

Definition at line 4388 of file FspsUpd.h.

13.37.2.20 SataTestRstPcieStorageDeviceInterface

```
UINT8 FSP_S_RESTRICTED_CONFIG::SataTestRstPcieStorageDeviceInterface[3]
```

Offset 0x0C28 - PCH Sata Test Rst Pcie Storage Device Interface Select the device interface (AHCI/NVME) for remapped device.

NO USE.

Definition at line 4288 of file FspsUpd.h.

13.37.2.21 SiSvPolicyEnable

```
UINT8 FSP_S_RESTRICTED_CONFIG::SiSvPolicyEnable
```

Offset 0x0C78 - Si Config SvPolicyEnable.

Platform specific common policies that used by several silicon components. SvPolicyEnable. $EN_DIS

Definition at line 4484 of file FspsUpd.h.

13.37.2.22 TestCnviLteCoex

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestCnviLteCoex
```

Offset 0x0C5B - CNVi LTE Coexistence Enable/Disable MFUART2 connection for coexistence between LTE and Wi-Fi/BT.

0: PLATFORM_POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4448 of file FspsUpd.h.

13.37.2.23 TestCnviSharedXtalClocking

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestCnviSharedXtalClocking
```

Offset 0x0C5E - CNVi Shared XTAL Clocking This option is used to tell CNVi that XTAL is being shared.

0: PLATFORM_POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4467 of file FspsUpd.h.

13.37.2.24 TestCnviWifiLtrEn

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestCnviWifiLtrEn
```

Offset 0x0C59 - CNVi WiFi LTR Enable/Disable CNVi WiFi LTR.

0: PLATFORM_POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4435 of file FspsUpd.h.

13.37.2.25 TestPchPmErDebugMode

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPchPmErDebugMode
```

Offset 0x0C55 - PCH PMC ER Debug mode Disable/Enable Energy Reporting Debug Mode.

$EN_DIS

Definition at line 4410 of file FspsUpd.h.

13.37.2.26 TestPchPmLatchEventsC10Exit

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPchPmLatchEventsC10Exit
```

Offset 0x0C5A - PCH Pm Latch events C10 exit PCH Pm Latch events C10 exit Enable.

0: POR, 1: force enable, 2: force disable

Definition at line 4441 of file FspsUpd.h.

13.37.2.27 TestPcieMpcSecureRegisterLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPcieMpcSecureRegisterLock
```

Offset 0x0C77 - MPC Secure Register Lock Enable/Disable Secure Register Lock, 0: PLATFORM_POR, 1: FO↩ RCE_ENABLE, 2: FORCE_DISABLE.

0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4478 of file FspsUpd.h.

13.37.2.28 TestSkipPostBootSai

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestSkipPostBootSai
```

Offset 0x0C7A - Skip POSTBOOT SAI This skips the Post Boot Sai programming.

0: PLATFORM_POR, 1: FORCE_ENABLE, 2: FORCE_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4496 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.38 FSP_S_TEST_CONFIG Struct Reference

Fsp S Test Configuration.

```
#include <FspsUpd.h>
```

Public Attributes

- UINT32 Signature

  Offset 0x07C0.
- UINT8 ChapDeviceEnable

  Offset 0x07C4 - Enable/Disable Device 7 Enable: Device 7 enabled, Disable (Default): Device 7 disabled $EN_DIS.
- UINT8 SkipPamLock

  Offset 0x07C5 - Skip PAM register lock Enable: PAM register will not be locked by RC, platform code should lock it, Disable(Default): PAM registers will be locked by RC $EN_DIS.
- UINT8 EdramTestMode

  Offset 0x07C6 - EDRAM Test Mode Enable: PAM register will not be locked by RC, platform code should lock it, Disable(Default): PAM registers will be locked by RC 0: EDRAM SW disable, 1: EDRAM SW Enable, 2: EDRAM HW mode.
- UINT8 DmiExtSync

  Offset 0x07C7 - DMI Extended Sync Control Enable: Enable DMI Extended Sync Control, Disable(Default): Disable DMI Extended Sync Control $EN_DIS.
- UINT8 DmiIot

  Offset 0x07C8 - DMI IOT Control Enable: Enable DMI IOT Control, Disable(Default): Disable DMI IOT Control $E←N_DIS.
- UINT8 PegMaxPayload [4]

  Offset 0x07C9 - PEG Max Payload size per root port 0xFF(Default):Auto, 0x1: Force 128B, 0x2: Force 256B 0xFF: Auto, 0x1: Force 128B, 0x2: Force 256B.
- UINT8 RenderStandby

  Offset 0x07CD - Enable/Disable IGFX RenderStandby Enable(Default): Enable IGFX RenderStandby, Disable←: Disable IGFX RenderStandby $EN_DIS.
- UINT8 PmSupport

  Offset 0x07CE - Enable/Disable IGFX PmSupport Enable(Default): Enable IGFX PmSupport, Disable: Disable IGFX PmSupport $EN_DIS.
- UINT8 CdynmaxClampEnable

  Offset 0x07CF - Enable/Disable CdynmaxClamp Enable(Default): Enable CdynmaxClamp, Disable: Disable CdynmaxClamp $EN_DIS.
- UINT8 VtdDisableDeprecated

  Offset 0x07D0 - Disable VT-d 0=Enable/FALSE(VT-d enabled), 1=Disable/TRUE (VT-d disabled) $EN_DIS.
- UINT8 GtFreqMax

  Offset 0x07D1 - GT Frequency Limit 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz.
- UINT8 DisableTurboGt

  Offset 0x07D2 - Disable Turbo GT 0=Disable: GT frequency is not limited, 1=Enable: Disables Turbo GT frequency $EN_DIS.
- UINT8 SaPostMemTestRsvd [11]

  Offset 0x07D3 - SaPostMemTestRsvd Reserved for SA Post-Mem Test $EN_DIS.
- UINT8 OneCoreRatioLimit

  Offset 0x07DE - 1-Core Ratio Limit 1-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 TwoCoreRatioLimit

  Offset 0x07DF - 2-Core Ratio Limit 2-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 ThreeCoreRatioLimit

  Offset 0x07E0 - 3-Core Ratio Limit 3-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 FourCoreRatioLimit

  Offset 0x07E1 - 4-Core Ratio Limit 4-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

- UINT8 Hwp

  Offset 0x07E2 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.
- UINT8 HdcControl

  Offset 0x07E3 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.
- UINT8 PowerLimit1Time

  Offset 0x07E4 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.
- UINT8 PowerLimit2

  Offset 0x07E5 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.
- UINT8 TurboPowerLimitLock

  *Offset 0x07E6 - Turbo settings Lock Lock all Turbo settings Enable/Disable; **0: Disable ,** 1: Enable $EN_DIS.*
- UINT8 PowerLimit3Time

  Offset 0x07E7 - Package PL3 time window Package PL3 time window range for this policy from 0 to 64ms.
- UINT8 PowerLimit3DutyCycle

  Offset 0x07E8 - Package PL3 Duty Cycle Package PL3 Duty Cycle; Valid Range is 0 to 100.
- UINT8 PowerLimit3Lock

  *Offset 0x07E9 - Package PL3 Lock Package PL3 Lock Enable/Disable; **0: Disable ; 1: Enable $EN_DIS.***
- UINT8 PowerLimit4Lock

  *Offset 0x07EA - Package PL4 Lock Package PL4 Lock Enable/Disable; **0: Disable ; 1: Enable $EN_DIS.***
- UINT8 TccActivationOffset

  Offset 0x07EB - TCC Activation Offset TCC Activation Offset.
- UINT8 TccOffsetClamp

  *Offset 0x07EC - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For Y SKU, the recommended default for this policy is **1: Enabled**, For all other SKUs the recommended default are **0: Disabled**.*
- UINT8 TccOffsetLock

  *Offset 0x07ED - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; 1: Enabled.*
- UINT8 NumberOfEntries

  Offset 0x07EE - Custom Ratio State Entries The number of custom ratio state entries, ranges from 0 to 40 for a valid custom ratio table.Sets the number of custom P-states.
- UINT8 Custom1PowerLimit1Time

  Offset 0x07EF - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.
- UINT8 Custom1TurboActivationRatio

  Offset 0x07F0 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.
- UINT8 Custom1ConfigTdpControl

  Offset 0x07F1 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
- UINT8 Custom2PowerLimit1Time

  Offset 0x07F2 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.
- UINT8 Custom2TurboActivationRatio

  Offset 0x07F3 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.
- UINT8 Custom2ConfigTdpControl

  Offset 0x07F4 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
- UINT8 Custom3PowerLimit1Time

  Offset 0x07F5 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.
- UINT8 Custom3TurboActivationRatio

  Offset 0x07F6 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.
- UINT8 Custom3ConfigTdpControl

  Offset 0x07F7 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
- UINT8 ConfigTdpLock

*Offset 0x07F8 - ConfigTdp mode settings Lock Lock the ConfigTdp mode settings from runtime changes; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 ConfigTdpBios

  *Offset 0x07F9 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.*

- UINT8 PsysPowerLimit1

  Offset 0x07FA - PL1 Enable value PL1 Enable value to limit average platform power.

- UINT8 PsysPowerLimit1Time

  Offset 0x07FB - PL1 timewindow PL1 timewindow in seconds.

- UINT8 PsysPowerLimit2

  Offset 0x07FC - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

- UINT8 MlcStreamerPrefetcher

  *Offset 0x07FD - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0: Disable; **1: Enable**.*

- UINT8 MlcSpatialPrefetcher

  *Offset 0x07FE - Enable or Disable MLC Spatial Prefetcher Enable or Disable MLC Spatial Prefetcher; 0: Disable; **1: Enable** $EN_DIS.*

- UINT8 MonitorMwaitEnable

  *Offset 0x07FF - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable**.*

- UINT8 MachineCheckEnable

  *Offset 0x0800 - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.*

- UINT8 DebugInterfaceEnable

  Offset 0x0801 - Deprecated DO NOT USE Enable or Disable processor debug features.

- UINT8 DebugInterfaceLockEnable

  *Offset 0x0802 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; **1: Enable**.*

- UINT8 ApIdleManner

  *Offset 0x0803 - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.*

- UINT8 ProcessorTraceOutputScheme

  *Offset 0x0804 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.*

- UINT8 ProcessorTraceEnable

  *Offset 0x0805 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.*

- UINT8 UnusedUpdSpace25 [2]

  Offset 0x0806.

- UINT64 ProcessorTraceMemBase

  Offset 0x0808 - Base of memory region allocated for Processor Trace Base address of memory region allocated for Processor Trace.

- UINT32 ProcessorTraceMemLength

  Offset 0x0810 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.

- UINT8 VoltageOptimization

  *Offset 0x0814 - Enable or Disable Voltage Optimization feature Enable or Disable Voltage Optimization feature 0: Disable; **1: Enable** $EN_DIS.*

- UINT8 Eist

  Offset 0x0815 - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

- UINT8 EnergyEfficientPState

  Offset 0x0816 - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.

- UINT8 EnergyEfficientTurbo

Offset 0x0817 - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.

- UINT8 TStates

  *Offset 0x0818 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.*

- UINT8 BiProcHot

  *Offset 0x0819 - Enable or Disable Bi-Directional PROCHOT# Enable or Disable Bi-Directional PROCHOT#; 0↩ : Disable; **1: Enable** $EN_DIS.*

- UINT8 DisableProcHotOut

  *Offset 0x081A - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; **1: Enable**.*

- UINT8 ProcHotResponse

  *Offset 0x081B - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.*

- UINT8 DisableVrThermalAlert

  *Offset 0x081C - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.*

- UINT8 AutoThermalReporting

  *Offset 0x081D - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; **1: Enable**.*

- UINT8 ThermalMonitor

  *Offset 0x081E - Enable or Disable Thermal Monitor Enable or Disable Thermal Monitor; 0: Disable; **1: Enable** $EN_DIS.*

- UINT8 Cx

  Offset 0x081F - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).

- UINT8 PmgCstCfgCtrlLock

  *Offset 0x0820 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; **1: Enable**.*

- UINT8 C1e

  Offset 0x0821 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

- UINT8 PkgCStateDemotion

  Offset 0x0822 - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.

- UINT8 PkgCStateUnDemotion

  Offset 0x0823 - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.

- UINT8 CStatePreWake

  Offset 0x0824 - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

- UINT8 TimedMwait

  Offset 0x0825 - Enable or Disable TimedMwait Support.

- UINT8 CstCfgCtrIoMwaitRedirection

  *Offset 0x0826 - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.*

- UINT8 PkgCStateLimit

  Offset 0x0827 - Set the Max Pkg Cstate Set the Max Pkg Cstate.

- UINT8 CstateLatencyControl0TimeUnit

  Offset 0x0828 - TimeUnit for C-State Latency Control0 TimeUnit for C-State Latency Control0; Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 CstateLatencyControl1TimeUnit

  Offset 0x0829 - TimeUnit for C-State Latency Control1 TimeUnit for C-State Latency Control1;Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 CstateLatencyControl2TimeUnit

  Offset 0x082A - TimeUnit for C-State Latency Control2 TimeUnit for C-State Latency Control2;Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 CstateLatencyControl3TimeUnit

  Offset 0x082B - TimeUnit for C-State Latency Control3 TimeUnit for C-State Latency Control3;Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 CstateLatencyControl4TimeUnit

Offset 0x082C - TimeUnit for C-State Latency Control4 Time - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 CstateLatencyControl5TimeUnit

  Offset 0x082D - TimeUnit for C-State Latency Control5 TimeUnit for C-State Latency Control5;Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.

- UINT8 PpmIrmSetting

  Offset 0x082E - Interrupt Redirection Mode Select Interrupt Redirection Mode Select.0: Fixed priority; 1: Round robin;2: Hash vector;4: PAIR with fixed priority;5: PAIR with round robin;6: PAIR with hash vector;7: No change.

- UINT8 ProcHotLock

  *Offset 0x082F - Lock prochot configuration Lock prochot configuration Enable/Disable; **0: Disable**; 1: Enable $EN↩ _DIS.*

- UINT8 ConfigTdpLevel

  *Offset 0x0830 - Configuration for boot TDP selection Configuration for boot TDP selection; **0: TDP Nominal**; 1: TDP Down; 2: TDP Up;0xFF : Deactivate.*

- UINT8 RaceToHalt

  Offset 0x0831 - Race To Halt Enable/Disable Race To Halt feature.

- UINT8 MaxRatio

  Offset 0x0832 - Max P-State Ratio Max P-State Ratio, Valid Range 0 to 0x7F.

- UINT8 StateRatio [40]

  Offset 0x0833 - P-state ratios for custom P-state table P-state ratios for custom P-state table.

- UINT8 StateRatioMax16 [16]

  Offset 0x085B - P-state ratios for max 16 version of custom P-state table P-state ratios for max 16 version of custom P-state table.

- UINT8 UnusedUpdSpace26

  Offset 0x086B.

- UINT16 PsysPmax

  Offset 0x086C - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.

- UINT16 CstateLatencyControl0Irtl

  Offset 0x086E - Interrupt Response Time Limit of C-State LatencyContol0 Interrupt Response Time Limit of C-State LatencyContol0.Range of value 0 to 0x3FF.

- UINT16 CstateLatencyControl1Irtl

  Offset 0x0870 - Interrupt Response Time Limit of C-State LatencyContol1 Interrupt Response Time Limit of C-State LatencyContol1.Range of value 0 to 0x3FF.

- UINT16 CstateLatencyControl2Irtl

  Offset 0x0872 - Interrupt Response Time Limit of C-State LatencyContol2 Interrupt Response Time Limit of C-State LatencyContol2.Range of value 0 to 0x3FF.

- UINT16 CstateLatencyControl3Irtl

  Offset 0x0874 - Interrupt Response Time Limit of C-State LatencyContol3 Interrupt Response Time Limit of C-State LatencyContol3.Range of value 0 to 0x3FF.

- UINT16 CstateLatencyControl4Irtl

  Offset 0x0876 - Interrupt Response Time Limit of C-State LatencyContol4 Interrupt Response Time Limit of C-State LatencyContol4.Range of value 0 to 0x3FF.

- UINT16 CstateLatencyControl5Irtl

  Offset 0x0878 - Interrupt Response Time Limit of C-State LatencyContol5 Interrupt Response Time Limit of C-State LatencyContol5.Range of value 0 to 0x3FF.

- UINT8 UnusedUpdSpace27 [2]

  Offset 0x087A.

- UINT32 PowerLimit1

  Offset 0x087C - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.

- UINT32 PowerLimit2Power

  Offset 0x0880 - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.

- UINT32 PowerLimit3

  Offset 0x0884 - Package PL3 power limit Package PL3 power limit.

- UINT32 PowerLimit4

  Offset 0x0888 - Package PL4 power limit Package PL4 power limit.
- UINT32 TccOffsetTimeWindowForRatl

  Offset 0x088C - Tcc Offset Time Window for RATL Package PL4 power limit.
- UINT32 Custom1PowerLimit1

  Offset 0x0890 - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.
- UINT32 Custom1PowerLimit2

  Offset 0x0894 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.
- UINT32 Custom2PowerLimit1

  Offset 0x0898 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.
- UINT32 Custom2PowerLimit2

  Offset 0x089C - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.
- UINT32 Custom3PowerLimit1

  Offset 0x08A0 - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.
- UINT32 Custom3PowerLimit2

  Offset 0x08A4 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.
- UINT32 PsysPowerLimit1Power

  Offset 0x08A8 - Platform PL1 power Platform PL1 power.
- UINT32 PsysPowerLimit2Power

  Offset 0x08AC - Platform PL2 power Platform PL2 power.
- UINT8 ThreeStrikeCounterDisable

  *Offset 0x08B0 - Set Three Strike Counter Disable False (default): Three Strike counter will be incremented and True: Prevents Three Strike counter from incrementing; **0: False**; 1: True.*
- UINT8 HwpInterruptControl

  *Offset 0x08B1 - Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT; **0: Disable**; 1: Enable.*
- UINT8 FiveCoreRatioLimit

  Offset 0x08B2 - 5-Core Ratio Limit 5-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 SixCoreRatioLimit

  Offset 0x08B3 - 6-Core Ratio Limit 6-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 SevenCoreRatioLimit

  Offset 0x08B4 - 7-Core Ratio Limit 7-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 EightCoreRatioLimit

  Offset 0x08B5 - 8-Core Ratio Limit 8-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.
- UINT8 EnableItbm

  Offset 0x08B6 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.
- UINT8 EnableItbmDriver

  Offset 0x08B7 - Intel Turbo Boost Max Technology 3.0 Driver.
- UINT8 C1StateAutoDemotion

  Offset 0x08B8 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.
- UINT8 C1StateUnDemotion

  Offset 0x08B9 - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.
- UINT8 CpuWakeUpTimer

  Offset 0x08BA - CpuWakeUpTimer Enable long CPU Wakeup Timer.
- UINT8 MinRingRatioLimit

  Offset 0x08BB - Minimum Ring ratio limit override Minimum Ring ratio limit override.

- UINT8 MaxRingRatioLimit

  Offset 0x08BC - Minimum Ring ratio limit override Maximum Ring ratio limit override.
- UINT8 C3StateAutoDemotion

  Offset 0x08BD - Enable or Disable C3 Cstate Demotion Enable or Disable C3 Cstate Demotion.
- UINT8 C3StateUnDemotion

  Offset 0x08BE - Enable or Disable C3 Cstate UnDemotion Enable or Disable C3 Cstate UnDemotion.
- UINT8 RatioLimitNumCore0

  Offset 0x08BF - Ratio Limit Num Core 0 Ratio Limit Num Core0: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore1

  Offset 0x08C0 - Ratio Limit Num Core 1 Ratio Limit Num Core1: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore2

  Offset 0x08C1 - Ratio Limit Num Core 2 Ratio Limit Num Core2: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore3

  Offset 0x08C2 - Ratio Limit Core 3 Ratio Limit Num Core3: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore4

  Offset 0x08C3 - Ratio Limit Num Core 4 Ratio Limit Num Core4: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore5

  Offset 0x08C4 - Ratio Limit Num Core 5 Ratio Limit Num Core5: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore6

  Offset 0x08C5 - Ratio Limit Num Core 6 Ratio Limit Num Core6: This register defines the active core ranges for each frequency point.
- UINT8 RatioLimitNumCore7

  Offset 0x08C6 - Ratio Limit Num Core 7 Ratio Limit Num Core7: This register defines the active core ranges for each frequency point.
- UINT8 DualTauBoost

  Offset 0x08C7 - Dual Tau Boost Enable, Disable Dual Tau Boost feature.
- UINT8 ItbmPeriodicSmmTimer

  Offset 0x08C8 - ITBMT 3.0 Runtime Periodic SMM timer Periodic SMM Polling timer for ITBMT 3.0 ***Default 4 - 8 Sec****.*
- UINT8 ReservedCpuPostMemTest [9]

  Offset 0x08C9 - ReservedCpuPostMemTest Reserved for CPU Post-Mem Test $EN_DIS.
- UINT8 SgxSinitDataFromTpm

  Offset 0x08D2 - SgxSinitDataFromTpm SgxSinitDataFromTpm default values.
- UINT8 EndOfPostMessage

  Offset 0x08D3 - End of Post message Test, Send End of Post message.
- UINT8 DisableD0I3SettingForHeci

  Offset 0x08D4 - D0I3 Setting for HECI Disable Test, 0: disable, 1: enable, Setting this option disables setting D0I3 bit for all HECI devices $EN_DIS.
- UINT8 UnusedUpdSpace28

  Offset 0x08D5.
- UINT16 PchHdaResetWaitTimer

  Offset 0x08D6 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.
- UINT8 PchLockDownGlobalSmi

  Offset 0x08D8 - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.
- UINT8 PchLockDownBiosInterface

  Offset 0x08D9 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.
- UINT8 PchUnlockGpioPads

Offset 0x08DA - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.

- UINT8 PchSbAccessUnlock

  Offset 0x08DB - PCH Unlock SideBand access The SideBand PortID mask for certain end point (e.g.
- UINT16 PcieRpLtrMaxSnoopLatency [24]

  Offset 0x08DC - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.
- UINT16 PcieRpLtrMaxNoSnoopLatency [24]

  Offset 0x090C - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.
- UINT8 PcieRpSnoopLatencyOverrideMode [24]

  Offset 0x093C - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.
- UINT8 PcieRpSnoopLatencyOverrideMultiplier [24]

  Offset 0x0954 - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.
- UINT16 PcieRpSnoopLatencyOverrideValue [24]

  Offset 0x096C - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.
- UINT8 PcieRpNonSnoopLatencyOverrideMode [24]

  Offset 0x099C - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.
- UINT8 PcieRpNonSnoopLatencyOverrideMultiplier [24]

  Offset 0x09B4 - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.
- UINT16 PcieRpNonSnoopLatencyOverrideValue [24]

  Offset 0x09CC - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.
- UINT8 PcieRpSlotPowerLimitScale [24]

  Offset 0x09FC - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.
- UINT16 PcieRpSlotPowerLimitValue [24]

  Offset 0x0A14 - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.
- UINT8 PcieRpUptp [24]

  Offset 0x0A44 - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.
- UINT8 PcieRpDptp [24]

  Offset 0x0A5C - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.
- UINT8 PcieEnablePort8xhDecode

  Offset 0x0A74 - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.
- UINT8 PchPciePort8xhDecodePortIndex

  Offset 0x0A75 - PCIE Port8xh Decode Port Index The Index of PCIe Port that is selected for Port8xh Decode (0 Based).
- UINT8 PchPmDisableEnergyReport

  Offset 0x0A76 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.
- UINT8 SataTestMode

  Offset 0x0A77 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.
- UINT8 PchXhciOcLock

  Offset 0x0A78 - PCH USB OverCurrent mapping lock enable If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.
- UINT8 Usb3HsioRxCtrlCompMult [10]

  Offset 0x0A79 - CTLE Rate control CPR RCOMP multiplier (Double Rate) CTLE Rate control CPR RCOMP multiplier (Double Rate), HSIO_RX_DWORD27 [31:24], One byte for each port.
- UINT8 ReservedPchPostMemTest [6]

  Offset 0x0A83 - ReservedPchPostMemTest Reserved for Pch Post-Mem Test $EN_DIS.
- UINT8 MctpBroadcastCycle

*Offset 0x0A89 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.*

- UINT8 EmmcUseCustomDlls

  Offset 0x0A8A - Use DLL values from policy Set if FSP should use HS400 DLL values from policy $EN_DIS.
- UINT8 UnusedUpdSpace29

  Offset 0x0A8B.
- UINT32 EmmcTxCmdDelayRegValue

  Offset 0x0A8C - Emmc Tx CMD Delay control register value Please see Tx CMD Delay Control register definition for help.
- UINT32 EmmcTxDataDelay1RegValue

  Offset 0x0A90 - Emmc Tx DATA Delay control 1 register value Please see Tx DATA Delay control 1 register definition for help.
- UINT32 EmmcTxDataDelay2RegValue

  Offset 0x0A94 - Emmc Tx DATA Delay control 2 register value Please see Tx DATA Delay control 2 register definition for help.
- UINT32 EmmcRxCmdDataDelay1RegValue

  Offset 0x0A98 - Emmc Rx CMD + DATA Delay control 1 register value Please see Rx CMD + DATA Delay control 1 register definition for help.
- UINT32 EmmcRxCmdDataDelay2RegValue

  Offset 0x0A9C - Emmc Rx CMD + DATA Delay control 2 register value Please see Rx CMD + DATA Delay control 2 register definition for help.
- UINT32 EmmcRxStrobeDelayRegValue

  Offset 0x0AA0 - Emmc Rx Strobe Delay control register value Please see Rx Strobe Delay control register definition for help.
- UINT8 SdCardUseCustomDlls

  Offset 0x0AA4 - Use tuned DLL values from policy Set if FSP should use HS400 DLL values from policy $EN_DIS.
- UINT8 UnusedUpdSpace30 [3]

  Offset 0x0AA5.
- UINT32 SdCardTxCmdDelayRegValue

  Offset 0x0AA8 - SdCard Tx CMD Delay control register value Please see Tx CMD Delay Control register definition for help.
- UINT32 SdCardTxDataDelay1RegValue

  Offset 0x0AAC - SdCard Tx DATA Delay control 1 register value Please see Tx DATA Delay control 1 register definition for help.
- UINT32 SdCardTxDataDelay2RegValue

  Offset 0x0AB0 - SdCard Tx DATA Delay control 2 register value Please see Tx DATA Delay control 2 register definition for help.
- UINT32 SdCardRxCmdDataDelay1RegValue

  Offset 0x0AB4 - SdCard Rx CMD + DATA Delay control 1 register value Please see Rx CMD + DATA Delay control 1 register definition for help.
- UINT32 SdCardRxCmdDataDelay2RegValue

  Offset 0x0AB8 - SdCard Rx CMD + DATA Delay control 2 register value Please see Rx CMD + DATA Delay control 2 register definition for help.
- UINT8 EnforceEDebugMode

  Offset 0x0ABC - Enforce Enhanced Debug Mode Determine if ME should enter Enhanced Debug Mode.
- UINT8 UnusedUpdSpace31 [3]

  Offset 0x0ABD.
- UINT32 LogoPixelHeight

  Offset 0x0AC0 - LogoPixelHeight Address Address of LogoPixelHeight.
- UINT32 LogoPixelWidth

  Offset 0x0AC4 - LogoPixelWidth Address Address of LogoPixelWidth.
- UINT8 UnusedUpdSpace32 [4]

  Offset 0x0AC8.
- UINT8 ReservedFspsTestUpd [4]

  Offset 0x0ACC.

13.38.1 Detailed Description

Fsp S Test Configuration.

Definition at line 2575 of file FspsUpd.h.

13.38.2 Member Data Documentation

13.38.2.1 ApIdleManner

```
UINT8 FSP_S_TEST_CONFIG::ApIdleManner
```

Offset 0x0803 - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.

1: HALT loop, 2: MWAIT loop, 3: RUN loop

Definition at line 2898 of file FspsUpd.h.

13.38.2.2 AutoThermalReporting

```
UINT8 FSP_S_TEST_CONFIG::AutoThermalReporting
```

Offset 0x081D - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2988 of file FspsUpd.h.

13.38.2.3 C1e

```
UINT8 FSP_S_TEST_CONFIG::C1e
```

Offset 0x0821 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

0: Disable; **1: Enable** $EN_DIS

Definition at line 3012 of file FspsUpd.h.

13.38.2.4 C1StateAutoDemotion

```
UINT8 FSP_S_TEST_CONFIG::C1StateAutoDemotion
```

Offset 0x08B8 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.

Disable; **1: Enable** $EN_DIS

Definition at line 3312 of file FspsUpd.h.

13.38.2.5 C1StateUnDemotion

```
UINT8 FSP_S_TEST_CONFIG::C1StateUnDemotion
```

Offset 0x08B9 - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.

Disable; **1: Enable** $EN_DIS

Definition at line 3318 of file FspsUpd.h.

13.38.2.6 C3StateAutoDemotion

```
UINT8 FSP_S_TEST_CONFIG::C3StateAutoDemotion
```

Offset 0x08BD - Enable or Disable C3 Cstate Demotion Enable or Disable C3 Cstate Demotion.

Disable; **1: Enable** $EN_DIS

Definition at line 3343 of file FspsUpd.h.

13.38.2.7 C3StateUnDemotion

```
UINT8 FSP_S_TEST_CONFIG::C3StateUnDemotion
```

Offset 0x08BE - Enable or Disable C3 Cstate UnDemotion Enable or Disable C3 Cstate UnDemotion.

Disable; **1: Enable** $EN_DIS

Definition at line 3349 of file FspsUpd.h.

13.38.2.8 ConfigTdpBios

```
UINT8 FSP_S_TEST_CONFIG::ConfigTdpBios
```

Offset 0x07F9 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2837 of file FspsUpd.h.

13.38.2.9 CpuWakeUpTimer

```
UINT8 FSP_S_TEST_CONFIG::CpuWakeUpTimer
```

Offset 0x08BA - CpuWakeUpTimer Enable long CPU Wakeup Timer.

When enabled, the cpu internal wakeup time is increased to 180 seconds. 0: Disable; **1: Enable** $EN_DIS

Definition at line 3325 of file FspsUpd.h.

13.38.2.10 CStatePreWake

```
UINT8 FSP_S_TEST_CONFIG::CStatePreWake
```

Offset 0x0824 - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

0: Disable; **1: Enable** $EN_DIS

Definition at line 3030 of file FspsUpd.h.

13.38.2.11 CstCfgCtrIoMwaitRedirection

```
UINT8 FSP_S_TEST_CONFIG::CstCfgCtrIoMwaitRedirection
```

Offset 0x0826 - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 3042 of file FspsUpd.h.

13.38.2.12 Custom1ConfigTdpControl

```
UINT8 FSP_S_TEST_CONFIG::Custom1ConfigTdpControl
```

Offset 0x07F1 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2793 of file FspsUpd.h.

13.38.2.13 Custom1PowerLimit1

```
UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit1
```

Offset 0x0890 - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3211 of file FspsUpd.h.

13.38.2.14 Custom1PowerLimit1Time

```
UINT8 FSP_S_TEST_CONFIG::Custom1PowerLimit1Time
```

Offset 0x07EF - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.

Valid Range 0 to 128, 0 = AUTO

Definition at line 2783 of file FspsUpd.h.

13.38.2.15 Custom1PowerLimit2

```
UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit2
```

Offset 0x0894 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3217 of file FspsUpd.h.

13.38.2.16 Custom1TurboActivationRatio

```
UINT8 FSP_S_TEST_CONFIG::Custom1TurboActivationRatio
```

Offset 0x07F0 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

Valid Range 0 to 255

Definition at line 2788 of file FspsUpd.h.

13.38.2.17 Custom2ConfigTdpControl

```
UINT8 FSP_S_TEST_CONFIG::Custom2ConfigTdpControl
```

Offset 0x07F4 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2809 of file FspsUpd.h.

13.38.2.18 Custom2PowerLimit1

```
UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit1
```

Offset 0x0898 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3223 of file FspsUpd.h.

13.38.2.19 Custom2PowerLimit1Time

```
UINT8 FSP_S_TEST_CONFIG::Custom2PowerLimit1Time
```

Offset 0x07F2 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.

Valid Range 0 to 128, 0 = AUTO

Definition at line 2799 of file FspsUpd.h.

13.38.2.20 Custom2PowerLimit2

```
UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit2
```

Offset 0x089C - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3229 of file FspsUpd.h.

13.38.2.21 Custom2TurboActivationRatio

```
UINT8 FSP_S_TEST_CONFIG::Custom2TurboActivationRatio
```

Offset 0x07F3 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

Valid Range 0 to 255

Definition at line 2804 of file FspsUpd.h.

13.38.2.22 Custom3ConfigTdpControl

```
UINT8 FSP_S_TEST_CONFIG::Custom3ConfigTdpControl
```

Offset 0x07F7 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2825 of file FspsUpd.h.

13.38.2.23 Custom3PowerLimit1

```
UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit1
```

Offset 0x08A0 - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3235 of file FspsUpd.h.

13.38.2.24 Custom3PowerLimit1Time

```
UINT8 FSP_S_TEST_CONFIG::Custom3PowerLimit1Time
```

Offset 0x07F5 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.

Valid Range 0 to 128, 0 = AUTO

Definition at line 2815 of file FspsUpd.h.

13.38.2.25 Custom3PowerLimit2

```
UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit2
```

Offset 0x08A4 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3241 of file FspsUpd.h.

13.38.2.26 Custom3TurboActivationRatio

```
UINT8 FSP_S_TEST_CONFIG::Custom3TurboActivationRatio
```

Offset 0x07F6 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

Valid Range 0 to 255

Definition at line 2820 of file FspsUpd.h.

13.38.2.27 Cx

```
UINT8 FSP_S_TEST_CONFIG::Cx
```

Offset 0x081F - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).

0: Disable; **1: Enable** $EN_DIS

Definition at line 3000 of file FspsUpd.h.

13.38.2.28 DebugInterfaceEnable

```
UINT8 FSP_S_TEST_CONFIG::DebugInterfaceEnable
```

Offset 0x0801 - Deprecated DO NOT USE Enable or Disable processor debug features.

Deprecated Enable or Disable processor debug features; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2886 of file FspsUpd.h.

13.38.2.29 DebugInterfaceLockEnable

```
UINT8 FSP_S_TEST_CONFIG::DebugInterfaceLockEnable
```

Offset 0x0802 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2892 of file FspsUpd.h.

13.38.2.30 DisableProcHotOut

```
UINT8 FSP_S_TEST_CONFIG::DisableProcHotOut
```

Offset 0x081A - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2970 of file FspsUpd.h.

13.38.2.31 DisableVrThermalAlert

```
UINT8 FSP_S_TEST_CONFIG::DisableVrThermalAlert
```

Offset 0x081C - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2982 of file FspsUpd.h.

13.38.2.32 DualTauBoost

```
UINT8 FSP_S_TEST_CONFIG::DualTauBoost
```

Offset 0x08C7 - Dual Tau Boost Enable, Disable Dual Tau Boost feature.

This is only applicable for CMLS; **0: Disable**; 1: Enable $EN_DIS

Definition at line 3396 of file FspsUpd.h.

13.38.2.33 EightCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::EightCoreRatioLimit
```

Offset 0x08B5 - 8-Core Ratio Limit 8-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 8-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255 0x0:0xFF

Definition at line 3294 of file FspsUpd.h.

13.38.2.34 Eist

```
UINT8 FSP_S_TEST_CONFIG::Eist
```

Offset 0x0815 - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

0: Disable; **1: Enable** $EN_DIS

Definition at line 2938 of file FspsUpd.h.

13.38.2.35 EnableItbm

```
UINT8 FSP_S_TEST_CONFIG::EnableItbm
```

Offset 0x08B6 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.

0: Disabled; **1: Enabled** $EN_DIS

Definition at line 3300 of file FspsUpd.h.

13.38.2.36 EnableItbmDriver

```
UINT8 FSP_S_TEST_CONFIG::EnableItbmDriver
```

Offset 0x08B7 - Intel Turbo Boost Max Technology 3.0 Driver.

Deprecated Intel Turbo Boost Max Technology 3.0 Driver **0: Disabled**; 1: Enabled $EN_DIS

Definition at line 3306 of file FspsUpd.h.

13.38.2.37 EndOfPostMessage

```
UINT8 FSP_S_TEST_CONFIG::EndOfPostMessage
```

Offset 0x08D3 - End of Post message Test, Send End of Post message.

Disable(0x0): Disable EOP message, Enable(0x1)(Default): Enable EOP message $EN_DIS

Definition at line 3421 of file FspsUpd.h.

13.38.2.38 EnergyEfficientPState

```
UINT8 FSP_S_TEST_CONFIG::EnergyEfficientPState
```

Offset 0x0816 - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.

Disable; **1: Enable** $EN_DIS

Definition at line 2945 of file FspsUpd.h.

13.38.2.39 EnergyEfficientTurbo

```
UINT8 FSP_S_TEST_CONFIG::EnergyEfficientTurbo
```

Offset 0x0817 - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.

Disable; 1: Enable, **2: Auto** / **Silicon default** 0: Disable, 1: Enable, 2: Auto

Definition at line 2952 of file FspsUpd.h.

13.38.2.40 EnforceEDebugMode

```
UINT8 FSP_S_TEST_CONFIG::EnforceEDebugMode
```

Offset 0x0ABC - Enforce Enhanced Debug Mode Determine if ME should enter Enhanced Debug Mode.

0: disable, 1: enable $EN_DIS

Definition at line 3652 of file FspsUpd.h.

13.38.2.41 FiveCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::FiveCoreRatioLimit
```

Offset 0x08B2 - 5-Core Ratio Limit 5-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 5-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255 0x0:0xFF

Definition at line 3273 of file FspsUpd.h.

13.38.2.42 FourCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::FourCoreRatioLimit
```

Offset 0x07E1 - 4-Core Ratio Limit 4-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 4-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255

Definition at line 2694 of file FspsUpd.h.

13.38.2.43 HdcControl

```
UINT8 FSP_S_TEST_CONFIG::HdcControl
```

Offset 0x07E3 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

0: Disabled; **1: Enabled** 2-3:Reserved $EN_DIS

Definition at line 2707 of file FspsUpd.h.

13.38.2.44 Hwp

```
UINT8 FSP_S_TEST_CONFIG::Hwp
```

Offset 0x07E2 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

0: Disable; **1: Enable;** 2-3:Reserved $EN_DIS

Definition at line 2701 of file FspsUpd.h.

13.38.2.45 HwpInterruptControl

```
UINT8 FSP_S_TEST_CONFIG::HwpInterruptControl
```

Offset 0x08B1 - Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 3266 of file FspsUpd.h.

13.38.2.46 ItbmPeriodicSmmTimer

```
UINT8 FSP_S_TEST_CONFIG::ItbmPeriodicSmmTimer
```

Offset 0x08C8 - ITBMT 3.0 Runtime Periodic SMM timer Periodic SMM Polling timer for ITBMT 3.0 **Default 4 - 8 Sec**.

0 = Diable periodic SMM, and Valid values 1 - 16ms , 2 - 32ms , 3 - 64ms , 4 - 8 sec , 5 - 16 sec, 6 - 32 sec, 7 - 64 sec.

Definition at line 3403 of file FspsUpd.h.

13.38.2.47 MachineCheckEnable

```
UINT8 FSP_S_TEST_CONFIG::MachineCheckEnable
```

Offset 0x0800 - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2880 of file FspsUpd.h.

13.38.2.48 MaxRingRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::MaxRingRatioLimit
```

Offset 0x08BC - Minimum Ring ratio limit override Maximum Ring ratio limit override.

0: Hardware defaults. Range: 0 - Max turbo ratio limit

Definition at line 3337 of file FspsUpd.h.

13.38.2.49 MctpBroadcastCycle

```
UINT8 FSP_S_TEST_CONFIG::MctpBroadcastCycle
```

Offset 0x0A89 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 3571 of file FspsUpd.h.

13.38.2.50 MinRingRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::MinRingRatioLimit
```

Offset 0x08BB - Minimum Ring ratio limit override Minimum Ring ratio limit override.

0: Hardware defaults. Range: 0 - Max turbo ratio limit

Definition at line 3331 of file FspsUpd.h.

13.38.2.51 MlcStreamerPrefetcher

```
UINT8 FSP_S_TEST_CONFIG::MlcStreamerPrefetcher
```

Offset 0x07FD - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0↩ : Disable; **1: Enable**.

$EN_DIS

Definition at line 2862 of file FspsUpd.h.

13.38.2.52 MonitorMwaitEnable

```
UINT8 FSP_S_TEST_CONFIG::MonitorMwaitEnable
```

Offset 0x07FF - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2874 of file FspsUpd.h.

13.38.2.53 NumberOfEntries

```
UINT8 FSP_S_TEST_CONFIG::NumberOfEntries
```

Offset 0x07EE - Custom Ratio State Entries The number of custom ratio state entries, ranges from 0 to 40 for a valid custom ratio table.Sets the number of custom P-states.

At least 2 states must be present

Definition at line 2777 of file FspsUpd.h.

13.38.2.54 OneCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::OneCoreRatioLimit
```

Offset 0x07DE - 1-Core Ratio Limit 1-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 1-Core Ratio Limit Must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit, 5-Core Ratio Limit, 6-Core Ratio Limit, 7-Core Ratio Limit, 8-Core Ratio Limit. Range is 0 to 255

Definition at line 2676 of file FspsUpd.h.

13.38.2.55 PchHdaResetWaitTimer

```
UINT16 FSP_S_TEST_CONFIG::PchHdaResetWaitTimer
```

Offset 0x08D6 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.

Default is 600.

Definition at line 3437 of file FspsUpd.h.

13.38.2.56 PchLockDownBiosInterface

```
UINT8 FSP_S_TEST_CONFIG::PchLockDownBiosInterface
```

Offset 0x08D9 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

$EN_DIS

Definition at line 3449 of file FspsUpd.h.

13.38.2.57 PchLockDownGlobalSmi

```
UINT8 FSP_S_TEST_CONFIG::PchLockDownGlobalSmi
```

Offset 0x08D8 - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.

$EN_DIS

Definition at line 3443 of file FspsUpd.h.

13.38.2.58 PchPmDisableEnergyReport

```
UINT8 FSP_S_TEST_CONFIG::PchPmDisableEnergyReport
```

Offset 0x0A76 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.

$EN_DIS

Definition at line 3540 of file FspsUpd.h.

13.38.2.59 PchSbAccessUnlock

```
UINT8 FSP_S_TEST_CONFIG::PchSbAccessUnlock
```

Offset 0x08DB - PCH Unlock SideBand access The SideBand PortID mask for certain end point (e.g.

PSFx) will be locked before 3rd party code execution. 0: Lock SideBand access; 1: Unlock SideBand access. $EN_DIS

Definition at line 3462 of file FspsUpd.h.

13.38.2.60 PchUnlockGpioPads

```
UINT8 FSP_S_TEST_CONFIG::PchUnlockGpioPads
```

Offset 0x08DA - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.

$EN_DIS

Definition at line 3455 of file FspsUpd.h.

13.38.2.61 PchXhciOcLock

```
UINT8 FSP_S_TEST_CONFIG::PchXhciOcLock
```

Offset 0x0A78 - PCH USB OverCurrent mapping lock enable If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.

$EN_DIS

Definition at line 3553 of file FspsUpd.h.

13.38.2.62 PcieEnablePort8xhDecode

```
UINT8 FSP_S_TEST_CONFIG::PcieEnablePort8xhDecode
```

Offset 0x0A74 - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.

0: Disable; 1: Enable. $EN_DIS

Definition at line 3529 of file FspsUpd.h.

13.38.2.63 PcieRpDptp

```
UINT8 FSP_S_TEST_CONFIG::PcieRpDptp[24]
```

Offset 0x0A5C - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 3522 of file FspsUpd.h.

13.38.2.64 PcieRpSlotPowerLimitScale

```
UINT8 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitScale[24]
```

Offset 0x09FC - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

Leave as 0 to set to default.

Definition at line 3507 of file FspsUpd.h.

13.38.2.65 PcieRpSlotPowerLimitValue

```
UINT16 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitValue[24]
```

Offset 0x0A14 - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.

Leave as 0 to set to default.

Definition at line 3512 of file FspsUpd.h.

13.38.2.66 PcieRpUptp

```
UINT8 FSP_S_TEST_CONFIG::PcieRpUptp[24]
```

Offset 0x0A44 - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 3517 of file FspsUpd.h.

13.38.2.67 PkgCStateDemotion

```
UINT8 FSP_S_TEST_CONFIG::PkgCStateDemotion
```

Offset 0x0822 - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.

0: Disable; 1: Enable $EN_DIS

Definition at line 3018 of file FspsUpd.h.

13.38.2.68 PkgCStateLimit

```
UINT8 FSP_S_TEST_CONFIG::PkgCStateLimit
```

Offset 0x0827 - Set the Max Pkg Cstate Set the Max Pkg Cstate.

Default set to Auto which limits the Max Pkg Cstate to deep C-state. Valid values 0 - C0/C1 , 1 - C2 , 2 - C3 , 3 - C6 , 4 - C7 , 5 - C7S , 6 - C8 , 7 - C9 , 8 - C10 , 254 - CPU Default , 255 - Auto

Definition at line 3049 of file FspsUpd.h.

13.38.2.69 PkgCStateUnDemotion

```
UINT8 FSP_S_TEST_CONFIG::PkgCStateUnDemotion
```

Offset 0x0823 - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.

0: Disable; 1: Enable $EN_DIS

Definition at line 3024 of file FspsUpd.h.

13.38.2.70 PmgCstCfgCtrlLock

```
UINT8 FSP_S_TEST_CONFIG::PmgCstCfgCtrlLock
```

Offset 0x0820 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 3006 of file FspsUpd.h.

13.38.2.71 PowerLimit1

```
UINT32 FSP_S_TEST_CONFIG::PowerLimit1
```

Offset 0x087C - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit. Valid Range 0 to 4095875 in Step size of 125

Definition at line 3181 of file FspsUpd.h.

13.38.2.72 PowerLimit1Time

```
UINT8 FSP_S_TEST_CONFIG::PowerLimit1Time
```

Offset 0x07E4 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.

0 = AUTO, uses 28 seconds. Valid values(Unit in seconds) 1 to 8 , 10 , 12 ,14 , 16 , 20 , 24 , 28 , 32 , 40 , 48 , 56 , 64 , 80 , 96 , 112 , 128

Definition at line 2714 of file FspsUpd.h.

13.38.2.73 PowerLimit2

```
UINT8 FSP_S_TEST_CONFIG::PowerLimit2
```

Offset 0x07E5 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

0 : Disable; **1: Enable** $EN_DIS

Definition at line 2720 of file FspsUpd.h.

13.38.2.74 PowerLimit2Power

```
UINT32 FSP_S_TEST_CONFIG::PowerLimit2Power
```

Offset 0x0880 - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3187 of file FspsUpd.h.

13.38.2.75 PowerLimit3

```
UINT32 FSP_S_TEST_CONFIG::PowerLimit3
```

Offset 0x0884 - Package PL3 power limit Package PL3 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3193 of file FspsUpd.h.

13.38.2.76 PowerLimit4

```
UINT32 FSP_S_TEST_CONFIG::PowerLimit4
```

Offset 0x0888 - Package PL4 power limit Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 1023875 in Step size of 125

Definition at line 3199 of file FspsUpd.h.

13.38.2.77 ProcessorTraceEnable

```
UINT8 FSP_S_TEST_CONFIG::ProcessorTraceEnable
```

Offset 0x0805 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2910 of file FspsUpd.h.

13.38.2.78 ProcessorTraceMemBase

```
UINT64 FSP_S_TEST_CONFIG::ProcessorTraceMemBase
```

Offset 0x0808 - Base of memory region allocated for Processor Trace Base address of memory region allocated for Processor Trace.

Processor Trace requires 2^N alignment and size in bytes per thread, from 4KB to 128MB. **0: Disable**

Definition at line 2920 of file FspsUpd.h.

13.38.2.79 ProcessorTraceMemLength

```
UINT32 FSP_S_TEST_CONFIG::ProcessorTraceMemLength
```

Offset 0x0810 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.

Processor Trace requires 2^N alignment and size in bytes per thread, from 4KB to 128MB. **0: Disable**

Definition at line 2926 of file FspsUpd.h.

13.38.2.80 ProcessorTraceOutputScheme

```
UINT8 FSP_S_TEST_CONFIG::ProcessorTraceOutputScheme
```

Offset 0x0804 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.

0: Single Range Output, 1: ToPA Output

Definition at line 2904 of file FspsUpd.h.

13.38.2.81 ProcHotResponse

```
UINT8 FSP_S_TEST_CONFIG::ProcHotResponse
```

Offset 0x081B - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2976 of file FspsUpd.h.

13.38.2.82 PsysPmax

```
UINT16 FSP_S_TEST_CONFIG::PsysPmax
```

Offset 0x086C - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.

0 - Auto Specified in 1/8 Watt increments. Range 0-1024 Watts. Value of 800 = 100W

Definition at line 3141 of file FspsUpd.h.

13.38.2.83 PsysPowerLimit1

```
UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit1
```

Offset 0x07FA - PL1 Enable value PL1 Enable value to limit average platform power.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2843 of file FspsUpd.h.

13.38.2.84 PsysPowerLimit1Power

```
UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit1Power
```

Offset 0x08A8 - Platform PL1 power Platform PL1 power.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3247 of file FspsUpd.h.

13.38.2.85 PsysPowerLimit1Time

```
UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit1Time
```

Offset 0x07FB - PL1 timewindow PL1 timewindow in seconds.

0 = AUTO, uses 28 seconds. Valid values(Unit in seconds) 1 to 8 , 10 , 12 ,14 , 16 , 20 , 24 , 28 , 32 , 40 , 48 , 56 , 64 , 80 , 96 , 112 , 128

Definition at line 2849 of file FspsUpd.h.

13.38.2.86 PsysPowerLimit2

```
UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit2
```

Offset 0x07FC - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2856 of file FspsUpd.h.

13.38.2.87 PsysPowerLimit2Power

```
UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit2Power
```

Offset 0x08AC - Platform PL2 power Platform PL2 power.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 3253 of file FspsUpd.h.

13.38.2.88 RaceToHalt

```
UINT8 FSP_S_TEST_CONFIG::RaceToHalt
```

Offset 0x0831 - Race To Halt Enable/Disable Race To Halt feature.

RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)Disable; **1: Enable** $EN_DIS

Definition at line 3110 of file FspsUpd.h.

13.38.2.89 SataTestMode

```
UINT8 FSP_S_TEST_CONFIG::SataTestMode
```

Offset 0x0A77 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

$EN_DIS

Definition at line 3546 of file FspsUpd.h.

13.38.2.90 SevenCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::SevenCoreRatioLimit
```

Offset 0x08B4 - 7-Core Ratio Limit 7-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 7-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255 0x0:0xFF

Definition at line 3287 of file FspsUpd.h.

13.38.2.91 SixCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::SixCoreRatioLimit
```

Offset 0x08B3 - 6-Core Ratio Limit 6-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 6-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255 0x0:0xFF

Definition at line 3280 of file FspsUpd.h.

13.38.2.92 StateRatio

```
UINT8 FSP_S_TEST_CONFIG::StateRatio[40]
```

Offset 0x0833 - P-state ratios for custom P-state table P-state ratios for custom P-state table.

NumberOfEntries has valid range between 0 to 40. For no. of P-States supported(NumberOfEntries) , State↩ Ratio[NumberOfEntries] are configurable. Valid Range of each entry is 0 to 0x7F

Definition at line 3122 of file FspsUpd.h.

13.38.2.93 StateRatioMax16

```
UINT8 FSP_S_TEST_CONFIG::StateRatioMax16[16]
```

Offset 0x085B - P-state ratios for max 16 version of custom P-state table P-state ratios for max 16 version of custom P-state table.

This table is used for OS versions limited to a max of 16 P-States. If the first entry of this table is 0, or if Number of Entries is 16 or less, then this table will be ignored, and up to the top 16 values of the StateRatio table will be used instead. Valid Range of each entry is 0 to 0x7F

Definition at line 3131 of file FspsUpd.h.

13.38.2.94 TccActivationOffset

```
UINT8 FSP_S_TEST_CONFIG::TccActivationOffset
```

Offset 0x07EB - TCC Activation Offset TCC Activation Offset.

Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated. TCC will be activated at TCC Activation Temperature, in volts.For Y SKU, the recommended default for this policy is **15**, For all other SKUs the recommended default are **0**

Definition at line 2756 of file FspsUpd.h.

13.38.2.95 TccOffsetClamp

```
UINT8 FSP_S_TEST_CONFIG::TccOffsetClamp
```

Offset 0x07EC - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For Y SKU, the recommended default for this policy is **1: Enabled**, For all other SKUs the recommended default are **0: Disabled**.

$EN_DIS

Definition at line 2764 of file FspsUpd.h.

13.38.2.96 TccOffsetLock

```
UINT8 FSP_S_TEST_CONFIG::TccOffsetLock
```

Offset 0x07ED - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; 1: Enabled.

$EN_DIS

Definition at line 2771 of file FspsUpd.h.

13.38.2.97 TccOffsetTimeWindowForRatl

```
UINT32 FSP_S_TEST_CONFIG::TccOffsetTimeWindowForRatl
```

Offset 0x088C - Tcc Offset Time Window for RATL Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 1023875 in Step size of 125

Definition at line 3205 of file FspsUpd.h.

13.38.2.98 ThreeCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::ThreeCoreRatioLimit
```

Offset 0x07E0 - 3-Core Ratio Limit 3-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 3-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255

Definition at line 2688 of file FspsUpd.h.

13.38.2.99 ThreeStrikeCounterDisable

```
UINT8 FSP_S_TEST_CONFIG::ThreeStrikeCounterDisable
```

Offset 0x08B0 - Set Three Strike Counter Disable False (default): Three Strike counter will be incremented and True: Prevents Three Strike counter from incrementing; **0: False**; 1: True.

0: False, 1: True

Definition at line 3260 of file FspsUpd.h.

13.38.2.100 TimedMwait

```
UINT8 FSP_S_TEST_CONFIG::TimedMwait
```

Offset 0x0825 - Enable or Disable TimedMwait Support.

Enable or Disable TimedMwait Support. **0: Disable**; 1: Enable $EN_DIS

Definition at line 3036 of file FspsUpd.h.

13.38.2.101 TStates

```
UINT8 FSP_S_TEST_CONFIG::TStates
```

Offset 0x0818 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2958 of file FspsUpd.h.

13.38.2.102 TwoCoreRatioLimit

```
UINT8 FSP_S_TEST_CONFIG::TwoCoreRatioLimit
```

Offset 0x07DF - 2-Core Ratio Limit 2-Core Ratio Limit: LFM to Fused, For overclocking part: LFM to 255.

This 2-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 255

Definition at line 2682 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.39 FSP_T_CONFIG Struct Reference

Fsp T Configuration.

```
#include <FsptUpd.h>
```

Public Attributes

- UINT8 PcdSerialIoUartDebugEnable

  Offset 0x0040 - PcdSerialIoUartDebugEnable Enable SerialIo Uart debug library with/without initializing SerialIo Uart device in FSP.
- UINT8 PcdSerialIoUartNumber

  Offset 0x0041 - PcdSerialIoUartNumber - FSPT Select SerialIo Uart Controller for debug.
- UINT8 PcdSerialIoUartMode

  Offset 0x0042 - PcdSerialIoUartMode - FSPT Select SerialIo Uart Controller mode 0:SerialIoUartDisabled, 1:Serial←IoUartPci, 2:SerialIoUartHidden, 3:SerialIoUartCom, 4:SerialIoUartSkipInit.
- UINT8 UnusedUpdSpace0

  Offset 0x0043.
- UINT32 PcdSerialIoUartBaudRate

  Offset 0x0044 - PcdSerialIoUartBaudRate - FSPT Set default BaudRate Supported from 0 - default to 6000000.
- UINT64 PcdPciExpressBaseAddress

  Offset 0x0048 - Pci Express Base Address Base address to be programmed for Pci Express.
- UINT32 PcdPciExpressRegionLength

  Offset 0x0050 - Pci Express Region Length Region Length to be programmed for Pci Express.
- UINT8 PcdSerialIoUartParity

  Offset 0x0054 - PcdSerialIoUartParity - FSPT Set default Parity.
- UINT8 PcdSerialIoUartDataBits

  Offset 0x0055 - PcdSerialIoUartDataBits - FSPT Set default word length.
- UINT8 PcdSerialIoUartStopBits

  Offset 0x0056 - PcdSerialIoUartStopBits - FSPT Set default stop bits.
- UINT8 PcdSerialIoUartAutoFlow

  Offset 0x0057 - PcdSerialIoUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.
- UINT8 PcdSerialIoUartPinMux

  *Offset 0x0058 - PcdSerialIoUartPinMux - FSPT Applies only to UART0 muxed with CNVI **0 = GPIO C8 to C11** 1 = GPIO F5 - F7 (PCH LP) J5 - J7 (PCH H) 0: GPIO C8 to C11, 1: GPIO F5 - F7 (PCH LP) J5 - J7 (PCH H)*
- UINT8 PcdLpcUartDebugEnable

  Offset 0x0059 - PcdLpcUartDebugEnable Enable to initialize LPC Uart device in FSP.
- UINT8 PcdDebugInterfaceFlags

  Offset 0x005A - Debug Interfaces Debug Interfaces.
- UINT8 PcdSerialDebugLevel

  Offset 0x005B - PcdSerialDebugLevel Serial Debug Message Level.
- UINT8 PcdIsaSerialUartBase

  Offset 0x005C - ISA Serial Base selection Select ISA Serial Base address.
- UINT8 UnusedUpdSpace1 [7]

  Offset 0x005D.
- UINT8 ReservedFsptUpd1 [20]

  Offset 0x0064.

13.39.1 Detailed Description

Fsp T Configuration.

Definition at line 68 of file FsptUpd.h.

13.39.2 Member Data Documentation

13.39.2.1 PcdDebugInterfaceFlags

```
UINT8 FSP_T_CONFIG::PcdDebugInterfaceFlags
```

Offset 0x005A - Debug Interfaces Debug Interfaces.

BIT0-RAM, BIT1-UART, BIT3-USB3, BIT4-Serial IO, BIT5-TraceHub, BIT2 - Not used.

Definition at line 149 of file FsptUpd.h.

13.39.2.2 PcdIsaSerialUartBase

```
UINT8 FSP_T_CONFIG::PcdIsaSerialUartBase
```

Offset 0x005C - ISA Serial Base selection Select ISA Serial Base address.

Default is 0x3F8. 0:0x3F8, 1:0x2F8

Definition at line 164 of file FsptUpd.h.

13.39.2.3 PcdLpcUartDebugEnable

```
UINT8 FSP_T_CONFIG::PcdLpcUartDebugEnable
```

Offset 0x0059 - PcdLpcUartDebugEnable Enable to initialize LPC Uart device in FSP.

0:Disable, 1:Enable

Definition at line 143 of file FsptUpd.h.

13.39.2.4 PcdSerialDebugLevel

```
UINT8 FSP_T_CONFIG::PcdSerialDebugLevel
```

Offset 0x005B - PcdSerialDebugLevel Serial Debug Message Level.

0:Disable, 1:Error Only, 2:Error & Warnings, 3:Load, Error, Warnings & Info, 4:Load, Error, Warnings, Info & Event, 5:Load, Error, Warnings, Info & Verbose. 0:Disable, 1:Error Only, 2:Error and Warnings, 3:Load Error Warnings and Info, 4:Load Error Warnings and Info, 5:Load Error Warnings Info and Verbose

Definition at line 158 of file FsptUpd.h.

13.39.2.5 PcdSerialIoUartAutoFlow

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartAutoFlow
```

Offset 0x0057 - PcdSerialIoUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.

0: Disable, 1:Enable

Definition at line 130 of file FsptUpd.h.

13.39.2.6 PcdSerialIoUartDataBits

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartDataBits
```

Offset 0x0055 - PcdSerialIoUartDataBits - FSPT Set default word length.

0: Default, 5,6,7,8

Definition at line 118 of file FsptUpd.h.

13.39.2.7 PcdSerialIoUartDebugEnable

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartDebugEnable
```

Offset 0x0040 - PcdSerialIoUartDebugEnable Enable SerialIo Uart debug library with/without initializing SerialIo Uart device in FSP.

0:Disable, 1:Enable and Initialize, 2:Enable without Initializing

Definition at line 74 of file FsptUpd.h.

13.39.2.8 PcdSerialIoUartNumber

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartNumber
```

Offset 0x0041 - PcdSerialIoUartNumber - FSPT Select SerialIo Uart Controller for debug.

Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 81 of file FsptUpd.h.

13.39.2.9 PcdSerialIoUartParity

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartParity
```

Offset 0x0054 - PcdSerialIoUartParity - FSPT Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 113 of file FsptUpd.h.

13.39.2.10 PcdSerialIoUartStopBits

```
UINT8 FSP_T_CONFIG::PcdSerialIoUartStopBits
```

Offset 0x0056 - PcdSerialIoUartStopBits - FSPT Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 124 of file FsptUpd.h.

The documentation for this struct was generated from the following file:

- FsptUpd.h

13.40 FSP_T_RESTRICTED_CONFIG Struct Reference

Fsp T Restricted Configuration.

```
#include <FsptUpd.h>
```

Public Attributes

- UINT32 Signature

  Offset 0x0098.
- UINT8 ReservedFsptRestrictedUpd [12]

  Offset 0x009C.

13.40.1 Detailed Description

Fsp T Restricted Configuration.

Definition at line 190 of file FsptUpd.h.

The documentation for this struct was generated from the following file:

- FsptUpd.h

13.41 FSP_T_TEST_CONFIG Struct Reference

Fsp T Test Configuration.

```
#include <FsptUpd.h>
```

Public Attributes

- UINT32 Signature

  Offset 0x0078.
- UINT8 ReservedFsptTestUpd [28]

  Offset 0x007C.

13.41.1 Detailed Description

Fsp T Test Configuration.

Definition at line 177 of file FsptUpd.h.

The documentation for this struct was generated from the following file:

- FsptUpd.h

13.42 FSPM_ARCH_CONFIG_PPI Struct Reference

This PPI provides FSP-M Arch Config PPI.

```
#include <FspmArchConfigPpi.h>
```

13.42.1 Detailed Description

This PPI provides FSP-M Arch Config PPI.

Definition at line 31 of file FspmArchConfigPpi.h.

The documentation for this struct was generated from the following file:

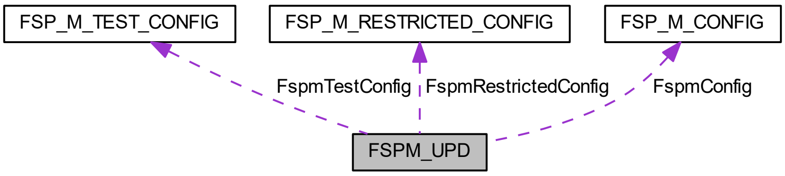
- FspmArchConfigPpi.h

13.43 FSPM_UPD Struct Reference

Fsp M UPD Configuration.

```
#include <FspmUpd.h>
```

Collaboration diagram for FSPM_UPD:



Public Attributes

- FSP_UPD_HEADER FspUpdHeader

  Offset 0x0000.
- FSPM_ARCH_UPD FspmArchUpd

  Offset 0x0020.
- FSP_M_CONFIG FspmConfig

  Offset 0x0040.
- FSP_M_TEST_CONFIG FspmTestConfig

  Offset 0x0558.
- FSP_M_RESTRICTED_CONFIG FspmRestrictedConfig

  Offset 0x0620.
- UINT8 UnusedUpdSpace14 [6]

  Offset 0x0730.
- UINT16 UpdTerminator

  Offset 0x0736.

13.43.1 Detailed Description

Fsp M UPD Configuration.

Definition at line 3881 of file FspmUpd.h.

The documentation for this struct was generated from the following file:

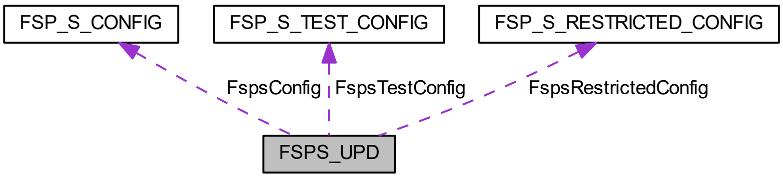
- FspmUpd.h

13.44 FSPS_UPD Struct Reference

Fsp S UPD Configuration.

```
#include <FspsUpd.h>
```

Collaboration diagram for FSPS_UPD:



Public Attributes

- FSP_UPD_HEADER FspUpdHeader

  Offset 0x0000.
- FSP_S_CONFIG FspsConfig

  Offset 0x0020.
- FSP_S_TEST_CONFIG FspsTestConfig

  Offset 0x07C0.
- FSP_S_RESTRICTED_CONFIG FspsRestrictedConfig

  Offset 0x0AD0.
- UINT8 UnusedUpdSpace36 [6]

  Offset 0x0C80.
- UINT16 UpdTerminator

  Offset 0x0C86.

13.44.1 Detailed Description

Fsp S UPD Configuration.

Definition at line 4509 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.45 FSPT_CORE_UPD Struct Reference

Fsp T Core UPD.

```
#include <FsptUpd.h>
```

Public Attributes

- UINT32 MicrocodeRegionBase

  Offset 0x0020.
- UINT32 MicrocodeRegionSize

  Offset 0x0024.
- UINT32 CodeRegionBase

  Offset 0x0028.
- UINT32 CodeRegionSize

  Offset 0x002C.
- UINT8 Reserved [16]

  Offset 0x0030.

13.45.1 Detailed Description

Fsp T Core UPD.

Definition at line 43 of file FsptUpd.h.

The documentation for this struct was generated from the following file:

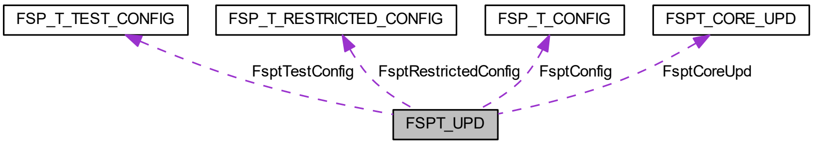
- FsptUpd.h

13.46 FSPT_UPD Struct Reference

Fsp T UPD Configuration.

```
#include <FsptUpd.h>
```

Collaboration diagram for FSPT_UPD:



Public Attributes

- FSP_UPD_HEADER FspUpdHeader

  Offset 0x0000.
- FSPT_CORE_UPD FsptCoreUpd

  Offset 0x0020.
- FSP_T_CONFIG FsptConfig

  Offset 0x0040.
- FSP_T_TEST_CONFIG FsptTestConfig

  Offset 0x0078.
- FSP_T_RESTRICTED_CONFIG FsptRestrictedConfig

  Offset 0x0098.
- UINT8 UnusedUpdSpace2 [6]

  Offset 0x00A8.
- UINT16 UpdTerminator

  Offset 0x00AE.

13.46.1 Detailed Description

Fsp T UPD Configuration.

Definition at line 203 of file FsptUpd.h.

The documentation for this struct was generated from the following file:

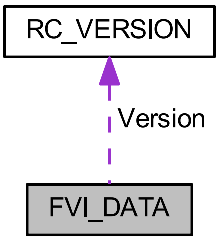
- FsptUpd.h

13.47 FVI_DATA Struct Reference

The string number for ComponentName and VersionString is always calculated dynamically.

```
#include <SiFviLib.h>
```

Collaboration diagram for FVI_DATA:



13.47.1 Detailed Description

The string number for ComponentName and VersionString is always calculated dynamically.

The initial value is ignored and should always be TO_BE_FILLED.

Definition at line 86 of file SiFviLib.h.

The documentation for this struct was generated from the following file:

- SiFviLib.h

13.48 GPIO_CONFIG Struct Reference

GPIO configuration structure used for pin programming.

```
#include <GpioConfig.h>
```

Public Attributes

- UINT32 PadMode: 5

  Pad Mode Pad can be set as GPIO or one of its native functions.
- UINT32 HostSoftPadOwn: 2

  Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.
- UINT32 Direction: 6

  GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.
- UINT32 OutputState: 2

  Output State Set Pad output value.
- UINT32 InterruptConfig: 9

  GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).
- UINT32 PowerConfig: 8

  GPIO Power Configuration.
- UINT32 ElectricalConfig: 9

  GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.
- UINT32 LockConfig: 4

  GPIO Lock Configuration This setting controls pads lock.
- UINT32 OtherSettings: 2

  Additional GPIO configuration Refer to definition of GPIO_OTHER_CONFIG for supported settings.
- UINT32 RsvdBits: 17

  Reserved bits for future extension.

13.48.1 Detailed Description

GPIO configuration structure used for pin programming.

Structure contains fields that can be used to configure pad.

Definition at line 55 of file GpioConfig.h.

13.48.2 Member Data Documentation

13.48.2.1 Direction

```
UINT32 GPIO_CONFIG::Direction
```

GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.

Refer to definition of GPIO_DIRECTION for supported settings.

Definition at line 76 of file GpioConfig.h.

13.48.2.2 ElectricalConfig

```
UINT32 GPIO_CONFIG::ElectricalConfig
```

GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.

Refer to definition of GPIO_ELECTRICAL_CONFIG for supported settings.

Definition at line 102 of file GpioConfig.h.

13.48.2.3 HostSoftPadOwn

```
UINT32 GPIO_CONFIG::HostSoftPadOwn
```

Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.

Refer to definition of GPIO_HOSTSW_OWN.

Definition at line 70 of file GpioConfig.h.

13.48.2.4 InterruptConfig

```
UINT32 GPIO_CONFIG::InterruptConfig
```

GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).

This setting is applicable only if GPIO is in GpioMode with input enabled. Refer to definition of GPIO_INT_CONFIG for supported settings.

Definition at line 90 of file GpioConfig.h.

13.48.2.5 LockConfig

```
UINT32 GPIO_CONFIG::LockConfig
```

GPIO Lock Configuration This setting controls pads lock.

Refer to definition of GPIO_LOCK_CONFIG for supported settings.

Definition at line 108 of file GpioConfig.h.

13.48.2.6 OutputState

```
UINT32 GPIO_CONFIG::OutputState
```

Output State Set Pad output value.

Refer to definition of GPIO_OUTPUT_STATE for supported settings. This setting takes place when output is enabled.

Definition at line 83 of file GpioConfig.h.

13.48.2.7 PadMode

```
UINT32 GPIO_CONFIG::PadMode
```

Pad Mode Pad can be set as GPIO or one of its native functions.

When in native mode setting Direction (except Inversion), OutputState, InterruptConfig, Host Software Pad Ownership and OutputStateLock are unnecessary. Refer to definition of GPIO_PAD_MODE. Refer to EDS for each native mode according to the pad.

Definition at line 64 of file GpioConfig.h.

13.48.2.8 PowerConfig

```
UINT32 GPIO_CONFIG::PowerConfig
```

GPIO Power Configuration.

This setting controls Pad Reset Configuration. Refer to definition of GPIO_RESET_CONFIG for supported settings.

Definition at line 96 of file GpioConfig.h.

The documentation for this struct was generated from the following file:

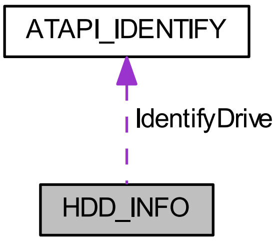
- GpioConfig.h

13.49 HDD_INFO Struct Reference

HDD_INFO.

```
#include <LegacyBios.h>
```

Collaboration diagram for HDD_INFO:



Public Attributes

- UINT16 Status

  Status of IDE device.
- UINT32 Bus

  PCI bus of IDE controller.
- UINT32 Device

  PCI device of IDE controller.
- UINT32 Function

  PCI function of IDE controller.
- UINT16 CommandBaseAddress

  Command ports base address.
- UINT16 ControlBaseAddress

  Control ports base address.
- UINT16 BusMasterAddress

  Bus master address.
- ATAPI_IDENTIFY IdentifyDrive [2]

  Data that identifies the drive data; one per possible attached drive.

13.49.1 Detailed Description

HDD_INFO.

Definition at line 532 of file LegacyBios.h.

13.49.2 Member Data Documentation

13.49.2.1 Status

```
UINT16 HDD_INFO::Status
```

Status of IDE device.

Values are defined below. There is one HDD_INFO structure per IDE controller. The IdentifyDrive is per drive. Index 0 is master and index 1 is slave.

Definition at line 538 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.50 LEGACY_DEVICE_FLAGS Struct Reference

LEGACY_DEVICE_FLAGS.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT32 A20Kybd: 1

  A20 controller by keyboard controller.
- UINT32 A20Port90: 1

  A20 controlled by port 0x92.
- UINT32 Reserved: 30

  Reserved for future usage.

13.50.1 Detailed Description

LEGACY_DEVICE_FLAGS.

Definition at line 505 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.51 PCIE_PORT_EQS Struct Reference

Data structure for passing static equalization data for programming.

```
#include <PcieInitLib.h>
```

13.51.1 Detailed Description

Data structure for passing static equalization data for programming.

Definition at line 111 of file PcieInitLib.h.

The documentation for this struct was generated from the following file:

- PcieInitLib.h

13.52 PCIE_PORT_SWEQ_DATA Struct Reference

PCIe Root Port description data structure, used as the interface between low level and high level.

```
#include <PcieInitLib.h>
```

13.52.1 Detailed Description

PCIe Root Port description data structure, used as the interface between low level and high level.

Definition at line 76 of file PcieInitLib.h.

The documentation for this struct was generated from the following file:

- PcieInitLib.h

13.53 PCIE_SWEQ_GPIO_CONFIG Struct Reference

Input Configuration Parameters for Software Equalization Support.

```
#include <PcieInitLib.h>
```

13.53.1 Detailed Description

Input Configuration Parameters for Software Equalization Support.

Definition at line 121 of file PcieInitLib.h.

The documentation for this struct was generated from the following file:

- PcieInitLib.h

13.54 PCIE_SWEQ_PRESET_SCORE Struct Reference

Data Output from Software Equalization.

```
#include <PcieInitLib.h>
```

13.54.1 Detailed Description

Data Output from Software Equalization.

Definition at line 154 of file PcieInitLib.h.

The documentation for this struct was generated from the following file:

- PcieInitLib.h

13.55 RC_VERSION Struct Reference

This structure contains the RC version details for FVI SMBIOS records.

```
#include <SiFviLib.h>
```

13.55.1 Detailed Description

This structure contains the RC version details for FVI SMBIOS records.

Definition at line 70 of file SiFviLib.h.

The documentation for this struct was generated from the following file:

- SiFviLib.h

13.56 SI_CONFIG Struct Reference

The Silicon Policy allows the platform code to publish a set of configuration information that the RC drivers will use to configure the silicon hardware.

```
#include <SiConfig.h>
```

Public Attributes

- CONFIG_BLOCK_HEADER Header

  Offset 0 - 27 Config Block Header.
- UINT32 CsmFlag: 1

  Offset 44 BIT0: CSM status flag.
- UINT32 SkipPostBootSai: 1
- UINT32 RsvdBits: 30

  Reserved.
- UINT32 TraceHubMemBase

  If Trace Hub is enabled and trace to memory is desired, Platform code or BootLoader needs to allocate trace hub memory as reserved, and save allocated memory base to TraceHubMemBase to ensure Trace Hub memory is configured properly.

13.56.1 Detailed Description

The Silicon Policy allows the platform code to publish a set of configuration information that the RC drivers will use to configure the silicon hardware.

Revision 1:

- Initial version. **Revision 2**:
- Added TraceHubMemBase **Revision 3**
- Deprecated SkipPostBootSai

Definition at line 56 of file SiConfig.h.

13.56.2 Member Data Documentation

13.56.2.1 SkipPostBootSai

```
UINT32 SI_CONFIG::SkipPostBootSai
```

Deprecated since revision 3

Definition at line 65 of file SiConfig.h.

13.56.2.2 TraceHubMemBase

```
UINT32 SI_CONFIG::TraceHubMemBase
```

If Trace Hub is enabled and trace to memory is desired, Platform code or BootLoader needs to allocate trace hub memory as reserved, and save allocated memory base to TraceHubMemBase to ensure Trace Hub memory is configured properly.

To get total trace hub memory size please refer to TraceHubCalculateTotalBufferSize ()

Noted: If EDKII memory service is used to allocate memory, it will require double memory size to support size-aligned memory allocation, so Platform code or FSP Wrapper code should ensure enough memory available for size-aligned TraceHub memory allocation.

Definition at line 78 of file SiConfig.h.

The documentation for this struct was generated from the following file:

- SiConfig.h

13.57 SI_PCH_DEVICE_INTERRUPT_CONFIG Struct Reference

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

```
#include <FspsUpd.h>
```

Public Attributes

- UINT8 Device

  Device number.
- UINT8 Function

  Device function.
- UINT8 IntX

  Interrupt pin: INTA-INTD (see SI_PCH_INT_PIN)
- UINT8 Irq

  IRQ to be set for device.

13.57.1 Detailed Description

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

Definition at line 74 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

- FspsUpd.h

13.58 SMM_ATTRIBUTES Struct Reference

SMM_ATTRIBUTES.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT16 Type: 3

  Access mechanism used to generate the soft SMI.
- UINT16 PortGranularity: 3

  The size of "port" in bits.
- UINT16 DataGranularity: 3

  The size of data in bits.
- UINT16 Reserved: 7

  Reserved for future use.

13.58.1 Detailed Description

SMM_ATTRIBUTES.

Definition at line 751 of file LegacyBios.h.

13.58.2 Member Data Documentation

13.58.2.1 DataGranularity

```
UINT16 SMM_ATTRIBUTES::DataGranularity
```

The size of data in bits.

Defined values are below.

Definition at line 766 of file LegacyBios.h.

13.58.2.2 PortGranularity

```
UINT16 SMM_ATTRIBUTES::PortGranularity
```

The size of "port" in bits.

Defined values are below.

Definition at line 761 of file LegacyBios.h.

13.58.2.3 Type

```
UINT16 SMM_ATTRIBUTES::Type
```

Access mechanism used to generate the soft SMI.

Defined types are below. The other values are reserved for future usage.

Definition at line 756 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

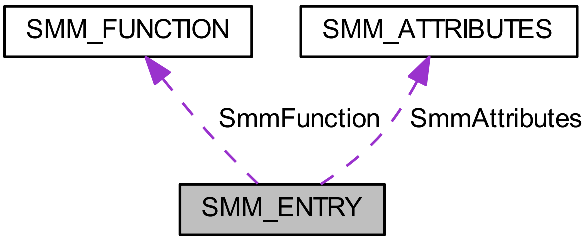
- LegacyBios.h

13.59 SMM_ENTRY Struct Reference

This structure assumes both port and data sizes are 1.

```
#include <LegacyBios.h>
```

Collaboration diagram for SMM_ENTRY:



Public Attributes

- SMM_ATTRIBUTES SmmAttributes

    Describes the access mechanism, SmmPort, and SmmData sizes.
- SMM_FUNCTION SmmFunction

    Function Soft SMI is to perform.
- UINT8 SmmPort

    SmmPort size depends upon SmmAttributes and ranges from2 bytes to 16 bytes.
- UINT8 SmmData

    SmmData size depends upon SmmAttributes and ranges from2 bytes to 16 bytes.

13.59.1 Detailed Description

This structure assumes both port and data sizes are 1.

SmmAttribute must be properly to reflect that assumption.

Definition at line 826 of file LegacyBios.h.

13.59.2 Member Data Documentation

13.59.2.1 SmmAttributes

```
SMM_ATTRIBUTES SMM_ENTRY::SmmAttributes
```

Describes the access mechanism, SmmPort, and SmmData sizes.

Type SMM_ATTRIBUTES is defined below.

Definition at line 831 of file LegacyBios.h.

13.59.2.2 SmmFunction

```
SMM_FUNCTION SMM_ENTRY::SmmFunction
```

Function Soft SMI is to perform.

Type SMM_FUNCTION is defined below.

Definition at line 836 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.60 SMM_FUNCTION Struct Reference

SMM_FUNCTION & relating constants.

```
#include <LegacyBios.h>
```

13.60.1 Detailed Description

SMM_FUNCTION & relating constants.

Definition at line 802 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

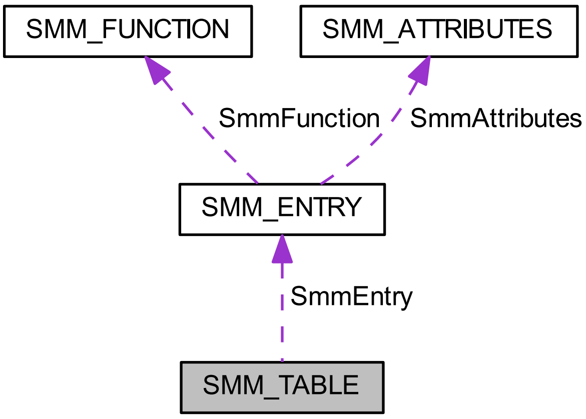
- LegacyBios.h

13.61 SMM_TABLE Struct Reference

SMM_TABLE.

```
#include <LegacyBios.h>
```

Collaboration diagram for SMM_TABLE:



Public Attributes

- UINT16 NumSmmEntries

  Number of entries represented by SmmEntry.
- SMM_ENTRY SmmEntry

  One entry per function. Type SMM_ENTRY is defined below.

13.61.1 Detailed Description

SMM_TABLE.

Definition at line 852 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

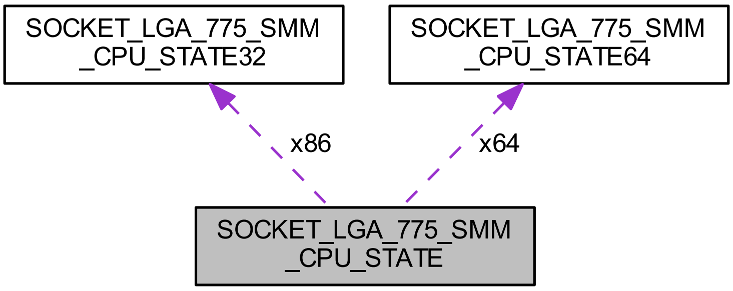
- LegacyBios.h

13.62 SOCKET_LGA_775_SMM_CPU_STATE Union Reference

Union of CPU save-state strcutures for IA32 and X64.

```
#include <SocketLga775Lib.h>
```

Collaboration diagram for SOCKET_LGA_775_SMM_CPU_STATE:


SOCKET_LGA_775_SMM_CPU_STATE32
SOCKET_LGA_775_SMM_CPU_STATE64
x86
x64
SOCKET_LGA_775_SMM_CPU_STATE

13.62.1 Detailed Description

Union of CPU save-state strcutures for IA32 and X64.

Definition at line 268 of file SocketLga775Lib.h.

The documentation for this union was generated from the following file:

- SocketLga775Lib.h

13.63 SOCKET_LGA_775_SMM_CPU_STATE32 Struct Reference

CPU save-state strcuture for IA32.

```
#include <SocketLga775Lib.h>
```

13.63.1 Detailed Description

CPU save-state strcuture for IA32.

Definition at line 168 of file SocketLga775Lib.h.

The documentation for this struct was generated from the following file:

- SocketLga775Lib.h

13.64 SOCKET_LGA_775_SMM_CPU_STATE64 Struct Reference

CPU save-state strcuture for X64.

```
#include <SocketLga775Lib.h>
```

13.64.1 Detailed Description

CPU save-state strcuture for X64.

Definition at line 206 of file SocketLga775Lib.h.

The documentation for this struct was generated from the following file:

- SocketLga775Lib.h

13.65 SVID_SID_VALUE Struct Reference

Subsystem Vendor ID / Subsystem ID.

```
#include <SiConfig.h>
```

13.65.1 Detailed Description

Subsystem Vendor ID / Subsystem ID.

Definition at line 92 of file SiConfig.h.

The documentation for this struct was generated from the following file:

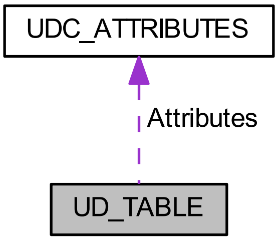
- SiConfig.h

13.66 UD_TABLE Struct Reference

UD_TABLE.

```
#include <LegacyBios.h>
```

Collaboration diagram for UD_TABLE:



Public Attributes

- UDC_ATTRIBUTES Attributes

  This field contains the bit-mapped attributes of the PARTIES information.
- UINT8 DeviceNumber

  This field contains the zero-based device on which the selected ServiceDataArea is present.
- UINT8 BbsTableEntryNumberForParentDevice

  This field contains the zero-based index into the BbsTable for the parent device.
- UINT8 BbsTableEntryNumberForBoot

  This field contains the zero-based index into the BbsTable for the boot entry.
- UINT8 BbsTableEntryNumberForHddDiag

  This field contains the zero-based index into the BbsTable for the HDD diagnostics entry.
- UINT8 BeerData [128]

  The raw Beer data.
- UINT8 ServiceAreaData [64]

  The raw data of selected service area.

13.66.1 Detailed Description

UD_TABLE.

Definition at line 886 of file LegacyBios.h.

13.66.2 Member Data Documentation

13.66.2.1 Attributes

```
UDC_ATTRIBUTES UD_TABLE::Attributes
```

This field contains the bit-mapped attributes of the PARTIES information.

Type UDC_ATTRIBUTES is defined below.

Definition at line 891 of file LegacyBios.h.

13.66.2.2 BbsTableEntryNumberForParentDevice

```
UINT8 UD_TABLE::BbsTableEntryNumberForParentDevice
```

This field contains the zero-based index into the BbsTable for the parent device.

This index allows the user to reference the parent device information such as PCI bus, device function.

Definition at line 904 of file LegacyBios.h.

13.66.2.3 DeviceNumber

```
UINT8 UD_TABLE::DeviceNumber
```

This field contains the zero-based device on which the selected ServiceDataArea is present.

It is 0 for master and 1 for the slave device.

Definition at line 897 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.67 UDC_ATTRIBUTES Struct Reference

UDC_ATTRIBUTES.

```
#include <LegacyBios.h>
```

Public Attributes

- UINT8 DirectoryServiceValidity: 1

  This bit set indicates that the ServiceAreaData is valid.
- UINT8 RabcaUsedFlag: 1

  This bit set indicates to use the Reserve Area Boot Code Address (RACBA) only if DirectoryServiceValidity is 0.
- UINT8 ExecuteHddDiagnosticsFlag: 1

  This bit set indicates to execute hard disk diagnostics.
- UINT8 Reserved: 5

  Reserved for future use.

13.67.1 Detailed Description

UDC_ATTRIBUTES.

Definition at line 860 of file LegacyBios.h.

13.67.2 Member Data Documentation

13.67.2.1 Reserved

```
UINT8 UDC_ATTRIBUTES::Reserved
```

Reserved for future use.

Set to 0.

Definition at line 880 of file LegacyBios.h.

The documentation for this struct was generated from the following file:

- LegacyBios.h

13.68 USB20_AFE Struct Reference

This structure configures per USB2 AFE settings.

```
#include <UsbConfig.h>
```

Public Attributes

- UINT8 Petxiset

  Per Port HS Preemphasis Bias (PERPORTPETXISET) 000b - 0mV 001b - 11.25mV 010b - 16.9mV 011b - 28.15mV 100b - 28.15mV 101b - 39.35mV 110b - 45mV 111b - 56.3mV.
- UINT8 Txiset

  Per Port HS Transmitter Bias (PERPORTTXISET) 000b - 0mV 001b - 11.25mV 010b - 16.9mV 011b - 28.15mV 100b - 28.15mV 101b - 39.35mV 110b - 45mV 111b - 56.3mV.
- UINT8 Predeemp

  Per Port HS Transmitter Emphasis (IUSBTXEMPHASISEN) 00b - Emphasis OFF 01b - De-emphasis ON 10b - Pre-emphasis ON 11b - Pre-emphasis & De-emphasis ON.
- UINT8 Pehalfbit

  Per Port Half Bit Pre-emphasis (PERPORTTXPEHALF) 1b - half-bit pre-emphasis 0b - full-bit pre-emphasis.

13.68.1 Detailed Description

This structure configures per USB2 AFE settings.

It allows to setup the port electrical parameters.

Definition at line 69 of file UsbConfig.h.

The documentation for this struct was generated from the following file:

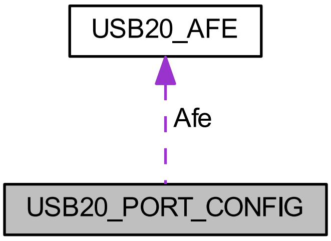
- UsbConfig.h

13.69 USB20_PORT_CONFIG Struct Reference

This structure configures per USB2 port physical settings.

```
#include <UsbConfig.h>
```

Collaboration diagram for USB20_PORT_CONFIG:



Public Attributes

- UINT32 OverCurrentPin: 8

  These members describe the specific over current pin number of USB 2.0 Port N.
- UINT32 Enable: 1

  *0: Disable; **1: Enable**.*
- UINT32 RsvdBits0: 23

  Reserved bits.
- USB20_AFE Afe

  Changing this policy values from default ones may require disabling USB2 PHY Sus Well Power Gating through Usb2PhySusPgEnable on PCH-LP.

13.69.1 Detailed Description

This structure configures per USB2 port physical settings.

It allows to setup the port location and port length, and configures the port strength accordingly.

Definition at line 112 of file UsbConfig.h.

13.69.2 Member Data Documentation

13.69.2.1 Afe

```
USB20_AFE USB20_PORT_CONFIG::Afe
```

Changing this policy values from default ones may require disabling USB2 PHY Sus Well Power Gating through Usb2PhySusPgEnable on PCH-LP.

USB2 AFE settings

Definition at line 126 of file UsbConfig.h.

13.69.2.2 OverCurrentPin

```
UINT32 USB20_PORT_CONFIG::OverCurrentPin
```

These members describe the specific over current pin number of USB 2.0 Port N.

It is SW's responsibility to ensure that a given port's bit map is set only for one OC pin Description. USB2 and USB3 on the same combo Port must use the same OC pin (see: USB_OVERCURRENT_PIN).

Definition at line 119 of file UsbConfig.h.

The documentation for this struct was generated from the following file:

- UsbConfig.h

13.70 USB30_PORT_CONFIG Struct Reference

This structure describes whether the USB3 Port N is enabled by platform modules.

```
#include <UsbConfig.h>
```

Public Attributes

- UINT32 OverCurrentPin: 8

  These members describe the specific over current pin number of USB 3.x Port N.
- UINT32 HsioTxDownscaleAmp: 8

  USB 3.0 TX Output Downscale Amplitude Adjustment (orate01margin) HSIO_TX_DWORD8[21:16] ***Default = 00h***
- UINT32 HsioTxDeEmph: 8

  USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting (ow2tapgen2deemph3p5) HSIO_TX_DWORD5[21:16] ***Default = 29h*** *(approximately -3.5dB De-Emphasis)*
- UINT32 Enable: 1

  0: Disable; ***1: Enable****.*
- UINT32 HsioTxDeEmphEnable: 1

  Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment, ***0: Disable****; 1: Enable.*
- UINT32 HsioTxDownscaleAmpEnable: 1

  Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment, ***0: Disable****; 1: Enable.*
- UINT32 RsvdBits0: 5

  Reserved bits.

13.70.1 Detailed Description

This structure describes whether the USB3 Port N is enabled by platform modules.

Definition at line 132 of file UsbConfig.h.

13.70.2 Member Data Documentation

13.70.2.1 OverCurrentPin

```
UINT32 USB30_PORT_CONFIG::OverCurrentPin
```

These members describe the specific over current pin number of USB 3.x Port N.

It is SW's responsibility to ensure that a given port's bit map is set only for one OC pin Description. USB2 and USB3 on the same combo Port must use the same OC pin (see: USB_OVERCURRENT_PIN).

Definition at line 139 of file UsbConfig.h.

The documentation for this struct was generated from the following file:

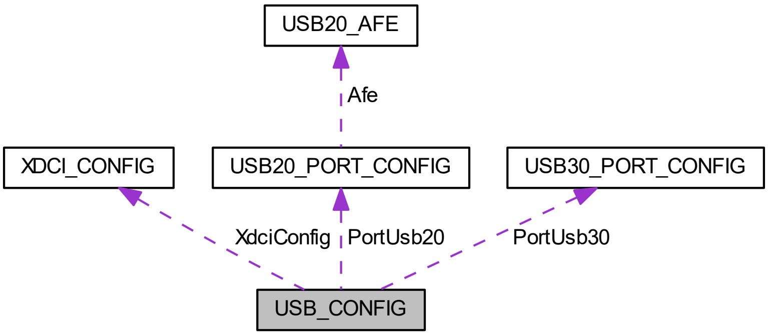
- UsbConfig.h

13.71 USB_CONFIG Struct Reference

This member describes the expected configuration of the USB controller, Platform modules may need to refer Setup options, schematic, BIOS specification to update this field.

```
#include <UsbConfig.h>
```

Collaboration diagram for USB_CONFIG:



Public Attributes

- CONFIG_BLOCK_HEADER Header

  Config Block Header.
- UINT32 EnableComplianceMode: 1

  This policy setting controls state of Compliance Mode enabling.
- UINT32 PdoProgramming: 1

  This policy option when set will make BIOS program Port Disable Override register during PEI phase.
- UINT32 OverCurrentEnable: 1

  This option allows for control whether USB should program the Overcurrent Pins mapping into xHCI.
- UINT32 XhciOcLock: 1

  ***(Test)** If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.*
- UINT32 Usb2PhySusPgEnable: 1

  ***(Test)** This policy option enables USB2 PHY SUS Well Power Gating functionality.*
- UINT32 LtrOverrideEnable: 1

  Enabling this feature will allow for overriding LTR values for xHCI controller.
- UINT32 RsvdBits0: 26

  Reserved bits.
- USB20_PORT_CONFIG PortUsb20 [MAX_USB2_PORTS]

  These members describe whether the USB2 Port N of PCH is enabled by platform modules.
- USB30_PORT_CONFIG PortUsb30 [MAX_USB3_PORTS]

  These members describe whether the USB3 Port N of PCH is enabled by platform modules.
- XDCI_CONFIG XdciConfig

  This member describes whether or not the xDCI controller should be enabled.
- USB30_HSIO_RX_CONFIG PortUsb30HsioRx [MAX_USB3_PORTS]

  This member describes policy options for RX signal tuning in ModPHY.
- UINT32 LtrHighIdleTimeOverride

  High Idle Time Control override value This setting is used only if LtrOverrideEnable is enabled.
- UINT32 LtrMediumIdleTimeOverride

  Medium Idle Time Control override value This setting is used only if LtrOverrideEnable is enabled.
- UINT32 LtrLowIdleTimeOverride

  Low Idle Time Control override value This setting is used only if LtrOverrideEnable is enabled.
- USB30_HSIO_TX_CONFIG PortUsb30HsioTx [MAX_USB3_PORTS]

  This member describes policy options for TX signal tuning in ModPHY.

13.71.1 Detailed Description

This member describes the expected configuration of the USB controller, Platform modules may need to refer Setup options, schematic, BIOS specification to update this field.

The Usb20OverCurrentPins and Usb30OverCurrentPins field must be updated by referring the schematic.

Revision 1:

- Initial version. **Revision 2**:
- USB 3.0 TX Output Unique Transition Bit Scale policies added **Revision 3**: Added USB 3.0 RX HsioCtrlCompMultEnable and HsioCtrlCompMult policies

Definition at line 315 of file UsbConfig.h.

13.71.2 Member Data Documentation

13.71.2.1 EnableComplianceMode

```
UINT32 USB_CONFIG::EnableComplianceMode
```

This policy setting controls state of Compliance Mode enabling.

Compliance Mode can be enabled for testing through this option but defualt setting is Disabled. **0:Disable**, 1: Enable

Definition at line 322 of file UsbConfig.h.

13.71.2.2 LtrOverrideEnable

```
UINT32 USB_CONFIG::LtrOverrideEnable
```

Enabling this feature will allow for overriding LTR values for xHCI controller.

Values used for programming will be taken from this config block and BIOS will disregard recommended ones. **0: disable - do not override recommended LTR values** 1: enable - override recommended LTR values

Definition at line 363 of file UsbConfig.h.

13.71.2.3 OverCurrentEnable

```
UINT32 USB_CONFIG::OverCurrentEnable
```

This option allows for control whether USB should program the Overcurrent Pins mapping into xHCI.

Disabling this feature will disable overcurrent detection functionality. Overcurrent Pin mapping data is contained in respective port structures (i.e. USB30_PORT_CONFIG) in OverCurrentPin field. By default this Overcurrent functionality should be enabled and disabled only for OBS debug usage. **1: Will program USB OC pin mapping in respective xHCI controller registers** 0: Will clear OC pin mapping allow for OBS usage of OC pins

Definition at line 338 of file UsbConfig.h.

13.71.2.4 PdoProgramming

```
UINT32 USB_CONFIG::PdoProgramming
```

This policy option when set will make BIOS program Port Disable Override register during PEI phase.

When disabled BIOS will not program the PDO during PEI phase and leave PDO register unlocked for later programming. If this is disabled, platform code MUST set it before booting into OS. **1: Enable**, 0: Disable

Definition at line 329 of file UsbConfig.h.

13.71.2.5 Usb2PhySusPgEnable

```
UINT32 USB_CONFIG::Usb2PhySusPgEnable
```

(Test) This policy option enables USB2 PHY SUS Well Power Gating functionality.

Please note this is ignored on PCH H **0: disable USB2 PHY SUS Well Power Gating** 1: enable USB2 PHY SUS Well Power Gating

Definition at line 356 of file UsbConfig.h.

13.71.2.6 XhciOcLock

```
UINT32 USB_CONFIG::XhciOcLock
```

(Test) If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.

OverCurrent mapping data is taken from respective port data structure from OverCurrentPin field. If Enable↩OverCurrent policy is enabled this also should be enabled, otherwise xHCI won't consume OC mapping data. **1: Program OCCFDONE bit and make xHCI consume OverCurrent mapping data** 0: Do not program OCCFDONE bit making it possible to use OBS debug on OC pins.

Definition at line 348 of file UsbConfig.h.

The documentation for this struct was generated from the following file:

- UsbConfig.h

13.72 XDCI_CONFIG Struct Reference

The XDCI_CONFIG block describes the configurations of the xDCI Usb Device controller.

```
#include <UsbConfig.h>
```

Public Attributes

- UINT32 Enable: 1

  This member describes whether or not the xDCI controller should be enabled.
- UINT32 RsvdBits0: 31

  Reserved bits.

13.72.1 Detailed Description

The XDCI_CONFIG block describes the configurations of the xDCI Usb Device controller.

Definition at line 164 of file UsbConfig.h.

13.72.2 Member Data Documentation

13.72.2.1 Enable

```
UINT32 XDCI_CONFIG::Enable
```

This member describes whether or not the xDCI controller should be enabled.

0: Disable; **1: Enable**.

Definition at line 169 of file UsbConfig.h.

The documentation for this struct was generated from the following file:

- UsbConfig.h

Chapter 14

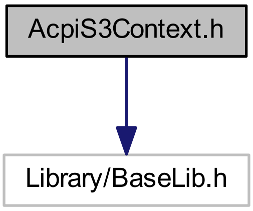
File Documentation

14.1 AcpiS3Context.h File Reference

Definitions for data structures used in S3 resume.

```
#include <Library/BaseLib.h>
```

Include dependency graph for AcpiS3Context.h:



14.1.1 Detailed Description

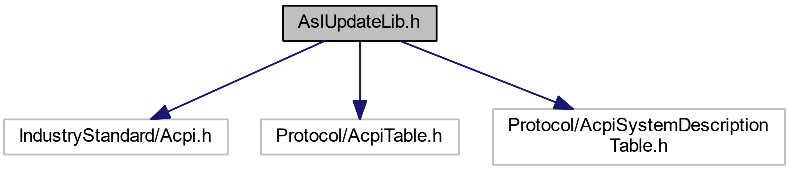
Definitions for data structures used in S3 resume.

14.2 AslUpdateLib.h File Reference

ASL dynamic update library definitions.

```
#include <IndustryStandard/Acpi.h>
#include <Protocol/AcpiTable.h>
#include <Protocol/AcpiSystemDescriptionTable.h>
```

Include dependency graph for AslUpdateLib.h:



Functions

- EFI_STATUS InitializeAslUpdateLib (VOID)

  Initialize the ASL update library state.
- EFI_STATUS UpdateNameAslCode (IN UINT32 AslSignature, IN VOID ∗Buffer, IN UINTN Length)

  This procedure will update immediate value assigned to a Name.
- EFI_STATUS UpdateMethodAslCode (IN UINT32 AslSignature, IN VOID ∗Buffer, IN UINTN Length)

  This procedure will update the name of ASL Method.
- EFI_STATUS LocateAcpiTableBySignature (IN UINT32 Signature, IN OUT EFI_ACPI_DESCRIPTION_HEADER ∗∗Table, IN OUT UINTN ∗Handle)

  This function uses the ACPI support protocol to locate an ACPI table using the .
- EFI_STATUS LocateAcpiTableByOemTableId (IN UINT8 ∗TableId, IN UINT8 TableIdSize, IN OUT EFI_ACPI_DESCRIPTION_HEADER ∗∗Table, IN OUT UINTN ∗Handle)

  This function uses the ACPI support protocol to locate an ACPI SSDT table.
- EFI_STATUS AcpiChecksum (IN VOID ∗Buffer, IN UINTN Size, IN UINTN ChecksumOffset)

  This function calculates and updates an UINT8 checksum.

14.2.1 Detailed Description

ASL dynamic update library definitions.

This library provides dymanic update to various ASL structures. There may be different libraries for different environments (PEI, BS, RT, SMM). Make sure you meet the requirements for the library (protocol dependencies, use restrictions, etc).

Copyright

Specification Reference:

14.2.2 Function Documentation

14.2.2.1 AcpiChecksum()

```
EFI_STATUS AcpiChecksum (
             IN VOID * Buffer,
             IN UINTN Size,
             IN UINTN ChecksumOffset )
```

This function calculates and updates an UINT8 checksum.

Parameters

in	*Buffer*	Pointer to buffer to checksum
in	*Size*	Number of bytes to checksum
in	*ChecksumOffset*	Offset to place the checksum result in

Return values

EFI_SUCCESS	The function completed successfully.

14.2.2.2 InitializeAslUpdateLib()

```
EFI_STATUS InitializeAslUpdateLib (
             VOID  )
```

Initialize the ASL update library state.

This must be called prior to invoking other library functions.

Return values

EFI_SUCCESS	The function completed successfully.

14.2.2.3 LocateAcpiTableByOemTableId()

```
EFI_STATUS LocateAcpiTableByOemTableId (
             IN UINT8 * TableId,
             IN UINT8 TableIdSize,
             IN OUT EFI_ACPI_DESCRIPTION_HEADER ** Table,
             IN OUT UINTN * Handle )
```

This function uses the ACPI support protocol to locate an ACPI SSDT table.

The table is located by searching for a matching OEM Table ID field. Partial match searches are supported via the TableIdSize parameter.

Parameters

in	*TableId*	Pointer to an ASCII string containing the OEM Table ID from the ACPI table header
in	*TableIdSize*	Length of the TableId to match. Table ID are 8 bytes long, this function will consider it a match if the first TableIdSize bytes match
in,out	*Table*	Updated with a pointer to the table
in,out	*Handle*	AcpiSupport protocol table handle for the table found
in,out	*Version*	See AcpiSupport protocol, GetAcpiTable function for use

Return values

EFI_SUCCESS	The function completed successfully.

14.2.2.4 LocateAcpiTableBySignature()

```
EFI_STATUS LocateAcpiTableBySignature (
             IN UINT32 Signature,
             IN OUT EFI_ACPI_DESCRIPTION_HEADER ** Table,
             IN OUT UINTN * Handle )
```

This function uses the ACPI support protocol to locate an ACPI table using the .

It is really only useful for finding tables that only have a single instance, e.g. FADT, FACS, MADT, etc. It is not good for locating SSDT, etc. Matches are determined by finding the table with ACPI table that has a matching signature and version.

Parameters

in	*Signature*	Pointer to an ASCII string containing the Signature to match
in,out	*Table*	Updated with a pointer to the table
in,out	*Handle*	AcpiSupport protocol table handle for the table found
in,out	*Version*	On input, the version of the table desired, on output, the versions the table belongs to

See also

AcpiSupport protocol for details

Return values

EFI_SUCCESS	The function completed successfully.

14.2.2.5 UpdateMethodAslCode()

```
EFI_STATUS UpdateMethodAslCode (
             IN UINT32 AslSignature,
             IN VOID * Buffer,
             IN UINTN Length )
```

This procedure will update the name of ASL Method.

Parameters

in	*AslSignature*	- The signature of Operation Region that we want to update.
in	*Buffer*	- source of data to be written over original aml
in	*Length*	- length of data to be overwritten

Return values

EFI_SUCCESS	- The function completed successfully.
EFI_NOT_FOUND	- Failed to locate AcpiTable.

14.2.2.6 UpdateNameAslCode()

```
EFI_STATUS UpdateNameAslCode (
             IN UINT32 AslSignature,
             IN VOID * Buffer,
             IN UINTN Length )
```

This procedure will update immediate value assigned to a Name.

Parameters

in	*AslSignature*	The signature of Operation Region that we want to update.
in	*Buffer*	source of data to be written over original aml
in	*Length*	length of data to be overwritten

Return values

EFI_SUCCESS	The function completed successfully.

14.3 CacheAsRamLib.h File Reference

Copyright (c) 2014, Intel Corporation.

Functions

- VOID DisableCacheAsRam (IN BOOLEAN DisableCar)
  This function disable CAR.

14.3.1 Detailed Description

Copyright (c) 2014, Intel Corporation.

All rights reserved.
This program and the accompanying materials are licensed and made available under the terms and conditions of the BSD License which accompanies this distribution. The full text of the license may be found at http://opensource.org/licenses/bsd-license.php.

THE PROGRAM IS DISTRIBUTED UNDER THE BSD LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED.

14.3.2 Function Documentation

14.3.2.1 DisableCacheAsRam()

```
VOID DisableCacheAsRam (
             IN BOOLEAN DisableCar )
```

This function disable CAR.

Parameters

in	*DisableCar*	TRUE means use INVD, FALSE means use WBINVD

14.4 ConsoleOutDevice.h File Reference

This GUID can be installed to the device handle to specify that the device is the console-out device.

14.4.1 Detailed Description

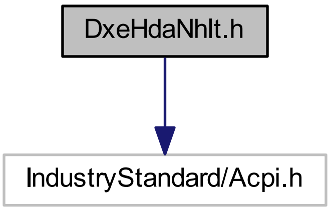
This GUID can be installed to the device handle to specify that the device is the console-out device.

14.5 DxeHdaNhlt.h File Reference

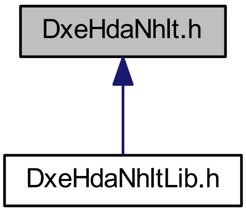
Header file for DxePchHdaNhltLib - NHLT structure definitions.

```
#include <IndustryStandard/Acpi.h>
```

Include dependency graph for DxeHdaNhlt.h:



This graph shows which files directly or indirectly include this file:



14.5.1 Detailed Description

Header file for DxePchHdaNhltLib - NHLT structure definitions.

Copyright

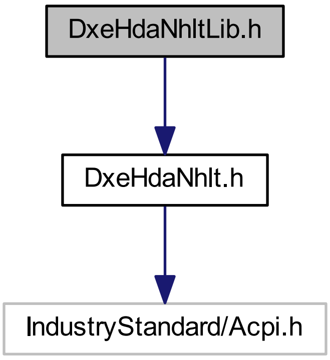
Specification Reference:

14.6 DxeHdaNhltLib.h File Reference

Prototype of the DxePchHdaNhltLib library.

```
#include <DxeHdaNhlt.h>
```

Include dependency graph for DxeHdaNhltLib.h:



Functions

- ENDPOINT_DESCRIPTOR ∗ GetNhltEndpoint (IN CONST NHLT_ACPI_TABLE ∗NhltTable, IN CONST U←INT8 EndpointIndex)

  Returns pointer to Endpoint ENDPOINT_DESCRIPTOR structure.
- SPECIFIC_CONFIG ∗ GetNhltEndpointDeviceCapabilities (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint)

  Returns pointer to Endpoint Specific Configuration SPECIFIC_CONFIG structure.
- FORMATS_CONFIG ∗ GetNhltEndpointFormatsConfig (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint)

  Returns pointer to all Formats Configuration FORMATS_CONFIG structure.
- FORMAT_CONFIG ∗ GetNhltEndpointFormat (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint, IN CO←NST UINT8 FormatIndex)

  Returns pointer to Format Configuration FORMAT_CONFIG structure.
- DEVICES_INFO ∗ GetNhltEndpointDevicesInfo (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint)

  Returns pointer to all Device Information DEVICES_INFO structure.
- DEVICE_INFO ∗ GetNhltEndpointDeviceInfo (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint, IN CONST UINT8 DeviceInfoIndex)

  Returns pointer to Device Information DEVICES_INFO structure.
- SPECIFIC_CONFIG ∗ GetNhltOedConfig (IN CONST NHLT_ACPI_TABLE ∗NhltTable)

  Returns pointer to OED Configuration SPECIFIC_CONFIG structure.
- VOID NhltFormatDump (IN CONST FORMAT_CONFIG ∗Format)

  Prints Format configuration.
- VOID NhltEndpointDump (IN CONST ENDPOINT_DESCRIPTOR ∗Endpoint)

  Prints Endpoint configuration.
- VOID NhltOedConfigDump (IN CONST SPECIFIC_CONFIG ∗OedConfig)

  Prints OED (Offload Engine Driver) configuration.
- VOID NhltAcpiTableDump (IN NHLT_ACPI_TABLE ∗NhltTable)

  Prints NHLT (Non HDA-Link Table) to be exposed via ACPI (aka.

14.6.1 Detailed Description

Prototype of the DxePchHdaNhltLib library.

Copyright

Specification Reference:

14.6.2 Function Documentation

14.6.2.1 GetNhltEndpoint()

```
ENDPOINT_DESCRIPTOR* GetNhltEndpoint (
             IN CONST NHLT_ACPI_TABLE * NhltTable,
             IN CONST UINT8 EndpointIndex )
```

Returns pointer to Endpoint ENDPOINT_DESCRIPTOR structure.

Parameters

in	**NhltTable*	Endpoint for which Format address is retrieved
in	*FormatIndex*	Index of Format to be retrieved

Return values

Pointer	to ENDPOINT_DESCRIPTOR structure with given index

14.6.2.2 GetNhltEndpointDeviceCapabilities()

```
SPECIFIC_CONFIG* GetNhltEndpointDeviceCapabilities (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint )
```

Returns pointer to Endpoint Specific Configuration SPECIFIC_CONFIG structure.

Parameters

in	**Endpoint*	Endpoint for which config address is retrieved

Return values

Pointer	to SPECIFIC_CONFIG structure with endpoint's capabilities

14.6.2.3 GetNhltEndpointDeviceInfo()

```
DEVICE_INFO* GetNhltEndpointDeviceInfo (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint,
             IN CONST UINT8 DeviceInfoIndex )
```

Returns pointer to Device Information DEVICES_INFO structure.

Parameters

in	**Endpoint*	Endpoint for which Device Info address is retrieved
in	*DeviceInfoIndex*	Index of Device Info to be retrieved

Return values

Pointer	to DEVICE_INFO structure with given index

14.6.2.4 GetNhltEndpointDevicesInfo()

```
DEVICES_INFO* GetNhltEndpointDevicesInfo (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint )
```

Returns pointer to all Device Information DEVICES_INFO structure.

Parameters

in	*∗Endpoint*	Endpoint for which DevicesInfo address is retrieved

Return values

Pointer	to DEVICES_INFO structure

14.6.2.5 GetNhltEndpointFormat()

```
FORMAT_CONFIG* GetNhltEndpointFormat (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint,
             IN CONST UINT8 FormatIndex )
```

Returns pointer to Format Configuration FORMAT_CONFIG structure.

Parameters

in	*∗Endpoint*	Endpoint for which Format address is retrieved
in	*FormatIndex*	Index of Format to be retrieved

Return values

Pointer	to FORMAT_CONFIG structure with given index

14.6.2.6 GetNhltEndpointFormatsConfig()

```
FORMATS_CONFIG* GetNhltEndpointFormatsConfig (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint )
```

Returns pointer to all Formats Configuration FORMATS_CONFIG structure.

Parameters

in	*∗Endpoint*	Endpoint for which Formats address is retrieved

Return values

Pointer	to FORMATS_CONFIG structure

14.6.2.7 GetNhltOedConfig()

```
SPECIFIC_CONFIG* GetNhltOedConfig (
             IN CONST NHLT_ACPI_TABLE * NhltTable )
```

Returns pointer to OED Configuration SPECIFIC_CONFIG structure.

Parameters

in	**NhltTable*	NHLT table for which OED address is retrieved

Return values

Pointer	to SPECIFIC_CONFIG structure with NHLT capabilities

14.6.2.8 NhltAcpiTableDump()

```
VOID NhltAcpiTableDump (
             IN NHLT_ACPI_TABLE * NhltTable )
```

Prints NHLT (Non HDA-Link Table) to be exposed via ACPI (aka.

OED (Offload Engine Driver) Configuration Table).

Parameters

in	**NhltTable*	The NHLT table to print

Return values

None	

14.6.2.9 NhltEndpointDump()

```
VOID NhltEndpointDump (
             IN CONST ENDPOINT_DESCRIPTOR * Endpoint )
```

Prints Endpoint configuration.

Parameters

in	**Endpoint*	Endpoint to be printed

Return values

None	

14.6.2.10 NhltFormatDump()

```
VOID NhltFormatDump (
            IN CONST FORMAT_CONFIG * Format )
```

Prints Format configuration.

Parameters

in	**Format*	Format to be printed

Return values

None	

14.6.2.11 NhltOedConfigDump()

```
VOID NhltOedConfigDump (
            IN CONST SPECIFIC_CONFIG * OedConfig )
```

Prints OED (Offload Engine Driver) configuration.

Parameters

in	**OedConfig*	OED to be printed

Return values

None	

14.7 FspErrorInfo.h File Reference

FSP Error Information HOB to describe errors inside FSP that bootloader may take some actions to handle those error scenarios.

Classes

- struct FSP_ERROR_INFO_HOB

FSP Error Information Block.

Macros

- #define FSP_ERROR_INFO_HOB_GUID

  GUID value indicating the FSP error information.

14.7.1 Detailed Description

FSP Error Information HOB to describe errors inside FSP that bootloader may take some actions to handle those error scenarios.

Copyright

Specification Reference:

14.8 FspErrorInfoLib.h File Reference

Library to provide service for sending FSP error information to bootloader.

Functions

- EFI_STATUS SendFspErrorInfo (IN EFI_GUID CallerId, IN EFI_GUID ErrorType, IN UINT32 Status)

  Function attempts to send FSP error information to bootloader by both FSP_ERROR_INFO_HOB and ReportStatusCode service.
- EFI_STATUS SendFspErrorInfoStatusCode (IN EFI_GUID CallerId, IN EFI_GUID ErrorType, IN EFI_STATUS Status)

  Function attempts to send FSP error information to bootloader by ReportStatusCode service.
- EFI_STATUS DumpFspErrorInfo (IN VOID ∗HobList)

  Function attempts to dump all FSP error information hobs.
- EFI_STATUS FspErrorStatusCodeReportWorker (IN EFI_STATUS_CODE_TYPE CodeType, IN EFI_STATUS_CODE_VALUE Value, IN UINT32 Instance, IN CONST EFI_GUID ∗CallerId, IN CONST EFI_STATUS_CODE_DATA ∗Data OPTIONAL)

  ReportStatusCode worker for FSP Error Information.

14.8.1 Detailed Description

Library to provide service for sending FSP error information to bootloader.

Copyright

Specification Reference:

14.8.2 Function Documentation

14.8.2.1 DumpFspErrorInfo()

```
EFI_STATUS DumpFspErrorInfo (
             IN VOID * HobList )
```

Function attempts to dump all FSP error information hobs.

Parameters

in	*HobList*	- Pointer to the HOB data structure.

Return values

EFI_SUCCESS	- No FSP_ERROR_INFO_HOB found.
EFI_DEVICE_ERROR	- At least one FSP_ERROR_INFO_HOB found.

14.8.2.2 FspErrorStatusCodeReportWorker()

```
EFI_STATUS FspErrorStatusCodeReportWorker (
             IN EFI_STATUS_CODE_TYPE CodeType,
             IN EFI_STATUS_CODE_VALUE Value,
             IN UINT32 Instance,
             IN CONST EFI_GUID * CallerId,
             IN CONST EFI_STATUS_CODE_DATA *Data OPTIONAL )
```

ReportStatusCode worker for FSP Error Information.

Parameters

CodeType	Always (EFI_ERROR_CODE | EFI_ERROR_UNRECOVERED)
Value	Always 0
Instance	Always 0
CallerId	This optional parameter may be used to identify the caller. It may be used to identify which internal component of the FSP was executing at the time of the error.
Data	This data contains FSP error type and status code.

Return values

EFI_SUCCESS	Show error status sent by FSP successfully.
RETURN_ABORTED	Function skipped as unrelated.

14.8.2.3 SendFspErrorInfo()

```
EFI_STATUS SendFspErrorInfo (
             IN EFI_GUID CallerId,
             IN EFI_GUID ErrorType,
             IN UINT32 Status )
```

Function attempts to send FSP error information to bootloader by both FSP_ERROR_INFO_HOB and Report↩ StatusCode service.

Parameters

in	*CallerId*	- GUID indicates which component is executing.
in	*ErrorType*	- GUID indicates what error was encountered.
in	*Status*	- EFI_STATUS code for the error.

Return values

EFI_SUCCESS	- The function always return EFI_SUCCESS.

14.8.2.4 SendFspErrorInfoStatusCode()

```
EFI_STATUS SendFspErrorInfoStatusCode (
             IN EFI_GUID CallerId,
             IN EFI_GUID ErrorType,
             IN EFI_STATUS Status )
```

Function attempts to send FSP error information to bootloader by ReportStatusCode service.

This typically is used by DXE drivers inside FSP which cannot create hob.

Parameters

in	*CallerId*	- GUID indicates which component is executing.
in	*ErrorType*	- GUID indicates what error was encountered.
in	*Status*	- EFI_STATUS code for the error.

Return values

EFI_SUCCESS	- The function always return EFI_SUCCESS.

14.9 FspFixedPcds.h File Reference

This file lists all FixedAtBuild PCDs referenced in FSP integration guide.

Macros

- #define PcdFspAreaBaseAddress 0xFFE30000

  FspAreaBaseAddress.
- #define PcdFspImageIdString $CMLFSP$

  FspImageIdString.
- #define PcdSiliconInitVersionMajor 0x09

  SiliconInitVersionMajor.
- #define PcdSiliconInitVersionMinor 0x00

  SiliconInitVersionMinor.
- #define PcdSiliconInitVersionRevision 0x7B

  SiliconInitVersionRevision.
- #define PcdSiliconInitVersionBuild 0x20

  SiliconInitVersionBuild.
- #define PcdGlobalDataPointerAddress 0xFED00148

  GlobalDataPointerAddress.
- #define PcdTemporaryRamBase 0xFEF00000

  TemporaryRamBase.
- #define PcdTemporaryRamSize 0x00040000

  TemporaryRamSize.
- #define PcdFspReservedBufferSize 0x100

  FspReservedBufferSize.

14.9.1 Detailed Description

This file lists all FixedAtBuild PCDs referenced in FSP integration guide.

Those value may vary in different FSP revision to meet different requirements.

14.10 FspInfoHob.h File Reference

Header file for FSP Information HOB.

14.10.1 Detailed Description

Header file for FSP Information HOB.

Copyright

Specification Reference:

14.11 FspmArchConfigPpi.h File Reference

Header file for FSP-M Arch Config PPI.

Classes

- struct FSPM_ARCH_CONFIG_PPI

  This PPI provides FSP-M Arch Config PPI.

Macros

- #define FSPM_ARCH_CONFIG_GUID

  Global ID for the FSPM_ARCH_CONFIG_PPI.

14.11.1 Detailed Description

Header file for FSP-M Arch Config PPI.

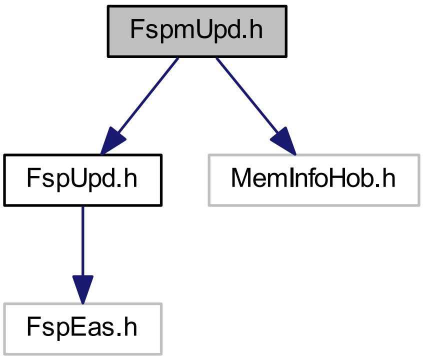
Copyright

14.12 FspmUpd.h File Reference

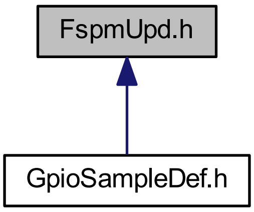
Copyright (c) 2021, Intel Corporation.

```
#include <FspUpd.h>
#include <MemInfoHob.h>
```

Include dependency graph for FspmUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct CHIPSET_INIT_INFO

  The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.
- struct FSP_M_CONFIG

  Fsp M Configuration.
- struct FSP_M_TEST_CONFIG

  Fsp M Test Configuration.
- struct FSP_M_RESTRICTED_CONFIG

  Fsp M Restricted Configuration.
- struct FSPM_UPD

  Fsp M UPD Configuration.

14.12.1 Detailed Description

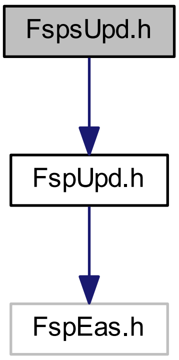
This file is automatically generated. Please do NOT modify !!!

14.13 FspsUpd.h File Reference

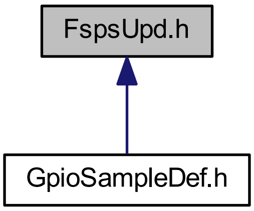
Copyright (c) 2021, Intel Corporation.

```
#include <FspUpd.h>
```

Include dependency graph for FspsUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct AZALIA_HEADER

  Azalia Header structure.
- struct AUDIO_AZALIA_VERB_TABLE

  Audio Azalia Verb Table structure.
- struct SI_PCH_DEVICE_INTERRUPT_CONFIG

  The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.
- struct FSP_S_CONFIG

  Fsp S Configuration.

- struct FSP_S_TEST_CONFIG

  Fsp S Test Configuration.
- struct FSP_S_RESTRICTED_CONFIG

  Fsp S Restricted Configuration.
- struct FSPS_UPD

  Fsp S UPD Configuration.

Macros

- #define SI_PCH_MAX_DEVICE_INTERRUPT_CONFIG 64

  Number of all PCH devices.

Enumerations

- enum SI_PCH_INT_PIN

  Refer to the definition of PCH_INT_PIN.

14.13.1 Detailed Description

This file is automatically generated. Please do NOT modify !!!

14.13.2 Enumeration Type Documentation

14.13.2.1 SI_PCH_INT_PIN

```
enum SI_PCH_INT_PIN
```

Refer to the definition of PCH_INT_PIN.

Enumerator

SiPchNoInt	No Interrupt Pin.

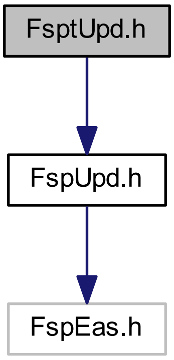
Definition at line 64 of file FspsUpd.h.

14.14 FsptUpd.h File Reference

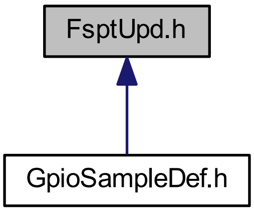
Copyright (c) 2021, Intel Corporation.

```
#include <FspUpd.h>
```

Include dependency graph for FsptUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct FSPT_CORE_UPD

  Fsp T Core UPD.
- struct FSP_T_CONFIG

  Fsp T Configuration.
- struct FSP_T_TEST_CONFIG

  Fsp T Test Configuration.
- struct FSP_T_RESTRICTED_CONFIG

  Fsp T Restricted Configuration.
- struct FSPT_UPD

  Fsp T UPD Configuration.

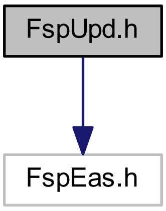
14.14.1 Detailed Description

This file is automatically generated. Please do NOT modify !!!

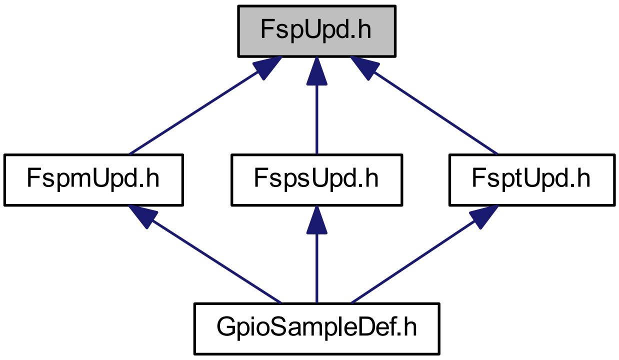
14.15 FspUpd.h File Reference

```
#include <FspEas.h>
```

Include dependency graph for FspUpd.h:



This graph shows which files directly or indirectly include this file:



14.15.1 Detailed Description

This file is automatically generated. Please do NOT modify !!!

14.16 GetFsptApiParameter.h File Reference

Library to get FSP-T API parameter.

Functions

- UINT32 SecGetFsptApiParameter (VOID)

  This function gets Fspt API parameter.

14.16.1 Detailed Description

Library to get FSP-T API parameter.

Copyright

INTEL CONFIDENTIAL Copyright 2019 Intel Corporation.

Specification Reference:

14.16.2 Function Documentation

14.16.2.1 SecGetFsptApiParameter()

```
UINT32 SecGetFsptApiParameter (
            VOID   )
```

This function gets Fspt API parameter.

Returns

The value of Fspt API parameter.

14.17 GpioConfig.h File Reference

Header file for GpioConfig structure used by GPIO library.

Classes

- struct GPIO_CONFIG

  GPIO configuration structure used for pin programming.

Macros

- #define B_GPIO_INT_CONFIG_INT_SOURCE_MASK 0x1F

  Mask for GPIO_INT_CONFIG for interrupt source.
- #define B_GPIO_INT_CONFIG_INT_TYPE_MASK 0xE0

  Mask for GPIO_INT_CONFIG for interrupt type.
- #define B_GPIO_ELECTRICAL_CONFIG_TERMINATION_MASK 0x1F

  Mask for GPIO_ELECTRICAL_CONFIG for termination value.
- #define B_GPIO_ELECTRICAL_CONFIG_1V8_TOLERANCE_MASK 0x60

  Mask for GPIO_ELECTRICAL_CONFIG for 1v8 tolerance setting.
- #define B_GPIO_LOCK_CONFIG_PAD_CONF_LOCK_MASK 0x3

  Mask for GPIO_LOCK_CONFIG for Pad Configuration Lock.
- #define B_GPIO_LOCK_CONFIG_OUTPUT_LOCK_MASK 0x5

  Mask for GPIO_LOCK_CONFIG for Pad Output Lock.
- #define B_GPIO_OTHER_CONFIG_RXRAW_MASK 0x3

  Mask for GPIO_OTHER_CONFIG for RxRaw1 setting.

Typedefs

- typedef UINT32 GPIO_PAD

  For any GpioPad usage in code use GPIO_PAD type.
- typedef UINT32 GPIO_GROUP

  For any GpioGroup usage in code use GPIO_GROUP type.

Enumerations

- enum GPIO_HARDWARE_DEFAULT
- enum GPIO_PAD_MODE

  GPIO Pad Mode Refer to GPIO documentation on native functions available for certain pad.
- enum GPIO_HOSTSW_OWN

  Host Software Pad Ownership modes This setting affects GPIO interrupt status registers.
- enum GPIO_DIRECTION

  GPIO Direction.
- enum GPIO_OUTPUT_STATE

  GPIO Output State This field is relevant only if output is enabled.
- enum GPIO_INT_CONFIG

  GPIO interrupt configuration This setting is applicable only if pad is in GPIO mode and has input enabled.
- enum GPIO_RESET_CONFIG

  GPIO Power Configuration GPIO_RESET_CONFIG allows to set GPIO Reset type (PADCFG_DW0.PadRstCfg) which will be used to reset certain GPIO settings.
- enum GPIO_ELECTRICAL_CONFIG

  GPIO Electrical Configuration Set GPIO termination and Pad Tolerance (applicable only for some pads) Field from GpioTermNone to GpioTermNative can be OR'ed with GpioTolerance1v8.
- enum GPIO_LOCK_CONFIG

  GPIO LockConfiguration Set GPIO configuration lock and output state lock.
- enum GPIO_OTHER_CONFIG

  Other GPIO Configuration GPIO_OTHER_CONFIG is used for less often settings and for future extensions Supported settings:

14.17.1 Detailed Description

Header file for GpioConfig structure used by GPIO library.

Copyright

Specification Reference:

14.17.2 Enumeration Type Documentation

14.17.2.1 GPIO_DIRECTION

```
enum GPIO_DIRECTION
```

GPIO Direction.

Enumerator

GpioDirDefault	Leave pad direction setting unmodified.
GpioDirInOut	Set pad for both output and input.
GpioDirInInvOut	Set pad for both output and input with inversion.
GpioDirIn	Set pad for input only.
GpioDirInInv	Set pad for input with inversion.
GpioDirOut	Set pad for output only.
GpioDirNone	Disable both output and input.

Definition at line 167 of file GpioConfig.h.

14.17.2.2 GPIO_ELECTRICAL_CONFIG

```
enum GPIO_ELECTRICAL_CONFIG
```

GPIO Electrical Configuration Set GPIO termination and Pad Tolerance (applicable only for some pads) Field from GpioTermNone to GpioTermNative can be OR'ed with GpioTolerance1v8.

Enumerator

GpioTermDefault	Leave termination setting unmodified.
GpioTermNone	none
GpioTermWpd5K	5kOhm weak pull-down
GpioTermWpd20K	20kOhm weak pull-down
GpioTermWpu1K	1kOhm weak pull-up
GpioTermWpu2K	2kOhm weak pull-up
GpioTermWpu5K	5kOhm weak pull-up
GpioTermWpu20K	20kOhm weak pull-up
GpioTermWpu1K2K	1kOhm & 2kOhm weak pull-up
GpioTermNative	Native function controls pads termination This setting is applicable only to some native modes. Please check EDS to determine which native functionality can control pads termination
GpioNoTolerance1v8	Disable 1.8V pad tolerance.
GpioTolerance1v8	Enable 1.8V pad tolerance.

Definition at line 296 of file GpioConfig.h.

14.17.2.3 GPIO_HARDWARE_DEFAULT

```
enum GPIO_HARDWARE_DEFAULT
```

Enumerator

GpioHardwareDefault	Leave setting unmodified.

Definition at line 118 of file GpioConfig.h.

14.17.2.4 GPIO_HOSTSW_OWN

```
enum GPIO_HOSTSW_OWN
```

Host Software Pad Ownership modes This setting affects GPIO interrupt status registers.

Depending on chosen ownership some GPIO Interrupt status register get updated and other masked. Please refer to EDS for HOSTSW_OWN register description.

Enumerator

GpioHostOwnDefault	Leave ownership value unmodified.
GpioHostOwnAcpi	Set HOST ownership to ACPI. Use this setting if pad is not going to be used by GPIO OS driver. If GPIO is configured to generate SCI/SMI/NMI then this setting must be used for interrupts to work
GpioHostOwnGpio	Set HOST ownership to GPIO Driver mode. Use this setting only if GPIO pad should be controlled by GPIO OS Driver. GPIO OS Driver will be able to control the pad if appropriate entry in ACPI exists (refer to ACPI specification for GpioIo and GpioInt descriptors)

Definition at line 146 of file GpioConfig.h.

14.17.2.5 GPIO_INT_CONFIG

```
enum GPIO_INT_CONFIG
```

GPIO interrupt configuration This setting is applicable only if pad is in GPIO mode and has input enabled.

GPIO_INT_CONFIG allows to choose which interrupt is generated (IOxAPIC/SCI/SMI/NMI) and how it is triggered (edge or level). Refer to PADCFG_DW0 register description in EDS for details on this settings. Field from Gpio↵ IntNmi to GpioIntApic can be OR'ed with GpioIntLevel to GpioIntBothEdge to describe an interrupt e.g. GpioIntApic

| GpioIntLevel If GPIO is set to cause an SCI then also GPI_GPE_EN is enabled for this pad. If GPIO is set to cause an NMI then also GPI_NMI_EN is enabled for this pad. Not all GPIO are capable of generating an SMI or NMI interrupt. When routing GPIO to cause an IOxAPIC interrupt care must be taken, as this interrupt cannot be shared and its IRQn number is not configurable. Refer to EDS for GPIO pads IRQ numbers (PADCFG_DW1.Int↩ Sel) If GPIO is under GPIO OS driver control and appropriate ACPI GpioInt descriptor exist then use only trigger type setting (from GpioIntLevel to GpioIntBothEdge). This type of GPIO Driver interrupt doesn't have any additional routing setting required to be set by BIOS. Interrupt is handled by GPIO OS Driver.

Enumerator

GpioIntDefault	Leave value of interrupt routing unmodified.
GpioIntDis	Disable IOxAPIC/SCI/SMI/NMI interrupt generation.
GpioIntNmi	Enable NMI interrupt only.
GpioIntSmi	Enable SMI interrupt only.
GpioIntSci	Enable SCI interrupt only.
GpioIntApic	Enable IOxAPIC interrupt only.
GpioIntLevel	Set interrupt as level triggered.
GpioIntEdge	Set interrupt as edge triggered (type of edge depends on input inversion)
GpioIntLvlEdgDis	Disable interrupt trigger.
GpioIntBothEdge	Set interrupt as both edge triggered.

Definition at line 207 of file GpioConfig.h.

14.17.2.6 GPIO_LOCK_CONFIG

```
enum GPIO_LOCK_CONFIG
```

GPIO LockConfiguration Set GPIO configuration lock and output state lock.

GpioLockPadConfig and GpioLockOutputState can be OR'ed. Lock settings reset is in Powergood domain. Care must be taken when using this setting as fields it locks may be reset by a different signal and can be controllable by what is in GPIO_RESET_CONFIG (PADCFG_DW0.PadRstCfg). GPIO library provides functions which allow to unlock a GPIO pad.

Enumerator

GpioLockDefault	Leave lock setting unmodified.
GpioPadConfigLock	Lock Pad Configuration.
GpioOutputStateLock	Lock GPIO pad output value.

Definition at line 329 of file GpioConfig.h.

14.17.2.7 GPIO_OTHER_CONFIG

```
enum GPIO_OTHER_CONFIG
```

Other GPIO Configuration GPIO_OTHER_CONFIG is used for less often settings and for future extensions Supported settings:

- RX raw override to '1' - allows to override input value to '1' This setting is applicable only if in input mode (both in GPIO and native usage). The override takes place at the internal pad state directly from buffer and before the RXINV.

Enumerator

GpioRxRaw1Default	Use default input override value.
GpioRxRaw1Dis	Don't override input.
GpioRxRaw1En	Override input to '1'.

Definition at line 346 of file GpioConfig.h.

14.17.2.8 GPIO_OUTPUT_STATE

```
enum GPIO_OUTPUT_STATE
```

GPIO Output State This field is relevant only if output is enabled.

Enumerator

GpioOutDefault	Leave output value unmodified.
GpioOutLow	Set output to low.
GpioOutHigh	Set output to high.

Definition at line 181 of file GpioConfig.h.

14.17.2.9 GPIO_PAD_MODE

```
enum GPIO_PAD_MODE
```

GPIO Pad Mode Refer to GPIO documentation on native functions available for certain pad.

If GPIO is set to one of NativeX modes then following settings are not applicable and can be skipped:

- Interrupt related settings
- Host Software Ownership
- Output/Input enabling/disabling
- Output lock

Definition at line 132 of file GpioConfig.h.

14.17.2.10 GPIO_RESET_CONFIG

```
enum GPIO_RESET_CONFIG
```

GPIO Power Configuration GPIO_RESET_CONFIG allows to set GPIO Reset type (PADCFG_DW0.PadRstCfg) which will be used to reset certain GPIO settings.

Refer to EDS for settings that are controllable by PadRstCfg.

Enumerator

GpioResetDefault	Leave value of pad reset unmodified.
GpioResetPwrGood	Deprecated settings. Maintained only for compatibility.GPP: RSMRST; GPD: DSW_PWROK; (PadRstCfg = 00b = "Powergood")
GpioResetDeep	Deep GPIO Reset (PadRstCfg = 01b = "Deep GPIO Reset")
GpioResetNormal	GPIO Reset (PadRstCfg = 10b = "GPIO Reset")
GpioResetResume	GPP: Reserved; GPD: RSMRST; (PadRstCfg = 11b = "Resume Reset")
GpioResumeReset	New GPIO reset configuration options. Resume Reset (RSMRST) GPP: PadRstCfg = 00b = "Powergood" GPD: PadRstCfg = 11b = "Resume Reset" Pad setting will reset on: • DeepSx transition • G3 Pad settings will not reset on: • S3/S4/S5 transition • Warm/Cold/Global reset
GpioHostDeepReset	Host Deep Reset PadRstCfg = 01b = "Deep GPIO Reset" Pad settings will reset on: • Warm/Cold/Global reset • DeepSx transition • G3 Pad settings will not reset on: • S3/S4/S5 transition
GpioPlatformReset	Platform Reset (PLTRST) PadRstCfg = 10b = "GPIO Reset" Pad settings will reset on: • S3/S4/S5 transition • Warm/Cold/Global reset • DeepSx transition • G3
GpioDswReset	Deep Sleep Well Reset (DSW_PWROK) GPP: not applicable GPD: PadRstCfg = 00b = "Powergood" Pad settings will reset on: • G3 Pad settings will not reset on: • S3/S4/S5 transition • Warm/Cold/Global reset • DeepSx transition

Definition at line 229 of file GpioConfig.h.

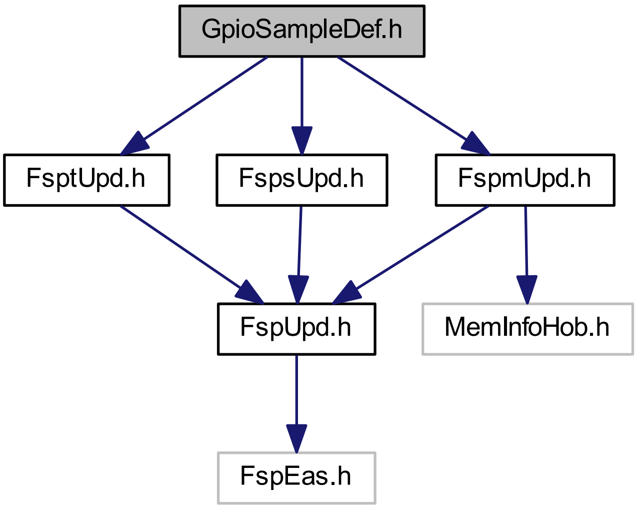
14.18 GpioSampleDef.h File Reference

Sample enum definitions for GPIO table.

```
#include <FsptUpd.h>
#include <FspmUpd.h>
```

```
#include <FspsUpd.h>
```

Include dependency graph for GpioSampleDef.h:



14.18.1 Detailed Description

Sample enum definitions for GPIO table.

Copyright

Specification Reference:

14.19 LegacyBios.h File Reference

The EFI Legacy BIOS Protocol is used to abstract legacy Option ROM usage under EFI and Legacy OS boot.

Classes

- struct EFI_COMPATIBILITY16_TABLE

  There is a table located within the traditional BIOS in either the 0xF000:xxxx or 0xE000:xxxx physical address range.
- struct EFI_DISPATCH_OPROM_TABLE

  EFI_DISPATCH_OPROM_TABLE.
- struct EFI_TO_COMPATIBILITY16_INIT_TABLE

  EFI_TO_COMPATIBILITY16_INIT_TABLE.
- struct DEVICE_PRODUCER_SERIAL

  DEVICE_PRODUCER_SERIAL.
- struct DEVICE_PRODUCER_PARALLEL

  @)
- struct DEVICE_PRODUCER_FLOPPY

  DEVICE_PRODUCER_FLOPPY.
- struct LEGACY_DEVICE_FLAGS

  LEGACY_DEVICE_FLAGS.
- struct DEVICE_PRODUCER_DATA_HEADER

  DEVICE_PRODUCER_DATA_HEADER.
- struct ATAPI_IDENTIFY

  ATAPI_IDENTIFY.
- struct HDD_INFO

  HDD_INFO.
- struct BBS_STATUS_FLAGS

  BBS_STATUS_FLAGS;.
- struct BBS_TABLE

  BBS_TABLE, device type values & boot priority values.
- struct SMM_ATTRIBUTES

  SMM_ATTRIBUTES.
- struct SMM_FUNCTION

  SMM_FUNCTION & relating constants.
- struct SMM_ENTRY

  This structure assumes both port and data sizes are 1.
- struct SMM_TABLE

  SMM_TABLE.
- struct UDC_ATTRIBUTES

  UDC_ATTRIBUTES.
- struct UD_TABLE

  UD_TABLE.
- struct EFI_TO_COMPATIBILITY16_BOOT_TABLE

  EFI_TO_COMPATIBILITY16_BOOT_TABLE.
- struct EFI_LEGACY_INSTALL_PCI_HANDLER

  EFI_LEGACY_INSTALL_PCI_HANDLER.
- struct EFI_EFLAGS_REG

  EFI_EFLAGS_REG.
- struct EFI_DWORD_REGS

  EFI_DWORD_REGS.
- struct EFI_FLAGS_REG

  EFI_FLAGS_REG.
- struct EFI_WORD_REGS

  EFI_WORD_REGS.
- struct EFI_BYTE_REGS

EFI_BYTE_REGS.

- union EFI_IA32_REGISTER_SET

  EFI_IA32_REGISTER_SET.
- struct _EFI_LEGACY_BIOS_PROTOCOL

  Abstracts the traditional BIOS from the rest of EFI.

Macros

- #define HDD_PRIMARY 0x01

  HDD_INFO status bits.
- #define NO_ROM 0x00

  Flags returned by CheckPciRom().
- #define ROM_WITH_CONFIG 0x04

  Not defined in the Framework CSM Specification.
- #define DEVICE_SERIAL_MODE_NORMAL 0x00

  DEVICE_PRODUCER_SERIAL's modes.
- #define DEVICE_PARALLEL_MODE_MODE_OUTPUT_ONLY 0x00

  DEVICE_PRODUCER_PARALLEL's modes.
- #define BBS_FLOPPY 0x01

  BBS device type values.
- #define BBS_DO_NOT_BOOT_FROM 0xFFFC

  BBS boot priority values.
- #define STANDARD_IO 0x00

  SMM_ATTRIBUTES type values.
- #define PORT_SIZE_8 0x00

  SMM_ATTRIBUTES port size constants.
- #define DATA_SIZE_8 0x00

SMM_ATTRIBUTES data size constants.

- #define INT15_D042 0x0000

  SMM_FUNCTION Function constants.

- #define STANDARD_OWNER 0x0

  SMM_FUNCTION Owner constants.

- #define EFI_SEGMENT(_Adr) (UINT16) ((UINT16) (((UINTN) (_Adr)) >> 4) & 0xf000)

  The following macros do not appear in the Framework CSM Specification and are kept for backward compatibility only.

Typedefs

- typedef BOOLEAN(∗ EFI_LEGACY_BIOS_INT86) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UINT8 BiosInt, IN OUT EFI_IA32_REGISTER_SET ∗Regs)

  Thunk to 16-bit real mode and execute a software interrupt with a vector of BiosInt.
- typedef BOOLEAN(∗ EFI_LEGACY_BIOS_FARCALL86) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UINT16 Segment, IN UINT16 Offset, IN EFI_IA32_REGISTER_SET ∗Regs, IN VOID ∗Stack, IN UINTN StackSize)

  Thunk to 16-bit real mode and call Segment:Offset.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_CHECK_ROM) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN EFI_HANDLE PciHandle, OUT VOID ∗∗RomImage, OPTIONAL OUT UINTN ∗RomSize, OPTIONAL OUT UINTN ∗Flags)

  Test to see if a legacy PCI ROM exists for this device.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_INSTALL_ROM) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN EFI_HANDLE PciHandle, IN VOID ∗∗RomImage, OUT UINTN ∗Flags, OUT UINT8 ∗DiskStart, OPTIONAL OUT UINT8 ∗DiskEnd, OPTIONAL OUT VOID ∗∗RomShadowAddress, OPTIONAL OUT UINT32 ∗ShadowedRomSize OPTIONAL)

  Load a legacy PC-AT OPROM on the PciHandle device.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_BOOT) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN BBS_BBS_DEVICE_PATH ∗BootOption, IN UINT32 LoadOptionsSize, IN VOID ∗LoadOptions)

  This function attempts to traditionally boot the specified BootOption.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_UPDATE_KEYBOARD_LED_STATUS) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UINT8 Leds)

  This function takes the Leds input parameter and sets/resets the BDA accordingly.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_GET_BBS_INFO) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, OUT UINT16 ∗HddCount, OUT HDD_INFO ∗∗HddInfo, OUT UINT16 ∗BbsCount, IN OUT BBS_TABLE ∗∗BbsTable)

  Retrieve legacy BBS info and assign boot priority.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_PREPARE_TO_BOOT_EFI) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, OUT UINT16 ∗BbsCount, OUT BBS_TABLE ∗∗BbsTable)

  Assign drive number to legacy HDD drives prior to booting an EFI aware OS so the OS can access drives without an EFI driver.

- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_BOOT_UNCONVENTIONAL_DEVICE) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UDC_ATTRIBUTES Attributes, IN UINTN BbsEntry, IN VOID ∗BeerData, IN VOID ∗ServiceAreaData)

  To boot from an unconventional device like parties and/or execute HDD diagnostics.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_SHADOW_ALL_LEGACY_OPROMS) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This)

  Shadow all legacy16 OPROMs that haven't been shadowed.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_GET_LEGACY_REGION) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UINTN LegacyMemorySize, IN UINTN Region, IN UINTN Alignment, OUT VOID ∗∗LegacyMemoryAddress)

  Get a region from the LegacyBios for S3 usage.
- typedef EFI_STATUS(∗ EFI_LEGACY_BIOS_COPY_LEGACY_REGION) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This, IN UINTN LegacyMemorySize, IN VOID ∗LegacyMemoryAddress, IN VOID ∗LegacyMemorySourceAddress)

  Get a region from the LegacyBios for Tiano usage.

Enumerations

- enum EFI_COMPATIBILITY_FUNCTIONS

  Functions provided by the CSM binary which communicate between the EfiCompatibility and Compatability16 code.

14.19.1 Detailed Description

The EFI Legacy BIOS Protocol is used to abstract legacy Option ROM usage under EFI and Legacy OS boot.

This file also includes all the related COMPATIBILIY16 structures and defintions.

Note: The names for EFI_IA32_REGISTER_SET elements were picked to follow well known naming conventions.

Thunk is the code that switches from 32-bit protected environment into the 16-bit real-mode environment. Reverse thunk is the code that does the opposite.

Revision Reference:

This protocol is defined in Framework for EFI Compatibility Support Module spec Version 0.98.

14.19.2 Macro Definition Documentation

14.19.2.1 EFI_SEGMENT

```
#define EFI_SEGMENT(
              _Adr ) (UINT16) ((UINT16) (((UINTN) (_Adr)) >> 4) & 0xf000)
```

The following macros do not appear in the Framework CSM Specification and are kept for backward compatibility only.

They convert 32-bit address (_Adr) to Segment:Offset 16-bit form.

Definition at line 1016 of file LegacyBios.h.

14.19.3 Typedef Documentation

14.19.3.1 EFI_LEGACY_BIOS_BOOT

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_BOOT) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN BBS_BBS_DE↩
VICE_PATH *BootOption, IN UINT32 LoadOptionsSize, IN VOID *LoadOptions)
```

This function attempts to traditionally boot the specified BootOption.

If the EFI context has been compromised, this function will not return. This procedure is not used for loading an EFI-aware OS off a traditional device. The following actions occur:

- Get EFI SMBIOS data structures, convert them to a traditional format, and copy to Compatibility16.
- Get a pointer to ACPI data structures and copy the Compatibility16 RSD PTR to F0000 block.
- Find the traditional SMI handler from a firmware volume and register the traditional SMI handler with the EFI SMI handler.
- Build onboard IDE information and pass this information to the Compatibility16 code.
- Make sure all PCI Interrupt Line registers are programmed to match 8259.
- Reconfigure SIO devices from EFI mode (polled) into traditional mode (interrupt driven).
- Shadow all PCI ROMs.
- Set up BDA and EBDA standard areas before the legacy boot.
- Construct the Compatibility16 boot memory map and pass it to the Compatibility16 code.
- Invoke the Compatibility16 table function Compatibility16PrepareToBoot(). This invocation causes a thunk into the Compatibility16 code, which sets all appropriate internal data structures. The boot device list is a parameter.
- Invoke the Compatibility16 Table function Compatibility16Boot(). This invocation causes a thunk into the Compatibility16 code, which does an INT19.
- If the Compatibility16Boot() function returns, then the boot failed in a graceful manner–meaning that the EFI code is still valid. An ungraceful boot failure causes a reset because the state of EFI code is unknown.

Parameters

in	*This*	The protocol instance pointer.
in	*BootOption*	The EFI Device Path from BootXXXX variable.
in	*LoadOptionSize*	The size of LoadOption in size.
in	*LoadOption*	LThe oadOption from BootXXXX variable.

Return values

EFI_DEVICE_ERROR	Failed to boot from any boot device and memory is uncorrupted. Note: This function normally does not returns. It will either boot the OS or reset the system if memory has been "corrupted" by loading a boot sector and passing control to it.

Definition at line 1287 of file LegacyBios.h.

14.19.3.2 EFI_LEGACY_BIOS_BOOT_UNCONVENTIONAL_DEVICE

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_BOOT_UNCONVENTIONAL_DEVICE) (IN EFI_LEGACY_BIOS_PROTOCOL
*This, IN UDC_ATTRIBUTES Attributes, IN UINTN BbsEntry, IN VOID *BeerData, IN VOID *Service←
AreaData)
```

To boot from an unconventional device like parties and/or execute HDD diagnostics.

Parameters

in	*This*	The protocol instance pointer.
in	*Attributes*	How to interpret the other input parameters.
in	*BbsEntry*	The 0-based index into the BbsTable for the parent device.
in	*BeerData*	A pointer to the 128 bytes of ram BEER data.
in	*ServiceAreaData*	A pointer to the 64 bytes of raw Service Area data. The caller must provide a pointer to the specific Service Area and not the start all Service Areas.

Return values

EFI_INVALID_PARAMETER	If error. Does NOT return if no error.

Definition at line 1376 of file LegacyBios.h.

14.19.3.3 EFI_LEGACY_BIOS_CHECK_ROM

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_CHECK_ROM) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN EFI_H←
ANDLE PciHandle, OUT VOID **RomImage, OPTIONAL OUT UINTN *RomSize, OPTIONAL OUT UINTN *Flags)
```

Test to see if a legacy PCI ROM exists for this device.

Optionally return the Legacy ROM instance for this PCI device.

Parameters

in	*This*	The protocol instance pointer.
in	*PciHandle*	The PCI PC-AT OPROM from this devices ROM BAR will be loaded
out	*RomImage*	Return the legacy PCI ROM for this device.
out	*RomSize*	The size of ROM Image.
out	*Flags*	Indicates if ROM found and if PC-AT. Multiple bits can be set as follows: • 00 = No ROM. • 01 = ROM Found. • 02 = ROM is a valid legacy ROM.

Return values

EFI_SUCCESS	The Legacy Option ROM available for this device
EFI_UNSUPPORTED	The Legacy Option ROM is not supported.

Definition at line 1206 of file LegacyBios.h.

14.19.3.4 EFI_LEGACY_BIOS_COPY_LEGACY_REGION

```
typedef EFI_STATUS( ∗ EFI_LEGACY_BIOS_COPY_LEGACY_REGION) (IN EFI_LEGACY_BIOS_PROTOCOL ∗This,
IN UINTN LegacyMemorySize, IN VOID ∗LegacyMemoryAddress, IN VOID ∗LegacyMemorySourceAddress)
```

Get a region from the LegacyBios for Tiano usage.

Can only be invoked once.

Parameters

in	*This*	The protocol instance pointer.
in	*LegacyMemorySize*	The size of data to copy.
in	*LegacyMemoryAddress*	The Legacy Region destination address. Note: must be in region assigned by LegacyBiosGetLegacyRegion.
in	*LegacyMemorySourceAddress*	The source of the data to copy.

Return values

EFI_SUCCESS	The Region assigned.
EFI_ACCESS_DENIED	Destination was outside an assigned region.

Definition at line 1445 of file LegacyBios.h.

14.19.3.5 EFI_LEGACY_BIOS_FARCALL86

```
typedef BOOLEAN( * EFI_LEGACY_BIOS_FARCALL86) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN UINT16
Segment, IN UINT16 Offset, IN EFI_IA32_REGISTER_SET *Regs, IN VOID *Stack, IN UINTN StackSize)
```

Thunk to 16-bit real mode and call Segment:Offset.

Regs will contain the 16-bit register context on entry and exit. Arguments can be passed on the Stack argument

Parameters

in	*This*	The protocol instance pointer.
in	*Segment*	The segemnt of 16-bit mode call.
in	*Offset*	The offset of 16-bit mdoe call.
in	*Reg*	Register contexted passed into (and returned) from thunk to 16-bit mode.
in	*Stack*	The caller allocated stack used to pass arguments.
in	*StackSize*	The size of Stack in bytes.

Return values

FALSE	Thunk completed with no BIOS errors in the target code. See Regs for status.
TRUE	There was a BIOS error in the target code.

Definition at line 1178 of file LegacyBios.h.

14.19.3.6 EFI_LEGACY_BIOS_GET_BBS_INFO

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_GET_BBS_INFO) (IN EFI_LEGACY_BIOS_PROTOCOL *This, OUT U←
INT16 *HddCount, OUT HDD_INFO **HddInfo, OUT UINT16 *BbsCount, IN OUT BBS_TABLE **BbsTable)
```

Retrieve legacy BBS info and assign boot priority.

Parameters

in	*This*	The protocol instance pointer.
out	*HddCount*	The number of HDD_INFO structures.
out	*HddInfo*	Onboard IDE controller information.
out	*BbsCount*	The number of BBS_TABLE structures.
in,out	*BbsTable*	Points to List of BBS_TABLE.

Return values

EFI_SUCCESS	Tables were returned.

Definition at line 1331 of file LegacyBios.h.

14.19.3.7 EFI_LEGACY_BIOS_GET_LEGACY_REGION

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_GET_LEGACY_REGION) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN
UINTN LegacyMemorySize, IN UINTN Region, IN UINTN Alignment, OUT VOID **LegacyMemoryAddress)
```

Get a region from the LegacyBios for S3 usage.

Parameters

in	*This*	The protocol instance pointer.
in	*LegacyMemorySize*	The size of required region.
in	*Region*	The region to use. 00 = Either 0xE0000 or 0xF0000 block. • Bit0 = 1 0xF0000 block. • Bit1 = 1 0xE0000 block.
in	*Alignment*	Address alignment. Bit mapped. The first non-zero bit from right is alignment.
out	*LegacyMemoryAddress*	The Region Assigned

Return values

EFI_SUCCESS	The Region was assigned.
EFI_ACCESS_DENIED	The function was previously invoked.
Other	The Region was not assigned.

Definition at line 1421 of file LegacyBios.h.

14.19.3.8 EFI_LEGACY_BIOS_INSTALL_ROM

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_INSTALL_ROM) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN E↩
FI_HANDLE PciHandle, IN VOID **RomImage, OUT UINTN *Flags, OUT UINT8 *DiskStart, OPTIONAL OUT
UINT8 *DiskEnd, OPTIONAL OUT VOID **RomShadowAddress, OPTIONAL OUT UINT32 *ShadowedRomSize OP↩
TIONAL)
```

Load a legacy PC-AT OPROM on the PciHandle device.

Return information about how many disks were added by the OPROM and the shadow address and size. DiskStart & DiskEnd are INT 13h drive letters. Thus 0x80 is C:

Parameters

in	*This*	The protocol instance pointer.
in	*PciHandle*	The PCI PC-AT OPROM from this devices ROM BAR will be loaded. This value is NULL if RomImage is non-NULL. This is the normal case.
in	*RomImage*	A PCI PC-AT ROM image. This argument is non-NULL if there is no hardware associated with the ROM and thus no PciHandle, otherwise is must be NULL. Example is PXE base code.

Parameters

out	*Flags*	The type of ROM discovered. Multiple bits can be set, as follows: • 00 = No ROM. • 01 = ROM found. • 02 = ROM is a valid legacy ROM.
out	*DiskStart*	The disk number of first device hooked by the ROM. If DiskStart is the same as DiskEnd no disked were hooked.
out	*DiskEnd*	disk number of the last device hooked by the ROM.
out	*RomShadowAddress*	Shadow address of PC-AT ROM.
out	*RomShadowSize*	Size of RomShadowAddress in bytes.

Return values

EFI_SUCCESS	Thunk completed, see Regs for status.
EFI_INVALID_PARAMETER	PciHandle not found

Definition at line 1243 of file LegacyBios.h.

14.19.3.9 EFI_LEGACY_BIOS_INT86

```
typedef BOOLEAN( * EFI_LEGACY_BIOS_INT86) (IN EFI_LEGACY_BIOS_PROTOCOL *This, IN UINT8 BiosInt,
IN OUT EFI_IA32_REGISTER_SET *Regs)
```

Thunk to 16-bit real mode and execute a software interrupt with a vector of BiosInt.

Regs will contain the 16-bit register context on entry and exit.

Parameters

in	*This*	The protocol instance pointer.
in	*BiosInt*	The processor interrupt vector to invoke.
in,out	*Reg*	Register contexted passed into (and returned) from thunk to 16-bit mode.

Return values

TRUE	Thunk completed with no BIOS errors in the target code. See Regs for status.
FALSE	There was a BIOS error in the target code.

Definition at line 1155 of file LegacyBios.h.

14.19.3.10 EFI_LEGACY_BIOS_PREPARE_TO_BOOT_EFI

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_PREPARE_TO_BOOT_EFI) (IN EFI_LEGACY_BIOS_PROTOCOL *This,
OUT UINT16 *BbsCount, OUT BBS_TABLE **BbsTable)
```

Assign drive number to legacy HDD drives prior to booting an EFI aware OS so the OS can access drives without an EFI driver.

Parameters

in	*This*	The protocol instance pointer.
out	*BbsCount*	The number of BBS_TABLE structures
out	*BbsTable*	List of BBS entries

Return values

EFI_SUCCESS	Drive numbers assigned.

Definition at line 1352 of file LegacyBios.h.

14.19.3.11 EFI_LEGACY_BIOS_SHADOW_ALL_LEGACY_OPROMS

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_SHADOW_ALL_LEGACY_OPROMS) (IN EFI_LEGACY_BIOS_PROTOCOL
*This)
```

Shadow all legacy16 OPROMs that haven't been shadowed.

Warning: Use this with caution. This routine disconnects all EFI drivers. If used externally, then the caller must re-connect EFI drivers.

Parameters

in	*This*	The protocol instance pointer.

Return values

EFI_SUCCESS	OPROMs were shadowed.

Definition at line 1397 of file LegacyBios.h.

14.19.3.12 EFI_LEGACY_BIOS_UPDATE_KEYBOARD_LED_STATUS

```
typedef EFI_STATUS( * EFI_LEGACY_BIOS_UPDATE_KEYBOARD_LED_STATUS) (IN EFI_LEGACY_BIOS_PROTOCOL
*This, IN UINT8 Leds)
```

This function takes the Leds input parameter and sets/resets the BDA accordingly.

Leds is also passed to Compatibility16 code, in case any special processing is required. This function is normally called from EFI Setup drivers that handle user-selectable keyboard options such as boot with NUM LOCK on/off. This function does not touch the keyboard or keyboard LEDs but only the BDA.

Parameters

in	*This*	The protocol instance pointer.
in	*Leds*	The status of current Scroll, Num & Cap lock LEDS: • Bit 0 is Scroll Lock 0 = Not locked. • Bit 1 is Num Lock. • Bit 2 is Caps Lock.

Return values

EFI_SUCCESS	The BDA was updated successfully.

Definition at line 1312 of file LegacyBios.h.

14.19.4 Enumeration Type Documentation

14.19.4.1 EFI_COMPATIBILITY_FUNCTIONS

```
enum EFI_COMPATIBILITY_FUNCTIONS
```

Functions provided by the CSM binary which communicate between the EfiCompatibility and Compatability16 code.

Inconsistent with the specification here: The member's name started with "Compatibility16" [defined in Intel Framework Compatibility Support Module Specification / 0.97 version] has been changed to "Legacy16" since keeping backward compatible.

Enumerator

Legacy16InitializeYourself	Causes the Compatibility16 code to do any internal initialization required. Input: AX = Compatibility16InitializeYourself ES:BX = Pointer to EFI_TO_COMPATIBILITY16_INIT_TABLE Return: AX = Return Status codes
Legacy16UpdateBbs	Causes the Compatibility16 BIOS to perform any drive number translations to match the boot sequence. Input: AX = Compatibility16UpdateBbs ES:BX = Pointer to EFI_TO_COMPATIBILITY16_BOOT_TABLE Return: AX = Returned status codes
Legacy16PrepareToBoot	Allows the Compatibility16 code to perform any final actions before booting. The Compatibility16 code is read/write. Input: AX = Compatibility16PrepareToBoot ES:BX = Pointer to EFI_TO_COMPATIBILITY16_BOOT_TABLE structure
	Return: AX = Returned status codes

Enumerator

Legacy16Boot	Causes the Compatibility16 BIOS to boot. The Compatibility16 code is Read/Only. Input: AX = Compatibility16Boot Output: AX = Returned status codes
Legacy16RetrieveLastBootDevice	Allows the Compatibility16 code to get the last device from which a boot was attempted. This is stored in CMOS and is the priority number of the last attempted boot device. Input: AX = Compatibility16RetrieveLastBootDevice Output: AX = Returned status codes BX = Priority number of the boot device.
Legacy16DispatchOprom	Allows the Compatibility16 code rehook INT13, INT18, and/or INT19 after dispatching a legacy OpROM. Input: AX = Compatibility16DispatchOprom ES:BX = Pointer to EFI_DISPATCH_OPROM_TABLE Output: AX = Returned status codes BX = Number of non-BBS-compliant devices found. Equals 0 if BBS compliant.
Legacy16GetTableAddress	Finds a free area in the 0xFxxxx or 0xExxxx region of the specified length and returns the address of that region. Input: AX = Compatibility16GetTableAddress BX = Allocation region 00 = Allocate from either 0xE0000 or 0xF0000 64 KB blocks. Bit 0 = 1 Allocate from 0xF0000 64 KB block Bit 1 = 1 Allocate from 0xE0000 64 KB block CX = Requested length in bytes. DX = Required address alignment. Bit mapped. First non-zero bit from the right is the alignment. Output: AX = Returned status codes DS:BX = Address of the region
Legacy16SetKeyboardLeds	Enables the EfiCompatibility module to do any nonstandard processing of keyboard LEDs or state. Input: AX = Compatibility16SetKeyboardLeds CL = LED status. Bit 0 Scroll Lock 0 = Off Bit 1 NumLock Bit 2 Caps Lock Output: AX = Returned status codes
Legacy16InstallPciHandler	Enables the EfiCompatibility module to install an interrupt handler for PCI mass media devices that do not have an OpROM associated with them. An example is SATA. Input: AX = Compatibility16InstallPciHandler ES:BX = Pointer to EFI_LEGACY_INSTALL_PCI_HANDLER structure Output: AX = Returned status codes

Definition at line 267 of file LegacyBios.h.

14.20 LegacyInterrupt.h File Reference

This protocol abstracts the PIRQ programming from the generic EFI Compatibility Support Modules (CSMs).

Typedefs

- typedef EFI_STATUS(∗ EFI_LEGACY_INTERRUPT_GET_NUMBER_PIRQS) (IN EFI_LEGACY_INTERRUPT_PROTOCOL ∗This, OUT UINT8 ∗NumberPirqs)

  Get the number of PIRQs this hardware supports.
- typedef EFI_STATUS(∗ EFI_LEGACY_INTERRUPT_GET_LOCATION) (IN EFI_LEGACY_INTERRUPT_PROTOCOL ∗This, OUT UINT8 ∗Bus, OUT UINT8 ∗Device, OUT UINT8 ∗Function)

  Gets the PCI location associated with this protocol.
- typedef EFI_STATUS(∗ EFI_LEGACY_INTERRUPT_READ_PIRQ) (IN EFI_LEGACY_INTERRUPT_PROTOCOL ∗This, IN UINT8 PirqNumber, OUT UINT8 ∗PirqData)

  Read the PIRQ register and return the data.
- typedef EFI_STATUS(∗ EFI_LEGACY_INTERRUPT_WRITE_PIRQ) (IN EFI_LEGACY_INTERRUPT_PROTOCOL ∗This, IN UINT8 PirqNumber, IN UINT8 PirqData)

  Write the specified PIRQ register with the given data.

14.20.1 Detailed Description

This protocol abstracts the PIRQ programming from the generic EFI Compatibility Support Modules (CSMs).

Revision Reference:

This protocol is defined in Framework for the EFI Compatibility Support Module specification. Version 0.97.

14.20.2 Typedef Documentation

14.20.2.1 EFI_LEGACY_INTERRUPT_GET_LOCATION

```
typedef EFI_STATUS( * EFI_LEGACY_INTERRUPT_GET_LOCATION) (IN EFI_LEGACY_INTERRUPT_PROTOCOL
*This, OUT UINT8 *Bus, OUT UINT8 *Device, OUT UINT8 *Function)
```

Gets the PCI location associated with this protocol.

Parameters

This	The Protocol instance pointer.
Bus	The PCI Bus.
Device	The PCI Device.
Function	The PCI Function.

Return values

EFI_SUCCESS	The Bus, Device, and Function were returned successfully.

Definition at line 59 of file LegacyInterrupt.h.

14.20.2.2 EFI_LEGACY_INTERRUPT_GET_NUMBER_PIRQS

```
typedef EFI_STATUS( * EFI_LEGACY_INTERRUPT_GET_NUMBER_PIRQS) (IN EFI_LEGACY_INTERRUPT_PROTOCOL
*This, OUT UINT8 *NumberPirqs)
```

Get the number of PIRQs this hardware supports.

Parameters

This	The protocol instance pointer.
NumberPirsq	The number of PIRQs that are supported.

Return values

EFI_SUCCESS	The number of PIRQs was returned successfully.

Definition at line 41 of file LegacyInterrupt.h.

14.20.2.3 EFI_LEGACY_INTERRUPT_READ_PIRQ

```
typedef EFI_STATUS( * EFI_LEGACY_INTERRUPT_READ_PIRQ) (IN EFI_LEGACY_INTERRUPT_PROTOCOL *This,
IN UINT8 PirqNumber, OUT UINT8 *PirqData)
```

Read the PIRQ register and return the data.

Parameters

This	The protocol instance pointer.
PirqNumber	The PIRQ register to read.
PirqData	The data read.

Return values

EFI_SUCCESS	The data was read.
EFI_INVALID_PARAMETER	Invalid PIRQ number.
EFI_DEVICE_ERROR	Operation was unsuccessful

Definition at line 79 of file LegacyInterrupt.h.

14.20.2.4 EFI_LEGACY_INTERRUPT_WRITE_PIRQ

```
typedef EFI_STATUS( * EFI_LEGACY_INTERRUPT_WRITE_PIRQ) (IN EFI_LEGACY_INTERRUPT_PROTOCOL *This,
IN UINT8 PirqNumber, IN UINT8 PirqData)
```

Write the specified PIRQ register with the given data.

Parameters

This	The protocol instance pointer.
PirqNumber	A PIRQ register to read.
PirqData	The data to write.

Return values

EFI_SUCCESS	The PIRQ was programmed.
EFI_INVALID_PARAMETER	Invalid PIRQ number.
EFI_DEVICE_ERROR	Operation was unsuccessful

Definition at line 98 of file LegacyInterrupt.h.

14.21 MemoryTypeInformation.h File Reference

This file defines: Memory Type Information GUID for HOB and Variable.

14.21.1 Detailed Description

This file defines: Memory Type Information GUID for HOB and Variable.

Memory Type Information Variable Name. Memory Type Information GUID HOB data structure.

The memory type information HOB and variable can be used to store the information for each memory type in Variable or HOB.

14.22 MmPciLib.h File Reference

Get Pci Express address library implementation.

Functions

- UINTN MmPciBase (IN UINT32 Bus, IN UINT32 Device, IN UINT32 Function)

  This procedure will get PCIE address.

14.22.1 Detailed Description

Get Pci Express address library implementation.

Copyright

Specification Reference:

14.22.2 Function Documentation

14.22.2.1 MmPciBase()

```
UINTN MmPciBase (
            IN UINT32 Bus,
            IN UINT32 Device,
            IN UINT32 Function )
```

This procedure will get PCIE address.

Parameters

in	*Bus*	Pci Bus Number
in	*Device*	Pci Device Number
in	*Function*	Pci Function Number

Return values

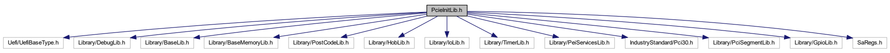
P↩ CIE	address

14.23 PcieInitLib.h File Reference

PCIe Initialization Library header file.

```
#include <Uefi/UefiBaseType.h>
#include <Library/DebugLib.h>
#include <Library/BaseLib.h>
#include <Library/BaseMemoryLib.h>
#include <Library/PostCodeLib.h>
#include <Library/HobLib.h>
#include <Library/IoLib.h>
#include <Library/TimerLib.h>
#include <Library/PeiServicesLib.h>
#include <IndustryStandard/Pci30.h>
#include <Library/PciSegmentLib.h>
#include <Library/GpioLib.h>
#include <SaRegs.h>
```

Include dependency graph for PcieInitLib.h:



Classes

- struct PCIE_PORT_SWEQ_DATA

  PCIe Root Port description data structure, used as the interface between low level and high level.
- struct PCIE_PORT_EQS

  Data structure for passing static equalization data for programming.
- struct PCIE_SWEQ_GPIO_CONFIG

  Input Configuration Parameters for Software Equalization Support.
- struct PCIE_SWEQ_PRESET_SCORE

  Data Output from Software Equalization.

Typedefs

- typedef VOID(∗ PCIE_DETECT_ENDPOINT_PRESENCE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength)

  PCIe Initialization Library Generic Low Level Function Calls All of these functions can be implemented using only PCIe specification level details.
- typedef UINT8(∗ PCIE_GET_PCIE_CAP_OFFSET) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Gets the PCIe Capability Structure Pointer.

- typedef BOOLEAN(∗ PCIE_DATA_LINK_LAYER_LINK_ACTIVE) (IN PCIE_SI_LOW_LEVEL_FUNCTION↩_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Checks if the Data Link Layer is in DL_Active state on the given root port.
- typedef BOOLEAN(∗ PCIE_GET_SLOT_PRESENCE_DETECT) (IN PCIE_SI_LOW_LEVEL_FUNCTION↩_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Returns the current value of the PCIe Slot Status Presence Detect bit.
- typedef VOID(∗ PCIE_SET_LINK_DISABLE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN P↩CIE_PORT_INFO ∗PciePort, IN BOOLEAN LinkDisable)

  Set the Link Disable bit in the PCIe Link Control Register.
- typedef VOID(∗ PCIE_RETRAIN_LINK) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_↩PORT_INFO ∗PciePort)

  Retrain the PCIe link.
- typedef UINT8(∗ PCIE_GET_NEGOTIATED_WIDTH) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Get Negotiated Link Width.
- typedef UINT8(∗ PCIE_GET_CURRENT_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Get Current Link Speed.
- typedef BOOLEAN(∗ PCIE_EXISTS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This)

  PCIe Initialization Library Silicon Specific Low Level Function Calls Enables Abstraction of Silicon details keeping this library generic.
- typedef VOID(∗ PCIE_GET_ROOT_PORTS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, OUT PCIE_PORT_INFO ∗PciePorts, OUT UINT8 ∗PciePortsLength)

  This function determines the topology of the PCIe bus interface that is being initialized using silicon defined mechanisms.
- typedef VOID(∗ PCIE_PROGRAM_STATIC_GEN3_EQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_EQS ∗PciePortEqs, IN UINT8 PciePortEqsLength)

  Programs static equalization settings for the given list of PCIe root ports.
- typedef EFI_STATUS(∗ PCIE_SET_GEN3_PHASE2_BYPASS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_↩CALLS ∗This, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength, IN BOOLEAN BypassPhase2)

  Sets Gen3 Equalization Phase 2 Bypass for all given Root Ports.
- typedef VOID(∗ PCIE_REPORT_LINK_STATUS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  This function reports a PCIe controller's link status
- typedef EFI_STATUS(∗ PCIE_WAIT_FOR_L0) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  PCIe Link Recovery Functions.
- typedef UINT8(∗ PCIE_GET_TARGET_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort)

  Get Target Link Speed.
- typedef VOID(∗ PCIE_SET_TARGET_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort, IN UINT8 TargetLinkSpeed)

  Set Target Link Speed.
- typedef EFI_STATUS(∗ PCIE_RESET_ENDPOINT_PERST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CA↩LLS ∗This, IN PCIE_PORT_INFO ∗PciePort, IN PCIE_SWEQ_INPUT_PARAMETERS ∗InputParameters)

  Resets the endpoint connected to the given root port by directly pulsing the PERST# signal.
- typedef EFI_STATUS(∗ PCIE_SET_PERST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN P↩CIE_PORT_INFO ∗PciePort, IN PCIE_SWEQ_INPUT_PARAMETERS ∗InputParameters, IN BOOLEAN AssertPerst)

  This function asserts/deasserts a GPIO that controls PERST#.
- typedef EFI_STATUS(∗ PCIE_RECOVER_LINK_WIDTH) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort, IN UINT8 OriginalLinkWidth)

Recovers a link width downgrade back to the original width.

- typedef EFI_STATUS(∗ PCIE_SET_PCH_GPIO) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN GPIO_PAD GpioPad, IN UINT8 Level)

  This function sets a GPIO to a particular level.
- typedef EFI_STATUS(∗ PCIE_ENSURE_LINK_IS_HEALTHY) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_SWEQ_INPUT_PARAMETERS ∗InputParameters, IN PCIE_PORT_INFO ∗PciePort, IN UINT8 OriginalLinkSpeed, IN UINT8 OriginalLinkWidth, OUT BOOLEAN ∗DeferredPlatformResetRequired)

  Check the status of the given PCIe link, detect and correct and downgrades.
- typedef UINT32(∗ PCIE_OPEN_MONITOR) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This)

  PCIe Error Counting Functions.
- typedef VOID(∗ PCIE_CLOSE_MONITOR) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN UINT32 MonitorPort)

  Close port for monitor.
- typedef UINT32(∗ PCIE_GET_ERROR_COUNT) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN UINT32 MonitorPort, IN PCIE_PORT_INFO ∗PciePort)

  Get Current Error Count.
- typedef VOID(∗ PCIE_CLEAR_ERROR_COUNT) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN UINT32 MonitorPort)

  Clear Current Error Count for all Root Ports.
- typedef EFI_STATUS(∗ PCIE_POLLING_COMPLIANCE_MODE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength, IN BOOLEAN Enable)

  Enable or Disable Polling Compliance Mode
- typedef VOID(∗ PCIE_PROGRAM_PORT_PHASE3_TXEQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort, IN UINT8 ∗Presets)

  Program TxEQs on the endpoint attached to the given root port.
- typedef VOID(∗ PCIE_PROGRAM_UNIFORM_PORT_PHASE3_TXEQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePort, IN UINT8 Preset)

  Program the same TxEQ to all lanes on the endpoint attached to the given root port.
- typedef EFI_STATUS(∗ PCIE_RUN_MARGIN_TEST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength, IN PCIE_SWEQ_INPUT_PARAMETERS ∗InputParameters, IN UINT32 MonitorPort, IN MARGIN_TEST_TYPE MarginTest, OUT PCIE_SWEQ_PORT_OUTPUT ∗MarginData, OUT BOOLEAN ∗DeferredPlatformResetRequired)

  Runs a Margin Test on the specified root ports.

Functions

- VOID PcieGen3SoftwareEqualization (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗PcieAccess, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength, IN PCIE_SWEQ_INPUT_PARAMETERS ∗InputParameters, OUT PCIE_SWEQ_OUTPUT ∗OutputData)

  PCIe Initialization Library Generic High Level Function Calls.
- VOID WaitForDataLinkLayerLinkActiveOnAllPorts (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗PcieAccess, IN PCIE_PORT_INFO ∗PciePorts, IN UINT8 PciePortsLength, IN BOOLEAN ForceCheck, IN OUT UINT32 ∗FailMask)

  Waits for the Data Link Layer on all given root ports to reach the DL_Active state.
- VOID WaitForDataLinkLayerLinkActive (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗PcieAccess, IN PCIE_PORT_INFO ∗PciePort)

  This function prints the time required for DL_Active to be set.
- VOID GetCoefficientsFromPreset (IN UINT8 Preset, IN UINT8 FullSwing, OUT UINT8 ∗PreCursor, OUT UINT8 ∗Cursor, OUT UINT8 ∗PostCursor)

  Computes the Pre-Cursor, Cursor, and Post-Cursor from a preset.

- BOOLEAN LinkIsDowngraded (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗PcieAccess, IN PCIE_P←ORT_INFO ∗PciePort, IN UINT8 OriginalLinkSpeed, IN UINT8 OriginalLinkWidth)

  Checks for link speed and width downgrades.
- UINT32 PcieLibFindCapId (IN UINT8 Segment, IN UINT8 Bus, IN UINT8 Device, IN UINT8 Function, IN UINT8 CapId)

  Find the Offset to a given Capabilities ID CAPID list:
- EFI_STATUS GetGenericPcieLowLevelFunctionCalls (OUT PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗PcieLowLevelFunctionCalls)

  This function gets the table of generic low level function calls for the PCIe interface.

14.23.1 Detailed Description

PCIe Initialization Library header file.

Copyright

Specification

14.23.2 Typedef Documentation

14.23.2.1 PCIE_CLEAR_ERROR_COUNT

```
typedef VOID( ∗ PCIE_CLEAR_ERROR_COUNT) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS ∗This, IN UINT32
MonitorPort)
```

Clear Current Error Count for all Root Ports.

Parameters

in	*This*	- Low level function table
in	*MonitorPort*	- Monitor Port

Definition at line 705 of file PcieInitLib.h.

14.23.2.2 PCIE_CLOSE_MONITOR

```
typedef VOID( * PCIE_CLOSE_MONITOR) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN UINT32
MonitorPort)
```

Close port for monitor.

Parameters

in	*This*	- Low level function table
in	*MonitorPort*	- Monitor Port

Definition at line 677 of file PcieInitLib.h.

14.23.2.3 PCIE_DATA_LINK_LAYER_LINK_ACTIVE

```
typedef BOOLEAN( * PCIE_DATA_LINK_LAYER_LINK_ACTIVE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS
*This, IN PCIE_PORT_INFO *PciePort)
```

Checks if the Data Link Layer is in DL_Active state on the given root port.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- Root Port to check for DL_Active

Return values

TRUE	- Data Link Layer is in DL_Active state
FALSE	- Data Link Layer is NOT in DL_Active state

Definition at line 327 of file PcieInitLib.h.

14.23.2.4 PCIE_DETECT_ENDPOINT_PRESENCE

```
typedef VOID( * PCIE_DETECT_ENDPOINT_PRESENCE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_INFO *PciePorts, IN UINT8 PciePortsLength)
```

PCIe Initialization Library Generic Low Level Function Calls All of these functions can be implemented using only PCIe specification level details.

However, it is possible to override the default implementation provided by this library with a Silicon Specific one if needed This function detects if an endpoint is attached to each given root port and if so, reads data from the endpoint and fills in the remaining fields of the PCIE_PORT_INFO structure that could not be filled before initial link training

Parameters

in	*This*	- Low level function table
out	*PciePorts*	- Array of PCIe Root Ports
out	*PciePortsLength*	- Length of the PciePorts array

Definition at line 295 of file PcieInitLib.h.

14.23.2.5 PCIE_ENSURE_LINK_IS_HEALTHY

```
typedef EFI_STATUS( * PCIE_ENSURE_LINK_IS_HEALTHY) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This,
IN PCIE_SWEQ_INPUT_PARAMETERS *InputParameters, IN PCIE_PORT_INFO *PciePort, IN UINT8 Original←
LinkSpeed, IN UINT8 OriginalLinkWidth, OUT BOOLEAN *DeferredPlatformResetRequired)
```

Check the status of the given PCIe link, detect and correct and downgrades.

Parameters

in	*This*	- Low level function table
in	*InputParameters*	- SW EQ Input Parameters
in	*PciePort*	- PCIe Root Port
in	*OriginalLinkSpeed*	- Expected speed of the PCIe link
in	*OriginalLinkWidth*	- Expected width of the PCIe link
out	*DeferredPlatformResetRequired*	- A platform reset is needed after saving Eq data to NVRAM

Return values

EFI_SUCCESS	- Link is running at the correct speed/width
EFI_UNSUPPORTED	- Unable to correct failure due to lack of GPIO PERST# support
EFI_INVALID_PARAMETER	- Unable to correct failure because the GPIO pin number is invalid
EFI_DEVICE_ERROR	- Unable to correct link downgrade
EFI_TIMEOUT	- Link did not successfully retrain

Definition at line 643 of file PcieInitLib.h.

14.23.2.6 PCIE_EXISTS

```
typedef BOOLEAN( * PCIE_EXISTS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This)
```

PCIe Initialization Library Silicon Specific Low Level Function Calls Enables Abstraction of Silicon details keeping this library generic.

This function determines if the silicon implements the PCIe bus interface that this instance of PCIE_SI_LOW_LE↩ VEL_FUNCTION_CALLS is intended for.

Return values

TRUE	- Silicon supports the bus interface
FALSE	- otherwise

Definition at line 415 of file PcieInitLib.h.

14.23.2.7 PCIE_GET_CURRENT_LINK_SPEED

```
typedef UINT8( * PCIE_GET_CURRENT_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_INFO *PciePort)
```

Get Current Link Speed.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Definition at line 396 of file PcieInitLib.h.

14.23.2.8 PCIE_GET_ERROR_COUNT

```
typedef UINT32( * PCIE_GET_ERROR_COUNT) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN UINT32
MonitorPort, IN PCIE_PORT_INFO *PciePort)
```

Get Current Error Count.

Parameters

in	*This*	- Low level function table
in	*MonitorPort*	- Monitor Port
in	*PciePort*	- PCIe Root Port

Definition at line 691 of file PcieInitLib.h.

14.23.2.9 PCIE_GET_NEGOTIATED_WIDTH

```
typedef UINT8( * PCIE_GET_NEGOTIATED_WIDTH) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PC↩
IE_PORT_INFO *PciePort)
```

Get Negotiated Link Width.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Definition at line 383 of file PcieInitLib.h.

14.23.2.10 PCIE_GET_PCIE_CAP_OFFSET

```
typedef UINT8( * PCIE_GET_PCIE_CAP_OFFSET) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCI↩
E_PORT_INFO *PciePort)
```

Gets the PCIe Capability Structure Pointer.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Return values

Offset	to the PCIe Capability Structure

Definition at line 311 of file PcieInitLib.h.

14.23.2.11 PCIE_GET_ROOT_PORTS

```
typedef VOID( * PCIE_GET_ROOT_PORTS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, OUT PCIE_POR↩
T_INFO *PciePorts, OUT UINT8 *PciePortsLength)
```

This function determines the topology of the PCIe bus interface that is being initialized using silicon defined mechanisms.

The PciePorts pointer must point to a pre-allocated array which is capable of containing the maximum number of root ports that this function will return. Generally this is done by a component specific entrypoint that can allocate the array on the stack using a fixed size appropriate for the HW. If this needs to be called from generic code, the generic code must allocate a buffer that can contain 256 entries (which should be avoided.)

Parameters

in	*This*	- Low level function table
out	*PciePorts*	- Array of Detected PCIe Root Ports
out	*PciePortsLength*	- Length of the PciePorts array

Definition at line 435 of file PcieInitLib.h.

14.23.2.12 PCIE_GET_SLOT_PRESENCE_DETECT

```
typedef BOOLEAN( * PCIE_GET_SLOT_PRESENCE_DETECT) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This,
IN PCIE_PORT_INFO *PciePort)
```

Returns the current value of the PCIe Slot Status Presence Detect bit.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Return values

Slot	Presence Detect bit state

Definition at line 342 of file PcieInitLib.h.

14.23.2.13 PCIE_GET_TARGET_LINK_SPEED

```
typedef UINT8( * PCIE_GET_TARGET_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN P↩
CIE_PORT_INFO *PciePort)
```

Get Target Link Speed.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Definition at line 521 of file PcieInitLib.h.

14.23.2.14 PCIE_OPEN_MONITOR

```
typedef UINT32( * PCIE_OPEN_MONITOR) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This)
```

PCIe Error Counting Functions.

Open port for monitor

Parameters

in	*This*	- Low level function table

Return values

Monitor	Port

Definition at line 665 of file PcieInitLib.h.

14.23.2.15 PCIE_POLLING_COMPLIANCE_MODE

```
typedef EFI_STATUS( * PCIE_POLLING_COMPLIANCE_MODE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This,
IN PCIE_PORT_INFO *PciePorts, IN UINT8 PciePortsLength, IN BOOLEAN Enable)
```

Enable or Disable Polling Compliance Mode

Parameters

in	*This*	- Low level function table
in	*PciePorts*	- PCIe Root Ports
in	*PciePortsLength*	- Length of PciePorts array
in	*Enable*	- TRUE to enable, FALSE to disable

Definition at line 720 of file PcieInitLib.h.

14.23.2.16 PCIE_PROGRAM_PORT_PHASE3_TXEQ

```
typedef VOID( * PCIE_PROGRAM_PORT_PHASE3_TXEQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_INFO *PciePort, IN UINT8 *Presets)
```

Program TxEQs on the endpoint attached to the given root port.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*Presets*	- Array of presets to program per lane must be of sufficient length to program all lanes

Definition at line 737 of file PcieInitLib.h.

14.23.2.17 PCIE_PROGRAM_STATIC_GEN3_EQ

```
typedef VOID( * PCIE_PROGRAM_STATIC_GEN3_EQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_EQS *PciePortEqs, IN UINT8 PciePortEqsLength)
```

Programs static equalization settings for the given list of PCIe root ports.

The PCIE_PORT_EQs structure is laid out such that the Root Port preset for PHYSICAL lane number PciePort←Eqs->PciePort->MaxPortLaneList[0] is PciePortEqs->RootPortPresets[0]. Note that physical lane numbers may not start at or include zero. Package pin 0 may not be mapped to a given Root Port

Parameters

in	*This*	- Low level function table
in	*PciePortEqs*	- Array of Root Ports + Eqs to program
in	*PciePortEqsLength*	- Number of Root Ports to program

Definition at line 454 of file PcieInitLib.h.

14.23.2.18 PCIE_PROGRAM_UNIFORM_PORT_PHASE3_TXEQ

```
typedef VOID( * PCIE_PROGRAM_UNIFORM_PORT_PHASE3_TXEQ) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS
*This, IN PCIE_PORT_INFO *PciePort, IN UINT8 Preset)
```

Program the same TxEQ to all lanes on the endpoint attached to the given root port.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*Preset*	- Preset to program

Definition at line 752 of file PcieInitLib.h.

14.23.2.19 PCIE_RECOVER_LINK_WIDTH

```
typedef EFI_STATUS( * PCIE_RECOVER_LINK_WIDTH) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_INFO *PciePort, IN UINT8 OriginalLinkWidth)
```

Recovers a link width downgrade back to the original width.

Generally this doesn't need to be called directly since EnsureLinkIsHealthy() checks link width in addition to other link health checks.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*OriginalLinkWidth*	- Original Link Width

Return values

EFI_SUCCESS	- Link is running at the correct width
EFI_DEVICE_ERROR	- Unable to correct link width downgrade
EFI_TIMEOUT	- Link did not successfully retrain

Definition at line 600 of file PcieInitLib.h.

14.23.2.20 PCIE_REPORT_LINK_STATUS

```
typedef VOID( * PCIE_REPORT_LINK_STATUS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCIE_↩
PORT_INFO *PciePort)
```

This function reports a PCIe controller's link status

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Definition at line 488 of file PcieInitLib.h.

14.23.2.21 PCIE_RESET_ENDPOINT_PERST

```
typedef EFI_STATUS( * PCIE_RESET_ENDPOINT_PERST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN
PCIE_PORT_INFO *PciePort, IN PCIE_SWEQ_INPUT_PARAMETERS *InputParameters)
```

Resets the endpoint connected to the given root port by directly pulsing the PERST# signal.

The minimum assertion time, T_PERST (100 usec), is defined in the PCIe CEM Specification.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*InputParameters*	- SW EQ Input Parameters

Return values

EFI_SUCCESS	- GPIO set successfully
EFI_UNSUPPORTED	- GPIO is not supported
EFI_INVALID_PARAMETER	- GPIO pin number is invalid
EFI_TIMEOUT	- Link did not train after pulsing PERST#

Definition at line 557 of file PcieInitLib.h.

14.23.2.22 PCIE_RETRAIN_LINK

```
typedef VOID( * PCIE_RETRAIN_LINK) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCIE_PORT_I←
NFO *PciePort)
```

Retrain the PCIe link.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Definition at line 370 of file PcieInitLib.h.

14.23.2.23 PCIE_RUN_MARGIN_TEST

```
typedef EFI_STATUS( * PCIE_RUN_MARGIN_TEST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN P←
CIE_PORT_INFO *PciePorts, IN UINT8 PciePortsLength, IN PCIE_SWEQ_INPUT_PARAMETERS *Input←
Parameters, IN UINT32 MonitorPort, IN MARGIN_TEST_TYPE MarginTest, OUT PCIE_SWEQ_PORT_OUTPUT
*MarginData, OUT BOOLEAN *DeferredPlatformResetRequired)
```

Runs a Margin Test on the specified root ports.

The MarginData parameter must be an array with capacity of PciePortsLength elements or more.

Parameters

in	*This*	- Low level function table
in	*PciePorts*	- PCIe Root Ports to margin
in	*PciePortsLength*	- Length of the PciePorts array
in	*InputParameters*	- SW EQ Input Parameters
in	*MonitorPort*	- Monitor Port
in	*MarginTest*	- Type of Margin Test to Run
out	*MarginData*	- Margin Data, must be array of size >= PciePortsLength
out	*DeferredPlatformResetRequired*	- A platform reset is needed after saving Eq data to NVRAM

Return values

EFI_SUCCESS	- Margin Data Generated Successfully

Definition at line 775 of file PcieInitLib.h.

14.23.2.24 PCIE_SET_GEN3_PHASE2_BYPASS

```
typedef EFI_STATUS( * PCIE_SET_GEN3_PHASE2_BYPASS) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This,
IN PCIE_PORT_INFO *PciePorts, IN UINT8 PciePortsLength, IN BOOLEAN BypassPhase2)
```

Sets Gen3 Equalization Phase 2 Bypass for all given Root Ports.

Parameters

in	*This*	- Low level function table
in	*PciePorts*	- PCIe Root Ports to program Phase2 for
in	*PciePortsLength*	- Length of the PciePorts array
in	*BypassPhase2*	- TRUE to enable Phase2 bypass, FALSE otherwise

Return values

EFI_SUCCESS	- Phase 2 bypass was successful
EFI_UNSUPPORTED	- Hardware does not support the given Phase2 bypass request

Definition at line 473 of file PcieInitLib.h.

14.23.2.25 PCIE_SET_LINK_DISABLE

```
typedef VOID( * PCIE_SET_LINK_DISABLE) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCIE_PO←-
RT_INFO *PciePort, IN BOOLEAN LinkDisable)
```

Set the Link Disable bit in the PCIe Link Control Register.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*LinkDisable*	- New value for link disable bit

Definition at line 356 of file PcieInitLib.h.

14.23.2.26 PCIE_SET_PCH_GPIO

```
typedef EFI_STATUS( * PCIE_SET_PCH_GPIO) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN GPIO_PAD
GpioPad, IN UINT8 Level)
```

This function sets a GPIO to a particular level.

Parameters

in	*This*	- Low level function table
in	*GpioPad*	- PCH GPIO Pad
in	*Level*	- 0 = Low, 1 = High

Return values

EFI_SUCCESS	- GPIO set successfully
EFI_UNSUPPORTED	- GPIO is not supported
EFI_INVALID_PARAMETER	- GPIO pin number is invalid

Definition at line 619 of file PcieInitLib.h.

14.23.2.27 PCIE_SET_PERST

```
typedef EFI_STATUS( * PCIE_SET_PERST) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCIE_POR↩
T_INFO *PciePort, IN PCIE_SWEQ_INPUT_PARAMETERS *InputParameters, IN BOOLEAN AssertPerst)
```

This function asserts/deasserts a GPIO that controls PERST#.

The minimum assertion time, T_PERST (100 usec), is defined in the PCIe CEM Specification.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*InputParameters*	- SW EQ Input Parameters
in	*AssertPerst*	- TRUE to assert PERST#, FALSE to deassert

Return values

EFI_SUCCESS	- GPIO set successfully
EFI_UNSUPPORTED	- GPIO is not supported
EFI_INVALID_PARAMETER	- GPIO pin number is invalid

Definition at line 578 of file PcieInitLib.h.

14.23.2.28 PCIE_SET_TARGET_LINK_SPEED

```
typedef VOID( * PCIE_SET_TARGET_LINK_SPEED) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PC↩
IE_PORT_INFO *PciePort, IN UINT8 TargetLinkSpeed)
```

Set Target Link Speed.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*TargetLinkSpeed*	- Target Link Speed

Definition at line 535 of file PcieInitLib.h.

14.23.2.29 PCIE_WAIT_FOR_L0

```
typedef EFI_STATUS( * PCIE_WAIT_FOR_L0) (IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS *This, IN PCIE_P↩
ORT_INFO *PciePort)
```

PCIe Link Recovery Functions.

Wait until link is up.

Parameters

in	*This*	- Low level function table
in	*PciePort*	- PCIe Root Port

Return values

EFI_SUCCESS	- Completed successfully before timeout
EFI_TIMEOUT	- Timed out

Definition at line 508 of file PcieInitLib.h.

14.23.3 Function Documentation

14.23.3.1 GetCoefficientsFromPreset()

```
VOID GetCoefficientsFromPreset (
             IN UINT8 Preset,
             IN UINT8 FullSwing,
             OUT UINT8 * PreCursor,
             OUT UINT8 * Cursor,
             OUT UINT8 * PostCursor )
```

Computes the Pre-Cursor, Cursor, and Post-Cursor from a preset.

Parameters

in	*Preset*	- Preset to compute coefficients for
in	*FullSwing*	- The full swing of the transmitter
out	*PreCursor*	- Computed Pre-Cursor
out	*Cursor*	- Computed Cursor
out	*PostCursor*	- Computed Post-Cursor

14.23.3.2 GetGenericPcieLowLevelFunctionCalls()

```
EFI_STATUS GetGenericPcieLowLevelFunctionCalls (
            OUT PCIE_SI_LOW_LEVEL_FUNCTION_CALLS * PcieLowLevelFunctionCalls )
```

This function gets the table of generic low level function calls for the PCIe interface.

These function calls use PCIe spec defined mechanisms and can be overrided by a silicon specific implementation if needed.

Parameters

out	*PcieLowLevel*	- Table of function calls for PCIe

Return values

EFI_SUCCESS	- Table of function calls returned successfully

14.23.3.3 LinkIsDowngraded()

```
BOOLEAN LinkIsDowngraded (
            IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS * PcieAccess,
            IN PCIE_PORT_INFO * PciePort,
            IN UINT8 OriginalLinkSpeed,
            IN UINT8 OriginalLinkWidth )
```

Checks for link speed and width downgrades.

Parameters

in	*PcieAccess*	- Low level function table
in	*PciePort*	- PCIe Root Port
in	*OriginalLinkSpeed*	- Original Speed of the Link
in	*OriginalLinkWidth*	- Original Width of the Link

14.23.3.4 PcieGen3SoftwareEqualization()

```
VOID PcieGen3SoftwareEqualization (
             IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS * PcieAccess,
             IN PCIE_PORT_INFO * PciePorts,
             IN UINT8 PciePortsLength,
             IN PCIE_SWEQ_INPUT_PARAMETERS * InputParameters,
             OUT PCIE_SWEQ_OUTPUT * OutputData )
```

PCIe Initialization Library Generic High Level Function Calls.

The PCIe Software Equalization algorithm. Provides an adaptive EQ Phase 3 implementation in software.

Parameters

in	*PcieAccess*	- Low level function table
in	*PciePorts*	- PCIe Root Ports to wait for
in	*PciePortsLength*	- Length of the PciePorts array
in	*InputParameters*	- Configuration options for SW EQ
out	*OutputData*	- The data that the algorithm generated

14.23.3.5 PcieLibFindCapId()

```
UINT32 PcieLibFindCapId (
             IN UINT8 Segment,
             IN UINT8 Bus,
             IN UINT8 Device,
             IN UINT8 Function,
             IN UINT8 CapId )
```

Find the Offset to a given Capabilities ID CAPID list:

- 0x01 = PCI Power Management Interface
- 0x04 = Slot Identification
- 0x05 = MSI Capability
- 0x10 = PCI Express Capability

Parameters

in	*Segment*	- Pci Segment Number
in	*Bus*	- PCI Bus Number
in	*Device*	- PCI Device Number
in	*Function*	- PCI Function Number
in	*CapId*	- CAPID to search for

Return values

0	- CAPID not found
Other	- CAPID found, Offset of desired CAPID

14.23.3.6 WaitForDataLinkLayerLinkActive()

```
VOID WaitForDataLinkLayerLinkActive (
            IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS * PcieAccess,
            IN PCIE_PORT_INFO * PciePort )
```

This function prints the time required for DL_Active to be set.

Quits after 100 msec.

Parameters

`in`	*This*	- Low level function table
`in`	*PciePort*	- PCIe Root Port

14.23.3.7 WaitForDataLinkLayerLinkActiveOnAllPorts()

```
VOID WaitForDataLinkLayerLinkActiveOnAllPorts (
            IN PCIE_SI_LOW_LEVEL_FUNCTION_CALLS * PcieAccess,
            IN PCIE_PORT_INFO * PciePorts,
            IN UINT8 PciePortsLength,
            IN BOOLEAN ForceCheck,
            IN OUT UINT32 * FailMask )
```

Waits for the Data Link Layer on all given root ports to reach the DL_Active state.

The user passes a fail mask that indicates which root ports to check. The function will update the fail mask to indicate which root ports successfully trained.

The fail mask is a bitmap based on PciePorts array indices. The array must be of length 8 or greater since the PciePorts array can have at most 256 entries.

Parameters

`in`	*PcieAccess*	- Low level function table
`in`	*PciePorts*	- PCIe Root Ports to wait for
`in`	*PciePortsLength*	- Length of the PciePorts array
`in`	*ForceCheck*	- TRUE to ignore current FailMask and check all root ports
`in,out`	*FailMask*	- Bitmap of root ports to check. Returns bitmap indicating which root ports failed to reach DL_Active. Array must be of length 8 or greater!

Parameters

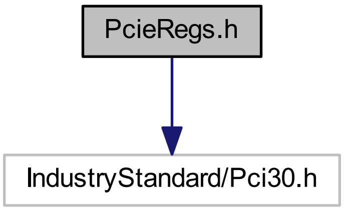
FailMask	[PCIE_ROOT_PORT_BITMAP_LENGTH]

14.24 PcieRegs.h File Reference

Register names for PCIE standard register.

```
#include <IndustryStandard/Pci30.h>
```

Include dependency graph for PcieRegs.h:



Macros

- #define R_PCI_BRIDGE_BNUM 0x18

  Bus Number Register.
- #define B_PCI_BRIDGE_BNUM_SBBN 0x00FF0000

  Subordinate Bus Number.
- #define B_PCI_BRIDGE_BNUM_SCBN 0x0000FF00

  Secondary Bus Number.
- #define B_PCI_BRIDGE_BNUM_PBN 0x000000FF

  Primary Bus Number.
- #define R_PCI_BRIDGE_IOBL 0x1C

  I/O Base and Limit Register.
- #define R_PCI_BRIDGE_MBL 0x20

  Memory Base and Limit Register.
- #define B_PCI_BRIDGE_MBL_ML 0xFFF00000

  Memory Limit.
- #define B_PCI_BRIDGE_MBL_MB 0x0000FFF0

  Memory Base.
- #define R_PCI_BRIDGE_PMBL 0x24

  Prefetchable Memory Base and Limit Register.
- #define B_PCI_BRIDGE_PMBL_PML 0xFFF00000

  Prefetchable Memory Limit.
- #define B_PCI_BRIDGE_PMBL_I64L 0x000F0000

  64-bit Indicator

- #define B_PCI_BRIDGE_PMBL_PMB 0x0000FFF0

  Prefetchable Memory Base.
- #define B_PCI_BRIDGE_PMBL_I64B 0x0000000F

  64-bit Indicator
- #define R_PCI_BRIDGE_PMBU32 0x28

  Prefetchable Memory Base Upper 32-Bit Register.
- #define R_PCI_BRIDGE_PMLU32 0x2C

  Prefetchable Memory Limit Upper 32-Bit Register.
- #define R_PCIE_CAP_ID_OFFSET 0x00

  Capability ID.
- #define R_PCIE_CAP_NEXT_PRT_OFFSET 0x01

  Next Capability Capability ID Pointer.
- #define R_PCIE_XCAP_OFFSET 0x02

  PCI Express Capabilities Register (Offset 02h)
- #define B_PCIE_XCAP_SI BIT8

  Slot Implemented.
- #define B_PCIE_XCAP_DT (BIT7 | BIT6 | BIT5 | BIT4)

  Device/Port Type.
- #define R_PCIE_DCAP_OFFSET 0x04

  Device Capabilities Register (Offset 04h)
- #define B_PCIE_DCAP_RBER BIT15

  Role-Based Error Reporting.
- #define B_PCIE_DCAP_E1AL (BIT11 | BIT10 | BIT9)

  Endpoint L1 Acceptable Latency.
- #define B_PCIE_DCAP_E0AL (BIT8 | BIT7 | BIT6)

  Endpoint L0s Acceptable Latency.
- #define B_PCIE_DCAP_MPS (BIT2 | BIT1 | BIT0)

  Max_Payload_Size Supported.
- #define R_PCIE_DCTL_OFFSET 0x08

  Device Control Register (Offset 08h)
- #define B_PCIE_DCTL_MPS (BIT7 | BIT6 | BIT5)

  Max_Payload_Size.
- #define B_PCIE_DCTL_URE BIT3

  Unsupported Request Reporting Enable.
- #define B_PCIE_DCTL_FEE BIT2

  Fatal Error Reporting Enable.
- #define B_PCIE_DCTL_NFE BIT1

  Non-Fatal Error Reporting Enable.
- #define B_PCIE_DCTL_CEE BIT0

  Correctable Error Reporting Enable.
- #define R_PCIE_DSTS_OFFSET 0x0A

  Device Status Register (Offset 0Ah)
- #define B_PCIE_DSTS_TDP BIT5

  Transactions Pending.
- #define B_PCIE_DSTS_APD BIT4

  AUX Power Detected.
- #define B_PCIE_DSTS_URD BIT3

  Unsupported Request Detected.
- #define B_PCIE_DSTS_FED BIT2

  Fatal Error Detected.
- #define B_PCIE_DSTS_NFED BIT1

Non-Fatal Error Detected.

- #define B_PCIE_DSTS_CED BIT0

  Correctable Error Detected.

- #define R_PCIE_LCAP_OFFSET 0x0C

  Link Capabilities Register (Offset 0Ch)

- #define B_PCIE_LCAP_ASPMOC BIT22

  ASPM Optionality Compliance.

- #define B_PCIE_LCAP_CPM BIT18

  Clock Power Management.

- #define B_PCIE_LCAP_EL1 (BIT17 | BIT16 | BIT15)

  L1 Exit Latency.

- #define B_PCIE_LCAP_EL0 (BIT14 | BIT13 | BIT12)

  L0s Exit Latency.

- #define B_PCIE_LCAP_APMS (BIT11 | BIT10)

  Active State Power Management (ASPM) Support.

- #define B_PCIE_LCAP_MLW 0x000003F0

  Maximum Link Width.

- #define B_PCIE_LCAP_MLS (BIT3 | BIT2 | BIT1 | BIT0)

  Max Link Speed.

- #define R_PCIE_LCTL_OFFSET 0x10

  Link Control Register (Offset 10h)

- #define B_PCIE_LCTL_ECPM BIT8

  Enable Clock Power Management.

- #define B_PCIE_LCTL_ES BIT7

  Extended Synch.

- #define B_PCIE_LCTL_CCC BIT6

  Common Clock Configuration.

- #define B_PCIE_LCTL_RL BIT5

  Retrain Link.

- #define B_PCIE_LCTL_LD BIT4

  Link Disable.

- #define B_PCIE_LCTL_ASPM (BIT1 | BIT0)

  Active State Power Management (ASPM) Control.

- #define R_PCIE_LSTS_OFFSET 0x12

  Link Status Register (Offset 12h)

- #define B_PCIE_LSTS_LA BIT13

  Data Link Layer Link Active.

- #define B_PCIE_LSTS_SCC BIT12

  Slot Clock Configuration.

- #define B_PCIE_LSTS_LT BIT11

  Link Training.

- #define B_PCIE_LSTS_NLW 0x03F0

  Negotiated Link Width.

- #define B_PCIE_LSTS_CLS 0x000F

  Current Link Speed.

- #define R_PCIE_SLCAP_OFFSET 0x14

  Slot Capabilities Register (Offset 14h)

- #define B_PCIE_SLCAP_PSN 0xFFF80000

  Physical Slot Number.

- #define N_PCIE_SLCAP_PSN 19

  Physical Slot Number.

- #define B_PCIE_SLCAP_SLS 0x00018000

  Slot Power Limit Scale.
- #define N_PCIE_SLCAP_SLS 15

  Slot Power Limit Scale.
- #define B_PCIE_SLCAP_SLV 0x00007F80

  Slot Power Limit Value.
- #define N_PCIE_SLCAP_SLV 7

  Slot Power Limit Value.
- #define B_PCIE_SLCAP_HPC BIT6

  Hot-Plug Capable.
- #define B_PCIE_SLCAP_HPS BIT5

  Hot-Plug Surprise.
- #define R_PCIE_SLCTL_OFFSET 0x18

  Slot Control Register (Offset 18h)
- #define B_PCIE_SLCTL_HPE BIT5

  Hot Plug Interrupt Enable.
- #define B_PCIE_SLCTL_PDE BIT3

  Presence Detect Changed Enable.
- #define R_PCIE_SLSTS_OFFSET 0x1A

  Slot Status Register (Offset 1Ah)
- #define B_PCIE_SLSTS_PDS BIT6

  Presence Detect State.
- #define B_PCIE_SLSTS_PDC BIT3

  Presence Detect Changed.
- #define R_PCIE_RCTL_OFFSET 0x1C

  Root Control Register (Offset 1Ch)
- #define B_PCIE_RCTL_PIE BIT3

  PME Interrupt Enable.
- #define B_PCIE_RCTL_SFE BIT2

  System Error on Fatal Error Enable.
- #define B_PCIE_RCTL_SNE BIT1

  System Error on Non-Fatal Error Enable.
- #define B_PCIE_RCTL_SCE BIT0

  System Error on Correctable Error Enable.
- #define R_PCIE_RSTS_OFFSET 0x20

  Root Status Register (Offset 20h)
- #define R_PCIE_DCAP2_OFFSET 0x24

  Device Capabilities 2 Register (Offset 24h)
- #define B_PCIE_DCAP2_OBFFS (BIT19 | BIT18)

  OBFF Supported.
- #define B_PCIE_DCAP2_LTRMS BIT11

  LTR Mechanism Supported.
- #define R_PCIE_DCTL2_OFFSET 0x28

  Device Control 2 Register (Offset 28h)
- #define B_PCIE_DCTL2_OBFFEN (BIT14 | BIT13)

  OBFF Enable.
- #define V_PCIE_DCTL2_OBFFEN_DIS 0

  Disabled.
- #define V_PCIE_DCTL2_OBFFEN_WAKE 3

  Enabled using WAKE# signaling.
- #define B_PCIE_DCTL2_LTREN BIT10

LTR Mechanism Enable.

- #define B_PCIE_DCTL2_CTD BIT4

  Completion Timeout Disable.
- #define B_PCIE_DCTL2_CTV (BIT3 | BIT2 | BIT1 | BIT0)

  Completion Timeout Value.
- #define R_PCIE_LCTL2_OFFSET 0x30

  Link Control 2 Register (Offset 30h)
- #define B_PCIE_LCTL2_SD BIT6

  Selectable de-emphasis (0 = -6dB, 1 = -3.5dB)
- #define B_PCIE_LCTL2_TLS (BIT3 | BIT2 | BIT1 | BIT0)

  Target Link Speed.
- #define R_PCIE_LSTS2_OFFSET 0x32

  Link Status 2 Register (Offset 32h)
- #define B_PCIE_LSTS2_LER BIT5

  Link Equalization Request.
- #define B_PCIE_LSTS2_EQP3S BIT4

  Equalization Phase 3 Successful.
- #define B_PCIE_LSTS2_EQP2S BIT3

  Equalization Phase 2 Successful.
- #define B_PCIE_LSTS2_EQP1S BIT2

  Equalization Phase 1 Successful.
- #define B_PCIE_LSTS2_EC BIT1

  Equalization Complete.
- #define B_PCIE_LSTS2_CDL BIT0

  Current De-emphasis Level.
- #define R_PCIE_PMC_OFFSET 0x02

  Power Management Capabilities Register.
- #define B_PCIE_PMC_PMES (BIT15 | BIT14 | BIT13 | BIT12 | BIT11)

  PME Support.
- #define B_PCIE_PMC_PMEC BIT3

  PME Clock.
- #define R_PCIE_PMCS_OFFST 0x04

  Power Management Status/Control Register.
- #define B_PCIE_PMCS_BPCE BIT23

  Bus Power/Clock Control Enable.
- #define B_PCIE_PMCS_B23S BIT22

  B2/B3 Support.
- #define B_PCIE_PMCS_PMES BIT15

  PME_Status.
- #define B_PCIE_PMCS_PMEE BIT8

  PME Enable.
- #define B_PCIE_PMCS_NSR BIT3

  No Soft Reset.
- #define B_PCIE_PMCS_PS (BIT1 | BIT0)

  Power State.
- #define B_PCIE_EXCAP_NCO 0xFFF00000

  Next Capability Offset.
- #define B_PCIE_EXCAP_CV 0x000F0000

  Capability Version.
- #define B_PCIE_EXCAP_CID 0x0000FFFF

  Capability ID.

- #define V_PCIE_EX_AEC_CID 0x0001

  Capability ID.
- #define R_PCIE_EX_UEM_OFFSET 0x08

  Uncorrectable Error Mask Register.
- #define B_PCIE_EX_UEM_CT BIT14

  Completion Timeout Mask.
- #define B_PCIE_EX_UEM_UC BIT16

  Unexpected Completion.
- #define V_PCIE_EX_ACS_CID 0x000D

  Capability ID.
- #define R_PCIE_EX_ACSCAPR_OFFSET 0x04

  ACS Capability Register.
- #define V_PCIE_EX_SPE_CID 0x0019

  Capability ID.
- #define R_PCIE_EX_LCTL3_OFFSET 0x04

  Link Control 3 Register.
- #define B_PCIE_EX_LCTL3_PE BIT0

  Perform Equalization.
- #define R_PCIE_EX_LES_OFFSET 0x08

  Lane Error Status.
- #define R_PCIE_EX_L01EC_OFFSET 0x0C

  Lane 0 and Lan 1 Equalization Control Register (Offset 0Ch)
- #define B_PCIE_EX_L01EC_UPL1TP 0x0F000000

  Upstream Port Lane 1 Transmitter Preset.
- #define B_PCIE_EX_L01EC_DPL1TP 0x000F0000

  Downstream Port Lane 1 Transmitter Preset.
- #define B_PCIE_EX_L01EC_UPL0TP 0x00000F00

  Upstream Port Transmitter Preset.
- #define B_PCIE_EX_L01EC_DPL0TP 0x0000000F

  Downstream Port Transmitter Preset.
- #define R_PCIE_EX_L23EC_OFFSET 0x10

  Lane 2 and Lane 3 Equalization Control Register (Offset 10h)
- #define B_PCIE_EX_L23EC_UPL3TP 0x0F000000

  Upstream Port Lane 3 Transmitter Preset.
- #define B_PCIE_EX_L23EC_DPL3TP 0x000F0000

  Downstream Port Lane 3 Transmitter Preset.
- #define B_PCIE_EX_L23EC_UPL2TP 0x00000F00

  Upstream Port Lane 2 Transmitter Preset.
- #define B_PCIE_EX_L23EC_DPL2TP 0x0000000F

  Downstream Port Lane 2 Transmitter Preset.
- #define V_PCIE_EX_DPC_CID 0x001D

  Capability ID.
- #define V_PCIE_EX_L1S_CID 0x001E

  Capability ID.
- #define R_PCIE_EX_L1SCAP_OFFSET 0x04

  L1 Sub-States Capabilities.
- #define B_PCIE_EX_L1SCAP_L1PSS BIT4

  L1 PM substates supported.
- #define B_PCIE_EX_L1SCAP_AL1SS BIT3

  ASPM L1.1 supported.
- #define B_PCIE_EX_L1SCAP_AL12S BIT2

ASPM L1.2 supported.

- #define B_PCIE_EX_L1SCAP_PPL11S BIT1

  PCI-PM L1.1 supported.
- #define B_PCIE_EX_L1SCAP_PPL12S BIT0

  PCI-PM L1.2 supported.
- #define R_PCIE_EX_L1SCTL1_OFFSET 0x08

  L1 Sub-States Control 1.
- #define B_PCIE_EX_L1SCTL1_L12LTRTLSV 0xE0000000

  L1.2 LTR Threshold Latency Scale Value.
- #define B_PCIE_EX_L1SCTL1_L12LTRTLV 0x03FF0000

  L1.2 LTR Threshold Latency Value.
- #define R_PCIE_EX_L1SCTL2_OFFSET 0x0C

  L1 Sub-States Control 2.
- #define V_PCIE_EX_PTM_CID 0x001F

  Capability ID.
- #define R_PCIE_EX_PTMCAP_OFFSET 0x04

  PTM Capabilities.
- #define B_PCIE_EX_PTMCAP_PTMRC BIT2

  PTM Root Capable.
- #define B_PCIE_EX_PTMCAP_PTMRSPC BIT1

  PTM Responder Capable.
- #define R_BASE_ADDRESS_OFFSET_0 0x0010

  Base Address Register 0.
- #define R_BASE_ADDRESS_OFFSET_1 0x0014

  Base Address Register 1.
- #define R_BASE_ADDRESS_OFFSET_2 0x0018

  Base Address Register 2.
- #define R_BASE_ADDRESS_OFFSET_3 0x001C

  Base Address Register 3.
- #define R_BASE_ADDRESS_OFFSET_4 0x0020

  Base Address Register 4.
- #define R_BASE_ADDRESS_OFFSET_5 0x0024

  Base Address Register 5.

14.24.1 Detailed Description

Register names for PCIE standard register.

Conventions:

- Prefixes: Definitions beginning with "R_" are registers Definitions beginning with "B_" are bits within registers Definitions beginning with "V_" are meaningful values within the bits Definitions beginning with "S_" are register sizes Definitions beginning with "N_" are the bit position

Copyright

Specification Reference:

14.25 PeiCpuAndPchTraceHubLib.h File Reference

Header file for CPU and PCH TraceHub Lib.

Functions

- UINT64 GetTraceHubPciBase (IN TRACE_HUB_DEVICE TraceHubDevice)

  Get Trace Hub PCI address.
- UINT32 GetTraceHubMtbBar (IN TRACE_HUB_DEVICE TraceHubDevice)

  Get Trace Hub MTB Bar.
- VOID ConfigureMscForTraceHub (IN TRACE_HUB_DEVICE TraceHubDevice, IN UINT32 Msc0Base, IN U↩ INT32 Msc0Size, IN UINT32 Msc1Base, IN UINT32 Msc1Size)

  Configure Trace Hub Msc operational region regarding to buffer base and size.
- VOID ConfigureMscForCpuAndPchTraceHub (IN UINT32 TraceHubMemBase)

  This function performs CPU and PCH Trace Hub Buffer initialization.
- BOOLEAN IsDebuggerInUse (IN TRACE_HUB_DEVICE TraceHubDevice)

  Check if debugger is in use.

14.25.1 Detailed Description

Header file for CPU and PCH TraceHub Lib.

Copyright

Specification Reference:

14.25.2 Function Documentation

14.25.2.1 ConfigureMscForCpuAndPchTraceHub()

```
VOID ConfigureMscForCpuAndPchTraceHub (
             IN UINT32 TraceHubMemBase )
```

This function performs CPU and PCH Trace Hub Buffer initialization.

Trace memopry buffers need to be allocated as reserved memory with UC attribute.

Parameters

in	*TraceHubMemBase*	Allocated Trace Hub memory base address

14.25.2.2 ConfigureMscForTraceHub()

```
VOID ConfigureMscForTraceHub (
             IN TRACE_HUB_DEVICE TraceHubDevice,
             IN UINT32 Msc0Base,
             IN UINT32 Msc0Size,
             IN UINT32 Msc1Base,
             IN UINT32 Msc1Size )
```

Configure Trace Hub Msc operational region regarding to buffer base and size.

Parameters

in	*TraceHubDevice*	Specify CPU or PCH trace hub device
in	*Msc0Base*	Base Address of MSC0BAR
in	*Msc0Size*	Size of MSC0Size
in	*Msc1Base*	Base Address of MSC1BAR
in	*Msc1Size*	Size of MSC1Size

14.25.2.3 GetTraceHubMtbBar()

```
UINT32 GetTraceHubMtbBar (
             IN TRACE_HUB_DEVICE TraceHubDevice )
```

Get Trace Hub MTB Bar.

Parameters

in	*TraceHubDevice*	Specify CPU or PCH trace hub device

Return values

UINT32	Trace Hub MTB bar

14.25.2.4 GetTraceHubPciBase()

```
UINT64 GetTraceHubPciBase (
             IN TRACE_HUB_DEVICE TraceHubDevice )
```

Get Trace Hub PCI address.

Parameters

in	*TraceHubDevice*	Specify CPU or PCH trace hub device

Return values

UINT64	Trace Hub Pci address

14.25.2.5 IsDebuggerInUse()

```
BOOLEAN IsDebuggerInUse (
             IN TRACE_HUB_DEVICE TraceHubDevice )
```

Check if debugger is in use.

Parameters

in	*TraceHubDevice*	Specify CPU or PCH trace hub device

Return values

TRUE	debugger is in use
FALSE	debugger is NOT in use

14.26 PeiPreMemSiDefaultPolicy.h File Reference

This file defines the function to initialize default silicon policy PPI.

Classes

- struct _PEI_PREMEM_SI_DEFAULT_POLICY_INIT_PPI

  This PPI provides function to install default silicon policy.

Typedefs

- typedef EFI_STATUS(∗ PEI_PREMEM_POLICY_INIT) (VOID)

  Initialize and install default silicon policy PPI.

14.26.1 Detailed Description

This file defines the function to initialize default silicon policy PPI.

Copyright

Specification Reference:

14.27 PeiSiDefaultPolicy.h File Reference

This file defines the function to initialize default silicon policy PPI.

Classes

- struct _PEI_SI_DEFAULT_POLICY_INIT_PPI

  This PPI provides function to install default silicon policy.

Typedefs

- typedef EFI_STATUS(∗ PEI_POLICY_INIT) (VOID)

  Initialize and install default silicon policy PPI.

14.27.1 Detailed Description

This file defines the function to initialize default silicon policy PPI.

Copyright

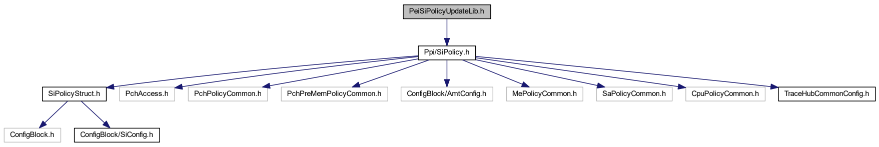
Specification Reference:

14.28 PeiSiPolicyUpdateLib.h File Reference

Header file for PEI SiPolicyUpdate Library.

```
#include <Ppi/SiPolicy.h>
```

Include dependency graph for PeiSiPolicyUpdateLib.h:



Functions

- EFI_STATUS UpdatePeiSiPolicy (IN OUT SI_POLICY_PPI ∗SiPolicy)

  This function performs Silicon PEI Policy initialization.
- EFI_STATUS UpdatePeiCpuPolicy (IN OUT SI_POLICY_PPI ∗SiPolicyPpi)

  This function performs CPU PEI Policy initialization in Post-memory.
- EFI_STATUS UpdatePeiSaPolicy (IN OUT SI_POLICY_PPI ∗SiPolicyPpi)

  This function performs SI PEI Policy initialization.
- EFI_STATUS UpdatePeiSaPolicyPreMem (IN OUT SI_PREMEM_POLICY_PPI ∗SiPreMemPolicyPpi)

  This function performs SA PEI Policy initialization for PreMem.
- EFI_STATUS UpdatePeiPchPolicy (IN OUT SI_POLICY_PPI ∗SiPolicy)

  This function performs PCH PEI Policy initialization.
- EFI_STATUS UpdatePeiPchPolicyPreMem (IN OUT SI_PREMEM_POLICY_PPI ∗SiPreMemPolicy)

  This function performs PCH PEI Policy initialization.
- EFI_STATUS UpdatePeiMePolicy (IN OUT SI_POLICY_PPI ∗SiPolicy)

  Update the ME Policy Library.
- EFI_STATUS UpdatePeiMePolicyPreMem (IN OUT SI_PREMEM_POLICY_PPI ∗SiPreMemPolicy)

  Update the ME Policy Library.
- EFI_STATUS UpdatePeiAmtPolicy (IN OUT SI_POLICY_PPI ∗SiPolicyPpi)

  Install the Active Management Policy Ppi Library.

14.28.1 Detailed Description

Header file for PEI SiPolicyUpdate Library.

Copyright

Specification Reference:

14.28.2 Function Documentation

14.28.2.1 UpdatePeiAmtPolicy()

```
EFI_STATUS UpdatePeiAmtPolicy (
             IN OUT SI_POLICY_PPI * SiPolicyPpi )
```

Install the Active Management Policy Ppi Library.

Parameters

in,out	*SiPolicyPpi*	PEI Si Policy

Return values

EFI_SUCCESS	Initialization complete.
EFI_UNSUPPORTED	The chipset is unsupported by this driver.
EFI_OUT_OF_RESOURCES	Do not have enough resources to initialize the driver.
EFI_DEVICE_ERROR	Device error, driver exits abnormally.

14.28.2.2 UpdatePeiCpuPolicy()

```
EFI_STATUS UpdatePeiCpuPolicy (
             IN OUT SI_POLICY_PPI * SiPolicyPpi )
```

This function performs CPU PEI Policy initialization in Post-memory.

Parameters

in,out	*SiPolicyPpi*	The SI Policy PPI instance

Return values

EFI_SUCCESS	The PPI is installed and initialized.
EFI	ERRORS The PPI is not successfully installed.
EFI_OUT_OF_RESOURCES	Do not have enough resources to initialize the driver

14.28.2.3 UpdatePeiMePolicy()

```
EFI_STATUS UpdatePeiMePolicy (
             IN OUT SI_POLICY_PPI * SiPolicy )
```

Update the ME Policy Library.

Parameters

in,out	*SiPolicyPpi*	The pointer to SiPolicyPpi

Return values

EFI_SUCCESS	Update complete.
Others	Update unsuccessful.

14.28.2.4 UpdatePeiMePolicyPreMem()

```
EFI_STATUS UpdatePeiMePolicyPreMem (
             IN OUT SI_PREMEM_POLICY_PPI * SiPreMemPolicy )
```

Update the ME Policy Library.

Parameters

in,out	*SiPreMemPolicy*	The SI PreMem Policy PPI instance

Return values

EFI_SUCCESS	Update complete.

14.28.2.5 UpdatePeiPchPolicy()

```
EFI_STATUS UpdatePeiPchPolicy (
             IN OUT SI_POLICY_PPI * SiPolicy )
```

This function performs PCH PEI Policy initialization.

Parameters

in,out	*SiPolicy*	The SI Policy PPI instance

Return values

EFI_SUCCESS	The PPI is installed and initialized.
EFI	ERRORS The PPI is not successfully installed.
EFI_OUT_OF_RESOURCES	Do not have enough resources to initialize the driver

14.28.2.6 UpdatePeiPchPolicyPreMem()

```
EFI_STATUS UpdatePeiPchPolicyPreMem (
            IN OUT SI_PREMEM_POLICY_PPI * SiPreMemPolicy )
```

This function performs PCH PEI Policy initialization.

Parameters

in,out	*SiPreMemPolicy*	The SI PreMem Policy PPI instance

Return values

EFI_SUCCESS	The PPI is installed and initialized.
EFI	ERRORS The PPI is not successfully installed.
EFI_OUT_OF_RESOURCES	Do not have enough resources to initialize the driver

14.28.2.7 UpdatePeiSaPolicy()

```
EFI_STATUS UpdatePeiSaPolicy (
            IN OUT SI_POLICY_PPI * SiPolicyPpi )
```

This function performs SI PEI Policy initialization.

Parameters

in,out	*SiPolicyPpi*	The SA Policy PPI instance

Return values

EFI_SUCCESS	The PPI is installed and initialized.

14.28.2.8 UpdatePeiSaPolicyPreMem()

```
EFI_STATUS UpdatePeiSaPolicyPreMem (
            IN OUT SI_PREMEM_POLICY_PPI * SiPreMemPolicyPpi )
```

This function performs SA PEI Policy initialization for PreMem.

Parameters

in,out	*SiPreMemPolicyPpi*	The SI PreMem Policy PPI instance

Return values

EFI_SUCCESS	Update complete.

14.28.2.9 UpdatePeiSiPolicy()

```
EFI_STATUS UpdatePeiSiPolicy (
             IN OUT SI_POLICY_PPI * SiPolicy )
```

This function performs Silicon PEI Policy initialization.

Parameters

in,out	*SiPolicy*	The Silicon Policy PPI instance

Return values

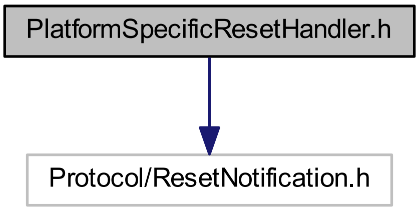
EFI_SUCCESS	The function completed successfully

14.29 PlatformSpecificResetHandler.h File Reference

This PPI provides services to register a platform specific handler for ResetSystem().

`#include <Protocol/ResetNotification.h>`

Include dependency graph for Ppi/PlatformSpecificResetHandler.h:



14.29.1 Detailed Description

This PPI provides services to register a platform specific handler for ResetSystem().

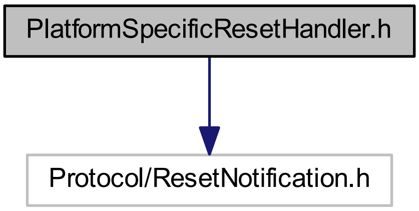
The registered handlers are processed after EDKII_PLATFORM_SPECIFIC_RESET_NOTIFICATION_PPI notifications.

14.30 PlatformSpecificResetHandler.h File Reference

This protocol provides services to register a platform specific handler for ResetSystem().

```
#include <Protocol/ResetNotification.h>
```

Include dependency graph for Protocol/PlatformSpecificResetHandler.h:



14.30.1 Detailed Description

This protocol provides services to register a platform specific handler for ResetSystem().

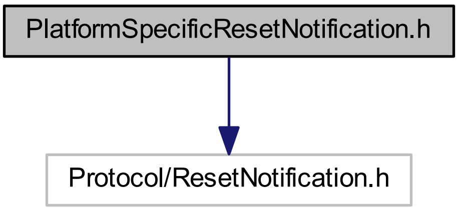
The registered handlers are called after the UEFI 2.7 Reset Notifications are processed

14.31 PlatformSpecificResetNotification.h File Reference

This PPI provides services to register a platform specific notification callback for ResetSystem().

```
#include <Protocol/ResetNotification.h>
```

Include dependency graph for PlatformSpecificResetNotification.h:


PlatformSpecificResetNotification.h
Protocol/ResetNotification.h

14.31.1 Detailed Description

This PPI provides services to register a platform specific notification callback for ResetSystem().

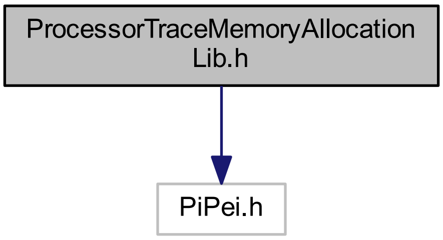
The registered handlers are processed after EDKII_PLATFORM_SPECIFIC_RESET_FILTER_PPI notifications and before EDKII_PLATFORM_SPECIFIC_RESET_HANDLER_PPI notifications.

14.32 ProcessorTraceMemoryAllocationLib.h File Reference

Prototype of Intel Processor Trace memory allocation library.

```
#include <PiPei.h>
```

Include dependency graph for ProcessorTraceMemoryAllocationLib.h:



Enumerations

- enum PROCESSOR_TRACE_MEM_SIZE

  Processor trace buffer size selection.

Functions

- EFI_STATUS ProcessorTraceAllocateMemory (IN PROCESSOR_TRACE_MEM_SIZE RequestedMemSize, OUT EFI_PHYSICAL_ADDRESS ∗BaseAddress, OUT UINT32 ∗LengthInBytes)

  Allocate memory region for Processor Trace, based on requested size per thread.

14.32.1 Detailed Description

Prototype of Intel Processor Trace memory allocation library.

Copyright

Specification Reference:

14.32.2 Function Documentation

14.32.2.1 ProcessorTraceAllocateMemory()

```
EFI_STATUS ProcessorTraceAllocateMemory (
             IN PROCESSOR_TRACE_MEM_SIZE RequestedMemSize,
             OUT EFI_PHYSICAL_ADDRESS * BaseAddress,
             OUT UINT32 * LengthInBytes )
```

Allocate memory region for Processor Trace, based on requested size per thread.

Parameters

in	*RequestedMemSize*	Requested size per thread, specified using PROCESSOR_TRACE_MEM_SIZE encoding
out	∗*BaseAddress*	Outputs a pointer to the base address of the allocated memory region. Base address is NULL on a failure.
out	∗*LengthInBytes*	Outputs a pointer to the size of the allocated memory region, in bytes.

Return values

EFI_SUCCESS	Successfully allocated the memory region
EFI_INVALID_PARAMETER	Invalid value for RequestedMemSize
EFI_OUT_OF_RESOURCES	AllocatePages failed to allocate the memory region

14.33 PttPTPInstanceGuid.h File Reference

GUID definition for the PTT device instance.

14.33.1 Detailed Description

GUID definition for the PTT device instance.

Copyright

Specification

14.34 RegsUsb.h File Reference

Register names for USB Host and device controller.

Macros

- #define N_XHCI_CFG_XHCC2_UNPPA 14

  Upstream Non-Posted Pre-Allocation.
- #define R_XHCI_CFG_XHCC3 0xFC

  XHC System Bus Configuration 3.
- #define R_XHCI_MEM_USBCMD 0x80

  USB Command.
- #define B_XHCI_MEM_USBCMD_RS BIT0

  Run/Stop.
- #define B_XHCI_MEM_USBCMD_RST BIT1

  Host Controller Reset.
- #define R_XHCI_MEM_USBSTS 0x84

  USB Status.
- #define B_XHCI_MEM_USBSTS_HCH BIT0

  Host Controller Halted.
- #define R_XHCI_MEM_PORTSC_START_OFFSET 0x480

  Port Status and Control Registers base offset.
- #define S_XHCI_MEM_PORTSC_PORT_SPACING 0x10

  Size of space between PortSC register for each port.
- #define B_XHCI_MEM_PORTSCXUSB2_WPR BIT31

  Warm Port Reset.
- #define B_XHCI_MEM_PORTSCXUSB2_CEC BIT23

  Port Config Error Change.
- #define B_XHCI_MEM_PORTSCXUSB2_PLC BIT22

  Port Link State Change.
- #define B_XHCI_MEM_PORTSCXUSB2_PRC BIT21

  Port Reset Change.
- #define B_XHCI_MEM_PORTSCXUSB2_OCC BIT20

  Over-current Change.
- #define B_XHCI_MEM_PORTSCXUSB2_WRC BIT19

Warm Port Reset Change.

- #define B_XHCI_MEM_PORTSCXUSB2_PEC BIT18

  Port Enabled Disabled Change.
- #define B_XHCI_MEM_PORTSCXUSB2_CSC BIT17

  Connect Status Change.
- #define B_XHCI_MEM_PORTSCXUSB2_LWS BIT16

  Port Link State Write Strobe.
- #define B_XHCI_MEM_PORTSCXUSB2_PLS (BIT5 | BIT6 | BIT7 | BIT8)

  Port Link State.
- #define B_XHCI_MEM_PORTSCXUSB2_PR BIT4

  Port Reset.
- #define B_XHCI_MEM_PORTSCXUSB2_PED BIT1

  Port Enable/Disabled.
- #define B_XHCI_MEM_PORTSCXUSB2_CCS BIT0

  Current Connect Status.
- #define B_XHCI_MEM_PORTPMSCXUSB2_PTC (BIT28 | BIT29 | BIT30 | BIT31)

  Port Test Control.
- #define B_XHCI_MEM_PORTSCXUSB3_WPR BIT31

  Warm Port Reset.
- #define B_XHCI_MEM_PORTSCXUSB3_CAS BIT24

  Cold Attach Status.
- #define B_XHCI_MEM_PORTSCXUSB3_CEC BIT23

  Port Config Error Change.
- #define B_XHCI_MEM_PORTSCXUSB3_PLC BIT22

  Port Link State Change.
- #define B_XHCI_MEM_PORTSCXUSB3_PRC BIT21

  Port Reset Change.
- #define B_XHCI_MEM_PORTSCXUSB3_OCC BIT20

  Over-current Change.
- #define B_XHCI_MEM_PORTSCXUSB3_WRC BIT19

  Warm Port Reset Change.
- #define B_XHCI_MEM_PORTSCXUSB3_PEC BIT18

  Port Enabled Disabled Change.
- #define B_XHCI_MEM_PORTSCXUSB3_CSC BIT17

  Connect Status Change.
- #define B_XHCI_MEM_PORTSCXUSB3_LWS BIT16

  Port Link State Write Strobe.
- #define B_XHCI_MEM_PORTSCXUSB3_PP BIT9

  Port Power.
- #define B_XHCI_MEM_PORTSCXUSB3_PLS (BIT8 | BIT7 | BIT6 | BIT5)

  Port Link State.
- #define V_XHCI_MEM_PORTSCXUSB3_PLS_POLLING 0x000000E0

  Link is in the Polling State.
- #define V_XHCI_MEM_PORTSCXUSB3_PLS_RXDETECT 0x000000A0

  Link is in the RxDetect State.
- #define V_XHCI_MEM_PORTSCXUSB3_PLS_DISABLED 0x00000080

  Link is in the RxDetect State.
- #define B_XHCI_MEM_PORTSCXUSB3_PR BIT4

  Port Reset.
- #define B_XHCI_MEM_PORTSCXUSB3_PED BIT1

  Port Enable/Disabled.

- #define B_XHCI_MEM_XECP_SUPP_USBX_2_CPC 0xFF00

  Mask for Compatible Port Count in Capability.
- #define N_XHCI_MEM_XECP_SUPP_USBX_2_CPC 8

  Shift for Compatible Port Count.
- #define R_XHCI_MEM_HOST_CTRL_ODMA_REG 0x8098

  Host Control ODMA Register.
- #define B_XHCI_MEM_PMCTRL_SSU3LFPS_DET 0xFF00

  SS U3 LFPS Detection Threshold Mask.
- #define N_XHCI_MEM_PMCTRL_SSU3LPFS_DET 8

  SS U3 LFPS Detection Threshold position.
- #define R_XHCI_MEM_PGCBCTRL 0x80A8

  PGCB Control.
- #define R_XHCI_MEM_HOST_CTRL_MISC_REG 0x80B0

  Host Controller Misc Reg.
- #define R_XHCI_MEM_HOST_CTRL_MISC_REG_2 0x80B4

  Host Controller Misc Reg 2.
- #define R_XHCI_MEM_SSPE 0x80B8

  Super Speed Port Enables.
- #define R_XHCI_MEM_AUX_CTRL_REG 0x80C0

  AUX_CTRL_REG - AUX Reset Control.
- #define R_XHCI_MEM_HOST_BW_OV_HS_REG 0x80C8

  HOST_BW_OV_HS_REG - High Speed TT Bandwidth Overhead.
- #define B_XHCI_MEM_HOST_BW_OV_HS_REG_OVHD_HSTTBW 0x0FFF

  Mask for Overhead per packet for HS-TT BW calculations value.
- #define B_XHCI_MEM_HOST_BW_OV_HS_REG_OVHD_HSBW 0xFFF000

  Mask for Overhead per packet for HS BW calculations value.
- #define R_XHCI_MEM_HOST_CTRL_PORT_LINK_REG 0x80EC

  SuperSpeed Port Link Control.
- #define R_XHCI_MEM_USB2_LINK_MGR_CTRL_REG1_DW1 0x80F0

  USB2_LINK_MGR_CTRL_REG1 - USB2 Port Link Control 1, 2, 3, 4.
- #define R_XHCI_MEM_USB2_LINK_MGR_CTRL_REG1_DW2 0x80F4

  USB2_LINK_MGR_CTRL_REG1 - USB2 Port Link Control 1, 2, 3, 4.
- #define R_XHCI_MEM_USB2_LINK_MGR_CTRL_REG1_DW3 0x80F8

  USB2_LINK_MGR_CTRL_REG1 - USB2 Port Link Control 1, 2, 3, 4.
- #define R_XHCI_MEM_USB2_LINK_MGR_CTRL_REG1_DW4 0x80FC

  USB2_LINK_MGR_CTRL_REG1 - USB2 Port Link Control 1, 2, 3, 4.
- #define R_XHCI_MEM_HOST_CTRL_BW_CTRL_REG 0x8100

  HOST_CTRL_BW_CTRL_REG - Host Controller Bandwidth Control Register.
- #define R_XHCI_MEM_HOST_IF_CTRL_REG 0x8108

  HOST_IF_CTRL_REG - Host Controller Interface Control Register.
- #define R_XHCI_MEM_HOST_CTRL_TRM_REG2 0x8110

  HOST_CTRL_TRM_REG2 - Host Controller Transfer Manager Control 2.
- #define R_XHCI_MEM_HOST_CTRL_BW_MAX_REG 0x8128

  HOST_CTRL_BW_MAX_REG - Max BW Control Reg 4.
- #define B_XHCI_MEM_HOST_CTRL_BW_MAX_REG_MAX_HS_BW 0xFFF000

  HOST_CTRL_BW_MAX_REG - Max. Number of BW units for HS ports.
- #define N_XHCI_MEM_HOST_CTRL_BW_MAX_REG_MAX_HS_BW 12

  HOST_CTRL_BW_MAX_REG - Max. Number of BW units for HS ports position.
- #define R_XHCI_MEM_HOST_IF_PWR_CTRL_REG0 0x8140

  HOST_IF_PWR_CTRL_REG0 - Power Scheduler Control 0.
- #define B_XHCI_MEM_HOST_IF_PWR_CTRL_REG0_AW 0xFFF000

Advance Wake (AW)

- #define R_XHCI_MEM_HOST_IF_PWR_CTRL_REG1 0x8144

  HOST_IF_PWR_CTRL_REG1 - Power Scheduler Control 1.
- #define R_XHCI_MEM_AUX_CTRL_REG2 0x8154

  AUX_CTRL_REG2 - Aux PM Control Register 2.
- #define R_XHCI_MEM_USB2PHYPM 0x8164

  USB2 PHY Power Management Control.
- #define R_XHCI_MEM_AUXCLKCTL 0x816C

  xHCI Aux Clock Control Register
- #define R_XHCI_MEM_USBLPM 0x8170

  USB LPM Parameters.
- #define B_XHCI_MEM_USBLPM_MIN_U2_ELFPS_D (BIT18 | BIT17 | BIT16)

  Min U2 Exit LFPS Duration.
- #define R_XHCI_MEM_XHCLTVCTL 0x8174

  xHC Latency Tolerance Parameters - LTV Control
- #define B_XHCI_MEM_XHCLTVCTL_USB2_PL0_LTV 0xFFF

  USB2 Port L0 LTV.
- #define R_XHCI_MEM_LTVHIT 0x817C

  xHC Latency Tolerance Parameters - High Idle Time Control
- #define R_XHCI_MEM_LTVMIT 0x8180

  xHC Latency Tolerance Parameters - Medium Idle Time Control
- #define R_XHCI_MEM_LTVLIT 0x8184

  xHC Latency Tolerance Parameters - Low Idle Time Control
- #define R_XHCI_MEM_XECP_CMDM_CTRL_REG1 0x818C

  Command Manager Control 1.
- #define R_XHCI_MEM_XECP_CMDM_CTRL_REG2 0x8190

  Command Manager Control 2.
- #define R_XHCI_MEM_XECP_CMDM_CTRL_REG3 0x8194

  Command Manager Control 3.
- #define R_XHCI_MEM_PDDIS 0x8198

  xHC Pulldown Disable Control
- #define R_XHCI_MEM_THROTT 0x819C

  XHCI Throttle Control.
- #define R_XHCI_MEM_LFPSPM 0x81A0

  LFPS PM Control.
- #define R_XHCI_MEM_THROTT2 0x81B4

  XHCI Throttle.
- #define R_XHCI_MEM_LFPSONCOUNT 0x81B8

  LFPS On Count.
- #define R_XHCI_MEM_D0I2CTRL 0x81BC

  D0I2 Control Register.
- #define B_XHCI_MEM_D0I2CTRL 0x3FDFFFF0

  D0I2 Control Register Mask.
- #define B_XHCI_MEM_D0I2CTRL_MSI_IDLE_THRESHOLD 0xFFF0

  Bitmask for MSI Idle Threshold.
- #define N_XHCI_MEM_D0I2CTRL_MSI_IDLE_THRESHOLD 4

  Bitshift for MSI Idle Threshold.
- #define N_XHCI_MEM_D0I2CTRL_MSID0I2PWT 16

  Bitshift for MSI D0i2 Pre Wake Time.
- #define N_XHCI_MEM_D0I2CTRL_D0I2_ENTRY_HYSTERESIS_TIMER 22

  Bitshift for D0i2 Entry Hysteresis Timer.

- #define N_XHCI_MEM_D0I2CTRL_D0I2_MIN_RESIDENCY 26

  Bitshift for D0i2 Minimum Residency.
- #define R_XHCI_MEM_D0I2SCH_ALARM_CTRL 0x81C0

  D0i2 Scheduler Alarm Control Register.
- #define B_XHCI_MEM_D0I2SCH_ALARM_CTRL 0x1FFF1FFF

  Bitmask for D0i2 Scheduler Alarm Control Register.
- #define N_XHCI_MEM_D0I2SCH_ALARM_CTRL_D0I2IT 16

  Bitshift for D0i2 Idle Time.
- #define R_XHCI_MEM_USB2PMCTRL 0x81C4

  USB2 Power Management Control.
- #define R_XHCI_MEM_AUX_CTRL_REG3 0x81C8

  Aux PM Control 3 Register.
- #define R_XHCI_MEM_TRBPRFCTRLREG1 0x81D0

  TRB Prefetch Control Register 1.
- #define R_XHCI_MEM_TRBPRFCACHEINVREG 0x81D8

  TRB Prefetch Cache Invalidation Register 1.
- #define B_XHCI_MEM_TRBPRFCACHEINVREG_EN_TRB_FLUSH 0x7F

  TRB Flushing for various commands.
- #define N_XHCI_MEM_TRBPRFCACHEINVREG_EN_TRB_FLUSH 17

  Enable TRB flushing for various command.
- #define R_XHCI_MEM_DBGDEV_CTRL_REG1 0x8754

  Debug Device Control Register 1.
- #define R_XHCI_MEM_PMCTRL2 0x8468

  PMCTRL2 - Power Management Control 2.
- #define R_XHCI_MEM_MULT_IN_SCH_POLICY 0x82A0

  Multiple IN Scheduler Policy Register.
- #define R_XHCI_MEM_MULT_IN_FAIRNESS_POLICY_1 0x82A4

  Fairness Policy Register 1.
- #define R_XHCI_MEM_PMREQ_CTRL_REG 0x83D0

  PMREQ Control Register.
- #define R_XHCI_MEM_ENH_CLK_GATE_CTRL 0x83D8

  Enhanced Clock Gate Control Policy Register.
- #define R_XHCI_MEM_USBLEGCTLSTS 0x8470

  USB Legacy Support Control Status.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIBAR BIT31

  SMI on BAR Status.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIPCIC BIT30

  SMI on PCI Command Status.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIOSC BIT29

  SMI on OS Ownership Change Status.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIBARE BIT15

  SMI on BAR Enable.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIPCICE BIT14

  SMI on PCI Command Enable.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIOSOE BIT13

  SMI on OS Ownership Enable.
- #define B_XHCI_MEM_USBLEGCTLSTS_SMIHSEE BIT4

  SMI on Host System Error Enable.
- #define B_XHCI_MEM_USBLEGCTLSTS_USBSMIE BIT0

  USB SMI Enable.
- #define R_PCH_XHCI_MEM_USB2PDO 0x84F8

USB2 Port Disable Override register.
- #define R_PCH_XHCI_MEM_USB3PDO 0x84FC

  USB3 Port Disable Override register.
- #define B_PCH_LP_XHCI_MEM_USB2PDO_MASK 0x3FF

  LP: Mask for 10 USB2 ports.
- #define B_PCH_H_XHCI_MEM_USB2PDO_MASK 0x7FFF

  H: Mask for 14 USB2 ports.
- #define B_PCH_LP_XHCI_MEM_USB3PDO_MASK 0x3F

  LP: Mask for 6 USB3 ports.
- #define B_PCH_H_XHCI_MEM_USB3PDO_MASK 0x3FF

  H: Mask for 10 USB3 ports.
- #define B_XHCI_MEM_SOCHWSTSAVE1_CMD_SSV BIT31

  CMD save indication that scratchpad data is valid.
- #define R_XHCI_MEM_AUDIO_OFFLOAD_CTR 0x91F4

  Audio Offload Control.
- #define B_XHCI_MEM_CAPABILITY_ID 0xFF

  Capability ID.
- #define B_XHCI_MEM_CAPABILITY_NEXT_CAP_PTR 0xFF00

  Next Capability Pointer.
- #define N_XHCI_MEM_CAPABILITY_NEXT_CAP_PTR 8

  Byte shift for next capability pointer.
- #define V_XHCI_MEM_DBC_DCID 0x0A

  Debug Capability ID.
- #define R_XHCI_MEM_DBC_DCCTRL 0x20

  Debug Capability Control Register (DCCTRL)
- #define B_XHCI_MEM_DBC_DCCTRL_DCR BIT0

  Debug Capability - DbC Run (DCR)
- #define R_XHCI_MEM_DBC_DCST 0x24

  Debug Capability Status Register (DCST)
- #define B_XHCI_MEM_DBC_DCST_DBG_PORT_NUMBER 0xFF

  Debug Port Number Mask.
- #define N_XHCI_MEM_DBC_DCST_DBG_PORT_NUMBER 24

  Debug Port Number Offset in DCST register.
- #define R_XHCI_MEM_DBC_DBCCTL 0x8760

  DBCCTL - DbC Control.
- #define B_XHCI_MEM_DBC_DBCCTL_DISC_RXD_CNT 0x1F

  Soft Disconnect RX Detect Count mask.
- #define N_XHCI_MEM_DBC_DBCCTL_DISC_RXD_CNT 2

  Soft Disconnect RX Detect Count bitshift.
- #define R_XHCI_MEM_U2OCM 0x90A4

  XHC USB2 Overcurrent Pin N Mapping.
- #define R_XHCI_MEM_U3OCM 0x9124

  XHC USB3 Overcurrent Pin N Mapping.
- #define R_XHCI_PCR_DAP_USB2PORT_STATUS_0 0x508

  DAP USB2 Port0 Status 0 Register.
- #define B_XHCI_PCR_DAP_USB2PORT_STATUS_0_OS 0xFF

  Operation State (OS) in DAP USB2 Port<N> Status 0 Register.
- #define V_XHCI_PCR_DAP_USB2PORT_STATUS_0_OS_DBC 0x40

  DBC Operation State.
- #define R_XDCI_CFG_PMCSR 0x84

  Power Management Control and Status Register.

- #define R_XDCI_CFG_GENERAL_PURPOSER_REG1 0xA0

  General Purpose PCI RW Register1.
- #define R_XDCI_CFG_CPGE 0xA2

  Chassis Power Gate Enable.
- #define R_XDCI_CFG_GENERAL_PURPOSER_REG4 0xAC

  General Purpose PCI RW Register4.
- #define R_XDCI_CFG_GENERAL_INPUT_REG 0xC0

  General Input Register.
- #define R_XDCI_MEM_GCTL 0xC110

  Xdci Global Ctrl.
- #define B_XDCI_MEM_GCTL_GHIBEREN BIT1

  Hibernation enable.
- #define R_XDCI_MEM_GUSB2PHYCFG 0xC200

  Global USB2 PHY Configuration Register.
- #define B_XDCI_MEM_GUSB2PHYCFG_SUSPHY BIT6

  Suspend USB2.0 HS/FS/LS PHY.
- #define R_XDCI_MEM_GUSB3PIPECTL0 0xC2C0

  Global USB3 PIPE Control Register 0.
- #define B_XDCI_MEM_GUSB3PIPECTL0_SUSPEN_EN BIT17

  Suspend USB3.0 SS PHY (Suspend_en)
- #define B_XDCI_MEM_GUSB3PIPECTL0_UX_IN_PX BIT27

  Ux Exit in Px.
- #define R_USB2_PCR_GLOBAL_PORT 0x4001

  USB2 GLOBAL PORT.
- #define R_USB2_PCR_PP_LANE_BASE_ADDR 0x4000

  PP LANE base address.
- #define V_USB2_PCR_PER_PORT 0x00

  USB2 PER PORT Addr[7:2] = 0x00.
- #define V_USB2_PCR_PER_PORT_RXISET 0x04

  PERPORTRXISET bits value in USB2 PER PORT register.
- #define V_USB2_PCR_UTMI_MISC_PER_PORT 0x08

  UTMI MISC REG PER PORT Addr[7:2] = 0x08.
- #define V_USB2_PCR_PER_PORT_2 0x26

  USB2 PER PORT 2 Addr[7:2] = 0x26.
- #define V_USB2_PCR_PER_PORT_2_HSSKEWSEL 0x01

  HSSKEWSEL bits value USB2 PER PORT2 register.
- #define V_USB2_PCR_PER_PORT_2_SKEWDELAY 0x03

  HSNPREDRVSEL bits value USB2 PER PORT2 register.
- #define R_USB2_PCR_GLB_ADP_VBUS_REG 0x402B

  GLB ADP VBUS REG.
- #define R_USB2_PCR_GLOBAL_PORT_2 0x402C

  USB2 GLOBAL PORT 2.
- #define R_USB2_PCR_PLLDIVRATIOS_0 0x7000

  PLLDIVRATIOS_0.
- #define R_USB2_PCR_CONFIG_0 0x7008

  CONFIG_0.
- #define R_USB2_PCR_CONFIG_3 0x7014

  CONFIG_3.
- #define R_USB2_PCR_DFT_1 0x7024

  DFT_1.
- #define R_USB2_PCR_SFRCONFIG_0 0x702C

SFRCONFIG_0.

- #define R_USB2_PCR_PLL1 0x7F02

  USB2 PLL1.

- #define R_USB2_PCR_PLL2 0x7F03

  USB2 PLL2.

- #define B_USB2_PCR_PLL2_FORCE_PLL_CYCLE BIT26

  Force PLL Cycle.

- #define B_USB2_PCR_PLL2_USB_PLL_LOCK BIT27

  USB PLL Lock.

- #define R_USB2_PCR_CFG_COMPBG 0x7F04

  USB2 COMPBG.

- #define R_XHCI_MEM_SSIC_CONF_REG2_PORT_1 0x880C

  SSIC Configuration Register 2 Port 1.

- #define R_XHCI_MEM_SSIC_CONF_REG2_PORT_2 0x883C

  SSIC Configuration Register 2 Port 2.

14.34.1 Detailed Description

Register names for USB Host and device controller.

Conventions:

- Register definition format: Prefix_[GenerationName]_[ComponentName]_SubsystemName_Register↩ Space_RegisterName
- Prefix: Definitions beginning with "R_" are registers Definitions beginning with "B_" are bits within registers Definitions beginning with "V_" are meaningful values within the bits Definitions beginning with "S_" are register size Definitions beginning with "N_" are the bit position
- [GenerationName]: Three letter acronym of the generation is used (e.g. SKL,KBL,CNL etc.). Register name without GenerationName applies to all generations.
- [ComponentName]: This field indicates the component name that the register belongs to (e.g. PCH, SA etc.) Register name without ComponentName applies to all components. Register that is specific to -H denoted by "_PCH_H_" in component name. Register that is specific to -LP denoted by "_PCH_LP_" in component name.
- SubsystemName: This field indicates the subsystem name of the component that the register belongs to (e.g. PCIE, USB, SATA, GPIO, PMC etc.).
- RegisterSpace: MEM - MMIO space register of subsystem. IO - IO space register of subsystem. PCR - Private configuration register of subsystem. CFG - PCI configuration space register of subsystem.
- RegisterName: Full register name.

Copyright

Specification Reference:

14.35 ResetSystemLib.h File Reference

System reset Library Services.

Functions

- VOID ResetCold (VOID)

  This function causes a system-wide reset (cold reset), in which all circuitry within the system returns to its initial state.
- VOID ResetWarm (VOID)

  This function causes a system-wide initialization (warm reset), in which all processors are set to their initial state.
- VOID ResetShutdown (VOID)

  This function causes the system to enter a power state equivalent to the ACPI G2/S5 or G3 states.
- VOID EnterS3WithImmediateWake (VOID)

  This function causes the system to enter S3 and then wake up immediately.
- VOID ResetPlatformSpecific (IN UINTN DataSize, IN VOID ∗ResetData)

  This function causes a systemwide reset.

14.35.1 Detailed Description

System reset Library Services.

This library class defines a set of methods that reset the whole system.

14.35.2 Function Documentation

14.35.2.1 EnterS3WithImmediateWake()

```
VOID EnterS3WithImmediateWake (
             VOID  )
```

This function causes the system to enter S3 and then wake up immediately.

If this function returns, it means that the system does not support S3 feature.

14.35.2.2 ResetCold()

```
VOID ResetCold (
             VOID  )
```

This function causes a system-wide reset (cold reset), in which all circuitry within the system returns to its initial state.

This type of reset is asynchronous to system operation and operates without regard to cycle boundaries.

If this function returns, it means that the system does not support cold reset.

14.35.2.3 ResetPlatformSpecific()

```
VOID ResetPlatformSpecific (
             IN UINTN DataSize,
             IN VOID * ResetData )
```

This function causes a systemwide reset.

The exact type of the reset is defined by the EFI_GUID that follows the Null-terminated Unicode string passed into ResetData. If the platform does not recognize the EFI_GUID in ResetData the platform must pick a supported reset type to perform.The platform may optionally log the parameters from any non-normal reset that occurs.

Parameters

in	*DataSize*	The size, in bytes, of ResetData.
in	*ResetData*	The data buffer starts with a Null-terminated string, followed by the EFI_GUID.

14.35.2.4 ResetShutdown()

```
VOID ResetShutdown (
             VOID  )
```

This function causes the system to enter a power state equivalent to the ACPI G2/S5 or G3 states.

If this function returns, it means that the system does not support shutdown reset.

14.35.2.5 ResetWarm()

```
VOID ResetWarm (
            VOID   )
```

This function causes a system-wide initialization (warm reset), in which all processors are set to their initial state.

Pending cycles are not corrupted.

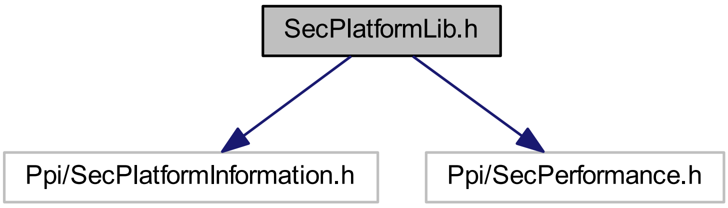
If this function returns, it means that the system does not support warm reset.

14.36 SecPlatformLib.h File Reference

Prototype of SEC Platform hook library.

```
#include <Ppi/SecPlatformInformation.h>
#include <Ppi/SecPerformance.h>
```

Include dependency graph for SecPlatformLib.h:



Functions

- EFI_PEI_PPI_DESCRIPTOR ∗ SecPlatformMain (IN OUT EFI_SEC_PEI_HAND_OFF ∗SecCoreData)

  A developer supplied function to perform platform specific operations.
- EFI_STATUS SecPlatformInformation (IN CONST EFI_PEI_SERVICES ∗∗PeiServices, IN OUT UINT64 ∗StructureSize, OUT EFI_SEC_PLATFORM_INFORMATION_RECORD ∗PlatformInformationRecord)

  This interface conveys state information out of the Security (SEC) phase into PEI.
- EFI_STATUS SecGetPerformance (IN CONST EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SEC_PERF↵ORMANCE_PPI ∗This, OUT FIRMWARE_SEC_PERFORMANCE ∗Performance)

  This interface conveys performance information out of the Security (SEC) phase into PEI.

14.36.1 Detailed Description

Prototype of SEC Platform hook library.

Copyright

Specification Reference:

14.36.2 Function Documentation

14.36.2.1 SecGetPerformance()

```
EFI_STATUS SecGetPerformance (
             IN CONST EFI_PEI_SERVICES ** PeiServices,
             IN PEI_SEC_PERFORMANCE_PPI * This,
             OUT FIRMWARE_SEC_PERFORMANCE * Performance )
```

This interface conveys performance information out of the Security (SEC) phase into PEI.

This service is published by the SEC phase. The SEC phase handoff has an optional EFI_PEI_PPI_DESCRIPTOR list as its final argument when control is passed from SEC into the PEI Foundation. As such, if the platform supports collecting performance data in SEC, this information is encapsulated into the data structure abstracted by this service. This information is collected for the boot-strap processor (BSP) on IA-32.

Parameters

in	*PeiServices*	The pointer to the PEI Services Table.
in	*This*	The pointer to this instance of the PEI_SEC_PERFORMANCE_PPI.
out	*Performance*	The pointer to performance data collected in SEC phase.

Return values

EFI_SUCCESS	The data was successfully returned.

14.36.2.2 SecPlatformInformation()

```
EFI_STATUS SecPlatformInformation (
             IN CONST EFI_PEI_SERVICES ** PeiServices,
             IN OUT UINT64 * StructureSize,
             OUT EFI_SEC_PLATFORM_INFORMATION_RECORD * PlatformInformationRecord )
```

This interface conveys state information out of the Security (SEC) phase into PEI.

Parameters

PeiServices	Pointer to the PEI Services Table.
StructureSize	Pointer to the variable describing size of the input buffer.
PlatformInformationRecord	Pointer to the EFI_SEC_PLATFORM_INFORMATION_RECORD.

Return values

EFI_SUCCESS	The data was successfully returned.
EFI_BUFFER_TOO_SMALL	The buffer was too small.

14.36.2.3 SecPlatformMain()

```
EFI_PEI_PPI_DESCRIPTOR* SecPlatformMain (
             IN OUT EFI_SEC_PEI_HAND_OFF * SecCoreData )
```

A developer supplied function to perform platform specific operations.

It's a developer supplied function to perform any operations appropriate to a given platform. It's invoked just before passing control to PEI core by SEC core. Platform developer may modify the SecCoreData passed to PEI Core. It returns a platform specific PPI list that platform wishes to pass to PEI core. The Generic SEC core module will merge this list to join the final list passed to PEI core.

Parameters

SecCoreData	The same parameter as passing to PEI core. It could be overridden by this function.

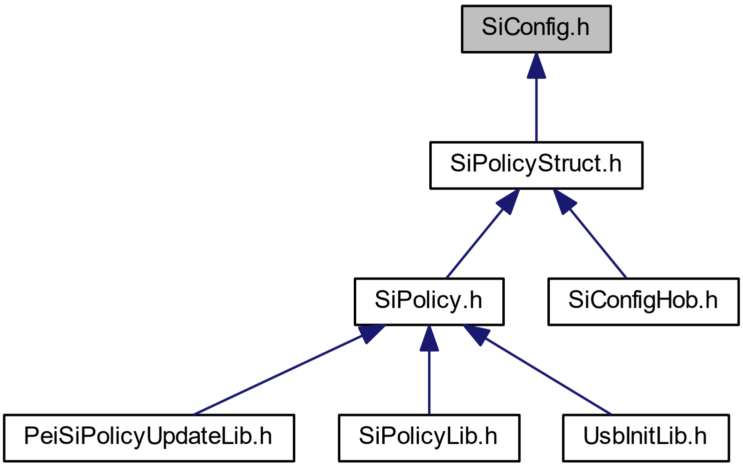
Returns

The platform specific PPI list to be passed to PEI core or NULL if there is no need of such platform specific PPI list.

14.37 SiConfig.h File Reference

Si Config Block.

This graph shows which files directly or indirectly include this file:



Classes

- struct SI_CONFIG

  The Silicon Policy allows the platform code to publish a set of configuration information that the RC drivers will use to configure the silicon hardware.
- struct SVID_SID_VALUE

  Subsystem Vendor ID / Subsystem ID.

14.37.1 Detailed Description

Si Config Block.

Copyright

Specification Reference:

14.38 SiConfigBlockLib.h File Reference

Prototype of the SiConfigBlockLib library.

Functions

- UINT16 GetComponentConfigBlockTotalSize (IN COMPONENT_BLOCK_ENTRY ∗ComponentBlocks, IN UINT16 TotalBlockCount)

  GetComponentConfigBlockTotalSize get config block table total size.
- EFI_STATUS AddComponentConfigBlocks (IN VOID ∗ConfigBlockTableAddress, IN COMPONENT_BLO↩ CK_ENTRY ∗ComponentBlocks, IN UINT16 TotalBlockCount)

  AddComponentConfigBlocks add all config blocks.

14.38.1 Detailed Description

Prototype of the SiConfigBlockLib library.

Copyright

Specification Reference:

14.38.2 Function Documentation

14.38.2.1 AddComponentConfigBlocks()

```
EFI_STATUS AddComponentConfigBlocks (
            IN VOID * ConfigBlockTableAddress,
            IN COMPONENT_BLOCK_ENTRY * ComponentBlocks,
            IN UINT16 TotalBlockCount )
```

AddComponentConfigBlocks add all config blocks.

Parameters

in	*ConfigBlockTableAddress*	The pointer to add config blocks
in	*ComponentBlocks*	Config blocks array
in	*TotalBlockCount*	Number of blocks

Return values

EFI_SUCCESS	The policy default is initialized.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.38.2.2 GetComponentConfigBlockTotalSize()

```
UINT16 GetComponentConfigBlockTotalSize (
            IN COMPONENT_BLOCK_ENTRY * ComponentBlocks,
            IN UINT16 TotalBlockCount )
```

GetComponentConfigBlockTotalSize get config block table total size.

Parameters

in	*ComponentBlocks*	Component blocks array
in	*TotalBlockCount*	Number of blocks

Return values

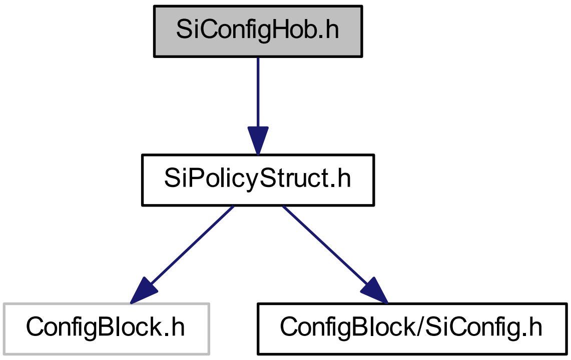
Size	of config block table

14.39 SiConfigHob.h File Reference

Silicon Config HOB is used for gathering platform related Intel silicon information and config setting.

```
#include <SiPolicyStruct.h>
```

Include dependency graph for SiConfigHob.h:



14.39.1 Detailed Description

Silicon Config HOB is used for gathering platform related Intel silicon information and config setting.

Copyright

Specification Reference:

14.40 SiFvi.h File Reference

Header file for Reference code Firmware Version Info Init Lib implementation.

Macros

- #define TO_BE_FILLED 0

  Non-static SMBIOS table data to be filled later with a dynamically generated value.
- #define TO_BE_FILLED_STRING " "

  Initial value should not be NULL.
- #define NO_STRING_AVAILABLE 0

  String references in SMBIOS tables.
- #define DEFAULT_FVI_DATA()

  The string number for ComponentName and VersionString is always calculated dynamically.
- #define CPU_FVI_STRING "Reference Code - CPU"

  CPU Data definitions.
- #define ME_FVI_STRING "Reference Code - ME"

  ME Data definitions.
- #define PCH_FVI_STRING "Reference Code - CML PCH"

  PCH Data definitions.
- #define SA_FVI_STRING "Reference Code - SA - System Agent"

  SA Data definitions.

Enumerations

- enum ME_FVI_INDEX

Functions

- VOID BuildFviInfoHob (VOID)

  Function definitions.
- EFI_STATUS UpdateFviInfo (IN UINT8 SmbiosOemType)

  Update All Smbios FVI OEM Type Data.

14.40.1 Detailed Description

Header file for Reference code Firmware Version Info Init Lib implementation.

Copyright

Specification Reference:

14.40.2 Macro Definition Documentation

14.40.2.1 DEFAULT_FVI_DATA

```
#define DEFAULT_FVI_DATA( )
```

Value:

```
{ \
  TO_BE_FILLED, \
  TO_BE_FILLED, \
  { \
    TO_BE_FILLED, \
    TO_BE_FILLED, \
    TO_BE_FILLED, \
    TO_BE_FILLED, \
  } \
}
```

The string number for ComponentName and VersionString is always calculated dynamically.

The initial value is ignored and should always be TO_BE_FILLED.

Definition at line 65 of file SiFvi.h.

14.40.2.2 NO_STRING_AVAILABLE

```
#define NO_STRING_AVAILABLE 0
```

String references in SMBIOS tables.

This eliminates the need for pointers. See the DMTF SMBIOS Specification v2.7.1, section 6.1.3.

Definition at line 48 of file SiFvi.h.

14.40.3 Enumeration Type Documentation

14.40.3.1 ME_FVI_INDEX

```
enum ME_FVI_INDEX
```

Enumerator

EnumMeRc	ME Reference Code Version.
EnumMebx	MEBx Version.
EnumMeFw	ME FW Version.

Definition at line 119 of file SiFvi.h.

14.40.4 Function Documentation

14.40.4.1 BuildFviInfoHob()

```
VOID BuildFviInfoHob (
             VOID  )
```

Function definitions.

Initialize all Smbios FVI OEM Type Data Hob

14.40.4.2 UpdateFviInfo()

```
EFI_STATUS UpdateFviInfo (
             IN UINT8 SmbiosOemType )
```

Update All Smbios FVI OEM Type Data.

Parameters

SmbiosOemType	- SMBIOS OEM Type

Return values

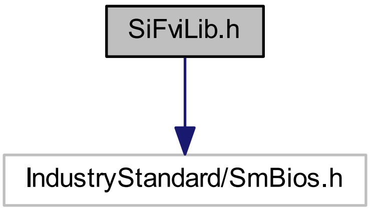
EFI_UNSUPPORTED	- Could not locate SMBIOS protocol
EFI_SUCCESS	- Successfully update FVI data

14.41 SiFviLib.h File Reference

Header file for Reference code Firmware Version Info Interface Lib implementation.

```
#include <IndustryStandard/SmBios.h>
```

Include dependency graph for SiFviLib.h:



Classes

- struct RC_VERSION

  This structure contains the RC version details for FVI SMBIOS records.
- struct FVI_DATA

  The string number for ComponentName and VersionString is always calculated dynamically.

Macros

- #define TO_BE_FILLED 0

  Non-static SMBIOS table data to be filled later with a dynamically generated value.
- #define TO_BE_FILLED_STRING " "

  Initial value should not be NULL.
- #define NO_STRING_AVAILABLE 0

  String references in SMBIOS tables.

Functions

- EFI_STATUS AddFviEntry (IN FVI_HEADER Header, IN FVI_DATA ∗Data, IN FVI_STRINGS ∗Strings)

  Create the Reference code version info as per Firmware Version Info (FVI) Interface Spec v0.8 and add the SMBIOS table using the SMBIOS protocol.

14.41.1 Detailed Description

Header file for Reference code Firmware Version Info Interface Lib implementation.

Copyright

Specification Reference:

14.41.2 Macro Definition Documentation

14.41.2.1 NO_STRING_AVAILABLE

```
#define NO_STRING_AVAILABLE 0
```

String references in SMBIOS tables.

This eliminates the need for pointers. See the DMTF SMBIOS Specification v2.7.1, section 6.1.3.

Definition at line 51 of file SiFviLib.h.

14.41.3 Function Documentation

14.41.3.1 AddFviEntry()

```
EFI_STATUS AddFviEntry (
             IN FVI_HEADER Header,
             IN FVI_DATA * Data,
             IN FVI_STRINGS * Strings )
```

Create the Reference code version info as per Firmware Version Info (FVI) Interface Spec v0.8 and add the SMBIOS table using the SMBIOS protocol.

Invoke this routine to add the table entry when all the Fvi data is finalized.

Precondition

- – EFI_SMBIOS_PROTOCOL in Native mode

Parameters

in	*Header*	The expanded header includes the standard SMBIOS table header, plus the Count of the number of elements in the Data and Strings arrays.
in	∗*Data*	Pointer to an array of Data blocks.
in	∗*Strings*	Pointer to an array of Strings. There are FVI_NUMBER_OF_STRINGS ∗ Count strings total.

Return values

EFI_SUCCESS	- if the data is successfully reported.
EFI_OUT_OF_RESOURCES	- if not able to get resources.
EFI_UNSUPPORTED	- if required DataHub or SMBIOS protocol is not available.

14.42 SiMtrrLib.h File Reference

Header file for Silicon code Mtrr Lib implementation.

Functions

- EFI_STATUS MtrrTransfer2DefaultWB (OUT MTRR_SETTINGS ∗MtrrSetting)

  Function attempts to transfer MTRRs default WriteBack and update MTRRs Setting.

14.42.1 Detailed Description

Header file for Silicon code Mtrr Lib implementation.

Copyright

Specification Reference:

14.42.2 Function Documentation

14.42.2.1 MtrrTransfer2DefaultWB()

```
EFI_STATUS MtrrTransfer2DefaultWB (
             OUT MTRR_SETTINGS * MtrrSetting )
```

Function attempts to transfer MTRRs default WriteBack and update MTRRs Setting.

Parameters

out	*MtrrSetting*	- A buffer holding all MTRRs content.

Return values

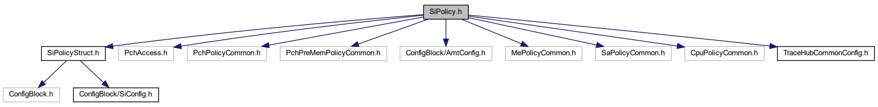
EFI_SUCCESS	- The function completed successfully. EFI_UNSUPPORTED - Mtrr is not supported. EFI_INVALID_PARAMETER - MtrrSetting is NULL.

14.43 SiPolicy.h File Reference

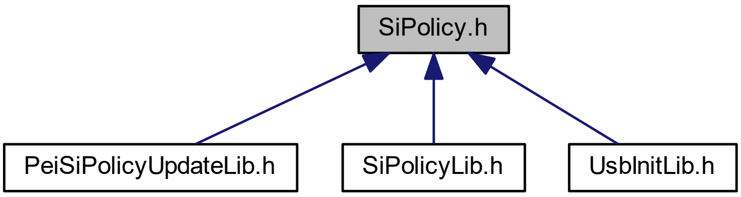
Silicon Policy PPI is used for specifying platform related Intel silicon information and policy setting.

```
#include <SiPolicyStruct.h>
#include <PchAccess.h>
#include <PchPolicyCommon.h>
#include <PchPreMemPolicyCommon.h>
#include <ConfigBlock/AmtConfig.h>
#include <MePolicyCommon.h>
#include <SaPolicyCommon.h>
#include <CpuPolicyCommon.h>
#include <TraceHubCommonConfig.h>
```

Include dependency graph for SiPolicy.h:



This graph shows which files directly or indirectly include this file:



14.43.1 Detailed Description

Silicon Policy PPI is used for specifying platform related Intel silicon information and policy setting.

This PPI is consumed by the silicon PEI modules and carried over to silicon DXE modules.

Copyright

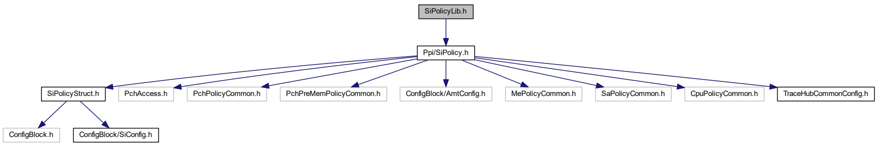
Specification Reference:

14.44 SiPolicyLib.h File Reference

Prototype of the SiPolicyLib library.

```
#include <Ppi/SiPolicy.h>
```

Include dependency graph for SiPolicyLib.h:



Functions

- VOID SiPreMemPrintPolicyPpi (IN SI_PREMEM_POLICY_PPI ∗SiPreMemPolicyPpi)

  Print whole SI_PREMEM_POLICY_PPI and serial out.
- VOID SiPrintPolicyPpi (IN SI_POLICY_PPI ∗SiPolicyPpi)

  Print whole SI_POLICY_PPI and serial out.
- EFI_STATUS SiCreatePreMemConfigBlocks (OUT SI_PREMEM_POLICY_PPI ∗∗SiPreMemPolicyPpi)

  SiCreatePreMemConfigBlocks creates the config blocksg of Silicon Policy.
- EFI_STATUS SiCreateConfigBlocks (OUT SI_POLICY_PPI ∗∗SiPolicyPpi)

  SiCreateConfigBlocks creates the config blocksg of Silicon Policy.
- EFI_STATUS SiPreMemInstallPolicyPpi (IN SI_PREMEM_POLICY_PPI ∗SiPreMemPolicyPpi)

  SiPreMemInstallPolicyPpi installs SiPreMemPolicyPpi.
- EFI_STATUS SiInstallPolicyPpi (IN SI_POLICY_PPI ∗SiPolicyPpi)

  SiInstallPolicyPpi installs SiPolicyPpi.
- VOID DumpSiPolicy (IN SI_POLICY_PPI ∗SiPolicyPpi)

  Print out all silicon policy information.
- UINT32 TraceHubCalculateTotalBufferSize (IN SI_PREMEM_POLICY_PPI ∗SiPreMemPolicyPpi)

  Calculate total trace buffer size and make it power of two, eliminate the total size within 512MB Please ensure CPU and PCH trace hub policy are configured before calling.
- EFI_STATUS SiPreMemInstallPolicyReadyPpi (VOID)

  SiPreMemInstallPolicyReadyPpi installs SiPreMemPolicyReadyPpi.
- EFI_STATUS SiInstallPolicyReadyPpi (VOID)

  SiInstallPolicyReadyPpi installs SiPolicyReadyPpi.

14.44.1 Detailed Description

Prototype of the SiPolicyLib library.

Copyright

Specification Reference:

14.44.2 Function Documentation

14.44.2.1 DumpSiPolicy()

```
VOID DumpSiPolicy (
            IN SI_POLICY_PPI * SiPolicyPpi )
```

Print out all silicon policy information.

Parameters

in	*SiPolicyPpi*	The pointer to Silicon Policy PPI instance

Return values

none	

14.44.2.2 SiCreateConfigBlocks()

```
EFI_STATUS SiCreateConfigBlocks (
            OUT SI_POLICY_PPI ** SiPolicyPpi )
```

SiCreateConfigBlocks creates the config blocksg of Silicon Policy.

It allocates and zero out buffer, and fills in the Intel default settings.

Parameters

out	*SiPolicyPpi*	The pointer to get Silicon Policy PPI instance

Return values

EFI_SUCCESS	The policy default is initialized.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.3 SiCreatePreMemConfigBlocks()

```
EFI_STATUS SiCreatePreMemConfigBlocks (
            OUT SI_PREMEM_POLICY_PPI ** SiPreMemPolicyPpi )
```

SiCreatePreMemConfigBlocks creates the config blocksg of Silicon Policy.

It allocates and zero out buffer, and fills in the Intel default settings.

Parameters

out	*SiPreMemPolicyPpi*	The pointer to get Silicon PREMEM Policy PPI instance

Return values

EFI_SUCCESS	The policy default is initialized.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.4 SiInstallPolicyPpi()

```
EFI_STATUS SiInstallPolicyPpi (
            IN SI_POLICY_PPI * SiPolicyPpi )
```

SiInstallPolicyPpi installs SiPolicyPpi.

While installed, RC assumes the Policy is ready and finalized. So please update and override any setting before calling this function.

Parameters

in	*SiPolicyPpi*	The pointer to Silicon Policy PPI instance

Return values

EFI_SUCCESS	The policy is installed.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.5 SiInstallPolicyReadyPpi()

```
EFI_STATUS SiInstallPolicyReadyPpi (
             VOID  )
```

SiInstallPolicyReadyPpi installs SiPolicyReadyPpi.

While installed, RC assumes the Policy is ready and finalized. So please update and override any setting before calling this function.

Return values

EFI_SUCCESS	The policy is installed.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.6 SiPreMemInstallPolicyPpi()

```
EFI_STATUS SiPreMemInstallPolicyPpi (
             IN SI_PREMEM_POLICY_PPI * SiPreMemPolicyPpi )
```

SiPreMemInstallPolicyPpi installs SiPreMemPolicyPpi.

While installed, RC assumes the Policy is ready and finalized. So please update and override any setting before calling this function.

Parameters

in	*SiPreMemPolicyPpi*	The pointer to Silicon PREMEM Policy PPI instance

Return values

EFI_SUCCESS	The policy is installed.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.7 SiPreMemInstallPolicyReadyPpi()

```
EFI_STATUS SiPreMemInstallPolicyReadyPpi (
             VOID  )
```

SiPreMemInstallPolicyReadyPpi installs SiPreMemPolicyReadyPpi.

While installed, RC assumes the Policy is ready and finalized. So please update and override any setting before calling this function.

Return values

EFI_SUCCESS	The policy is installed.
EFI_OUT_OF_RESOURCES	Insufficient resources to create buffer

14.44.2.8 SiPreMemPrintPolicyPpi()

```
VOID SiPreMemPrintPolicyPpi (
             IN SI_PREMEM_POLICY_PPI * SiPreMemPolicyPpi )
```

Print whole SI_PREMEM_POLICY_PPI and serial out.

Parameters

in	*SiPreMemPolicyPpi*	The RC PREMEM Policy PPI instance

14.44.2.9 SiPrintPolicyPpi()

```
VOID SiPrintPolicyPpi (
             IN SI_POLICY_PPI * SiPolicyPpi )
```

Print whole SI_POLICY_PPI and serial out.

Parameters

in	*SiPolicyPpi*	The RC Policy PPI instance

14.44.2.10 TraceHubCalculateTotalBufferSize()

```
UINT32 TraceHubCalculateTotalBufferSize (
             IN SI_PREMEM_POLICY_PPI * SiPreMemPolicyPpi )
```

Calculate total trace buffer size and make it power of two, eliminate the total size within 512MB Please ensure CPU and PCH trace hub policy are configured before calling.

Parameters

in	*SiPreMemPolicyPpi*	The pointer to get Silicon Policy PPI instance

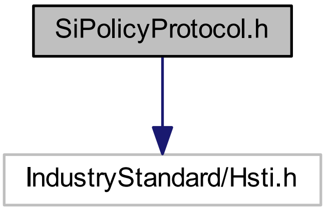
Return values

UINT32	Total size of trace buffers

14.45 SiPolicyProtocol.h File Reference

Protocol used for specifying platform related Silicon information and policy setting.

`#include <IndustryStandard/Hsti.h>`
Include dependency graph for SiPolicyProtocol.h:



Classes

- struct DXE_SI_POLICY_PROTOCOL

  The protocol allows the platform code to publish a set of configuration information that the Silicon drivers will use to configure the processor in the DXE phase.

14.45.1 Detailed Description

Protocol used for specifying platform related Silicon information and policy setting.

Copyright

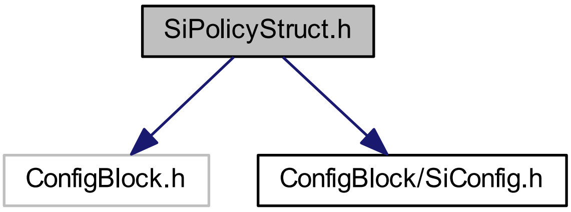
Specification

14.46 SiPolicyStruct.h File Reference

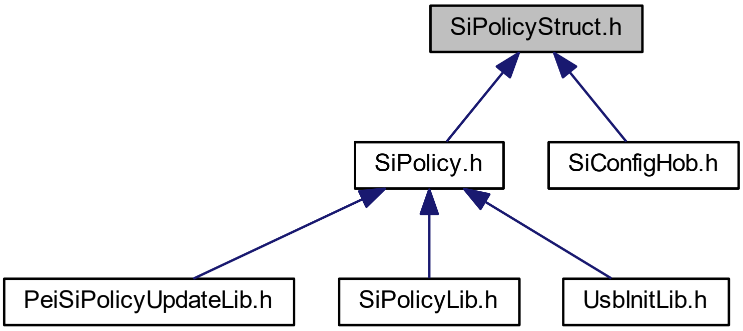
Intel reference code configuration policies.

```
#include <ConfigBlock.h>
#include <ConfigBlock/SiConfig.h>
```

Include dependency graph for SiPolicyStruct.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct _SI_PREMEM_POLICY_STRUCT

  SI Policy PPI in Pre-Mem
  All SI config block change history will be listed here

  .
- struct _SI_POLICY_STRUCT

  SI Policy PPI
  All SI config block change history will be listed here

  .

Macros

- #define SI_POLICY_REVISION 1

  Silicon Policy revision number Any change to this structure will result in an update in the revision number.
- #define SI_PREMEM_POLICY_REVISION 1

  Silicon pre-memory Policy revision number Any change to this structure will result in an update in the revision number.

14.46.1 Detailed Description

Intel reference code configuration policies.

Copyright

Specification Reference:

14.46.2 Macro Definition Documentation

14.46.2.1 SI_POLICY_REVISION

```
#define SI_POLICY_REVISION 1
```

Silicon Policy revision number Any change to this structure will result in an update in the revision number.

This member specifies the revision of the Silicon Policy. This field is used to indicate change to the policy structure.

Revision 1:

- Initial version.

Definition at line 51 of file SiPolicyStruct.h.

14.46.2.2 SI_PREMEM_POLICY_REVISION

```
#define SI_PREMEM_POLICY_REVISION 1
```

Silicon pre-memory Policy revision number Any change to this structure will result in an update in the revision number.

Revision 1:

- Initial version.

Definition at line 60 of file SiPolicyStruct.h.

14.47 SmmAccess.h File Reference

EFI SMM Access PPI definition.

Classes

- struct _PEI_SMM_ACCESS_PPI

  EFI SMM Access PPI is used to control the visibility of the SMRAM on the platform.

Typedefs

- typedef EFI_STATUS(∗ PEI_SMM_OPEN) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_ACCESS_PPI ∗This, IN UINTN DescriptorIndex)

  Opens the SMRAM area to be accessible by a PEIM driver.
- typedef EFI_STATUS(∗ PEI_SMM_CLOSE) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_ACCESS_PPI ∗This, IN UINTN DescriptorIndex)

  Inhibits access to the SMRAM.
- typedef EFI_STATUS(∗ PEI_SMM_LOCK) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_ACCESS_PPI ∗This, IN UINTN DescriptorIndex)

  Inhibits access to the SMRAM.
- typedef EFI_STATUS(∗ PEI_SMM_CAPABILITIES) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_ACCESS_PPI ∗This, IN OUT UINTN ∗SmramMapSize, IN OUT EFI_SMRAM_DESCRIPTOR ∗SmramMap)

  Queries the memory controller for the possible regions that will support SMRAM.

14.47.1 Detailed Description

EFI SMM Access PPI definition.

This PPI is used to control the visibility of the SMRAM on the platform. It abstracts the location and characteristics of SMRAM. The expectation is that the north bridge or memory controller would publish this PPI.

The principal functionality found in the memory controller includes the following:

- Exposing the SMRAM to all non-SMM agents, or the "open" state
- Shrouding the SMRAM to all but the SMM agents, or the "closed" state
- Preserving the system integrity, or "locking" the SMRAM, such that the settings cannot be perturbed by either boot service or runtime agents

14.47.2 Typedef Documentation

14.47.2.1 PEI_SMM_CAPABILITIES

```
typedef EFI_STATUS( * PEI_SMM_CAPABILITIES) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_ACCESS_PPI
*This, IN OUT UINTN *SmramMapSize, IN OUT EFI_SMRAM_DESCRIPTOR *SmramMap)
```

Queries the memory controller for the possible regions that will support SMRAM.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The pointer to the SmmAccessPpi Interface.
SmramMapSize	The pointer to the variable containing size of the buffer to contain the description information.
SmramMap	The buffer containing the data describing the Smram region descriptors.

Return values

EFI_BUFFER_TOO_SMALL	The user did not provide a sufficient buffer.
EFI_SUCCESS	The user provided a sufficiently-sized buffer.

Definition at line 122 of file SmmAccess.h.

14.47.2.2 PEI_SMM_CLOSE

```
typedef EFI_STATUS( * PEI_SMM_CLOSE) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_ACCESS_PPI
*This, IN UINTN DescriptorIndex)
```

Inhibits access to the SMRAM.

This function "closes" SMRAM so that it is not visible while outside of SMM. The function should return EFI_UNS←UPPORTED if the hardware does not support hiding of SMRAM.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The pointer to the SMM Access Interface.
DescriptorIndex	The region of SMRAM to Close.

Return values

EFI_SUCCESS	The region was successfully closed.
EFI_DEVICE_ERROR	The region could not be closed because locked by chipset.
EFI_INVALID_PARAMETER	The descriptor index was out of bounds.

Definition at line 76 of file SmmAccess.h.

14.47.2.3 PEI_SMM_LOCK

```
typedef EFI_STATUS( * PEI_SMM_LOCK) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_ACCESS_PPI
*This, IN UINTN DescriptorIndex)
```

Inhibits access to the SMRAM.

This function prohibits access to the SMRAM region. This function is usually implemented such that it is a write-once operation.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The pointer to the SMM Access Interface.
DescriptorIndex	The region of SMRAM to Close.

Return values

EFI_SUCCESS	The region was successfully locked.
EFI_DEVICE_ERROR	The region could not be locked because at least one range is still open.
EFI_INVALID_PARAMETER	The descriptor index was out of bounds.

Definition at line 100 of file SmmAccess.h.

14.47.2.4 PEI_SMM_OPEN

```
typedef EFI_STATUS( * PEI_SMM_OPEN) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_ACCESS_PPI
*This, IN UINTN DescriptorIndex)
```

Opens the SMRAM area to be accessible by a PEIM driver.

This function "opens" SMRAM so that it is visible while not inside of SMM. The function should return EFI_UNSUPPORTED if the hardware does not support hiding of SMRAM. The function should return EFI_DEVICE_ERROR if the SMRAM configuration is locked.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The pointer to the SMM Access Interface.
DescriptorIndex	The region of SMRAM to Open.

Return values

EFI_SUCCESS	The region was successfully opened.
EFI_DEVICE_ERROR	The region could not be opened because locked by chipset.
EFI_INVALID_PARAMETER	The descriptor index was out of bounds.

Definition at line 53 of file SmmAccess.h.

14.48 SmmControl.h File Reference

EFI SMM Control PPI definition.

Classes

- struct _PEI_SMM_CONTROL_PPI

    PEI SMM Control PPI is used to initiate SMI/PMI activations.

Typedefs

- typedef EFI_STATUS(∗ PEI_SMM_ACTIVATE) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_CONTROL_PPI ∗This, IN OUT INT8 ∗ArgumentBuffer OPTIONAL, IN OUT UINTN ∗ArgumentBufferSize OPTIONAL, IN BOOLEAN Periodic OPTIONAL, IN UINTN ActivationInterval OPTIONAL)

    Invokes SMI activation from either the preboot or runtime environment.
- typedef EFI_STATUS(∗ PEI_SMM_DEACTIVATE) (IN EFI_PEI_SERVICES ∗∗PeiServices, IN PEI_SMM_CONTROL_PPI ∗This, IN BOOLEAN Periodic OPTIONAL)

    Clears any system state that was created in response to the Active call.

14.48.1 Detailed Description

EFI SMM Control PPI definition.

This PPI is used to initiate SMI/PMI activations. This protocol could be published by either:

- A processor driver to abstract the SMI/PMI IPI
- The driver that abstracts the ASIC that is supporting the APM port, such as the ICH in an Intel chipset Because of the possibility of performing SMI or PMI IPI transactions, the ability to generate this event from a platform chipset agent is an optional capability for both IA-32 and Itanium-based systems.

14.48.2 Typedef Documentation

14.48.2.1 PEI_SMM_ACTIVATE

```
typedef EFI_STATUS( * PEI_SMM_ACTIVATE) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_CONTROL_PPI
*This, IN OUT INT8 *ArgumentBuffer OPTIONAL, IN OUT UINTN *ArgumentBufferSize OPTIONAL, IN BOOLEAN Periodic OPTIONAL, IN UINTN ActivationInterval OPTIONAL)
```

Invokes SMI activation from either the preboot or runtime environment.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The PEI_SMM_CONTROL_PPI instance.
ArgumentBuffer	The optional sized data to pass into the protocol activation.
ArgumentBufferSize	The optional size of the data.
Periodic	An optional mechanism to periodically repeat activation.
ActivationInterval	An optional parameter to repeat at this period one time or, if the Periodic Boolean is set, periodically.

Return values

EFI_SUCCESS	The SMI/PMI has been engendered.
EFI_DEVICE_ERROR	The timing is unsupported.
EFI_INVALID_PARAMETER	The activation period is unsupported.
EFI_NOT_STARTED	The SMM base service has not been initialized.

Definition at line 53 of file SmmControl.h.

14.48.2.2 PEI_SMM_DEACTIVATE

```
typedef EFI_STATUS( * PEI_SMM_DEACTIVATE) (IN EFI_PEI_SERVICES **PeiServices, IN PEI_SMM_CONTROL_PPI
*This, IN BOOLEAN Periodic OPTIONAL)
```

Clears any system state that was created in response to the Active call.

Parameters

PeiServices	General purpose services available to every PEIM.
This	The PEI_SMM_CONTROL_PPI instance.
Periodic	Optional parameter to repeat at this period one time or, if the Periodic Boolean is set, periodically.

Return values

EFI_SUCCESS	The SMI/PMI has been engendered.
EFI_DEVICE_ERROR	The source could not be cleared.
EFI_INVALID_PARAMETER	The service did not support the Periodic input argument.

Definition at line 77 of file SmmControl.h.

14.49 SmmVariable.h File Reference

EFI SMM Variable Protocol is related to EDK II-specific implementation of variables and intended for use as a means to store data in the EFI SMM environment.

Classes

- struct _EFI_SMM_VARIABLE_PROTOCOL

  EFI SMM Variable Protocol is intended for use as a means to store data in the EFI SMM environment.

14.49.1 Detailed Description

EFI SMM Variable Protocol is related to EDK II-specific implementation of variables and intended for use as a means to store data in the EFI SMM environment.

14.50 SocketLga775Lib.h File Reference

Public include file for CPU definitions and CPU library functions that apply to CPUs that fit into an LGA775 spocket.

Classes

- struct SOCKET_LGA_775_SMM_CPU_STATE32

  CPU save-state strcuture for IA32.
- struct SOCKET_LGA_775_SMM_CPU_STATE64

  CPU save-state strcuture for X64.
- union SOCKET_LGA_775_SMM_CPU_STATE

  Union of CPU save-state strcutures for IA32 and X64.

Macros

- #define SMM_IO_LENGTH_BYTE 0x01

  SMM Save State IOMisc related defines.

14.50.1 Detailed Description

Public include file for CPU definitions and CPU library functions that apply to CPUs that fit into an LGA775 spocket.

Module Name: SocketLga775Lib.h

Copyright

Specification

14.51 StallPpiLib.h File Reference

Header file for a library to install StallPpi.

Functions

- EFI_STATUS InstallStallPpi (VOID)

  This function is to install StallPpi.

14.51.1 Detailed Description

Header file for a library to install StallPpi.

Copyright

Specification Reference:

14.51.2 Function Documentation

14.51.2.1 InstallStallPpi()

```
EFI_STATUS InstallStallPpi (
             VOID   )
```

This function is to install StallPpi.

Return values

EFI_SUCCESS	if Ppi is installed successfully.

14.52 TempRamExitPpi.h File Reference

This file defines the Silicon Temp Ram Exit PPI which implements the MTRR values initialization.

Classes

- struct _FSP_TEMP_RAM_EXIT_PPI

  This PPI provides function to program MTRR values.

Macros

- #define FSP_TEMP_RAM_EXIT_GUID

  Global ID for the FSP_TEMP_RAM_EXIT_PPI.

Typedefs

- typedef EFI_STATUS(∗ FSP_TEMP_RAM_EXIT) (IN VOID ∗TempRamExitParamPtr)

  Program MTRR values and print MTRRs.

14.52.1 Detailed Description

This file defines the Silicon Temp Ram Exit PPI which implements the MTRR values initialization.

Copyright

Specification Reference:

14.53 TpmInitialized.h File Reference

Tag GUID that must be installed by the TPM PEIM after the TPM hardware is initialized.

Macros

- #define PEI_TPM_INITIALIZED_PPI_GUID

  Global ID for the PEI_TPM_INITIALIZED_PPI which always uses a NULL interface.
- #define PEI_TPM_INITIALIZATION_DONE_PPI_GUID

  Global ID for the PEI_TPM_INITIALIZATION_DONE_PPI which always uses a NULL interface.

14.53.1 Detailed Description

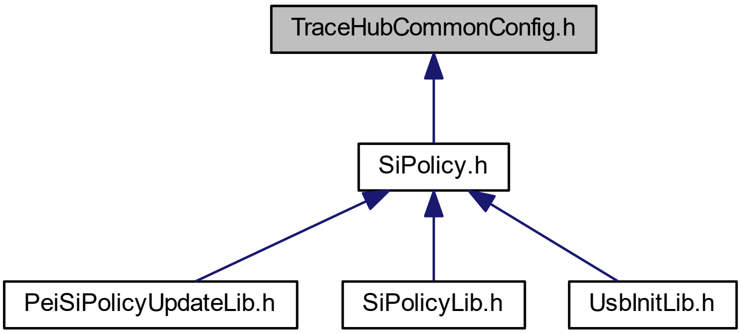
Tag GUID that must be installed by the TPM PEIM after the TPM hardware is initialized.

PEIMs that must execute after TPM hardware initialization may use this GUID in their dependency expressions.

14.54 TraceHubCommonConfig.h File Reference

Common configurations for CPU and PCH trace hub.

This graph shows which files directly or indirectly include this file:



Enumerations

- enum TRACE_HUB_ENABLE_MODE

  The TRACE_HUB_ENABLE_MODE describes the desired TraceHub mode of operation.
- enum TRACE_BUFFER_SIZE

  The TRACE_BUFFER_SIZE describes the desired TraceHub buffer size.

14.54.1 Detailed Description

Common configurations for CPU and PCH trace hub.

Copyright

Specification Reference:

14.54.2 Enumeration Type Documentation

14.54.2.1 TRACE_HUB_ENABLE_MODE

```
enum TRACE_HUB_ENABLE_MODE
```

The TRACE_HUB_ENABLE_MODE describes the desired TraceHub mode of operation.

Enumerator

TraceHubModeDisabled	TraceHub Disabled.
TraceHubModeTargetDebugger	TraceHub Target Debugger mode, debug on target device itself, config to PCI mode.
TraceHubModeHostDebugger	TraceHub Host Debugger mode, debugged by host with cable attached, config to ACPI mode.

Definition at line 41 of file TraceHubCommonConfig.h.

14.55 UsbConfig.h File Reference

Common USB policy shared between PCH and CPU Contains general features settings for xHCI and xDCI.

Classes

- struct USB20_AFE

  This structure configures per USB2 AFE settings.
- struct USB20_PORT_CONFIG

  This structure configures per USB2 port physical settings.
- struct USB30_PORT_CONFIG

  This structure describes whether the USB3 Port N is enabled by platform modules.
- struct XDCI_CONFIG

  The XDCI_CONFIG block describes the configurations of the xDCI Usb Device controller.
- struct USB_CONFIG

  This member describes the expected configuration of the USB controller, Platform modules may need to refer Setup options, schematic, BIOS specification to update this field.

Macros

- #define PCH_USB_OC_PINS_MAX 8

  Maximal possible number of USB Over Current pins.
- #define B_XHCI_HSIO_CTRL_ADAPT_OFFSET_CFG_EN BIT0

  Enable the write to Signed Magnatude number added to the CTLE code bit.
- #define B_XHCI_HSIO_FILTER_SELECT_N_EN BIT1

  Enable the write to LFPS filter select for n.
- #define B_XHCI_HSIO_FILTER_SELECT_P_EN BIT2

  Enable the write to LFPS filter select for p.
- #define B_XHCI_HSIO_LFPS_CFG_PULLUP_DWN_RES_EN BIT3

  Enable the write to olfpscfgpullupdwnres.
- #define B_XHCI_HSIO_CTL_COMP_MULT_EN BIT4

  Enable the write to o_ctlercomp_h_mult3_7_0.

Enumerations

- enum USB_OVERCURRENT_PIN

  Overcurrent pins, the values match the setting of EDS, please refer to EDS for more details.

14.55.1 Detailed Description

Common USB policy shared between PCH and CPU Contains general features settings for xHCI and xDCI.

Copyright

> INTEL CONFIDENTIAL Copyright 2017 - 2020 Intel Corporation.

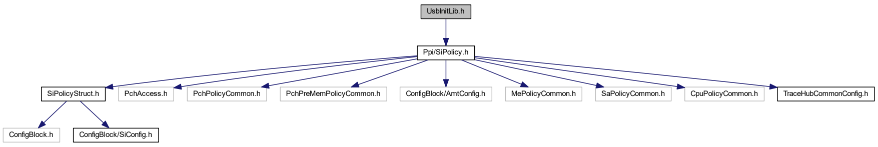
Specification Reference:

14.56 UsbInitLib.h File Reference

Header file for USB initialization library.

```
#include <Ppi/SiPolicy.h>
```

Include dependency graph for UsbInitLib.h:



Functions

- VOID XdciConfigure (IN USB_CONFIG ∗UsbConfig, IN UINT64 XhciPciMmBase)

  Common entry point for PCH and CPU xDCI controller.
- VOID XhciConfigure (IN USB_CONFIG ∗UsbConfig, IN UINT64 XhciPciMmBase)

  Common entry point for PCH and CPU xHCI controller.
- VOID XhciConfigureAfterInit (IN USB_CONFIG ∗UsbConfig, IN UINT64 XhciPciMmBase)

  Configure xHCI after initialization.
- VOID XhciLockConfiguration (IN USB_CONFIG ∗UsbConfig, IN UINT64 XhciPciBase)

  Locks xHCI configuration by setting the proper lock bits in controller.
- VOID Usb2AfeProgramming (IN USB_CONFIG ∗UsbConfig)

  Tune the USB 2.0 high-speed signals quality.

14.56.1 Detailed Description

Header file for USB initialization library.

Copyright

> INTEL CONFIDENTIAL Copyright 2017 - 2018 Intel Corporation.

Specification Reference:

14.56.2 Function Documentation

14.56.2.1 Usb2AfeProgramming()

```
VOID Usb2AfeProgramming (
            IN USB_CONFIG * UsbConfig )
```

Tune the USB 2.0 high-speed signals quality.

Parameters

in	*UsbConfig*	The USB_CONFIG policy instance

14.56.2.2 XdciConfigure()

```
VOID XdciConfigure (
             IN USB_CONFIG * UsbConfig,
             IN UINT64 XhciPciMmBase )
```

Common entry point for PCH and CPU xDCI controller.

Parameters

in	*UsbConfig*	The USB_CONFIG policy instance
in	*XdciPciMmBase*	xDCI PCI config space address

14.56.2.3 XhciConfigure()

```
VOID XhciConfigure (
             IN USB_CONFIG * UsbConfig,
             IN UINT64 XhciPciMmBase )
```

Common entry point for PCH and CPU xHCI controller.

Parameters

in	*UsbConfig*	The USB_CONFIG policy instance
in	*XhciPciMmBase*	xHCI PCI config space address

14.56.2.4 XhciConfigureAfterInit()

```
VOID XhciConfigureAfterInit (
             IN USB_CONFIG * UsbConfig,
             IN UINT64 XhciPciMmBase )
```

Configure xHCI after initialization.

Parameters

in	*UsbConfig*	The USB_CONFIG policy instance
in	*XhciPciMmBase*	XHCI PCI CFG Base Address

14.56.2.5 XhciLockConfiguration()

```
VOID XhciLockConfiguration (
             IN USB_CONFIG * UsbConfig,
             IN UINT64 XhciPciBase )
```

Locks xHCI configuration by setting the proper lock bits in controller.

Parameters

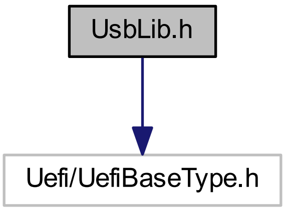
in	*UsbConfig*	The USB_CONFIG policy instance
in	*XhciPciBase*	xHCI PCI config space address

14.57 UsbLib.h File Reference

Header file of available functions in general USB Library.

```
#include <Uefi/UefiBaseType.h>
```

Include dependency graph for UsbLib.h:



14.57.1 Detailed Description

Header file of available functions in general USB Library.

Copyright

Specification Reference:

Index