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

Thu Jun 28 2018 21:44:49

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.

Copyright ©Intel Corporation. All rights reserved.

Contents

1 INTRODUCTION 1

2 FSP OVERVIEW 3

3 FSP INTEGRATION 5

4 FSP OUTPUT 11

5 FSP POSTCODE 15

6 Class Index 19

6.1 Class List . . . 19

7 File Index 21

7.1 File List . . . 21

8 Class Documentation 23

8.1 AUDIO_AZALIA_VERB_TABLE Struct Reference . . . 23

8.1.1 Detailed Description . . . 23

8.2 AZALIA_HEADER Struct Reference . . . 24

8.2.1 Detailed Description . . . 24

8.3 DIMM_INFO Struct Reference . . . 24

8.3.1 Detailed Description . . . 25

8.4 FSP_M_CONFIG Struct Reference . . . 25

8.4.1 Detailed Description . . . 35

8.4.2 Member Data Documentation . . . 35

8.4.2.1 ActiveCoreCount . . . 35

8.4.2.2 ApertureSize . . . 35

8.4.2.3 Avx2RatioOffset . . . 36

8.4.2.4 Avx3RatioOffset . . . 36

8.4.2.5 BclkAdaptiveVoltage . . . 36

8.4.2.6 BiosGuard . . . 36

8.4.2.7 BistOnReset . . . 36

8.4.2.8 BootFrequency . . . 36

8.4.2.9 CleanMemory . . . 36
8.4.2.10 CmdTriStateDis . . . 37
8.4.2.11 CoreMaxOcRatio . . . 37
8.4.2.12 CorePllVoltageOffset . . . 37
8.4.2.13 CoreVoltageAdaptive . . . 37
8.4.2.14 CoreVoltageMode . . . 37
8.4.2.15 CoreVoltageOverride . . . 37
8.4.2.16 CpuRatio . . . 37
8.4.2.17 CpuRatioOverride . . . 38
8.4.2.18 DdrFreqLimit . . . 38
8.4.2.19 DmiDeEmphasis . . . 38
8.4.2.20 DmiGen3EndPointHint . . . 38
8.4.2.21 DmiGen3EndPointPreset . . . 38
8.4.2.22 DmiGen3ProgramStaticEq . . . 38
8.4.2.23 DmiGen3RootPortPreset . . . 39
8.4.2.24 EnableC6Dram . . . 39
8.4.2.25 EnableSgx . . . 39
8.4.2.26 EnableTraceHub . . . 39
8.4.2.27 EvLoader . . . 39
8.4.2.28 FClkFrequency . . . 39
8.4.2.29 FlashWearOutProtection . . . 39
8.4.2.30 GtPllVoltageOffset . . . 40
8.4.2.31 HeciTimeouts . . . 40
8.4.2.32 IgdDvmt50PreAlloc . . . 40
8.4.2.33 InitPcieAspmAfterOprom . . . 40
8.4.2.34 InternalGfx . . . 40
8.4.2.35 JtagC10PowerGateDisable . . . 40
8.4.2.36 McPllVoltageOffset . . . 40
8.4.2.37 MmioSize . . . 41
8.4.2.38 OcLock . . . 41
8.4.2.39 PcdDebugInterfaceFlags . . . 41
8.4.2.40 PcdIsaSerialUartBase . . . 41
8.4.2.41 PcdSerialDebugBaudRate . . . 41
8.4.2.42 PcdSerialDebugLevel . . . 41
8.4.2.43 PcdSerialIoUartNumber . . . 41
8.4.2.44 PchAcpiBase . . . 42
8.4.2.45 PchHpetBase . . . 42
8.4.2.46 PchHpetBdfValid . . . 42
8.4.2.47 PchHpetBusNumber . . . 42
8.4.2.48 PchHpetDeviceNumber . . . 42

8.4.2.49 PchHpetEnable . . . 42
8.4.2.50 PchHpetFunctionNumber . . . 42
8.4.2.51 PchLpcEnhancePort8xhDecoding . . . 42
8.4.2.52 PchNumRsvdSmbusAddresses . . . 43
8.4.2.53 PchPmPciePllSsc . . . 43
8.4.2.54 PchPort80Route . . . 43
8.4.2.55 PcieRpEnableMask . . . 43
8.4.2.56 PeciC10Reset . . . 43
8.4.2.57 PeciSxReset . . . 43
8.4.2.58 PegDataPtr . . . 43
8.4.2.59 PegDisableSpreadSpectrumClocking . . . 44
8.4.2.60 PrmrrSize . . . 44
8.4.2.61 ProbelessTrace . . . 44
8.4.2.62 Ratio . . . 44
8.4.2.63 RealtimeMemoryTiming . . . 44
8.4.2.64 RefClk . . . 44
8.4.2.65 RingDownBin . . . 44
8.4.2.66 RingMaxOcRatio . . . 45
8.4.2.67 RingMinOcRatio . . . 45
8.4.2.68 RingPllVoltageOffset . . . 45
8.4.2.69 RMT . . . 45
8.4.2.70 SaGv . . . 45
8.4.2.71 SaPllVoltageOffset . . . 45
8.4.2.72 SinitMemorySize . . . 45
8.4.2.73 SmbusArpEnable . . . 46
8.4.2.74 SmbusEnable . . . 46
8.4.2.75 SpdProfileSelected . . . 46
8.4.2.76 TjMaxOffset . . . 46
8.4.2.77 tRTP . . . 46
8.4.2.78 TsegSize . . . 46
8.4.2.79 TvbRatioClipping . . . 46
8.4.2.80 TvbVoltageOptimization . . . 47
8.4.2.81 Txt . . . 47
8.4.2.82 TxtDprMemoryBase . . . 47
8.4.2.83 TxtDprMemorySize . . . 47
8.4.2.84 TxtHeapMemorySize . . . 47
8.4.2.85 TxtImplemented . . . 47
8.4.2.86 VddVoltage . . . 47
8.4.2.87 VmxEnable . . . 48
8.5 FSP_M_TEST_CONFIG Struct Reference . . . 48

8.5.1 Detailed Description . . . 51
8.5.2 Member Data Documentation . . . 51
8.5.2.1 BdatEnable . . . 51
8.5.2.2 BiosAcmBase . . . 51
8.5.2.3 BiosAcmSize . . . 51
8.5.2.4 BiosSize . . . 51
8.5.2.5 BypassPhySyncReset . . . 51
8.5.2.6 ChipsetInitMessage . . . 51
8.5.2.7 DisableHeciRetry . . . 52
8.5.2.8 DisableMessageCheck . . . 52
8.5.2.9 DmiGen3EqPh2Enable . . . 52
8.5.2.10 DmiGen3EqPh3Method . . . 52
8.5.2.11 DmiVc1 . . . 52
8.5.2.12 DmiVcm . . . 52
8.5.2.13 Gen3SwEqAlwaysAttempt . . . 52
8.5.2.14 Gen3SwEqEnableVocTest . . . 53
8.5.2.15 Gen3SwEqJitterDwellTime . . . 53
8.5.2.16 Gen3SwEqJitterErrorTarget . . . 53
8.5.2.17 Gen3SwEqNumberOfPresets . . . 53
8.5.2.18 Gen3SwEqVocDwellTime . . . 53
8.5.2.19 Gen3SwEqVocErrorTarget . . . 54
8.5.2.20 HeciCommunication2 . . . 54
8.5.2.21 IderDeviceEnable . . . 54
8.5.2.22 KtDeviceEnable . . . 54
8.5.2.23 LockPTMregs . . . 54
8.5.2.24 PanelPowerEnable . . . 54
8.5.2.25 PchDciEn . . . 54
8.5.2.26 Peg0Gen3EqPh2Enable . . . 55
8.5.2.27 Peg0Gen3EqPh3Method . . . 55
8.5.2.28 Peg1Gen3EqPh2Enable . . . 55
8.5.2.29 Peg1Gen3EqPh3Method . . . 55
8.5.2.30 Peg2Gen3EqPh2Enable . . . 55
8.5.2.31 Peg2Gen3EqPh3Method . . . 55
8.5.2.32 PegGen3EndPointHint . . . 56
8.5.2.33 PegGen3EndPointPreset . . . 56
8.5.2.34 PegGen3ProgramStaticEq . . . 56
8.5.2.35 PegGen3RootPortPreset . . . 56
8.5.2.36 PegGenerateBdatMarginTable . . . 56
8.5.2.37 PegRxCemLoopbackLane . . . 56
8.5.2.38 PegRxCemNonProtocolAwareness . . . 56

8.5.2.39 ScanExtGfxForLegacyOpRom . . . 57
8.5.2.40 SkipMbpHob . . . 57
8.5.2.41 SmbusDynamicPowerGating . . . 57
8.5.2.42 SmbusSpdWriteDisable . . . 57
8.5.2.43 TgaSize . . . 57
8.5.2.44 TotalFlashSize . . . 57
8.5.2.45 TxtLcpPdBase . . . 57
8.5.2.46 TxtLcpPdSize . . . 58
8.5.2.47 WdtDisableAndLock . . . 58
8.6 FSP_S_CONFIG Struct Reference . . . 58
8.6.1 Detailed Description . . . 73
8.6.2 Member Data Documentation . . . 74
8.6.2.1 AcLoadline . . . 74
8.6.2.2 AcousticNoiseMitigation . . . 74
8.6.2.3 AmtEnabled . . . 74
8.6.2.4 AmtSolEnabled . . . 74
8.6.2.5 AsfEnabled . . . 74
8.6.2.6 DcLoadline . . . 74
8.6.2.7 DelayUsbPdoProgramming . . . 74
8.6.2.8 DevIntConfigPtr . . . 75
8.6.2.9 DmiSuggestedSetting . . . 75
8.6.2.10 Early8254ClockGatingEnable . . . 75
8.6.2.11 EcCmdLock . . . 75
8.6.2.12 EcCmdProvisionEav . . . 75
8.6.2.13 EnableTcoTimer . . . 75
8.6.2.14 EsataSpeedLimit . . . 75
8.6.2.15 FastPkgCRampDisableGt . . . 76
8.6.2.16 FastPkgCRampDisableIa . . . 76
8.6.2.17 FastPkgCRampDisableSa . . . 76
8.6.2.18 FwProgress . . . 76
8.6.2.19 GpioIrqRoute . . . 76
8.6.2.20 Heci3Enabled . . . 76
8.6.2.21 IccMax . . . 76
8.6.2.22 ImonOffset . . . 77
8.6.2.23 ImonSlope . . . 77
8.6.2.24 IslVrCmd . . . 77
8.6.2.25 ManageabilityMode . . . 77
8.6.2.26 MeUnconfigIsValid . . . 77
8.6.2.27 MicrocodePatchAddress . . . 77
8.6.2.28 NumOfDevIntConfig . . . 77

8.6.2.29 PchCio2Enable . . . 78
8.6.2.30 PchCrid . . . 78
8.6.2.31 PchDisableComplianceMode . . . 78
8.6.2.32 PchDmiAspm . . . 78
8.6.2.33 PchDmiTsawEn . . . 78
8.6.2.34 PchHdaDspEnable . . . 78
8.6.2.35 PchHdaDspEndpointBluetooth . . . 78
8.6.2.36 PchHdaDspEndpointI2s . . . 78
8.6.2.37 PchHdaDspFeatureMask . . . 79
8.6.2.38 PchHdaDspUaaCompliance . . . 79
8.6.2.39 PchHdaEnable . . . 79
8.6.2.40 PchHdaIDispCodecDisconnect . . . 79
8.6.2.41 PchHdaIoBufferOwnership . . . 79
8.6.2.42 PchHdaPme . . . 79
8.6.2.43 PchIoApicBdfValid . . . 80
8.6.2.44 PchIoApicBusNumber . . . 80
8.6.2.45 PchIoApicDeviceNumber . . . 80
8.6.2.46 PchIoApicEntry24_119 . . . 80
8.6.2.47 PchIoApicFunctionNumber . . . 80
8.6.2.48 PchIoApicId . . . 80
8.6.2.49 PchIoApicRangeSelect . . . 80
8.6.2.50 PchIshEnable . . . 80
8.6.2.51 PchIshGp0GpioAssign . . . 81
8.6.2.52 PchIshGp1GpioAssign . . . 81
8.6.2.53 PchIshGp2GpioAssign . . . 81
8.6.2.54 PchIshGp3GpioAssign . . . 81
8.6.2.55 PchIshGp4GpioAssign . . . 81
8.6.2.56 PchIshGp5GpioAssign . . . 81
8.6.2.57 PchIshGp6GpioAssign . . . 81
8.6.2.58 PchIshGp7GpioAssign . . . 82
8.6.2.59 PchIshI2c0GpioAssign . . . 82
8.6.2.60 PchIshI2c1GpioAssign . . . 82
8.6.2.61 PchIshI2c2GpioAssign . . . 82
8.6.2.62 PchIshPdtUnlock . . . 82
8.6.2.63 PchIshSpiGpioAssign . . . 82
8.6.2.64 PchIshUart0GpioAssign . . . 82
8.6.2.65 PchIshUart1GpioAssign . . . 82
8.6.2.66 PchLanClkReqSupported . . . 83
8.6.2.67 PchLanEnable . . . 83
8.6.2.68 PchLanK1OffEnable . . . 83

8.6.2.69 PchLanLtrEnable . . . 83
8.6.2.70 PchLockDownBiosLock . . . 83
8.6.2.71 PchLockDownSpiEiss . . . 83
8.6.2.72 PchMemoryThrottlingEnable . . . 83
8.6.2.73 PchPcieDeviceOverrideTablePtr . . . 84
8.6.2.74 PchPmCapsuleResetType . . . 84
8.6.2.75 PchPmDeepSxPol . . . 84
8.6.2.76 PchPmDisableDsxAcPresentPulldown . . . 84
8.6.2.77 PchPmDisableNativePowerButton . . . 84
8.6.2.78 PchPmLanWakeFromDeepSx . . . 84
8.6.2.79 PchPmLpcClockRun . . . 84
8.6.2.80 PchPmMeWakeSts . . . 85
8.6.2.81 PchPmPcieWakeFromDeepSx . . . 85
8.6.2.82 PchPmPmeB0S5Dis . . . 85
8.6.2.83 PchPmPwrBtnOverridePeriod . . . 85
8.6.2.84 PchPmPwrCycDur . . . 85
8.6.2.85 PchPmSlpAMinAssert . . . 85
8.6.2.86 PchPmSlpLanLowDc . . . 85
8.6.2.87 PchPmSlpS0Enable . . . 86
8.6.2.88 PchPmSlpS0VmEnable . . . 86
8.6.2.89 PchPmSlpS3MinAssert . . . 86
8.6.2.90 PchPmSlpS4MinAssert . . . 86
8.6.2.91 PchPmSlpStrchSusUp . . . 86
8.6.2.92 PchPmSlpSusMinAssert . . . 86
8.6.2.93 PchPmWolEnableOverride . . . 86
8.6.2.94 PchPmWolOvrWkSts . . . 87
8.6.2.95 PchPmWoWlanDeepSxEnable . . . 87
8.6.2.96 PchPmWoWlanEnable . . . 87
8.6.2.97 PchPort61hEnable . . . 87
8.6.2.98 PchPwrOptEnable . . . 87
8.6.2.99 PchScsEmmcHs400DllDataValid . . . 87
8.6.2.100 PchScsEmmcHs400TuningRequired . . . 87
8.6.2.101 PchSirqEnable . . . 88
8.6.2.102 PchSirqMode . . . 88
8.6.2.103 PchSkyCamPortACtleEnable . . . 88
8.6.2.104 PchSkyCamPortATermOvrEnable . . . 88
8.6.2.105 PchSkyCamPortATrimEnable . . . 88
8.6.2.106 PchSkyCamPortBCtleEnable . . . 88
8.6.2.107 PchSkyCamPortBTermOvrEnable . . . 88
8.6.2.108 PchSkyCamPortBTrimEnable . . . 88

8.6.2.109 PchSkyCamPortCDCtleEnable . . . 89
8.6.2.110 PchSkyCamPortCTermOvrEnable . . . 89
8.6.2.111 PchSkyCamPortCTrimEnable . . . 89
8.6.2.112 PchSkyCamPortDTermOvrEnable . . . 89
8.6.2.113 PchSkyCamPortDTrimEnable . . . 89
8.6.2.114 PchSubSystemId . . . 89
8.6.2.115 PchSubSystemVendorId . . . 89
8.6.2.116 PchThermalDeviceEnable . . . 90
8.6.2.117 PchTsmicLock . . . 90
8.6.2.118 PchTTEnable . . . 90
8.6.2.119 PchTTLock . . . 90
8.6.2.120 PchTTState13Enable . . . 90
8.6.2.121 PcieAllowNoLtrIccPllShutdown . . . 90
8.6.2.122 PcieComplianceTestMode . . . 90
8.6.2.123 PcieDisableRootPortClockGating . . . 91
8.6.2.124 PcieEnablePeerMemoryWrite . . . 91
8.6.2.125 PcieEqPh3LaneParamCm . . . 91
8.6.2.126 PcieEqPh3LaneParamCp . . . 91
8.6.2.127 PcieRpAspm . . . 91
8.6.2.128 PcieRpClkReqNumber . . . 91
8.6.2.129 PcieRpClkReqSupport . . . 91
8.6.2.130 PcieRpClkSrcNumber . . . 92
8.6.2.131 PcieRpCompletionTimeout . . . 92
8.6.2.132 PcieRpDeviceResetPad . . . 92
8.6.2.133 PcieRpFunctionSwap . . . 92
8.6.2.134 PcieRpGen3EqPh3Method . . . 92
8.6.2.135 PcieRpL1Substates . . . 92
8.6.2.136 PcieRpPcieSpeed . . . 92
8.6.2.137 PcieRpPhysicalSlotNumber . . . 93
8.6.2.138 PcieSwEqCoeffListCm . . . 93
8.6.2.139 PcieSwEqCoeffListCp . . . 93
8.6.2.140 PortUsb20Enable . . . 93
8.6.2.141 PortUsb30Enable . . . 93
8.6.2.142 Psi1Threshold . . . 93
8.6.2.143 Psi2Threshold . . . 93
8.6.2.144 Psi3Enable . . . 94
8.6.2.145 Psi3Threshold . . . 94
8.6.2.146 PsysOffset . . . 94
8.6.2.147 PsysSlope . . . 94
8.6.2.148 PxRcConfig . . . 94

8.6.2.149 SataEnable . . . 94
8.6.2.150 SataMode . . . 94
8.6.2.151 SataP0TDispFinit . . . 95
8.6.2.152 SataP1TDispFinit . . . 95
8.6.2.153 SataPortsDevSlp . . . 95
8.6.2.154 SataPortsDmVal . . . 95
8.6.2.155 SataPortsEnable . . . 95
8.6.2.156 SataPwrOptEnable . . . 95
8.6.2.157 SataRstHddUnlock . . . 95
8.6.2.158 SataRstIrrt . . . 95
8.6.2.159 SataRstIrrtOnly . . . 96
8.6.2.160 SataRstLedLocate . . . 96
8.6.2.161 SataRstOromUiBanner . . . 96
8.6.2.162 SataRstPcieDeviceResetDelay . . . 96
8.6.2.163 SataRstRaid0 . . . 96
8.6.2.164 SataRstRaid1 . . . 96
8.6.2.165 SataRstRaid10 . . . 96
8.6.2.166 SataRstRaid5 . . . 97
8.6.2.167 SataRstRaidAlternateId . . . 97
8.6.2.168 SataRstSmartStorage . . . 97
8.6.2.169 SataSalpSupport . . . 97
8.6.2.170 SataThermalSuggestedSetting . . . 97
8.6.2.171 SciIrqSelect . . . 97
8.6.2.172 ScsEmmcEnabled . . . 97
8.6.2.173 ScsEmmcHs400Enabled . . . 97
8.6.2.174 ScsSdCardEnabled . . . 98
8.6.2.175 SendEcCmd . . . 98
8.6.2.176 SendVrMbxCmd . . . 98
8.6.2.177 SendVrMbxCmd1 . . . 98
8.6.2.178 SerialIoDebugUartNumber . . . 98
8.6.2.179 SerialIoDevMode . . . 98
8.6.2.180 SerialIoGpio . . . 99
8.6.2.181 ShowSpiController . . . 99
8.6.2.182 SlowSlewRateForGt . . . 99
8.6.2.183 SlowSlewRateForIa . . . 99
8.6.2.184 SlowSlewRateForSa . . . 99
8.6.2.185 SpiFlashCfgLockDown . . . 99
8.6.2.186 SsicPortEnable . . . 99
8.6.2.187 TcoIrqSelect . . . 100
8.6.2.188 TdcPowerLimit . . . 100

8.6.2.189 TdcTimeWindow . . . 100
8.6.2.190 TTSuggestedSetting . . . 100
8.6.2.191 TurboMode . . . 100
8.6.2.192 Usb2AfePehalfbit . . . 100
8.6.2.193 Usb2AfePetxiset . . . 100
8.6.2.194 Usb2AfePredeemp . . . 101
8.6.2.195 Usb2AfeTxiset . . . 101
8.6.2.196 Usb3HsioTxDeEmph . . . 101
8.6.2.197 Usb3HsioTxDeEmphEnable . . . 101
8.6.2.198 Usb3HsioTxDownscaleAmp . . . 101
8.6.2.199 Usb3HsioTxDownscaleAmpEnable . . . 101
8.6.2.200 VrPowerDeliveryDesign . . . 101
8.6.2.201 VrVoltageLimit . . . 102
8.6.2.202 WatchDog . . . 102
8.6.2.203 WatchDogTimerBios . . . 102
8.6.2.204 WatchDogTimerOs . . . 102
8.6.2.205 XdciEnable . . . 102
8.7 FSP_S_TEST_CONFIG Struct Reference . . . 102
8.7.1 Detailed Description . . . 110
8.7.2 Member Data Documentation . . . 110
8.7.2.1 ApHandoffManner . . . 110
8.7.2.2 ApIdleManner . . . 110
8.7.2.3 AutoThermalReporting . . . 110
8.7.2.4 C1e . . . 110
8.7.2.5 ConfigTdpBios . . . 110
8.7.2.6 CStatePreWake . . . 110
8.7.2.7 CstCfgCtrIoMwaitRedirection . . . 111
8.7.2.8 Custom1ConfigTdpControl . . . 111
8.7.2.9 Custom1PowerLimit1 . . . 111
8.7.2.10 Custom1PowerLimit1Time . . . 111
8.7.2.11 Custom1PowerLimit2 . . . 111
8.7.2.12 Custom1TurboActivationRatio . . . 111
8.7.2.13 Custom2ConfigTdpControl . . . 111
8.7.2.14 Custom2PowerLimit1 . . . 112
8.7.2.15 Custom2PowerLimit1Time . . . 112
8.7.2.16 Custom2PowerLimit2 . . . 112
8.7.2.17 Custom2TurboActivationRatio . . . 112
8.7.2.18 Custom3ConfigTdpControl . . . 112
8.7.2.19 Custom3PowerLimit1 . . . 112
8.7.2.20 Custom3PowerLimit1Time . . . 112

8.7.2.21 Custom3PowerLimit2 . . . 113
8.7.2.22 Custom3TurboActivationRatio . . . 113
8.7.2.23 Cx . . . 113
8.7.2.24 DebugInterfaceEnable . . . 113
8.7.2.25 DebugInterfaceLockEnable . . . 113
8.7.2.26 DisableProcHotOut . . . 113
8.7.2.27 DisableVrThermalAlert . . . 113
8.7.2.28 EightCoreRatioLimit . . . 114
8.7.2.29 Eist . . . 114
8.7.2.30 EndOfPostMessage . . . 114
8.7.2.31 EnergyEfficientPState . . . 114
8.7.2.32 EnergyEfficientTurbo . . . 114
8.7.2.33 FiveCoreRatioLimit . . . 114
8.7.2.34 FourCoreRatioLimit . . . 114
8.7.2.35 HdcControl . . . 115
8.7.2.36 Hwp . . . 115
8.7.2.37 MachineCheckEnable . . . 115
8.7.2.38 MlcStreamerPrefetcher . . . 115
8.7.2.39 MonitorMwaitEnable . . . 115
8.7.2.40 NumberOfEntries . . . 115
8.7.2.41 OneCoreRatioLimit . . . 115
8.7.2.42 PchHdaResetWaitTimer . . . 116
8.7.2.43 PchLockDownBiosInterface . . . 116
8.7.2.44 PchLockDownGlobalSmi . . . 116
8.7.2.45 PchLockDownRtcLock . . . 116
8.7.2.46 PchPmDisableEnergyReport . . . 116
8.7.2.47 PchSbAccessUnlock . . . 116
8.7.2.48 PchSbiUnlock . . . 116
8.7.2.49 PcieEnablePort8xhDecode . . . 117
8.7.2.50 PcieRpDptp . . . 117
8.7.2.51 PcieRpSlotPowerLimitScale . . . 117
8.7.2.52 PcieRpSlotPowerLimitValue . . . 117
8.7.2.53 PcieRpUptp . . . 117
8.7.2.54 PkgCStateDemotion . . . 117
8.7.2.55 PkgCStateLimit . . . 117
8.7.2.56 PkgCStateUnDemotion . . . 118
8.7.2.57 PmgCstCfgCtrlLock . . . 118
8.7.2.58 PowerLimit1 . . . 118
8.7.2.59 PowerLimit1Time . . . 118
8.7.2.60 PowerLimit2 . . . 118

8.7.2.61 PowerLimit2Power . . . 118
8.7.2.62 PowerLimit3 . . . 118
8.7.2.63 PowerLimit3Time . . . 118
8.7.2.64 PowerLimit4 . . . 119
8.7.2.65 ProcHotResponse . . . 119
8.7.2.66 ProcTraceEnable . . . 119
8.7.2.67 ProcTraceOutputScheme . . . 119
8.7.2.68 PsysPmax . . . 119
8.7.2.69 PsysPowerLimit1 . . . 119
8.7.2.70 PsysPowerLimit1Power . . . 119
8.7.2.71 PsysPowerLimit2 . . . 120
8.7.2.72 PsysPowerLimit2Power . . . 120
8.7.2.73 RaceToHalt . . . 120
8.7.2.74 SataTestMode . . . 120
8.7.2.75 SevenCoreRatioLimit . . . 120
8.7.2.76 SixCoreRatioLimit . . . 120
8.7.2.77 StateRatio . . . 120
8.7.2.78 TccActivationOffset . . . 121
8.7.2.79 TccOffsetClamp . . . 121
8.7.2.80 TccOffsetLock . . . 121
8.7.2.81 TccOffsetTimeWindowForRatl . . . 121
8.7.2.82 ThreeCoreRatioLimit . . . 121
8.7.2.83 ThreeStrikeCounterDisable . . . 121
8.7.2.84 TimedMwait . . . 121
8.7.2.85 TStates . . . 122
8.7.2.86 TwoCoreRatioLimit . . . 122
8.8 FSP_T_CONFIG Struct Reference . . . 122
8.8.1 Detailed Description . . . 122
8.8.2 Member Data Documentation . . . 122
8.8.2.1 PcdSerialIoUartDebugEnable . . . 123
8.8.2.2 PcdSerialIoUartNumber . . . 123
8.9 FSPM_UPD Struct Reference . . . 123
8.9.1 Detailed Description . . . 124
8.10 FSPS_UPD Struct Reference . . . 124
8.10.1 Detailed Description . . . 124
8.11 FSPT_CORE_UPD Struct Reference . . . 125
8.11.1 Detailed Description . . . 125
8.12 FSPT_UPD Struct Reference . . . 125
8.12.1 Detailed Description . . . 126
8.13 GPIO_CONFIG Struct Reference . . . 126

8.13.1 Detailed Description . . . 127
8.13.2 Member Data Documentation . . . 127
8.13.2.1 Direction . . . 127
8.13.2.2 ElectricalConfig . . . 127
8.13.2.3 HostSoftPadOwn . . . 127
8.13.2.4 InterruptConfig . . . 127
8.13.2.5 LockConfig . . . 127
8.13.2.6 OutputState . . . 127
8.13.2.7 PadMode . . . 128
8.13.2.8 PowerConfig . . . 128
8.14 MEMORY_PLATFORM_DATA Struct Reference . . . 128
8.14.1 Detailed Description . . . 128
8.15 SI_CHIPSET_INIT_INFO Struct Reference . . . 128
8.15.1 Detailed Description . . . 128
8.16 SI_PCH_DEVICE_INTERRUPT_CONFIG Struct Reference . . . 129
8.16.1 Detailed Description . . . 129
8.17 SMBIOS_CACHE_INFO Struct Reference . . . 129
8.17.1 Detailed Description . . . 130
8.18 SMBIOS_PROCESSOR_INFO Struct Reference . . . 130
8.18.1 Detailed Description . . . 131

9 File Documentation **133**

9.1 CpuConfigFspData.h File Reference . . . 133
9.1.1 Detailed Description . . . 133
9.2 DoxygenFspIntegrationGuide.h File Reference . . . 134
9.2.1 Detailed Description . . . 134
9.3 FspmUpd.h File Reference . . . 134
9.3.1 Detailed Description . . . 135
9.4 FspsUpd.h File Reference . . . 136
9.4.1 Detailed Description . . . 137
9.4.2 Enumeration Type Documentation . . . 137
9.4.2.1 SI_PCH_INT_PIN . . . 137
9.5 FsptUpd.h File Reference . . . 138
9.5.1 Detailed Description . . . 138
9.6 FspUpd.h File Reference . . . 139
9.6.1 Detailed Description . . . 140
9.7 GpioConfig.h File Reference . . . 140
9.7.1 Detailed Description . . . 142
9.7.2 Enumeration Type Documentation . . . 142
9.7.2.1 GPIO_DIRECTION . . . 142

9.7.2.2 GPIO_ELECTRICAL_CONFIG . . . 142
9.7.2.3 GPIO_HARDWARE_DEFAULT . . . 143
9.7.2.4 GPIO_HOSTSW_OWN . . . 143
9.7.2.5 GPIO_INT_CONFIG . . . 143
9.7.2.6 GPIO_LOCK_CONFIG . . . 144
9.7.2.7 GPIO_OTHER_CONFIG . . . 144
9.7.2.8 GPIO_OUTPUT_STATE . . . 144
9.7.2.9 GPIO_PAD_MODE . . . 145
9.7.2.10 GPIO_RESET_CONFIG . . . 145
9.8 GpioSampleDef.h File Reference . . . 146
9.8.1 Detailed Description . . . 146
9.9 MemInfoHob.h File Reference . . . 147
9.9.1 Detailed Description . . . 148
9.10 SmbiosCacheInfoHob.h File Reference . . . 148
9.10.1 Detailed Description . . . 149
9.11 SmbiosProcessorInfoHob.h File Reference . . . 149
9.11.1 Detailed Description . . . 149

Index **151**

Chapter 1

INTRODUCTION

1 Introduction

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 Kabylake platforms with Kabylake/Skylake processor and Sunrise point Platform Controller Hub (PCH).

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.

1.3 Related Documents

- *Platform Initialization (PI) Specification v1.4* located at http://www.uefi.org/specifications
- *UEFI Specification v2.5* 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

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

Chapter 2

FSP OVERVIEW

FSP Overview

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.

2.2 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.

2.2.1 Package Layout

- **Docs (Auto generated)**
  - Kabylake_FSP_Integration_Guide.pdf (this doc)
  - Kabylake_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)
- KabylakeFspBinPkg.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 FSP Integration

3.1 Assumptions Used in this Document

The FSP for the Kabylake platform is built with a preferred base address of 0xFFF40000 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.

3.2 Boot Flow

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

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.

3.4 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 FSP-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 current FSP ImageId string in the FSP information header is **$KBLFSP$** and the ImageRevision field is **0x03060000.(3.6.0.0)**.

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) 0xFED00148 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 this register will work fine.

3.6 FSP APIs

This release of the Kabylake 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.

3.6.1 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 from 0xFEF0_0000 to 0xFEF4_0000 out of which 0xFEF0_0000(ECX) to 0xFEF3_FF00(EDX) is usable area for both bootloader and FSP binary, remaining 0x100 bytes of space reserved by FSP for TempRamInit if temporary RAM initialization is done by FSP.

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 TempRamInit 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

3.6.2 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 stack use through **FSPM_UPD.FspmArchUpd.StackBase** and **FSPM_UPD.FspmArchUpd.StackSize** UPDs.

The minimum FSP stack size required for this revision of FSP is 160KB, stack base is 0xFEF17F00 by default.

The base address of HECI device (Bus 0, Device 22, Function 0) is required to be initialized prior to perform FspMemoryInit 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.

3.6.3 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 *TempRamExitParamPtr*.

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.

Memory range	Cache Attribute
0x00000000 - 0x0009FFFF	Write back
0x000C0000 - Top of Low Memory	Write back
0xFF800000 - 0xFFFFFFFF (Flash region)	Write protect
0x1000000000 - Top of High Memory	Write back

If the boot loader wish to reconfigure the MTRRs differently, it can be overridden immediately after this API call.

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 MicrocodeRegionBase 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, Display, Sky Cam, Camera, PCI Express, Vt-d, straps (cores, hyper-threading, BIST, ..)

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.

On normal boot CPU S3 Resume Data HOB is produced in this phase. This CPU S3 Resume Data HOB is described in section 4.4. Unless UPD SkipMpInit is enabled, on S3 resume, this data (not the entire HOB) must be passed through UPD CpuS3ResumeData, and optionally final S3 boot MTRRs is passed through UPD CpuS3ResumeMtrrData. During S3 resume unless SkipMpInit is enabled, GDT base and length and IDT base and length on APs are programmed to that of the BSP.

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.

3.6.5.1 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.

3.6.5.2 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).

3.6.5.3 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

3.7 Memory Map

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

3.8 Porting recommendation

Here listed some notes or recommendation when porting with FSP.

3.8.1 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)
```

3.8.2 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)
```

3.8.3 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.

3.8.4 Verify below settings are correct for your platforms

Settings	Values
PCIEXBAR_BASE_ADDRESS	0xE0000000 -> PciExBar
MCH_BASE_ADDRESS	0xFED10000 -> MchBar
DMI_BASE_ADDRESS	0xFED18000 -> DmiBar
EP_BASE_ADDRESS	0xFED19000 -> EpBar
EDRAM_BASE_ADDRESS	0xFED80000 -> EdramBar
DEFAULT_OPTION_ROM_TEMP_BAR	0x80000000 -> OpRomScanTempMmioBar
DEFAULT_OPTION_ROM_TEMP_MEM_LIMIT	0xC0000000 -> OpRomScanTempMmioLimit

Note

:

- It is recommended that you do not change these settings as it may require significant changes to the System Agent reference code.
- Those memory regions should be reserved from any memory service functions in platform code so it will not cause any conflict when other modules or drivers allocating memory resource.
- 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_ADDR↩ ESS than the recommended one.

3.8.5 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 4

FSP OUTPUT

4 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.

4.1 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 } }
```

4.2 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. Note: The Smbios Cache Info Hob & Smbios Processor Info Hob won't be published on S3 boot.

```
#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;
```

4.3 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;
```

4.4 CPU S3 Resume Data HOB

The FSP will report the CPU S3 Resume Data through a GUIDED HOB with below GUID. This data (not the entire HOB) must be passed during S3 resume passed in UPD CpuS3ResumeData except if UPD SkipMpInit is enabled.

```
#define CPU_S3_RESUME_DATA_HOB_GUID \
{ 0x3972d4c1, 0xf206, 0x463f, { 0x80, 0xa4, 0xd9, 0x62, 0x79, 0x0a, 0xe5, 0x49 }}
```

Chapter 5

FSP POSTCODE

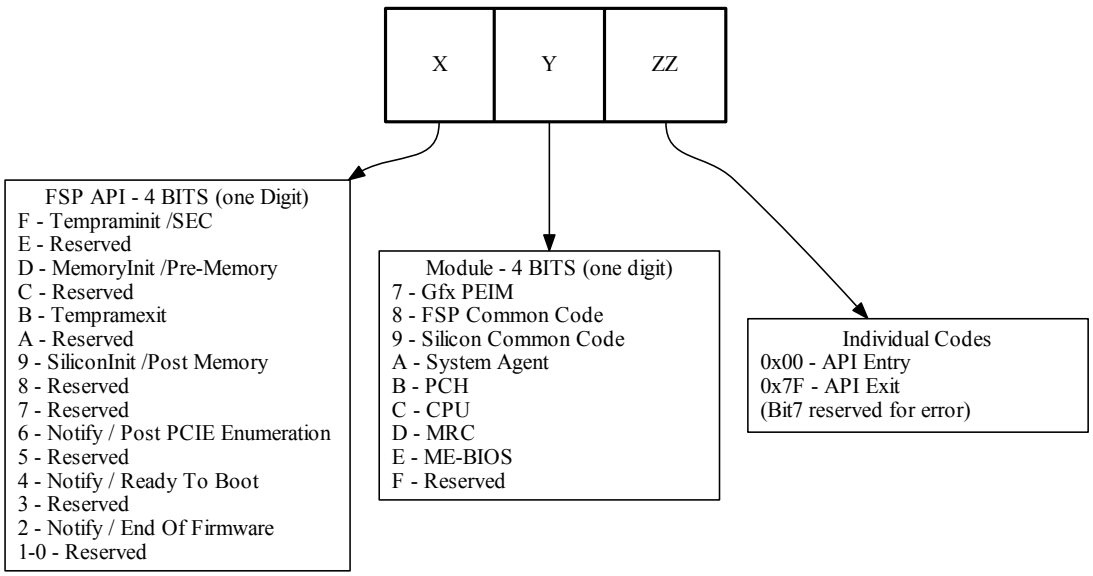
5 FSP PostCode

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

5.1 PostCode Info

Below diagram represents the 16 bit PostCode usage in FSP.



5.1.1 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

5.1.2 FspMemoryInit API Status Codes (0xDxxx)

PostCode	Module	Description
0xD800	FSP	FspMemoryInit API Entry
0xD87F	FSP	FSpMemoryInit API Exit
0xDA00	SA	Pre-Mem SaInit Entry
0xDA01	SA	DeviceConfigurePreMem Start
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
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
0xDA7F	SA	Pre-Mem SaInit Exit
0xDB00	PCH	PCH API Entry
0xDC00	CPU	Pre-Mem Entry
0xDC7F	CPU	Pre-Mem Exit

5.1.3 TempRamExit API Status Codes (0xBxxx)

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

5.1.3 FspSiliconInit API Status Codes (0x9xxx)

PostCode	Module	Description
0x9800	FSP	FspSiliconInit API Entry
0x987F	FSP	FspSiliconInit API Exit
0x9A00	SA	Post-Mem 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
0x9A10	SA	Initializing SA Overclocking
0x9A14	SA	Initializing SA SkyCam device
0x9A16	SA	Initializing SA GMM device
0x9A18	SA	Internal Device and Misc Configurations
0x9A1A	SA	SaProgramLlcWays Start
0x9A20	SA	Initializing PciExpressInitPostMem
0x9A30	SA	Initializing Vtd
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	SaPeiPolicyDump Start
0x9A6F	SA	SaSResetComplete Exit
0x9A70	SA	SaS3ResumeAtEndOfPei Callback Entry
0x9A7F	SA	SaS3ResumeAtEndOfPei Callback Exit
0x9B7F	PCH	Post-Mem ScInit Entry
0x9B01	PCH	Post-Mem Program HSIO ModPHY settings
0x9B02	PCH	Post-Mem SMBus configuration
0x9B03	PCH	Post-Mem LPC configuration
0x9B04	PCH	Post-Mem SATA initialization
0x9B05	PCH	Post-Mem PCIe initialization
0x9B06	PCH	Post-Mem xHCI initialization
0x9B07	PCH	Post-Mem xDCI initialization
0x9B08	PCH	Post-Mem HD Audio initialization
0x9B09	PCH	Post-Mem GMM configuration
0x9B0A	PCH	Post-Mem LPSS initialization
0x9B0B	PCH	Post-Mem SCS initialization
0x9B0C	PCH	Post-Mem ISH initialization
0x9B0D	PCH	Post-Mem ITSS configuration
0x9B40	PCH	Post-Mem OnEndOfPEI Entry
0x9B4F	PCH	Post-Mem OnEndOfPEI Exit
0x9B7F	PCH	Post-Mem ScInit Exit

0x9C00	CPU	Post-Mem Entry
0x9C7F	CPU	Post-Mem Exit

5.1.4 NotifyPhase API Status Codes (0x6xxx)

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

Chapter 6

Class Index

6.1 Class List

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

AUDIO_AZALIA_VERB_TABLE
Audio Azalia Verb Table structure . . . 23
AZALIA_HEADER
Azalia Header structure . . . 24
DIMM_INFO
Memory SMBIOS & OC Memory Data Hob . . . 24
FSP_M_CONFIG
Fsp M Configuration . . . 25
FSP_M_TEST_CONFIG
Fsp M Test Configuration . . . 48
FSP_S_CONFIG
Fsp S Configuration . . . 58
FSP_S_TEST_CONFIG
Fsp S Test Configuration . . . 102
FSP_T_CONFIG
Fsp T Configuration . . . 122
FSPM_UPD
Fsp M UPD Configuration . . . 123
FSPS_UPD
Fsp S UPD Configuration . . . 124
FSPT_CORE_UPD
Fsp T Core UPD . . . 125
FSPT_UPD
Fsp T UPD Configuration . . . 125
GPIO_CONFIG
GPIO configuration structure used for pin programming . . . 126
MEMORY_PLATFORM_DATA
Memory Platform Data Hob . . . 128
SI_CHIPSET_INIT_INFO
The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC . . . 128
SI_PCH_DEVICE_INTERRUPT_CONFIG
The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device . . . 129
SMBIOS_CACHE_INFO
SMBIOS Cache Info HOB Structure . . . 129
SMBIOS_PROCESSOR_INFO
SMBIOS Processor Info HOB Structure . . . 130

Chapter 7

File Index

7.1 File List

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

CpuConfigFspData.h
: FSP CPU Data Config Block . . . 133

DoxygenFspIntegrationGuide.h
: This file contains doxygen KabylakeFspIntegration Guide . . . 134

FspmUpd.h . . . 134

FspsUpd.h . . . 136

FsptUpd.h . . . 138

FspUpd.h . . . 139

GpioConfig.h
: Header file for GpioConfig structure used by GPIO library . . . 140

GpioSampleDef.h . . . 146

MemInfoHob.h
: This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs . . . 147

SmbiosCacheInfoHob.h
: Header file for SMBIOS Cache Info HOB . . . 148

SmbiosProcessorInfoHob.h
: Header file for SMBIOS Processor Info HOB . . . 149

Chapter 8

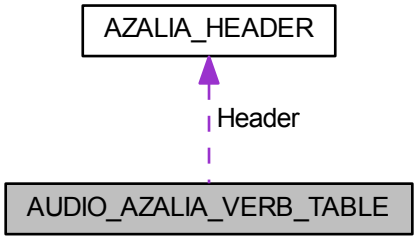
Class Documentation

8.1 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.

8.1.1 Detailed Description

Audio Azalia Verb Table structure.

Definition at line 58 of file FspsUpd.h.

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

- FspsUpd.h

8.2 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.

8.2.1 Detailed Description

Azalia Header structure.

Definition at line 46 of file FspsUpd.h.

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

- FspsUpd.h

8.3 DIMM_INFO Struct Reference

Memory SMBIOS & OC Memory Data Hob.

`#include <MemInfoHob.h>`

Public Attributes

- UINT8 Status

  See MrcDimmStatus for the definition of this field.
- UINT32 DimmCapacity

  DIMM size in MBytes.
- 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]

  Save SPD Manufacturing information needed for SMBIOS structure creation.

8.3.1 Detailed Description

Memory SMBIOS & OC Memory Data Hob.

Definition at line 188 of file MemInfoHob.h.

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

- MemInfoHob.h

8.4 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 in Memory.
- UINT32 MemorySpdPtr01

  Offset 0x004C - Memory SPD Pointer Channel 0 Dimm 1 Pointer to SPD data in Memory.
- UINT32 MemorySpdPtr10

  Offset 0x0050 - Memory SPD Pointer Channel 1 Dimm 0 Pointer to SPD data in Memory.
- UINT32 MemorySpdPtr11

  Offset 0x0054 - Memory SPD Pointer Channel 1 Dimm 1 Pointer to SPD data in Memory.
- 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 - RcompResister settings Indicates RcompReister settings: Board-dependent.
- UINT16 RcompTarget [5]

  Offset 0x0088 - RcompTarget settings RcompTarget settings: board-dependent.
- 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 MrcFastBoot

  Offset 0x0095 - MRC Fast Boot Enables/Disable the MRC fast path thru the MRC $EN_DIS.

- UINT8 UnusedUpdSpace0 [2]

  Offset 0x0096.

- UINT32 IedSize

  Offset 0x0098 - Intel Enhanced Debug Intel Enhanced Debug (IED): 0=Disabled, 0x400000=Enabled and 4MB S↩ MRAM occupied 0 : Disable, 0x400000 : Enable.

- UINT32 TsegSize

  Offset 0x009C - Tseg Size Size of SMRAM memory reserved.

- UINT16 MmioSize

  Offset 0x00A0 - MMIO Size Size of MMIO space reserved for devices.

- UINT8 ProbelessTrace

  Offset 0x00A2 - Probeless Trace Probeless Trace: 0=Disabled, 1=Enable.

- UINT8 UnusedUpdSpace1 [2]

  Offset 0x00A3.

- UINT8 SmbusEnable

  Offset 0x00A5 - Enable SMBus Enable/disable SMBus controller.

- UINT8 EnableTraceHub

  Offset 0x00A6 - Enable Trace Hub Enable/disable Trace Hub function.

- UINT8 UnusedUpdSpace2 [60]

  Offset 0x00A7.

- UINT8 IgdDvmt50PreAlloc

  Offset 0x00E3 - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.

- UINT8 InternalGfx

  Offset 0x00E4 - Internal Graphics Enable/disable internal graphics.

- UINT8 ApertureSize

  Offset 0x00E5 - Aperture Size Select the Aperture Size.

- UINT8 SaGv

  Offset 0x00E6 - SA GV System Agent dynamic frequency support and when enabled memory will be training at two different frequencies.

- UINT8 RMT

  Offset 0x00E7 - Rank Margin Tool Enable/disable Rank Margin Tool.

- UINT16 DdrFreqLimit

  Offset 0x00E8 - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.

- UINT8 UserBd

  Offset 0x00EA - 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 UnusedUpdSpace3 [105]

  Offset 0x00EB.

- UINT32 MmaTestContentPtr

  Offset 0x0154 - MMA Test Content Pointer Pointer to MMA Test Content in Memory.

- UINT32 MmaTestContentSize

  Offset 0x0158 - MMA Test Content Size Size of MMA Test Content in Memory.

- UINT32 MmaTestConfigPtr

  Offset 0x015C - MMA Test Config Pointer Pointer to MMA Test Config in Memory.

- UINT32 MmaTestConfigSize

  Offset 0x0160 - MMA Test Config Size Size of MMA Test Config in Memory.

- UINT8 UnusedUpdSpace4 [19]

  Offset 0x0164.
- UINT8 SpdProfileSelected

  Offset 0x0177 - SPD Profile Selected Select DIMM timing profile.
- UINT16 VddVoltage

  Offset 0x0178 - Memory Voltage Memory Voltage Override (Vddq).
- UINT8 RefClk

  Offset 0x017A - Memory Reference Clock Automatic, 100MHz, 133MHz.
- UINT8 Ratio

  Offset 0x017B - Memory Ratio Automatic or the frequency will equal ratio times reference clock.
- UINT8 OddRatioMode

  Offset 0x017C - QCLK Odd Ratio Adds 133 or 100 MHz to QCLK frequency, depending on RefClk $EN_DIS.
- UINT8 tCL

  Offset 0x017D - tCL CAS Latency, 0: AUTO, max: 31.
- UINT16 tFAW

  Offset 0x017E - tFAW Min Four Activate Window Delay Time, 0: AUTO, max: 63.
- UINT16 tRAS

  Offset 0x0180 - tRAS RAS Active Time, 0: AUTO, max: 64.
- UINT8 tCWL

  Offset 0x0182 - tCWL Min CAS Write Latency Delay Time, 0: AUTO, max: 20.
- UINT8 tRCDtRP

  Offset 0x0183 - tRCD/tRP RAS to CAS delay time and Row Precharge delay time, 0: AUTO, max: 63.
- UINT16 tREFI

  Offset 0x0184 - tREFI Refresh Interval, 0: AUTO, max: 65535.
- UINT16 tRFC

  Offset 0x0186 - tRFC Min Refresh Recovery Delay Time, 0: AUTO, max: 1023.
- UINT8 tRRD

  Offset 0x0188 - tRRD Min Row Active to Row Active Delay Time, 0: AUTO, max: 15.
- UINT8 tRTP

  Offset 0x0189 - tRTP Min Internal Read to Precharge Command Delay Time, 0: AUTO, max: 15.
- UINT8 tWR

  Offset 0x018A - tWR Min Write Recovery Time, 0: AUTO, legal values: 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 24 0:Auto, 5:5, 6:6, 7:7, 8:8, 10:10, 12:12, 14:14, 16:16, 18:18, 20:20, 24:24.
- UINT8 tWTR

  Offset 0x018B - tWTR Min Internal Write to Read Command Delay Time, 0: AUTO, max: 28.
- UINT8 NModeSupport

  Offset 0x018C - NMode System command rate, range 0-2, 0 means auto, 1 = 1N, 2 = 2N.
- UINT8 DllBwEn0

  Offset 0x018D - DllBwEn[0] DllBwEn[0], for 1067 (0..7)
- UINT8 DllBwEn1

  Offset 0x018E - DllBwEn[1] DllBwEn[1], for 1333 (0..7)
- UINT8 DllBwEn2

  Offset 0x018F - DllBwEn[2] DllBwEn[2], for 1600 (0..7)
- UINT8 DllBwEn3

  Offset 0x0190 - DllBwEn[3] DllBwEn[3], for 1867 and up (0..7)
- UINT8 CmdTriStateDis

  *Offset 0x0191 - Command Tristate Support Enable/Disable Command Tristate; **0: Enable**; 1: Disable.*
- UINT8 UnusedUpdSpace5 [14]

  Offset 0x0192.
- UINT32 Heci1BarAddress

  Offset 0x01A0 - HECI1 BAR address BAR address of HECI1.

- UINT32 Heci2BarAddress

  Offset 0x01A4 - HECI2 BAR address BAR address of HECI2.
- UINT32 Heci3BarAddress

  Offset 0x01A8 - HECI3 BAR address BAR address of HECI3.
- UINT8 HeciTimeouts

  Offset 0x01AC - HECI Timeouts Enable/Disable.
- UINT8 UnusedUpdSpace6 [115]

  Offset 0x01AD.
- UINT16 SgDelayAfterPwrEn

  Offset 0x0220 - SG dGPU Power Delay SG dGPU delay interval after power enabling: 0=Minimal, 1000=Maximum, default is 300=300 microseconds.
- UINT16 SgDelayAfterHoldReset

  Offset 0x0222 - SG dGPU Reset Delay SG dGPU delay interval for Reset complete: 0=Minimal, 1000=Maximum, default is 100=100 microseconds.
- UINT16 MmioSizeAdjustment

  Offset 0x0224 - 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 0x0226 - Enable/Disable DMI GEN3 Static EQ Phase1 programming Program DMI Gen3 EQ Phase1 Static Presets.
- UINT8 Peg0Enable

  Offset 0x0227 - 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 0x0228 - 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 0x0229 - 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 Peg0MaxLinkSpeed

  Offset 0x022A - 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 0x022B - 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 0x022C - 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 Peg0MaxLinkWidth

  Offset 0x022D - 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 0x022E - 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 0x022F - 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 Peg0PowerDownUnusedLanes

Offset 0x0230 - 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 0x0231 - 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 0x0232 - 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 InitPcieAspmAfterOprom

  Offset 0x0233 - 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 0x0234 - PCIe Disable Spread Spectrum Clocking PCIe Disable Spread Spectrum Clocking.

- UINT8 DmiGen3RootPortPreset [4]

  Offset 0x0235 - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.

- UINT8 DmiGen3EndPointPreset [4]

  Offset 0x0239 - DMI Gen3 End port preset values per lane Used for programming DMI Gen3 preset values per lane.

- UINT8 DmiGen3EndPointHint [4]

  Offset 0x023D - DMI Gen3 End port Hint values per lane Used for programming DMI Gen3 Hint values per lane.

- UINT8 DmiGen3RxCtlePeaking [2]

  Offset 0x0241 - DMI Gen3 RxCTLEp per-Bundle control Range: 0-15, 3 is default for each bundle, must be specified based upon platform design.

- UINT8 DmiDeEmphasis

  Offset 0x0243 - DeEmphasis control for DMI DeEmphasis control for DMI.

- UINT8 PegGen3RxCtlePeaking [8]

  Offset 0x0244 - PEG Gen3 RxCTLEp per-Bundle control Range: 0-15, 12 is default for each bundle, must be specified based upon platform design.

- UINT32 PegDataPtr

  Offset 0x024C - 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 [16]

  Offset 0x0250 - 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 UnusedUpdSpace7 [1]

  Offset 0x0260.

- UINT8 PegRootPortHPE [3]

  Offset 0x0261 - PCIe Hot Plug Enable/Disable per port 0(Default): Disable, 1: Enable.

- UINT32 GttMmAdr

  Offset 0x0264 - Temporary MMIO address for GTTMMADR The reference code will use the information in this structure in order to reset PCIe Gen3 devices during equalization, if necessary.

- UINT16 GttSize

  Offset 0x0268 - Selection of iGFX GTT Memory size 1=2MB, 2=4MB, 3=8MB, Default is 3 1:2MB, 2:4MB, 3:8MB.

- UINT8 PrimaryDisplay

  Offset 0x026A - 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.

- UINT8 SaRtd3Pcie0Gpio [24]

  Offset 0x026B - Switchable Graphics GPIO information for PEG 0 Switchable Graphics GPIO information for PEG 0, for Reset, power and wake GPIOs.

- UINT8 SaRtd3Pcie1Gpio [24]

  Offset 0x0283 - Switchable Graphics GPIO information for PEG 1 Switchable Graphics GPIO information for PEG 1, for Reset, power and wake GPIOs.

- UINT8 SaRtd3Pcie2Gpio [24]

Offset 0x029B - Switchable Graphics GPIO information for PEG 2 Switchable Graphics GPIO information for PEG 2, for Reset, power and wake GPIOs.

- UINT8 RootPortDev

  Offset 0x02B3 - PEG root port Device number for Switchable Graphics dGPU Device number to indicate which PEG root port has dGPU.

- UINT8 RootPortFun

  Offset 0x02B4 - PEG root port Function number for Switchable Graphics dGPU Function number to indicate which PEG root port has dGPU.

- UINT8 TxtImplemented

  Offset 0x02B5 - Enable/Disable MRC TXT dependency When enabled MRC execution will wait for TXT initialization to be done first.

- UINT8 SaOcSupport

  Offset 0x02B6 - Enable/Disable SA OcSupport Enable: Enable SA OcSupport, Disable(Default): Disable SA Oc↩ Support $EN_DIS.

- UINT8 GtsVoltageMode

  Offset 0x02B7 - GT slice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.

- UINT8 GtusVoltageMode

  Offset 0x02B8 - GT unslice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.

- UINT8 GtsMaxOcRatio

  Offset 0x02B9 - Maximum GTs turbo ratio override 0(Default)=Minimal/Auto, 60=Maximum.

- UINT16 GtsVoltageOffset

  Offset 0x02BA - The voltage offset applied to GT slice 0(Default)=Minimal, 1000=Maximum.

- UINT16 GtsVoltageOverride

  Offset 0x02BC - The GT slice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtsExtraTurboVoltage

  Offset 0x02BE - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtusVoltageOffset

  Offset 0x02C0 - voltage offset applied to GT unslice 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtusVoltageOverride

  Offset 0x02C2 - GT unslice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 GtusExtraTurboVoltage

  Offset 0x02C4 - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.

- UINT16 SaVoltageOffset

  Offset 0x02C6 - voltage offset applied to the SA 0(Default)=Minimal, 1000=Maximum.

- UINT8 EdramRatio

  Offset 0x02C8 - EDRAM ratio override EdramRatio is deprecated on Kabylake.

- UINT8 GtusMaxOcRatio

  Offset 0x02C9 - Maximum GTus turbo ratio override 0(Default)=Minimal, 60=Maximum.

- UINT8 BistOnReset

  *Offset 0x02CA - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.*

- UINT8 SkipStopPbet

  *Offset 0x02CB - Skip Stop PBET Timer Enable/Disable Skip Stop PBET Timer; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 EnableC6Dram

  Offset 0x02CC - C6DRAM power gating feature This feature is not supported.

- UINT8 OcSupport

  *Offset 0x02CD - Over clocking support Over clocking support; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 OcLock

  *Offset 0x02CE - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.*

- UINT8 CoreMaxOcRatio

Offset 0x02CF - 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 0x02D0 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.*
- UINT8 RingMinOcRatio

  Offset 0x02D1 - Minimum clr turbo ratio override Minimum clr turbo ratio override.
- UINT8 RingMaxOcRatio

  Offset 0x02D2 - 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 0x02D3 - Hyper Threading Enable/Disable Enable or Disable Hyper Threading; 0: Disable; **1: Enable** $EN↩ _DIS.*
- UINT8 CpuRatioOverride

  *Offset 0x02D4 - Enable or Disable CPU Ratio Override Enable or Disable CPU Ratio Override; **0: Disable**; 1: Enable.*
- UINT8 CpuRatio

  Offset 0x02D5 - CPU ratio value CPU ratio value.
- UINT8 BootFrequency

  Offset 0x02D6 - Boot frequency Sets the boot frequency starting from reset vector.
- UINT8 ActiveCoreCount

  Offset 0x02D7 - Number of active cores Number of active cores(Depends on Number of cores).
- UINT8 FClkFrequency

  *Offset 0x02D8 - Processor Early Power On Configuration FCLK setting **0: 800 MHz (ULT/ULX)**.*
- UINT8 JtagC10PowerGateDisable

  *Offset 0x02D9 - Power JTAG in C10 and deeper power states Power JTAG in C10 and deeper power states; **0: Disable**; 1: Enable.*
- UINT8 VmxEnable

  *Offset 0x02DA - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.*
- UINT8 Avx2RatioOffset

  Offset 0x02DB - AVX2 Ratio Offset 0(Default)= No Offset.
- UINT16 CoreVoltageOverride

  Offset 0x02DC - core voltage override The core voltage override which is applied to the entire range of cpu core frequencies.
- UINT16 CoreVoltageAdaptive

  Offset 0x02DE - Core Turbo voltage Adaptive Extra Turbo voltage applied to the cpu core when the cpu is operating in turbo mode.
- UINT16 CoreVoltageOffset

  Offset 0x02E0 - Core Turbo voltage Offset The voltage offset applied to the core while operating in turbo mode.Valid Range 0 to 1000.
- UINT8 CorePllVoltageOffset

  Offset 0x02E2 - Core PLL voltage offset Core PLL voltage offset.
- UINT8 RingDownBin

  Offset 0x02E3 - Ring Downbin Ring Downbin enable/disable.
- UINT8 BclkAdaptiveVoltage

  Offset 0x02E4 - BCLK Adaptive Voltage Enable When enabled, the CPU V/F curves are aware of BCLK frequency when calculated.
- UINT8 BiosGuard

  Offset 0x02E5 - BiosGuard Enable/Disable.
- UINT8 EnableSgx

  Offset 0x02E6 - EnableSgx Enable/Disable.
- UINT8 Txt

  Offset 0x02E7 - Txt Enable/Disable.
- UINT32 PrmrrSize

Offset 0x02E8 - PrmrrSize Enable/Disable.

- UINT32 SinitMemorySize

  Offset 0x02EC - SinitMemorySize Enable/Disable.

- UINT64 TxtDprMemoryBase

  Offset 0x02F0 - TxtDprMemoryBase Enable/Disable.

- UINT32 TxtDprMemorySize

  Offset 0x02F8 - TxtDprMemorySize Enable/Disable.

- UINT32 TxtHeapMemorySize

  Offset 0x02FC - TxtHeapMemorySize Enable/Disable.

- UINT8 FlashWearOutProtection

  Offset 0x0300 - FlashWearOutProtection Enable/Disable.

- UINT8 TvbRatioClipping

  Offset 0x0301 - Thermal Velocity Boost Ratio clipping 0(Default): Disabled, 1: Enabled.

- UINT8 TvbVoltageOptimization

  Offset 0x0302 - Thermal Velocity Boost voltage optimization 0: Disabled, 1: Enabled(Default).

- UINT8 ReservedSecurityPreMem [7]

  Offset 0x0303 - ReservedSecurityPreMem Reserved for Security Pre-Mem $EN_DIS.

- UINT8 PchHpetEnable

  Offset 0x030A - PCH HPET Enabled Enable/disable PCH HPET.

- UINT8 PchHpetBdfValid

  Offset 0x030B - PCH HPET BDF valid Whether the BDF value is valid.

- UINT32 PchHpetBase

  Offset 0x030C - The HPET Base Address The HPET base address.

- UINT8 PchHpetBusNumber

  Offset 0x0310 - PCH HPET Bus Number Bus Number HPETn used as Requestor / Completer ID.

- UINT8 PchHpetDeviceNumber

  Offset 0x0311 - PCH HPET Device Number Device Number HPETn used as Requestor / Completer ID.

- UINT8 PchHpetFunctionNumber

  Offset 0x0312 - PCH HPET Function Number Function Number HPETn used as Requestor / Completer ID.

- UINT8 PchPcieHsioRxSetCtleEnable [24]

  Offset 0x0313 - Enable PCH HSIO PCIE Rx Set Ctle Enable PCH PCIe Gen 3 Set CTLE Value.

- UINT8 PchPcieHsioRxSetCtle [24]

  Offset 0x032B - PCH HSIO PCIE Rx Set Ctle Value PCH PCIe Gen 3 Set CTLE Value.

- UINT8 PchPcieHsioTxGen1DownscaleAmpEnable [24]

  Offset 0x0343 - Enble PCH HSIO PCIE TX Gen 1 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen1DownscaleAmp [24]

  Offset 0x035B - 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 0x0373 - Enable PCH HSIO PCIE TX Gen 2 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DownscaleAmp [24]

  Offset 0x038B - 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 0x03A3 - Enable PCH HSIO PCIE TX Gen 3 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen3DownscaleAmp [24]

  Offset 0x03BB - 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 0x03D3 - Enable PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen1DeEmph [24]

  Offset 0x03EB - 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 0x0403 - Enable PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DeEmph3p5 [24]

  Offset 0x041B - 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 0x0433 - Enable PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchPcieHsioTxGen2DeEmph6p0 [24]

  Offset 0x044B - 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 0x0463 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioRxGen1EqBoostMag [8]

  Offset 0x046B - 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 0x0473 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioRxGen2EqBoostMag [8]

  Offset 0x047B - 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 0x0483 - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioRxGen3EqBoostMag [8]

  Offset 0x048B - 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 0x0493 - Enable PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen1DownscaleAmp [8]

  Offset 0x049B - 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 0x04A3 - Enable PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen2DownscaleAmp [8]

  Offset 0x04AB - 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 0x04B3 - Enable PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen3DownscaleAmp [8]

  Offset 0x04BB - 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 0x04C3 - Enable PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.

- UINT8 PchSataHsioTxGen1DeEmph [8]

  Offset 0x04CB - 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 0x04D3 - Enable PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
- UINT8 PchSataHsioTxGen2DeEmph [8]

  Offset 0x04DB - 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 0x04E3 - Enable PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
- UINT8 PchSataHsioTxGen3DeEmph [8]

  Offset 0x04EB - 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 0x04F3 - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.
- UINT16 PchAcpiBase

  Offset 0x04F4 - PCH Acpi Base Power management I/O base address.
- UINT8 PchPort80Route

  Offset 0x04F6 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.
- UINT8 SmbusArpEnable

  Offset 0x04F7 - Enable SMBus ARP support Enable SMBus ARP support.
- UINT16 PchSmbusIoBase

  Offset 0x04F8 - SMBUS Base Address SMBUS Base Address (IO space).
- UINT8 PchNumRsvdSmbusAddresses

  Offset 0x04FA - Number of RsvdSmbusAddressTable.
- UINT8 UnusedUpdSpace8

  Offset 0x04FB.
- UINT32 RsvdSmbusAddressTablePtr

  Offset 0x04FC - Point of RsvdSmbusAddressTable Array of addresses reserved for non-ARP-capable SMBus devices.
- UINT32 TraceHubMemReg0Size

  Offset 0x0500 - Trace Hub Memory Region 0 Trace Hub Memory Region 0.
- UINT32 TraceHubMemReg1Size

  Offset 0x0504 - Trace Hub Memory Region 1 Trace Hub Memory Region 1.
- UINT32 PcieRpEnableMask

  Offset 0x0508 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.
- UINT8 PcdDebugInterfaceFlags

  Offset 0x050C - Debug Interfaces Debug Interfaces.
- UINT8 PcdSerialIoUartNumber

  Offset 0x050D - SerialIo Uart Number Selection Select SerialIo Uart Controller for debug.
- UINT8 PcdIsaSerialUartBase

  Offset 0x050E - ISA Serial Base selection Select ISA Serial Base address.
- UINT8 PchPmPciePllSsc

  Offset 0x050F - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.
- UINT8 PeciC10Reset

  Offset 0x0510 - Enable or Disable Peci C10 Reset command Enable or Disable Peci C10 Reset command; ***0: Disable;*** *1: Enable.*
- UINT8 PeciSxReset

Offset 0x0511 - Enable or Disable Peci Sx Reset command Enable or Disable Peci Sx Reset command; ***0: Disable;*** *1: Enable.*

- UINT8 PcdSerialDebugBaudRate

  Offset 0x0512 - PcdSerialDebugBaudRate Baud Rate for Serial Debug Messages.

- UINT8 PcdSerialDebugLevel

  Offset 0x0513 - PcdSerialDebugLevel Serial Debug Message Level.

- UINT8 EvLoader

  Offset 0x0514 - Enable or Disable EV Loader Enable or Disable EV Loader; ***0: Disable;*** *1: Enable.*

- UINT8 GtPllVoltageOffset

  Offset 0x0515 - GT PLL voltage offset Core PLL voltage offset.

- UINT8 RingPllVoltageOffset

  Offset 0x0516 - Ring PLL voltage offset Core PLL voltage offset.

- UINT8 SaPllVoltageOffset

  Offset 0x0517 - System Agent PLL voltage offset Core PLL voltage offset.

- UINT8 McPllVoltageOffset

  Offset 0x0518 - Memory Controller PLL voltage offset Core PLL voltage offset.

- UINT8 RealtimeMemoryTiming

  Offset 0x0519 - Realtime Memory Timing 0(Default): Disabled, 1: Enabled.

- UINT8 Avx3RatioOffset

  Offset 0x051A - AVX3 Ratio Offset 0(Default)= No Offset.

- UINT8 CleanMemory

  Offset 0x051B - Ask MRC to clear memory content Ask MRC to clear memory content ***0: Do not Clear Memory;*** *1: Clear Memory.*

- UINT8 TjMaxOffset

  Offset 0x051C - TjMax Offset TjMax offset.

- UINT8 ReservedFspmUpd [3]

  Offset 0x051D.

8.4.1 Detailed Description

Fsp M Configuration.

Definition at line 57 of file FspmUpd.h.

8.4.2 Member Data Documentation

8.4.2.1 UINT8 FSP_M_CONFIG::ActiveCoreCount

Offset 0x02D7 - 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 797 of file FspmUpd.h.

8.4.2.2 UINT8 FSP_M_CONFIG::ApertureSize

Offset 0x00E5 - Aperture Size Select the Aperture Size.

0:128 MB, 1:256 MB, 2:512 MB

Definition at line 209 of file FspmUpd.h.

8.4.2.3 UINT8 FSP_M_CONFIG::Avx2RatioOffset

Offset 0x02DB - 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 822 of file FspmUpd.h.

8.4.2.4 UINT8 FSP_M_CONFIG::Avx3RatioOffset

Offset 0x051A - 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 1272 of file FspmUpd.h.

8.4.2.5 UINT8 FSP_M_CONFIG::BclkAdaptiveVoltage

Offset 0x02E4 - 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 858 of file FspmUpd.h.

8.4.2.6 UINT8 FSP_M_CONFIG::BiosGuard

Offset 0x02E5 - BiosGuard Enable/Disable.

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

Definition at line 864 of file FspmUpd.h.

8.4.2.7 UINT8 FSP_M_CONFIG::BistOnReset

Offset 0x02CA - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 717 of file FspmUpd.h.

8.4.2.8 UINT8 FSP_M_CONFIG::BootFrequency

Offset 0x02D6 - 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 790 of file FspmUpd.h.

8.4.2.9 UINT8 FSP_M_CONFIG::CleanMemory

Offset 0x051B - 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 1278 of file FspmUpd.h.

8.4.2.10 UINT8 FSP_M_CONFIG::CmdTriStateDis

Offset 0x0191 - Command Tristate Support Enable/Disable Command Tristate; **0: Enable**; 1: Disable.

$EN_DIS

Definition at line 387 of file FspmUpd.h.

8.4.2.11 UINT8 FSP_M_CONFIG::CoreMaxOcRatio

Offset 0x02CF - 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 747 of file FspmUpd.h.

8.4.2.12 UINT8 FSP_M_CONFIG::CorePllVoltageOffset

Offset 0x02E2 - Core PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 844 of file FspmUpd.h.

8.4.2.13 UINT16 FSP_M_CONFIG::CoreVoltageAdaptive

Offset 0x02DE - 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 834 of file FspmUpd.h.

8.4.2.14 UINT8 FSP_M_CONFIG::CoreVoltageMode

Offset 0x02D0 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.

$EN_DIS

Definition at line 753 of file FspmUpd.h.

8.4.2.15 UINT16 FSP_M_CONFIG::CoreVoltageOverride

Offset 0x02DC - 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 828 of file FspmUpd.h.

8.4.2.16 UINT8 FSP_M_CONFIG::CpuRatio

Offset 0x02D5 - CPU ratio value CPU ratio value.

Valid Range 0 to 63

Definition at line 782 of file FspmUpd.h.

8.4.2.17 UINT8 FSP_M_CONFIG::CpuRatioOverride

Offset 0x02D4 - Enable or Disable CPU Ratio Override Enable or Disable CPU Ratio Override; **0: Disable**; 1: Enable.

Note

If disabled, BIOS will use the default max non-turbo ratio, and will not use any flex ratio setting. $EN_DIS

Definition at line 777 of file FspmUpd.h.

8.4.2.18 UINT16 FSP_M_CONFIG::DdrFreqLimit

Offset 0x00E8 - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.

Options are 1067, 1333, 1600, 1867, 2133, 2400 and 0 for Auto. 1067:1067, 1333:1333, 1600:1600, 1867:1867, 2133:2133, 2400:2400, 0:Auto

Definition at line 230 of file FspmUpd.h.

8.4.2.19 UINT8 FSP_M_CONFIG::DmiDeEmphasis

Offset 0x0243 - DeEmphasis control for DMI DeEmphasis control for DMI.

0=-6dB, 1(Default)=-3.5 dB 0: -6dB, 1: -3.5dB

Definition at line 566 of file FspmUpd.h.

8.4.2.20 UINT8 FSP_M_CONFIG::DmiGen3EndPointHint[4]

Offset 0x023D - 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 555 of file FspmUpd.h.

8.4.2.21 UINT8 FSP_M_CONFIG::DmiGen3EndPointPreset[4]

Offset 0x0239 - 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 550 of file FspmUpd.h.

8.4.2.22 UINT8 FSP_M_CONFIG::DmiGen3ProgramStaticEq

Offset 0x0226 - 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 441 of file FspmUpd.h.

8.4.2.23 UINT8 FSP_M_CONFIG::DmiGen3RootPortPreset[4]

Offset 0x0235 - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.

Range: 0-9, 4 is default for each lane

Definition at line 545 of file FspmUpd.h.

8.4.2.24 UINT8 FSP_M_CONFIG::EnableC6Dram

Offset 0x02CC - C6DRAM power gating feature This feature is not supported.

BIOS is required to disable. **0: Disable** $EN_DIS

Definition at line 729 of file FspmUpd.h.

8.4.2.25 UINT8 FSP_M_CONFIG::EnableSgx

Offset 0x02E6 - EnableSgx Enable/Disable.

0: Disable, Enable/Disable SGX feature, 1: enable $EN_DIS

Definition at line 870 of file FspmUpd.h.

8.4.2.26 UINT8 FSP_M_CONFIG::EnableTraceHub

Offset 0x00A6 - Enable Trace Hub Enable/disable Trace Hub function.

$EN_DIS

Definition at line 187 of file FspmUpd.h.

8.4.2.27 UINT8 FSP_M_CONFIG::EvLoader

Offset 0x0514 - Enable or Disable EV Loader Enable or Disable EV Loader; **0: Disable;** 1: Enable.

$EN_DIS

Definition at line 1235 of file FspmUpd.h.

8.4.2.28 UINT8 FSP_M_CONFIG::FClkFrequency

Offset 0x02D8 - 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 804 of file FspmUpd.h.

8.4.2.29 UINT8 FSP_M_CONFIG::FlashWearOutProtection

Offset 0x0300 - FlashWearOutProtection Enable/Disable.

0: Disable, Enable/Disable FlashWearOutProtection feature, 1: enable $EN_DIS

Definition at line 907 of file FspmUpd.h.

8.4.2.30 UINT8 FSP_M_CONFIG::GtPllVoltageOffset

Offset 0x0515 - GT PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63 0x0:0xFF

Definition at line 1241 of file FspmUpd.h.

8.4.2.31 UINT8 FSP_M_CONFIG::HeciTimeouts

Offset 0x01AC - HECI Timeouts Enable/Disable.

0: Disable, disable timeout check for HECI, 1: enable $EN_DIS

Definition at line 412 of file FspmUpd.h.

8.4.2.32 UINT8 FSP_M_CONFIG::IgdDvmt50PreAlloc

Offset 0x00E3 - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.

0x00:0 MB, 0x01:32 MB, 0x02:64 MB

Definition at line 197 of file FspmUpd.h.

8.4.2.33 UINT8 FSP_M_CONFIG::InitPcieAspmAfterOprom

Offset 0x0233 - 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 533 of file FspmUpd.h.

8.4.2.34 UINT8 FSP_M_CONFIG::InternalGfx

Offset 0x00E4 - Internal Graphics Enable/disable internal graphics.

$EN_DIS

Definition at line 203 of file FspmUpd.h.

8.4.2.35 UINT8 FSP_M_CONFIG::JtagC10PowerGateDisable

Offset 0x02D9 - Power JTAG in C10 and deeper power states Power JTAG in C10 and deeper power states; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 810 of file FspmUpd.h.

8.4.2.36 UINT8 FSP_M_CONFIG::McPllVoltageOffset

Offset 0x0518 - Memory Controller PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63 0x0:0xFF

Definition at line 1259 of file FspmUpd.h.

8.4.2.37 UINT16 FSP_M_CONFIG::MmioSize

Offset 0x00A0 - MMIO Size Size of MMIO space reserved for devices.

0(Default)=Auto, non-Zero=size in MB

Definition at line 164 of file FspmUpd.h.

8.4.2.38 UINT8 FSP_M_CONFIG::OcLock

Offset 0x02CE - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 741 of file FspmUpd.h.

8.4.2.39 UINT8 FSP_M_CONFIG::PcdDebugInterfaceFlags

Offset 0x050C - Debug Interfaces Debug Interfaces.

BIT0-RAM, BIT1-UART, BIT3-USB3, BIT4-Serial IO, BIT5-TraceHub, BIT2 - Not used.

Definition at line 1184 of file FspmUpd.h.

8.4.2.40 UINT8 FSP_M_CONFIG::PcdIsaSerialUartBase

Offset 0x050E - ISA Serial Base selection Select ISA Serial Base address.

Default is 0x3F8. 0:0x3F8, 1:0x2F8

Definition at line 1196 of file FspmUpd.h.

8.4.2.41 UINT8 FSP_M_CONFIG::PcdSerialDebugBaudRate

Offset 0x0512 - 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 1220 of file FspmUpd.h.

8.4.2.42 UINT8 FSP_M_CONFIG::PcdSerialDebugLevel

Offset 0x0513 - 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 1229 of file FspmUpd.h.

8.4.2.43 UINT8 FSP_M_CONFIG::PcdSerialIoUartNumber

Offset 0x050D - SerialIo Uart Number Selection Select SerialIo Uart Controller for debug.

0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 1190 of file FspmUpd.h.

8.4.2.44 UINT16 FSP_M_CONFIG::PchAcpiBase

Offset 0x04F4 - PCH Acpi Base Power management I/O base address.

Default is 0x1800.

Definition at line 1131 of file FspmUpd.h.

8.4.2.45 UINT32 FSP_M_CONFIG::PchHpetBase

Offset 0x030C - The HPET Base Address The HPET base address.

Default is 0xFED00000.

Definition at line 945 of file FspmUpd.h.

8.4.2.46 UINT8 FSP_M_CONFIG::PchHpetBdfValid

Offset 0x030B - PCH HPET BDF valid Whether the BDF value is valid.

0: Disable; 1: Enable. $EN_DIS

Definition at line 940 of file FspmUpd.h.

8.4.2.47 UINT8 FSP_M_CONFIG::PchHpetBusNumber

Offset 0x0310 - PCH HPET Bus Number Bus Number HPETn used as Requestor / Completer ID.

Default is 0xF0.

Definition at line 950 of file FspmUpd.h.

8.4.2.48 UINT8 FSP_M_CONFIG::PchHpetDeviceNumber

Offset 0x0311 - PCH HPET Device Number Device Number HPETn used as Requestor / Completer ID.

Default is 0x1F.

Definition at line 955 of file FspmUpd.h.

8.4.2.49 UINT8 FSP_M_CONFIG::PchHpetEnable

Offset 0x030A - PCH HPET Enabled Enable/disable PCH HPET.

$EN_DIS

Definition at line 934 of file FspmUpd.h.

8.4.2.50 UINT8 FSP_M_CONFIG::PchHpetFunctionNumber

Offset 0x0312 - PCH HPET Function Number Function Number HPETn used as Requestor / Completer ID.

Default is 0x00.

Definition at line 960 of file FspmUpd.h.

8.4.2.51 UINT8 FSP_M_CONFIG::PchLpcEnhancePort8xhDecoding

Offset 0x04F3 - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.

$EN_DIS

Definition at line 1126 of file FspmUpd.h.

8.4.2.52 UINT8 FSP_M_CONFIG::PchNumRsvdSmbusAddresses

Offset 0x04FA - Number of RsvdSmbusAddressTable.

The number of elements in the RsvdSmbusAddressTable.

Definition at line 1153 of file FspmUpd.h.

8.4.2.53 UINT8 FSP_M_CONFIG::PchPmPciePllSsc

Offset 0x050F - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.

The default is 0xFF: AUTO - No BIOS override.

Definition at line 1202 of file FspmUpd.h.

8.4.2.54 UINT8 FSP_M_CONFIG::PchPort80Route

Offset 0x04F6 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.

$EN_DIS

Definition at line 1137 of file FspmUpd.h.

8.4.2.55 UINT32 FSP_M_CONFIG::PcieRpEnableMask

Offset 0x0508 - 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 1178 of file FspmUpd.h.

8.4.2.56 UINT8 FSP_M_CONFIG::PeciC10Reset

Offset 0x0510 - Enable or Disable Peci C10 Reset command Enable or Disable Peci C10 Reset command; **0: Disable;** 1: Enable.

$EN_DIS

Definition at line 1208 of file FspmUpd.h.

8.4.2.57 UINT8 FSP_M_CONFIG::PeciSxReset

Offset 0x0511 - Enable or Disable Peci Sx Reset command Enable or Disable Peci Sx Reset command; **0: Disable;** 1: Enable.

$EN_DIS

Definition at line 1214 of file FspmUpd.h.

8.4.2.58 UINT32 FSP_M_CONFIG::PegDataPtr

Offset 0x024C - 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 578 of file FspmUpd.h.

8.4.2.59 UINT8 FSP_M_CONFIG::PegDisableSpreadSpectrumClocking

Offset 0x0234 - 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 540 of file FspmUpd.h.

8.4.2.60 UINT32 FSP_M_CONFIG::PrmrrSize

Offset 0x02E8 - PrmrrSize Enable/Disable.

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

Definition at line 881 of file FspmUpd.h.

8.4.2.61 UINT8 FSP_M_CONFIG::ProbelessTrace

Offset 0x00A2 - 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 171 of file FspmUpd.h.

8.4.2.62 UINT8 FSP_M_CONFIG::Ratio

Offset 0x017B - 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 293 of file FspmUpd.h.

8.4.2.63 UINT8 FSP_M_CONFIG::RealtimeMemoryTiming

Offset 0x0519 - 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 1266 of file FspmUpd.h.

8.4.2.64 UINT8 FSP_M_CONFIG::RefClk

Offset 0x017A - Memory Reference Clock Automatic, 100MHz, 133MHz.

0:Auto, 1:133MHz, 2:100MHz

Definition at line 286 of file FspmUpd.h.

8.4.2.65 UINT8 FSP_M_CONFIG::RingDownBin

Offset 0x02E3 - 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 851 of file FspmUpd.h.

8.4.2.66 UINT8 FSP_M_CONFIG::RingMaxOcRatio

Offset 0x02D2 - 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 764 of file FspmUpd.h.

8.4.2.67 UINT8 FSP_M_CONFIG::RingMinOcRatio

Offset 0x02D1 - Minimum clr turbo ratio override Minimum clr turbo ratio override.

0: Hardware defaults. Range: 0-255

Definition at line 758 of file FspmUpd.h.

8.4.2.68 UINT8 FSP_M_CONFIG::RingPllVoltageOffset

Offset 0x0516 - Ring PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63 0x0:0xFF

Definition at line 1247 of file FspmUpd.h.

8.4.2.69 UINT8 FSP_M_CONFIG::RMT

Offset 0x00E7 - Rank Margin Tool Enable/disable Rank Margin Tool.

$EN_DIS

Definition at line 223 of file FspmUpd.h.

8.4.2.70 UINT8 FSP_M_CONFIG::SaGv

Offset 0x00E6 - 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 217 of file FspmUpd.h.

8.4.2.71 UINT8 FSP_M_CONFIG::SaPllVoltageOffset

Offset 0x0517 - System Agent PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63 0x0:0xFF

Definition at line 1253 of file FspmUpd.h.

8.4.2.72 UINT32 FSP_M_CONFIG::SinitMemorySize

Offset 0x02EC - SinitMemorySize Enable/Disable.

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

Definition at line 886 of file FspmUpd.h.

8.4.2.73 UINT8 FSP_M_CONFIG::SmbusArpEnable

Offset 0x04F7 - Enable SMBus ARP support Enable SMBus ARP support.

$EN_DIS

Definition at line 1143 of file FspmUpd.h.

8.4.2.74 UINT8 FSP_M_CONFIG::SmbusEnable

Offset 0x00A5 - Enable SMBus Enable/disable SMBus controller.

$EN_DIS

Definition at line 181 of file FspmUpd.h.

8.4.2.75 UINT8 FSP_M_CONFIG::SpdProfileSelected

Offset 0x0177 - 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 272 of file FspmUpd.h.

8.4.2.76 UINT8 FSP_M_CONFIG::TjMaxOffset

Offset 0x051C - 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 0 - 63

Definition at line 1284 of file FspmUpd.h.

8.4.2.77 UINT8 FSP_M_CONFIG::tRTP

Offset 0x0189 - 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 345 of file FspmUpd.h.

8.4.2.78 UINT32 FSP_M_CONFIG::TsegSize

Offset 0x009C - Tseg Size Size of SMRAM memory reserved.

0x400000 for Release build and 0x1000000 for Debug build 0x0400000:4MB, 0x01000000:16MB

Definition at line 159 of file FspmUpd.h.

8.4.2.79 UINT8 FSP_M_CONFIG::TvbRatioClipping

Offset 0x0301 - 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 915 of file FspmUpd.h.

8.4.2.80 UINT8 FSP_M_CONFIG::TvbVoltageOptimization

Offset 0x0302 - 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 922 of file FspmUpd.h.

8.4.2.81 UINT8 FSP_M_CONFIG::Txt

Offset 0x02E7 - Txt Enable/Disable.

0: Disable, Enable/Disable Txt feature, 1: enable $EN_DIS

Definition at line 876 of file FspmUpd.h.

8.4.2.82 UINT64 FSP_M_CONFIG::TxtDprMemoryBase

Offset 0x02F0 - TxtDprMemoryBase Enable/Disable.

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

Definition at line 891 of file FspmUpd.h.

8.4.2.83 UINT32 FSP_M_CONFIG::TxtDprMemorySize

Offset 0x02F8 - TxtDprMemorySize Enable/Disable.

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

Definition at line 896 of file FspmUpd.h.

8.4.2.84 UINT32 FSP_M_CONFIG::TxtHeapMemorySize

Offset 0x02FC - TxtHeapMemorySize Enable/Disable.

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

Definition at line 901 of file FspmUpd.h.

8.4.2.85 UINT8 FSP_M_CONFIG::TxtImplemented

Offset 0x02B5 - 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 643 of file FspmUpd.h.

8.4.2.86 UINT16 FSP_M_CONFIG::VddVoltage

Offset 0x0178 - Memory Voltage Memory Voltage Override (Vddq).

Default = no override 0:Default, 1100:1.10 Volts, 1150:1.15 Volts, 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 280 of file FspmUpd.h.

8.4.2.87 UINT8 FSP_M_CONFIG::VmxEnable

Offset 0x02DA - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 816 of file FspmUpd.h.

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

- FspmUpd.h

8.5 FSP_M_TEST_CONFIG Struct Reference

Fsp M Test Configuration.

`#include <FspmUpd.h>`

Public Attributes

- UINT32 Signature

  Offset 0x0520.
- UINT8 SkipExtGfxScan

  Offset 0x0524 - Skip external display device scanning Enable: Do not scan for external display device, Disable (Default): Scan external display devices $EN_DIS.
- UINT8 BdatEnable

  Offset 0x0525 - Generate BIOS Data ACPI Table Enable: Generate BDAT for MRC RMT or SA PCIe data.
- UINT8 ScanExtGfxForLegacyOpRom

  Offset 0x0526 - 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 0x0527 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.
- UINT8 DmiVc1

  Offset 0x0528 - Enable/Disable DmiVc1 Enable/Disable DmiVc1.
- UINT8 DmiVcm

  Offset 0x0529 - Enable/Disable DmiVcm Enable/Disable DmiVcm.
- UINT8 DmiMaxLinkSpeed

  Offset 0x052A - 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 0x052B - DMI Equalization Phase 2 DMI Equalization Phase 2.
- UINT8 DmiGen3EqPh3Method

  Offset 0x052C - DMI Gen3 Equalization Phase3 DMI Gen3 Equalization Phase3.
- UINT8 Peg0Gen3EqPh2Enable

  Offset 0x052D - Phase2 EQ enable on the PEG 0:1:0.
- UINT8 Peg1Gen3EqPh2Enable

  Offset 0x052E - Phase2 EQ enable on the PEG 0:1:1.
- UINT8 Peg2Gen3EqPh2Enable

  Offset 0x052F - Phase2 EQ enable on the PEG 0:1:2.
- UINT8 Peg0Gen3EqPh3Method

  Offset 0x0530 - Phase3 EQ method on the PEG 0:1:0.
- UINT8 Peg1Gen3EqPh3Method

  Offset 0x0531 - Phase3 EQ method on the PEG 0:1:1.

- UINT8 Peg2Gen3EqPh3Method

  Offset 0x0532 - Phase3 EQ method on the PEG 0:1:2.
- UINT8 PegGen3ProgramStaticEq

  Offset 0x0533 - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program PEG Gen3 EQ Phase1 Static Presets.
- UINT8 Gen3SwEqAlwaysAttempt

  Offset 0x0534 - PEG Gen3 SwEq Always Attempt Gen3 Software Equalization will be executed every boot.
- UINT8 Gen3SwEqNumberOfPresets

  Offset 0x0535 - 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 0x0536 - 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 0x0537 - PPCIe 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 0x0538 - PCIe Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specificied Lane (0 - 15) will be used for RxCEMLoopback.
- UINT8 PegGenerateBdatMarginTable

  Offset 0x0539 - Generate PCIe BDAT Margin Table Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.
- UINT8 UnusedUpdSpace9 [6]

  Offset 0x053A.
- UINT8 PegRxCemNonProtocolAwareness

  Offset 0x0540 - 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 0x0541 - 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 0x0542 - 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 PanelPowerEnable

  Offset 0x0543 - Panel Power Enable Control for enabling/disabling VDD force bit (Required only for early enabling of eDP panel).
- UINT8 PegGen3RootPortPreset [16]

  Offset 0x0544 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.
- UINT8 PegGen3EndPointPreset [16]

  Offset 0x0554 - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.
- UINT8 PegGen3EndPointHint [16]

  Offset 0x0564 - PEG Gen3 End port Hint values per lane Used for programming PEG Gen3 Hint values per lane.
- UINT16 Gen3SwEqJitterDwellTime

  Offset 0x0574 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.
- UINT16 Gen3SwEqJitterErrorTarget

  Offset 0x0576 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.
- UINT16 Gen3SwEqVocDwellTime

  Offset 0x0578 - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.
- UINT16 Gen3SwEqVocErrorTarget

Offset 0x057A - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.

- UINT8 SaPreMemTestRsvd [4]

  Offset 0x057C - SaPreMemTestRsvd Reserved for SA Pre-Mem Test $EN_DIS.
- UINT64 BiosAcmBase

  Offset 0x0580 - BiosAcmBase Enable/Disable.
- UINT32 BiosAcmSize

  Offset 0x0588 - BiosAcmSize Enable/Disable.
- UINT32 TgaSize

  Offset 0x058C - TgaSize Enable/Disable.
- UINT64 TxtLcpPdBase

  Offset 0x0590 - TxtLcpPdBase Enable/Disable.
- UINT64 TxtLcpPdSize

  Offset 0x0598 - TxtLcpPdSize Enable/Disable.
- UINT16 TotalFlashSize

  Offset 0x05A0 - TotalFlashSize Enable/Disable.
- UINT16 BiosSize

  Offset 0x05A2 - BiosSize Enable/Disable.
- UINT8 PchDciEn

  Offset 0x05A4 - PCH Dci Enable Enable/disable PCH Dci.
- UINT8 PchDciAutoDetect

  Offset 0x05A5 - PCH Dci Auto Detect Deprecated $EN_DIS.
- UINT8 SmbusDynamicPowerGating

  Offset 0x05A6 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.
- UINT8 WdtDisableAndLock

  Offset 0x05A7 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.
- UINT8 SmbusSpdWriteDisable

  Offset 0x05A8 - SMBUS SPD Write Disable Set/Clear Smbus SPD Write Disable.
- UINT8 ChipsetInitMessage

  Offset 0x05A9 - ChipsetInit HECI message Enable/Disable.
- UINT8 BypassPhySyncReset

  Offset 0x05AA - Bypass ChipsetInit sync reset.
- UINT8 DidInitStat

  Offset 0x05AB - Force ME DID Init Status Test, 0: disable, 1: Success, 2: No Memory in Channels, 3: Memory Init Error, 4: Memory not preserved across reset, Set ME DID init stat value $EN_DIS.
- UINT8 DisableCpuReplacedPolling

  Offset 0x05AC - CPU Replaced Polling Disable Test, 0: disable, 1: enable, Setting this option disables CPU replacement polling loop $EN_DIS.
- UINT8 SendDidMsg

  Offset 0x05AD - 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 DisableHeciRetry

  Offset 0x05AE - Retry mechanism for HECI APIs Test, 0: disable, 1: enable, Enable/Disable HECI retry.
- UINT8 DisableMessageCheck

  Offset 0x05AF - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.
- UINT8 SkipMbpHob

  Offset 0x05B0 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.
- UINT8 HeciCommunication2

  Offset 0x05B1 - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.
- UINT8 KtDeviceEnable

  Offset 0x05B2 - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

- UINT8 IderDeviceEnable

  Offset 0x05B3 - Enable IDEr Test, 0: disable, 1: enable, Enable or Disable IDEr.
- UINT8 ReservedFspmTestUpd [12]

  Offset 0x05B4.

8.5.1 Detailed Description

Fsp M Test Configuration.

Definition at line 1293 of file FspmUpd.h.

8.5.2 Member Data Documentation

8.5.2.1 UINT8 FSP_M_TEST_CONFIG::BdatEnable

Offset 0x0525 - 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 1310 of file FspmUpd.h.

8.5.2.2 UINT64 FSP_M_TEST_CONFIG::BiosAcmBase

Offset 0x0580 - BiosAcmBase Enable/Disable.

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

Definition at line 1546 of file FspmUpd.h.

8.5.2.3 UINT32 FSP_M_TEST_CONFIG::BiosAcmSize

Offset 0x0588 - BiosAcmSize Enable/Disable.

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

Definition at line 1551 of file FspmUpd.h.

8.5.2.4 UINT16 FSP_M_TEST_CONFIG::BiosSize

Offset 0x05A2 - BiosSize Enable/Disable.

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

Definition at line 1576 of file FspmUpd.h.

8.5.2.5 UINT8 FSP_M_TEST_CONFIG::BypassPhySyncReset

Offset 0x05AA - Bypass ChipsetInit sync reset.

0: disable, 1: enable, Set Enable to bypass the reset after ChipsetInit HECI message. $EN_DIS

Definition at line 1620 of file FspmUpd.h.

8.5.2.6 UINT8 FSP_M_TEST_CONFIG::ChipsetInitMessage

Offset 0x05A9 - ChipsetInit HECI message Enable/Disable.

0: Disable, 1: enable, Enable or disable ChipsetInit HECI message. If disabled, it prevents from sending ChipsetInit HECI message. $EN_DIS

Definition at line 1614 of file FspmUpd.h.

8.5.2.7 UINT8 FSP_M_TEST_CONFIG::DisableHeciRetry

Offset 0x05AE - Retry mechanism for HECI APIs Test, 0: disable, 1: enable, Enable/Disable HECI retry.

$EN_DIS

Definition at line 1646 of file FspmUpd.h.

8.5.2.8 UINT8 FSP_M_TEST_CONFIG::DisableMessageCheck

Offset 0x05AF - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.

$EN_DIS

Definition at line 1652 of file FspmUpd.h.

8.5.2.9 UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh2Enable

Offset 0x052B - 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 1349 of file FspmUpd.h.

8.5.2.10 UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh3Method

Offset 0x052C - 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 1359 of file FspmUpd.h.

8.5.2.11 UINT8 FSP_M_TEST_CONFIG::DmiVc1

Offset 0x0528 - Enable/Disable DmiVc1 Enable/Disable DmiVc1.

Enable = 1, Disable (Default) = 0 $EN_DIS

Definition at line 1329 of file FspmUpd.h.

8.5.2.12 UINT8 FSP_M_TEST_CONFIG::DmiVcm

Offset 0x0529 - Enable/Disable DmiVcm Enable/Disable DmiVcm.

Enable (Default) = 1, Disable = 0 $EN_DIS

Definition at line 1335 of file FspmUpd.h.

8.5.2.13 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqAlwaysAttempt

Offset 0x0534 - 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 1425 of file FspmUpd.h.

8.5.2.14 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqEnableVocTest

Offset 0x0536 - 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 1443 of file FspmUpd.h.

8.5.2.15 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterDwellTime

Offset 0x0574 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.

Warning

Do not change from the default

Definition at line 1520 of file FspmUpd.h.

8.5.2.16 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterErrorTarget

Offset 0x0576 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.

Warning

Do not change from the default

Definition at line 1525 of file FspmUpd.h.

8.5.2.17 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqNumberOfPresets

Offset 0x0535 - 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 1435 of file FspmUpd.h.

8.5.2.18 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocDwellTime

Offset 0x0578 - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.

Warning

Do not change from the default

Definition at line 1530 of file FspmUpd.h.

8.5.2.19 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocErrorTarget

Offset 0x057A - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.

Warning

Do not change from the default

Definition at line 1535 of file FspmUpd.h.

8.5.2.20 UINT8 FSP_M_TEST_CONFIG::HeciCommunication2

Offset 0x05B1 - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.

$EN_DIS

Definition at line 1664 of file FspmUpd.h.

8.5.2.21 UINT8 FSP_M_TEST_CONFIG::IderDeviceEnable

Offset 0x05B3 - Enable IDEr Test, 0: disable, 1: enable, Enable or Disable IDEr.

$EN_DIS

Definition at line 1676 of file FspmUpd.h.

8.5.2.22 UINT8 FSP_M_TEST_CONFIG::KtDeviceEnable

Offset 0x05B2 - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

$EN_DIS

Definition at line 1670 of file FspmUpd.h.

8.5.2.23 UINT8 FSP_M_TEST_CONFIG::LockPTMregs

Offset 0x0527 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.

Enable(Default)=1, Disable=0 $EN_DIS

Definition at line 1323 of file FspmUpd.h.

8.5.2.24 UINT8 FSP_M_TEST_CONFIG::PanelPowerEnable

Offset 0x0543 - 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 1500 of file FspmUpd.h.

8.5.2.25 UINT8 FSP_M_TEST_CONFIG::PchDciEn

Offset 0x05A4 - PCH Dci Enable Enable/disable PCH Dci.

$EN_DIS

Definition at line 1582 of file FspmUpd.h.

8.5.2.26 UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh2Enable

Offset 0x052D - 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 1366 of file FspmUpd.h.

8.5.2.27 UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh3Method

Offset 0x0530 - 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 1390 of file FspmUpd.h.

8.5.2.28 UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh2Enable

Offset 0x052E - 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 1373 of file FspmUpd.h.

8.5.2.29 UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh3Method

Offset 0x0531 - 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 1400 of file FspmUpd.h.

8.5.2.30 UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh2Enable

Offset 0x052F - 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 1380 of file FspmUpd.h.

8.5.2.31 UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh3Method

Offset 0x0532 - 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 1410 of file FspmUpd.h.

8.5.2.32 UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointHint[16]

Offset 0x0564 - 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 1515 of file FspmUpd.h.

8.5.2.33 UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointPreset[16]

Offset 0x0554 - 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 1510 of file FspmUpd.h.

8.5.2.34 UINT8 FSP_M_TEST_CONFIG::PegGen3ProgramStaticEq

Offset 0x0533 - 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 1417 of file FspmUpd.h.

8.5.2.35 UINT8 FSP_M_TEST_CONFIG::PegGen3RootPortPreset[16]

Offset 0x0544 - 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 1505 of file FspmUpd.h.

8.5.2.36 UINT8 FSP_M_TEST_CONFIG::PegGenerateBdatMarginTable

Offset 0x0539 - 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 1464 of file FspmUpd.h.

8.5.2.37 UINT8 FSP_M_TEST_CONFIG::PegRxCemLoopbackLane

Offset 0x0538 - 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 1456 of file FspmUpd.h.

8.5.2.38 UINT8 FSP_M_TEST_CONFIG::PegRxCemNonProtocolAwareness

Offset 0x0540 - 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 1477 of file FspmUpd.h.

8.5.2.39 UINT8 FSP_M_TEST_CONFIG::ScanExtGfxForLegacyOpRom

Offset 0x0526 - 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 1317 of file FspmUpd.h.

8.5.2.40 UINT8 FSP_M_TEST_CONFIG::SkipMbpHob

Offset 0x05B0 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.

$EN_DIS

Definition at line 1658 of file FspmUpd.h.

8.5.2.41 UINT8 FSP_M_TEST_CONFIG::SmbusDynamicPowerGating

Offset 0x05A6 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.

$EN_DIS

Definition at line 1594 of file FspmUpd.h.

8.5.2.42 UINT8 FSP_M_TEST_CONFIG::SmbusSpdWriteDisable

Offset 0x05A8 - 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 1607 of file FspmUpd.h.

8.5.2.43 UINT32 FSP_M_TEST_CONFIG::TgaSize

Offset 0x058C - TgaSize Enable/Disable.

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

Definition at line 1556 of file FspmUpd.h.

8.5.2.44 UINT16 FSP_M_TEST_CONFIG::TotalFlashSize

Offset 0x05A0 - TotalFlashSize Enable/Disable.

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

Definition at line 1571 of file FspmUpd.h.

8.5.2.45 UINT64 FSP_M_TEST_CONFIG::TxtLcpPdBase

Offset 0x0590 - TxtLcpPdBase Enable/Disable.

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

Definition at line 1561 of file FspmUpd.h.

8.5.2.46 UINT64 FSP_M_TEST_CONFIG::TxtLcpPdSize

Offset 0x0598 - TxtLcpPdSize Enable/Disable.

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

Definition at line 1566 of file FspmUpd.h.

8.5.2.47 UINT8 FSP_M_TEST_CONFIG::WdtDisableAndLock

Offset 0x05A7 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.

$EN_DIS

Definition at line 1600 of file FspmUpd.h.

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

- FspmUpd.h

8.6 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 PchHdaEnable

  Offset 0x002D - Enable Intel HD Audio (Azalia) Enable/disable Azalia controller.
- UINT8 PchHdaDspEnable

  Offset 0x002E - Enable HD Audio DSP Enable/disable HD Audio DSP feature.
- UINT8 PchHdaIoBufferOwnership

  Offset 0x002F - Select HDAudio IoBuffer Ownership Indicates the ownership of the I/O buffer between Intel HD Audio link vs I2S0 / I2S port.
- UINT8 PchCio2Enable

  Offset 0x0030 - Enable CIO2 Controller Enable/disable SKYCAM CIO2 Controller.
- UINT8 ScsEmmcEnabled

  Offset 0x0031 - Enable eMMC Controller Enable/disable eMMC Controller.
- UINT8 ScsEmmcHs400Enabled

  Offset 0x0032 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.
- UINT8 ScsSdCardEnabled

  Offset 0x0033 - Enable SdCard Controller Enable/disable SD Card Controller.

- UINT8 PchIshEnable

  Offset 0x0034 - Enable PCH ISH Controller Enable/disable ISH Controller.
- UINT8 ShowSpiController

  Offset 0x0035 - Show SPI controller Enable/disable to show SPI controller.
- UINT8 SpiFlashCfgLockDown

  Offset 0x0036 - Flash Configuration Lock Down Enable/disable flash lock down.
- UINT8 UnusedUpdSpace0

  Offset 0x0037.
- UINT32 MicrocodeRegionBase

  Offset 0x0038 - MicrocodeRegionBase Memory Base of Microcode Updates.
- UINT32 MicrocodeRegionSize

  Offset 0x003C - MicrocodeRegionSize Size of Microcode Updates.
- UINT8 TurboMode

  Offset 0x0040 - Turbo Mode Enable/Disable Turbo mode.
- UINT8 SataSalpSupport

  Offset 0x0041 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.
- UINT8 SataPortsEnable [8]

  Offset 0x0042 - Enable SATA ports Enable/disable SATA ports.
- UINT8 SataPortsDevSlp [8]

  Offset 0x004A - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.
- UINT8 PortUsb20Enable [16]

  Offset 0x0052 - Enable USB2 ports Enable/disable per USB2 ports.
- UINT8 PortUsb30Enable [10]

  Offset 0x0062 - Enable USB3 ports Enable/disable per USB3 ports.
- UINT8 XdciEnable

  Offset 0x006C - Enable xDCI controller Enable/disable to xDCI controller.
- UINT8 SsicPortEnable

  Offset 0x006D - Enable XHCI SSIC Enable Enable/disable XHCI SSIC port.
- UINT8 UnusedUpdSpace1

  Offset 0x006E.
- UINT8 NumOfDevIntConfig

  Offset 0x006F - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.
- UINT32 DevIntConfigPtr

  Offset 0x0070 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.
- UINT8 SerialIoDevMode [11]

  Offset 0x0074 - Enable SerialIo Device Mode 0:Disabled, 1:ACPI Mode, 2:PCI Mode, 3:Hidden mode, 4:Legacy UA↩ RT mode - Enable/disable SerialIo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5,SPI0,SPI1,UART0,UART1,UART2 device mode respectively.
- UINT8 PxRcConfig [8]

  Offset 0x007F - PIRQx to IRQx Map Config PIRQx to IRQx mapping.
- UINT8 GpioIrqRoute

  Offset 0x0087 - Select GPIO IRQ Route GPIO IRQ Select.
- UINT8 SciIrqSelect

  Offset 0x0088 - Select SciIrqSelect SCI IRQ Select.
- UINT8 TcoIrqSelect

  Offset 0x0089 - Select TcoIrqSelect TCO IRQ Select.
- UINT8 TcoIrqEnable

  Offset 0x008A - Enable/Disable Tco IRQ Enable/disable TCO IRQ $EN_DIS.
- UINT8 PchHdaVerbTableEntryNum

  Offset 0x008B - PCH HDA Verb Table Entry Number Number of Entries in Verb Table.
- UINT32 PchHdaVerbTablePtr

Offset 0x008C - PCH HDA Verb Table Pointer Pointer to Array of pointers to Verb Table.

- UINT8 UnusedUpdSpace2

  Offset 0x0090.

- UINT8 SataEnable

  Offset 0x0091 - Enable SATA Enable/disable SATA controller.

- UINT8 SataMode

  Offset 0x0092 - SATA Mode Select SATA controller working mode.

- UINT8 Usb2AfePetxiset [16]

  Offset 0x0093 - USB Per Port HS Preemphasis Bias USB Per Port HS Preemphasis Bias.

- UINT8 Usb2AfeTxiset [16]

  Offset 0x00A3 - USB Per Port HS Transmitter Bias USB Per Port HS Transmitter Bias.

- UINT8 Usb2AfePredeemp [16]

  Offset 0x00B3 - USB Per Port HS Transmitter Emphasis USB Per Port HS Transmitter Emphasis.

- UINT8 Usb2AfePehalfbit [16]

  Offset 0x00C3 - USB Per Port Half Bit Pre-emphasis USB Per Port Half Bit Pre-emphasis.

- UINT8 Usb3HsioTxDeEmphEnable [10]

  Offset 0x00D3 - 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 0x00DD - 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 0x00E7 - 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 0x00F1 - USB 3.0 TX Output Downscale Amplitude Adjustment USB 3.0 TX Output Downscale Amplitude Adjustment, HSIO_TX_DWORD8[21:16], ***Default = 00h****.*

- UINT8 PchLanEnable

  Offset 0x00FB - Enable LAN Enable/disable LAN controller.

- UINT8 DelayUsbPdoProgramming

  Offset 0x00FC - Delay USB PDO Programming Enable/disable delay of PDO programming for USB from PEI phase to DXE phase.

- UINT8 UnusedUpdSpace3 [23]

  Offset 0x00FD.

- UINT8 PcieRpClkReqSupport [24]

  Offset 0x0114 - Enable PCIE RP CLKREQ Support Enable/disable PCIE Root Port CLKREQ support.

- UINT8 PcieRpClkReqNumber [24]

  Offset 0x012C - Configure CLKREQ Number Configure Root Port CLKREQ Number if CLKREQ is supported.

- UINT8 UnusedUpdSpace4 [5]

  Offset 0x0144.

- UINT8 Heci3Enabled

  Offset 0x0149 - HECI3 state The HECI3 state from Mbp for reference in S3 path or when MbpHob is not installed.

- UINT8 UnusedUpdSpace5 [9]

  Offset 0x014A.

- UINT8 AmtEnabled

  Offset 0x0153 - AMT Switch Enable/Disable.

- UINT8 WatchDog

  Offset 0x0154 - WatchDog Timer Switch Enable/Disable.

- UINT8 AsfEnabled

  Offset 0x0155 - ASF Switch Enable/Disable.

- UINT8 ManageabilityMode

  Offset 0x0156 - Manageability Mode set by Mebx Enable/Disable.

- UINT8 FwProgress

  Offset 0x0157 - PET Progress Enable/Disable.
- UINT16 WatchDogTimerOs

  Offset 0x0158 - OS Timer 16 bits Value, Set OS watchdog timer.
- UINT16 WatchDogTimerBios

  Offset 0x015A - BIOS Timer 16 bits Value, Set BIOS watchdog timer.
- UINT8 AmtSolEnabled

  Offset 0x015C - SOL Switch Enable/Disable.
- UINT8 PcieRpClkSrcNumber [24]

  Offset 0x015D - Configure CLKSRC Number Configure Root Port CLKSRC Number.
- UINT8 UnusedUpdSpace6 [139]

  Offset 0x0175.
- UINT16 DefaultSvid

  Offset 0x0200 - Subsystem Vendor ID for SA devices Subsystem ID that will be programmed to SA devices: Default SubSystemVendorId=0x8086.
- UINT16 DefaultSid

  Offset 0x0202 - Subsystem Device ID for SA devices Subsystem ID that will be programmed to SA devices: Default SubSystemId=0x2015.
- UINT8 CridEnable

  Offset 0x0204 - Enable/Disable SA CRID Enable: SA CRID, Disable (Default): SA CRID $EN_DIS.
- UINT8 DmiAspm

  Offset 0x0205 - DMI ASPM 0=Disable, 2(Default)=L1 0:Disable, 2:L1.
- UINT16 PegPhysicalSlotNumber [3]

  Offset 0x0206 - PCIe Physical Slot Number per root port Physical Slot Number per root port.
- UINT8 PegDeEmphasis [3]

  Offset 0x020C - PCIe DeEmphasis control per root port 0: -6dB, 1(Default): -3.5dB 0:-6dB, 1:-3.5dB.
- UINT8 PegSlotPowerLimitValue [3]

  Offset 0x020F - PCIe Slot Power Limit value per root port Slot power limit value per root port.
- UINT8 PegSlotPowerLimitScale [3]

  Offset 0x0212 - 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 PavpEnable

  Offset 0x0215 - Enable/Disable PavpEnable Enable(Default): Enable PavpEnable, Disable: Disable PavpEnable $↩ EN_DIS.
- UINT8 CdClock

  Offset 0x0216 - 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 0x0217 - Enable/Disable PeiGraphicsPeimInit Enable: Enable PeiGraphicsPeimInit, Disable(Default): Disable PeiGraphicsPeimInit $EN_DIS.
- UINT8 SaImguEnable

  Offset 0x0218 - Enable/Disable SA IMGU(SKYCAM) Enable(Default): Enable SA IMGU(SKYCAM), Disable: Disable SA IMGU(SKYCAM) $EN_DIS.
- UINT8 GmmEnable

  Offset 0x0219 - Enable or disable GMM device 0=Disable, 1(Default)=Enable $EN_DIS.
- UINT8 X2ApicOptOut

  Offset 0x021A - State of X2APIC_OPT_OUT bit in the DMAR table 0=Disable/Clear, 1=Enable/Set $EN_DIS.
- UINT8 UnusedUpdSpace7 [1]

  Offset 0x021B.
- UINT32 VtdBaseAddress [2]

  Offset 0x021C - Base addresses for VT-d function MMIO access Base addresses for VT-d MMIO access per VT-d engine.

- UINT8 UnusedUpdSpace8 [19]

  Offset 0x0224.
- UINT8 SaPostMemProductionRsvd [16]

  Offset 0x0237 - SaPostMemProductionRsvd Reserved for SA Post-Mem Production $EN_DIS.
- UINT8 UnusedUpdSpace9 [7]

  Offset 0x0247.
- UINT8 Psi3Enable [5]

  *Offset 0x024E - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; **1: Enable**.*
- UINT8 Psi4Enable [5]

  *Offset 0x0253 - 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 0x0258 - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.
- UINT8 ImonOffset [5]

  Offset 0x025D - Imon offset correction PCODE MMIO Mailbox: Imon offset correction.
- UINT8 VrConfigEnable [5]

  *Offset 0x0262 - Enable/Disable BIOS configuration of VR Enable/Disable BIOS configuration of VR; **0: Disable**; 1: Enable.For all VR Indexes.*
- UINT8 TdcEnable [5]

  *Offset 0x0267 - 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 0x026C - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.
- UINT8 TdcLock [5]

  *Offset 0x0271 - Thermal Design Current Lock PCODE MMIO Mailbox: Thermal Design Current Lock; **0: Disable**; 1: Enable.For all VR Indexes.*
- UINT8 PsysSlope

  Offset 0x0276 - Platform Psys slope correction PCODE MMIO Mailbox: Platform Psys slope correction.
- UINT8 PsysOffset

  Offset 0x0277 - Platform Psys offset correction PCODE MMIO Mailbox: Platform Psys offset correction.
- UINT8 AcousticNoiseMitigation

  Offset 0x0278 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.
- UINT8 FastPkgCRampDisableIa

  Offset 0x0279 - 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 0x027A - 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 0x027B - 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 0x027C - 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 UnusedUpdSpace10 [9]

  Offset 0x027D.
- UINT16 TdcPowerLimit [5]

  Offset 0x0286 - Thermal Design Current current limit PCODE MMIO Mailbox: Thermal Design Current current limit.
- UINT32 VrPowerDeliveryDesign

  Offset 0x0290 - CPU VR Power Delivery Design Used to communicate the power delivery design capability of the board.
- UINT8 UnusedUpdSpace11 [4]

Offset 0x0294.

- UINT16 AcLoadline [5]

  Offset 0x0298 - AcLoadline PCODE MMIO Mailbox: AcLoadline in 1/100 mOhms (ie.

- UINT16 DcLoadline [5]

  Offset 0x02A2 - DcLoadline PCODE MMIO Mailbox: DcLoadline in 1/100 mOhms (ie.

- UINT16 Psi1Threshold [5]

  Offset 0x02AC - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cuttof in 1/4 Amp increments.

- UINT16 Psi2Threshold [5]

  Offset 0x02B6 - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cuttof in 1/4 Amp increments.

- UINT16 Psi3Threshold [5]

  Offset 0x02C0 - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cuttof in 1/4 Amp increments.

- UINT16 IccMax [5]

  Offset 0x02CA - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.

- UINT16 VrVoltageLimit [5]

  Offset 0x02D4 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.

- UINT8 UnusedUpdSpace12

  Offset 0x02DE.

- UINT8 FastPkgCRampDisableGt

  Offset 0x02DF - 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 0x02E0 - 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 UnusedUpdSpace13

  Offset 0x02E1.

- UINT8 SendVrMbxCmd

  Offset 0x02E2 - Enable VR specific mailbox command VR specific mailbox commands.

- UINT8 SendVrMbxCmd1

  Offset 0x02E3 - Select VR specific mailbox command to send VR specific mailbox commands.

- UINT32 CpuS3ResumeMtrrData

  Offset 0x02E4 - CpuS3ResumeMtrrData Pointer to CPU S3 Resume MTRR Data.

- CPU_CONFIG_FSP_DATA CpuConfig

  Offset 0x02E8 - Cpu Configuration Cpu Configuration data.

- UINT64 MicrocodePatchAddress

  Offset 0x02F0 - MicrocodePatchAddress Pointer to microcode patch that is suitable for this processor.

- UINT16 CpuS3ResumeMtrrDataSize

  Offset 0x02F8 - CpuS3ResumeMtrrDataSize Size of S3 resume MTRR data.

- UINT8 UnusedUpdSpace14

  Offset 0x02FA.

- UINT8 PchSkyCamPortATermOvrEnable

  Offset 0x02FB - Enable SkyCam PortA Termination override Enable/disable PortA Termination override.

- UINT8 PchSkyCamPortBTermOvrEnable

  Offset 0x02FC - Enable SkyCam PortB Termination override Enable/disable PortB Termination override.

- UINT8 PchSkyCamPortCTermOvrEnable

  Offset 0x02FD - Enable SkyCam PortC Termination override Enable/disable PortC Termination override.

- UINT8 PchSkyCamPortDTermOvrEnable

  Offset 0x02FE - Enable SkyCam PortD Termination override Enable/disable PortD Termination override.

- UINT8 PchSkyCamPortATrimEnable

  Offset 0x02FF - Enable SkyCam PortA Clk Trim Enable/disable PortA Clk Trim.

- UINT8 PchSkyCamPortBTrimEnable

  Offset 0x0300 - Enable SkyCam PortB Clk Trim Enable/disable PortB Clk Trim.
- UINT8 PchSkyCamPortCTrimEnable

  Offset 0x0301 - Enable SkyCam PortC Clk Trim Enable/disable PortC Clk Trim.
- UINT8 PchSkyCamPortDTrimEnable

  Offset 0x0302 - Enable SkyCam PortD Clk Trim Enable/disable PortD Clk Trim.
- UINT8 PchSkyCamPortACtleEnable

  Offset 0x0303 - Enable SkyCam PortA Ctle Enable/disable PortA Ctle.
- UINT8 PchSkyCamPortBCtleEnable

  Offset 0x0304 - Enable SkyCam PortB Ctle Enable/disable PortB Ctle.
- UINT8 PchSkyCamPortCDCtleEnable

  Offset 0x0305 - Enable SkyCam PortCD Ctle Enable/disable PortCD Ctle.
- UINT8 PchSkyCamPortACtleCapValue

  Offset 0x0306 - Enable SkyCam PortA Ctle Cap Value Enable/disable PortA Ctle Cap Value.
- UINT8 PchSkyCamPortBCtleCapValue

  Offset 0x0307 - Enable SkyCam PortB Ctle Cap Value Enable/disable PortB Ctle Cap Value.
- UINT8 PchSkyCamPortCDCtleCapValue

  Offset 0x0308 - Enable SkyCam PortCD Ctle Cap Value Enable/disable PortCD Ctle Cap Value.
- UINT8 PchSkyCamPortACtleResValue

  Offset 0x0309 - Enable SkyCam PortA Ctle Res Value Enable/disable PortA Ctle Res Value.
- UINT8 PchSkyCamPortBCtleResValue

  Offset 0x030A - Enable SkyCam PortB Ctle Res Value Enable/disable PortB Ctle Res Value.
- UINT8 PchSkyCamPortCDCtleResValue

  Offset 0x030B - Enable SkyCam PortCD Ctle Res Value Enable/disable PortCD Ctle Res Value.
- UINT8 PchSkyCamPortAClkTrimValue

  Offset 0x030C - Enable SkyCam PortA Clk Trim Value Enable/disable PortA Clk Trim Value.
- UINT8 PchSkyCamPortBClkTrimValue

  Offset 0x030D - Enable SkyCam PortB Clk Trim Value Enable/disable PortB Clk Trim Value.
- UINT8 PchSkyCamPortCClkTrimValue

  Offset 0x030E - Enable SkyCam PortC Clk Trim Value Enable/disable PortC Clk Trim Value.
- UINT8 PchSkyCamPortDClkTrimValue

  Offset 0x030F - Enable SkyCam PortD Clk Trim Value Enable/disable PortD Clk Trim Value.
- UINT16 PchSkyCamPortADataTrimValue

  Offset 0x0310 - Enable SkyCam Port A Data Trim Value Enable/disable Port A Data Trim Value.
- UINT16 PchSkyCamPortBDataTrimValue

  Offset 0x0312 - Enable SkyCam Port B Data Trim Value Enable/disable Port B Data Trim Value.
- UINT16 PchSkyCamPortCDDataTrimValue

  Offset 0x0314 - Enable SkyCam C/D Data Trim Value Enable/disable C/D Data Trim Value.
- UINT8 PchDmiAspm

  Offset 0x0316 - Enable DMI ASPM ASPM on PCH side of the DMI Link.
- UINT8 PchPwrOptEnable

  Offset 0x0317 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.
- UINT8 PchWriteProtectionEnable [5]

  Offset 0x0318 - PCH Flash Protection Ranges Write Enble Write or erase is blocked by hardware.
- UINT8 PchReadProtectionEnable [5]

  Offset 0x031D - PCH Flash Protection Ranges Read Enble Read is blocked by hardware.
- UINT16 PchProtectedRangeLimit [5]

  Offset 0x0322 - 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 0x032C - PCH Protect Range Base Left shifted address by 12 bits with address bits 11:0 are assumed to be 0.

- UINT8 PchHdaPme

  Offset 0x0336 - Enable Pme Enable Azalia wake-on-ring.
- UINT8 PchHdaIoBufferVoltage

  Offset 0x0337 - IO Buffer Voltage I/O Buffer Voltage Mode Select: 0: 3.3V, 1: 1.8V.
- UINT8 PchHdaVcType

  Offset 0x0338 - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.
- UINT8 PchHdaLinkFrequency

  Offset 0x0339 - HD Audio Link Frequency HDA Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 0: 6MHz, , 1: 12MHz, 2: 24MHz.
- UINT8 PchHdaIDispLinkFrequency

  Offset 0x033A - iDisp-Link Frequency iDisp-Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 4: 96MHz, 3: 48MHz.
- UINT8 PchHdaIDispLinkTmode

  Offset 0x033B - iDisp-Link T-mode iDisp-Link T-Mode (PCH_HDAUDIO_IDISP_TMODE enum): 0: 2T, 1: 1T.
- UINT8 PchHdaDspUaaCompliance

  Offset 0x033C - 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 0x033D - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.
- UINT8 PchHdaDspEndpointDmic

  Offset 0x033E - DSP DMIC Select (PCH_HDAUDIO_DMIC_TYPE enum) 0: Disable; 1: 2ch array; 2: 4ch array; 3: 1ch array.
- UINT8 PchHdaDspEndpointBluetooth

  Offset 0x033F - DSP Bluetooth enablement 0: Disable; 1: Enable.
- UINT32 PchHdaDspFeatureMask

  Offset 0x0340 - Bitmask of supported DSP features [BIT0] - WoV; [BIT1] - BT Sideband; [BIT2] - Codec VAD; [BIT5] - BT Intel HFP; [BIT6].
- UINT32 PchHdaDspPpModuleMask

  Offset 0x0344 - Bitmask of supported DSP Pre/Post-Processing Modules Deprecated: Specific pre/post-processing module bit position must be coherent with the ACPI implementation: _SB.PCI0.HDAS._DSM Function 3: Query Pre/Post Processing Module Support.
- UINT8 PchHdaDspEndpointI2s

  Offset 0x0348 - DSP I2S enablement 0: Disable; 1: Enable.
- UINT8 PchIoApicBdfValid

  Offset 0x0349 - Enable PCH Io Apic Set to 1 if BDF value is valid.
- UINT8 PchIoApicBusNumber

  Offset 0x034A - PCH Io Apic Bus Number Bus/Device/Function used as Requestor / Completer ID.
- UINT8 PchIoApicDeviceNumber

  Offset 0x034B - PCH Io Apic Device Number Bus/Device/Function used as Requestor / Completer ID.
- UINT8 PchIoApicFunctionNumber

  Offset 0x034C - PCH Io Apic Function Number Bus/Device/Function used as Requestor / Completer ID.
- UINT8 PchIoApicEntry24_119

  Offset 0x034D - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.
- UINT8 PchIoApicId

  Offset 0x034E - PCH Io Apic ID This member determines IOAPIC ID.
- UINT8 PchIoApicRangeSelect

  Offset 0x034F - PCH Io Apic Range Select Define address bits 19:12 for the IOxAPIC range.
- UINT8 PchIshSpiGpioAssign

  Offset 0x0350 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshUart0GpioAssign

  Offset 0x0351 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.

- UINT8 PchIshUart1GpioAssign

  Offset 0x0352 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c0GpioAssign

  Offset 0x0353 - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c1GpioAssign

  Offset 0x0354 - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshI2c2GpioAssign

  Offset 0x0355 - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp0GpioAssign

  Offset 0x0356 - Enable PCH ISH GP_0 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp1GpioAssign

  Offset 0x0357 - Enable PCH ISH GP_1 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp2GpioAssign

  Offset 0x0358 - Enable PCH ISH GP_2 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp3GpioAssign

  Offset 0x0359 - Enable PCH ISH GP_3 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp4GpioAssign

  Offset 0x035A - Enable PCH ISH GP_4 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp5GpioAssign

  Offset 0x035B - Enable PCH ISH GP_5 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp6GpioAssign

  Offset 0x035C - Enable PCH ISH GP_6 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshGp7GpioAssign

  Offset 0x035D - Enable PCH ISH GP_7 GPIO pin assigned 0: Disable; 1: Enable.
- UINT8 PchIshPdtUnlock

  Offset 0x035E - PCH ISH PDT Unlock Msg 0: False; 1: True.
- UINT8 PchLanLtrEnable

  Offset 0x035F - Enable PCH Lan LTR capabilty of PCH internal LAN 0: Disable; 1: Enable.
- UINT8 PchLanK1OffEnable

  Offset 0x0360 - Enable PCH Lan use CLKREQ for GbE power management 0: Disable; 1: Enable.
- UINT8 PchLanClkReqSupported

  Offset 0x0361 - Indicate whether dedicated CLKREQ# is supported 0: Disable; 1: Enable.
- UINT8 PchLanClkReqNumber

  Offset 0x0362 - CLKREQ# used by GbE Valid if ClkReqSupported is TRUE.
- UINT8 PchLockDownBiosLock

  Offset 0x0363 - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:RegD↩ Ch[5]) for the BIOS region protection.
- UINT8 PchLockDownSpiEiss

  Offset 0x0364 - Enable LOCKDOWN SPI Eiss Enable InSMM.STS (EISS) in SPI.
- UINT8 PchCrid

  Offset 0x0365 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.
- UINT16 PchSubSystemVendorId

  Offset 0x0366 - PCH Sub system vendor ID Default Subsystem Vendor ID of the PCH devices.
- UINT16 PchSubSystemId

  Offset 0x0368 - PCH Sub system ID Default Subsystem ID of the PCH devices.
- UINT8 PchLegacyIoLowLatency

  Offset 0x036A - PCH Legacy IO Low Latency Enable todo $EN_DIS.
- UINT8 UnusedUpdSpace15 [5]

  Offset 0x036B.
- UINT8 PcieRpHotPlug [24]

Offset 0x0370 - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.

- UINT8 PcieRpPmSci [24]

  Offset 0x0388 - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.
- UINT8 PcieRpExtSync [24]

  Offset 0x03A0 - Enable PCIE RP Ext Sync Indicate whether the extended synch is enabled.
- UINT8 PcieRpTransmitterHalfSwing [24]

  Offset 0x03B8 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.
- UINT8 PcieRpClkReqDetect [24]

  Offset 0x03D0 - Enable PCIE RP Clk Req Detect Probe CLKREQ# signal before enabling CLKREQ# based power management.
- UINT8 PcieRpAdvancedErrorReporting [24]

  Offset 0x03E8 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.
- UINT8 PcieRpUnsupportedRequestReport [24]

  Offset 0x0400 - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.
- UINT8 PcieRpFatalErrorReport [24]

  Offset 0x0418 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.
- UINT8 PcieRpNoFatalErrorReport [24]

  Offset 0x0430 - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.
- UINT8 PcieRpCorrectableErrorReport [24]

  Offset 0x0448 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.
- UINT8 PcieRpSystemErrorOnFatalError [24]

  Offset 0x0460 - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.
- UINT8 PcieRpSystemErrorOnNonFatalError [24]

  Offset 0x0478 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.
- UINT8 PcieRpSystemErrorOnCorrectableError [24]

  Offset 0x0490 - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.
- UINT8 PcieRpMaxPayload [24]

  Offset 0x04A8 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH_PCIE_MAX_↩ PAYLOAD.
- UINT8 PcieRpDeviceResetPadActiveHigh [24]

  Offset 0x04C0 - PCIE RP Device Reset Pad Active High Indicated whether PERST# is active 0: Low; 1: High, See: DeviceResetPad.
- UINT8 PcieRpPcieSpeed [24]

  Offset 0x04D8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.
- UINT8 PcieRpGen3EqPh3Method [24]

  Offset 0x04F0 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_ME↩ THOD).
- UINT8 PcieRpPhysicalSlotNumber [24]

  Offset 0x0508 - PCIE RP Physical Slot Number Indicates the slot number for the root port.
- UINT8 PcieRpCompletionTimeout [24]

  Offset 0x0520 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_↩ TIMEOUT).
- UINT32 PcieRpDeviceResetPad [24]

  Offset 0x0538 - PCIE RP Device Reset Pad The PCH pin assigned to device PERST# signal if available, zero otherwise.
- UINT8 PcieRpAspm [24]

  Offset 0x0598 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).
- UINT8 PcieRpL1Substates [24]

  Offset 0x05B0 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUB↩ STATES_CONTROL).
- UINT8 PcieRpLtrEnable [24]

Offset 0x05C8 - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.

- UINT8 PcieRpLtrConfigLock [24]

  Offset 0x05E0 - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.

- UINT8 PcieEqPh3LaneParamCm [24]

  Offset 0x05F8 - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.

- UINT8 PcieEqPh3LaneParamCp [24]

  Offset 0x0610 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.

- UINT8 PcieSwEqCoeffListCm [5]

  Offset 0x0628 - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.

- UINT8 PcieSwEqCoeffListCp [5]

  Offset 0x062D - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

- UINT8 PcieDisableRootPortClockGating

  Offset 0x0632 - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.

- UINT8 PcieEnablePeerMemoryWrite

  Offset 0x0633 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

- UINT8 PcieAllowNoLtrIccPllShutdown

  Offset 0x0634 - PCIE Allow No Ltr Icc PLL Shutdown Allows BIOS to control ICC PLL Shutdown by determining PCIe devices are LTR capable or leaving untouched.

- UINT8 PcieComplianceTestMode

  Offset 0x0635 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

- UINT16 PcieDetectTimeoutMs

  Offset 0x0636 - PCIE Rp Detect Timeout Ms Will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

- UINT8 PcieRpFunctionSwap

  Offset 0x0638 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.

- UINT8 PchPmPmeB0S5Dis

  Offset 0x0639 - 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 PchPmSlpS0VmEnable

  Offset 0x063A - PCH Pm Slp S0 Voltage Margining Enable Indicates platform has support for VCCPrim_Core Voltage Margining in SLP_S0# asserted state.

- UINT8 UnusedUpdSpace16 [5]

  Offset 0x063B.

- UINT8 PchPmWolEnableOverride

  Offset 0x0640 - 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 0x0641 - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.

- UINT8 PchPmWoWlanEnable

  Offset 0x0642 - PCH Pm WoW lan Enable Determine if WLAN wake from Sx, corresponds to the HOST_WLAN_P↩ P_EN bit in the PWRM_CFG3 register.

- UINT8 PchPmWoWlanDeepSxEnable

  Offset 0x0643 - 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 0x0644 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.

- UINT8 PchPmDeepSxPol

  Offset 0x0645 - PCH Pm Deep Sx Pol Deep Sx Policy.

- UINT8 PchPmSlpS3MinAssert

Offset 0x0646 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.

- UINT8 PchPmSlpS4MinAssert

  Offset 0x0647 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.
- UINT8 PchPmSlpSusMinAssert

  Offset 0x0648 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.
- UINT8 PchPmSlpAMinAssert

  Offset 0x0649 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.
- UINT8 UnusedUpdSpace17 [6]

  Offset 0x064A.
- UINT8 PchPmLpcClockRun

  Offset 0x0650 - PCH Pm Lpc Clock Run This member describes whether or not the LPC ClockRun feature of PCH should be enabled.
- UINT8 PchPmSlpStrchSusUp

  Offset 0x0651 - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.
- UINT8 PchPmSlpLanLowDc

  Offset 0x0652 - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.
- UINT8 PchPmPwrBtnOverridePeriod

  Offset 0x0653 - PCH Pm Pwr Btn Override Period PCH power button override period.
- UINT8 PchPmDisableDsxAcPresentPulldown

  Offset 0x0654 - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRESENT in deep SX and during G3 exit.
- UINT8 PchPmCapsuleResetType

  Offset 0x0655 - PCH Pm Capsule Reset Type Deprecated: Determines type of reset issued during UpdateCapsule().
- UINT8 PchPmDisableNativePowerButton

  Offset 0x0656 - PCH Pm Disable Native Power Button Power button native mode disable.
- UINT8 PchPmSlpS0Enable

  Offset 0x0657 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.
- UINT8 PchPmMeWakeSts

  Offset 0x0658 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS) register.
- UINT8 PchPmWolOvrWkSts

  Offset 0x0659 - PCH Pm WOL_OVR_WK_STS Clear the WOL_OVR_WK_STS bit in the Power and Reset Status (PRSTS) register.
- UINT8 PchPmPwrCycDur

  Offset 0x065A - PCH Pm Reset Power Cycle Duration Could be customized in the unit of second.
- UINT8 UnusedUpdSpace18

  Offset 0x065B.
- UINT8 PchPort61hEnable

  Offset 0x065C - PCH Port 61h Config Enable/Disable Used for the emulation feature for Port61h read.
- UINT8 SataPwrOptEnable

  Offset 0x065D - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.
- UINT8 EsataSpeedLimit

  Offset 0x065E - PCH Sata eSATA Speed Limit When enabled, BIOS will configure the PxSCTL.SPD to 2 to limit the eSATA port speed.
- UINT8 SataSpeedLimit

  Offset 0x065F - PCH Sata Speed Limit Indicates the maximum speed the SATA controller can support 0h: PchSataSpeedDefault.
- UINT8 SataPortsHotPlug [8]

  Offset 0x0660 - Enable SATA Port HotPlug Enable SATA Port HotPlug.
- UINT8 SataPortsInterlockSw [8]

  Offset 0x0668 - Enable SATA Port Interlock Sw Enable SATA Port Interlock Sw.
- UINT8 SataPortsExternal [8]

Offset 0x0670 - Enable SATA Port External Enable SATA Port External.

- UINT8 SataPortsSpinUp [8]

  Offset 0x0678 - Enable SATA Port SpinUp Enable the COMRESET initialization Sequence to the device.
- UINT8 SataPortsSolidStateDrive [8]

  Offset 0x0680 - Enable SATA Port Solid State Drive 0: HDD; 1: SSD.
- UINT8 SataPortsEnableDitoConfig [8]

  Offset 0x0688 - Enable SATA Port Enable Dito Config Enable DEVSLP Idle Timeout settings (DmVal, DitoVal).
- UINT8 SataPortsDmVal [8]

  Offset 0x0690 - Enable SATA Port DmVal DITO multiplier.
- UINT16 SataPortsDitoVal [8]

  Offset 0x0698 - Enable SATA Port DmVal DEVSLP Idle Timeout (DITO), Default is 625.
- UINT8 SataPortsZpOdd [8]

  Offset 0x06A8 - Enable SATA Port ZpOdd Support zero power ODD.
- UINT8 SataRstRaidAlternateId

  Offset 0x06B0 - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.
- UINT8 SataRstRaid0

  Offset 0x06B1 - PCH Sata Rst Raid0 RAID0.
- UINT8 SataRstRaid1

  Offset 0x06B2 - PCH Sata Rst Raid1 RAID1.
- UINT8 SataRstRaid10

  Offset 0x06B3 - PCH Sata Rst Raid10 RAID10.
- UINT8 SataRstRaid5

  Offset 0x06B4 - PCH Sata Rst Raid5 RAID5.
- UINT8 SataRstIrrt

  Offset 0x06B5 - PCH Sata Rst Irrt Intel Rapid Recovery Technology.
- UINT8 SataRstOromUiBanner

  Offset 0x06B6 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.
- UINT8 SataRstOromUiDelay

  Offset 0x06B7 - PCH Sata Rst Orom Ui Delay 00b: 2 secs; 01b: 4 secs; 10b: 6 secs; 11: 8 secs (see: PCH_SAT↩ A_OROM_DELAY).
- UINT8 SataRstHddUnlock

  Offset 0x06B8 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.
- UINT8 SataRstLedLocate

  Offset 0x06B9 - 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 0x06BA - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.
- UINT8 SataRstSmartStorage

  Offset 0x06BB - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.
- UINT8 SataRstPcieEnable [3]

  Offset 0x06BC - PCH Sata Rst Pcie Storage Remap enable Enable Intel RST for PCIe Storage remapping.
- UINT8 SataRstPcieStoragePort [3]

  Offset 0x06BF - PCH Sata Rst Pcie Storage Port Intel RST for PCIe Storage remapping - PCIe Port Selection (1-based, 0 = autodetect).
- UINT8 SataRstPcieDeviceResetDelay [3]

  Offset 0x06C2 - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.
- UINT8 PchScsEmmcHs400TuningRequired

  Offset 0x06C5 - Enable eMMC HS400 Training Determine if HS400 Training is required.
- UINT8 PchScsEmmcHs400DllDataValid

  Offset 0x06C6 - Set HS400 Tuning Data Valid Set if HS400 Tuning Data Valid.
- UINT8 PchScsEmmcHs400RxStrobeDll1

Offset 0x06C7 - Rx Strobe Delay Control Rx Strobe Delay Control - Rx Strobe Delay DLL 1 (HS400 Mode).

- UINT8 PchScsEmmcHs400TxDataDll

  Offset 0x06C8 - Tx Data Delay Control Tx Data Delay Control 1 - Tx Data Delay (HS400 Mode).
- UINT8 PchScsEmmcHs400DriverStrength

  Offset 0x06C9 - I/O Driver Strength I/O driver strength: 0 - 33 Ohm, 1 - 40 Ohm, 2 - 50 Ohm.
- UINT8 SerialIoGpio

  Offset 0x06CA - Enable Pch Serial IO GPIO Determines if enable Serial IO GPIO.
- UINT8 SerialIoI2cVoltage [6]

  Offset 0x06CB - IO voltage for I2C controllers Selects the IO voltage for I2C controllers, 0: PchSerialIoIs33V, 1: PchSerialIoIs18V.
- UINT8 SerialIoSpiCsPolarity [2]

  Offset 0x06D1 - SPI ChipSelect signal polarity Selects SPI ChipSelect signal polarity.
- UINT8 SerialIoUartHwFlowCtrl [3]

  Offset 0x06D3 - Enables UART hardware flow control, CTS and RTS lines Enables UART hardware flow control, CTS and RTS linesh.
- UINT8 SerialIoDebugUartNumber

  Offset 0x06D6 - UART Number For Debug Purpose UART number for debug purpose.
- UINT8 SerialIoEnableDebugUartAfterPost

  Offset 0x06D7 - Enable Debug UART Controller Enable debug UART controller after post.
- UINT8 PchSirqEnable

  Offset 0x06D8 - Enable Serial IRQ Determines if enable Serial IRQ.
- UINT8 PchSirqMode

  Offset 0x06D9 - Serial IRQ Mode Select Serial IRQ Mode Select, 0: quiet mode, 1: continuous mode.
- UINT8 PchStartFramePulse

  Offset 0x06DA - Start Frame Pulse Width Start Frame Pulse Width, 0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: Pch↩ Sfpw8Clk.
- UINT8 PchThermalDeviceEnable

  Offset 0x06DB - Enable Thermal Device Enable Thermal Device.
- UINT16 PchT0Level

  Offset 0x06DC - Thermal Throttling Custimized T0Level Value Custimized T0Level value.
- UINT16 PchT1Level

  Offset 0x06DE - Thermal Throttling Custimized T1Level Value Custimized T1Level value.
- UINT16 PchT2Level

  Offset 0x06E0 - Thermal Throttling Custimized T2Level Value Custimized T2Level value.
- UINT8 PchTsmicLock

  Offset 0x06E2 - Thermal Device SMI Enable This locks down SMI Enable on Alert Thermal Sensor Trip.
- UINT8 PchTTEnable

  Offset 0x06E3 - Enable The Thermal Throttle Enable the thermal throttle function.
- UINT8 PchTTState13Enable

  Offset 0x06E4 - 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 0x06E5 - Thermal Throttle Lock Thermal Throttle Lock.
- UINT8 TTSuggestedSetting

  Offset 0x06E6 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.
- UINT8 TTCrossThrottling

  Offset 0x06E7 - Enable PCH Cross Throttling Enable/Disable PCH Cross Throttling $EN_DIS.
- UINT8 PchDmiTsawEn

  Offset 0x06E8 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.
- UINT8 DmiSuggestedSetting

  Offset 0x06E9 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.

- UINT8 DmiTS0TW

  Offset 0x06EA - Thermal Sensor 0 Target Width Thermal Sensor 0 Target Width.
- UINT8 DmiTS1TW

  Offset 0x06EB - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.
- UINT8 DmiTS2TW

  Offset 0x06EC - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.
- UINT8 DmiTS3TW

  Offset 0x06ED - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.
- UINT8 SataP0T1M

  Offset 0x06EE - Port 0 T1 Multipler Port 0 T1 Multipler.
- UINT8 SataP0T2M

  Offset 0x06EF - Port 0 T2 Multipler Port 0 T2 Multipler.
- UINT8 SataP0T3M

  Offset 0x06F0 - Port 0 T3 Multipler Port 0 T3 Multipler.
- UINT8 SataP0TDisp

  Offset 0x06F1 - Port 0 Tdispatch Port 0 Tdispatch.
- UINT8 SataP1T1M

  Offset 0x06F2 - Port 1 T1 Multipler Port 1 T1 Multipler.
- UINT8 SataP1T2M

  Offset 0x06F3 - Port 1 T2 Multipler Port 1 T2 Multipler.
- UINT8 SataP1T3M

  Offset 0x06F4 - Port 1 T3 Multipler Port 1 T3 Multipler.
- UINT8 SataP1TDisp

  Offset 0x06F5 - Port 1 Tdispatch Port 1 Tdispatch.
- UINT8 SataP0Tinact

  Offset 0x06F6 - Port 0 Tinactive Port 0 Tinactive.
- UINT8 SataP0TDispFinit

  Offset 0x06F7 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.
- UINT8 SataP1Tinact

  Offset 0x06F8 - Port 1 Tinactive Port 1 Tinactive.
- UINT8 SataP1TDispFinit

  Offset 0x06F9 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.
- UINT8 SataThermalSuggestedSetting

  Offset 0x06FA - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.
- UINT8 PchMemoryThrottlingEnable

  Offset 0x06FB - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryPmsyncEnable [2]

  Offset 0x06FC - Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryC0TransmitEnable [2]

  Offset 0x06FE - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT8 PchMemoryPinSelection [2]

  Offset 0x0700 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
- UINT16 PchTemperatureHotLevel

  Offset 0x0702 - Thermal Device Temperature Decides the temperature.
- UINT8 PchDisableComplianceMode

  Offset 0x0704 - Disable XHCI Compliance Mode This policy will disable XHCI compliance mode on all ports.
- UINT8 Usb2OverCurrentPin [16]

  Offset 0x0705 - USB2 Port Over Current Pin Describe the specific over current pin number of USB 2.0 Port N.
- UINT8 Usb3OverCurrentPin [10]

  Offset 0x0715 - USB3 Port Over Current Pin Describe the specific over current pin number of USB 3.0 Port N.
- UINT8 Early8254ClockGatingEnable

Offset 0x071F - Enable 8254 Static Clock Gating in early POST time Set 8254CGE=1 is required for C11 support.

- UINT8 SataRstOptaneMemory

  Offset 0x0720 - PCH Sata Rst Optane Memory Optane Memory $EN_DIS.

- UINT8 SataRstCpuAttachedStorage

  Offset 0x0721 - PCH SATA RST CPU attached storage RST CPU attached storage $EN_DIS.

- UINT8 UnusedUpdSpace19 [2]

  Offset 0x0722.

- UINT32 PchPcieDeviceOverrideTablePtr

  Offset 0x0724 - Pch PCIE device override table pointer The PCIe device table is being used to override PCIe device ASPM settings.

- UINT8 EnableTcoTimer

  Offset 0x0728 - Enable TCO timer.

- UINT8 EcCmdProvisionEav

  Offset 0x0729 - EcCmdProvisionEav Ephemeral Authorization Value default values.

- UINT8 EcCmdLock

  Offset 0x072A - EcCmdLock EcCmdLock default values.

- UINT8 UnusedUpdSpace20 [5]

  Offset 0x072B.

- UINT64 SendEcCmd

  Offset 0x0730 - SendEcCmd SendEcCmd function pointer.

- UINT64 BgpdtHash [4]

  Offset 0x0738 - BgpdtHash[4] BgpdtHash values.

- UINT64 BiosGuardModulePtr

  Offset 0x0758 - BiosGuardModulePtr BiosGuardModulePtr default values.

- UINT32 BiosGuardAttr

  Offset 0x0760 - BiosGuardAttr BiosGuardAttr default values.

- UINT8 SgxSinitNvsData

  Offset 0x0764 - SgxSinitNvsData SgxSinitNvsData default values.

- UINT8 UnusedUpdSpace21 [3]

  Offset 0x0765.

- UINT64 SgxEpoch0

  Offset 0x0768 - SgxEpoch0 SgxEpoch0 default values.

- UINT64 SgxEpoch1

  Offset 0x0770 - SgxEpoch1 SgxEpoch1 default values.

- UINT8 MeUnconfigOnRtcClear

  Offset 0x0778 - Enable/Disable ME Unconfig on RTC clear Enable(Default): Enable ME Unconfig On Rtc Clear, Disable: Disable ME Unconfig On Rtc Clear $EN_DIS.

- UINT8 MeUnconfigIsValid

  Offset 0x0779 - Check if MeUnconfigOnRtcClear is valid The MeUnconfigOnRtcClear item could be not valid due to CMOS is clear.

- UINT8 IslVrCmd

  Offset 0x077A - Activates VR mailbox command for Intersil VR C-state issues.

- UINT8 ReservedFspsUpd [5]

  Offset 0x077B.

8.6.1 Detailed Description

Fsp S Configuration.

Definition at line 88 of file FspsUpd.h.

8.6.2 Member Data Documentation

8.6.2.1 UINT16 FSP_S_CONFIG::AcLoadline[5]

Offset 0x0298 - 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 688 of file FspsUpd.h.

8.6.2.2 UINT8 FSP_S_CONFIG::AcousticNoiseMitigation

Offset 0x0278 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.

0: Disabled; 1: Enabled $EN_DIS

Definition at line 633 of file FspsUpd.h.

8.6.2.3 UINT8 FSP_S_CONFIG::AmtEnabled

Offset 0x0153 - AMT Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable AMT functionality. $EN_DIS

Definition at line 410 of file FspsUpd.h.

8.6.2.4 UINT8 FSP_S_CONFIG::AmtSolEnabled

Offset 0x015C - SOL Switch Enable/Disable.

0: Disable, 1: enable, Serial Over Lan enable/disable state by Mebx $EN_DIS

Definition at line 453 of file FspsUpd.h.

8.6.2.5 UINT8 FSP_S_CONFIG::AsfEnabled

Offset 0x0155 - ASF Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable ASF functionality. $EN_DIS

Definition at line 422 of file FspsUpd.h.

8.6.2.6 UINT16 FSP_S_CONFIG::DcLoadline[5]

Offset 0x02A2 - 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 694 of file FspsUpd.h.

8.6.2.7 UINT8 FSP_S_CONFIG::DelayUsbPdoProgramming

Offset 0x00FC - Delay USB PDO Programming Enable/disable delay of PDO programming for USB from PEI phase to DXE phase.

0: disable, 1: enable $EN_DIS

Definition at line 373 of file FspsUpd.h.

8.6.2.8 UINT32 FSP_S_CONFIG::DevIntConfigPtr

Offset 0x0070 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.

The address of the table of PCH_DEVICE_INTERRUPT_CONFIG.

Definition at line 251 of file FspsUpd.h.

8.6.2.9 UINT8 FSP_S_CONFIG::DmiSuggestedSetting

Offset 0x06E9 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.

$EN_DIS

Definition at line 1843 of file FspsUpd.h.

8.6.2.10 UINT8 FSP_S_CONFIG::Early8254ClockGatingEnable

Offset 0x071F - Enable 8254 Static Clock Gating in early POST time Set 8254CGE=1 is required for C11 support.

However, set 8254CGE=1 in POST time might fail to boot legacy OS which using 8254 timer. Make sure it won't break legacy OS boot before enabling this. $EN_DIS

Definition at line 1982 of file FspsUpd.h.

8.6.2.11 UINT8 FSP_S_CONFIG::EcCmdLock

Offset 0x072A - EcCmdLock EcCmdLock default values.

Locks Ephemeral Authorization Value sent previously

Definition at line 2024 of file FspsUpd.h.

8.6.2.12 UINT8 FSP_S_CONFIG::EcCmdProvisionEav

Offset 0x0729 - EcCmdProvisionEav Ephemeral Authorization Value default values.

Provisions an ephemeral shared secret to the EC

Definition at line 2019 of file FspsUpd.h.

8.6.2.13 UINT8 FSP_S_CONFIG::EnableTcoTimer

Offset 0x0728 - 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 2014 of file FspsUpd.h.

8.6.2.14 UINT8 FSP_S_CONFIG::EsataSpeedLimit

Offset 0x065E - 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 1561 of file FspsUpd.h.

8.6.2.15 UINT8 FSP_S_CONFIG::FastPkgCRampDisableGt

Offset 0x02DF - 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 733 of file FspsUpd.h.

8.6.2.16 UINT8 FSP_S_CONFIG::FastPkgCRampDisableIa

Offset 0x0279 - 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 640 of file FspsUpd.h.

8.6.2.17 UINT8 FSP_S_CONFIG::FastPkgCRampDisableSa

Offset 0x02E0 - 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 740 of file FspsUpd.h.

8.6.2.18 UINT8 FSP_S_CONFIG::FwProgress

Offset 0x0157 - PET Progress Enable/Disable.

0: Disable, 1: enable, Enable/Disable PET Events Progress to receive PET Events. $EN_DIS

Definition at line 435 of file FspsUpd.h.

8.6.2.19 UINT8 FSP_S_CONFIG::GpioIrqRoute

Offset 0x0087 - Select GPIO IRQ Route GPIO IRQ Select.

The valid value is 14 or 15.

Definition at line 270 of file FspsUpd.h.

8.6.2.20 UINT8 FSP_S_CONFIG::Heci3Enabled

Offset 0x0149 - 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 400 of file FspsUpd.h.

8.6.2.21 UINT16 FSP_S_CONFIG::IccMax[5]

Offset 0x02CA - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.

0-255A in 1/4 A units. 400 = 100A

Definition at line 717 of file FspsUpd.h.

8.6.2.22 UINT8 FSP_S_CONFIG::ImonOffset[5]

Offset 0x025D - Imon offset 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 591 of file FspsUpd.h.

8.6.2.23 UINT8 FSP_S_CONFIG::ImonSlope[5]

Offset 0x0258 - 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 585 of file FspsUpd.h.

8.6.2.24 UINT8 FSP_S_CONFIG::IslVrCmd

Offset 0x077A - 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 2087 of file FspsUpd.h.

8.6.2.25 UINT8 FSP_S_CONFIG::ManageabilityMode

Offset 0x0156 - Manageability Mode set by Mebx Enable/Disable.

0: Disable, 1: enable, Enable or disable Manageability Mode. $EN_DIS

Definition at line 428 of file FspsUpd.h.

8.6.2.26 UINT8 FSP_S_CONFIG::MeUnconfigIsValid

Offset 0x0779 - Check if MeUnconfigOnRtcClear is valid The MeUnconfigOnRtcClear item could be not valid due to CMOS is clear.

$EN_DIS

Definition at line 2081 of file FspsUpd.h.

8.6.2.27 UINT64 FSP_S_CONFIG::MicrocodePatchAddress

Offset 0x02F0 - MicrocodePatchAddress Pointer to microcode patch that is suitable for this processor.

0:Disable, 1:Enable

Definition at line 775 of file FspsUpd.h.

8.6.2.28 UINT8 FSP_S_CONFIG::NumOfDevIntConfig

Offset 0x006F - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.

If this is not zero, the DevIntConfigPtr must not be NULL.

Definition at line 246 of file FspsUpd.h.

8.6.2.29 UINT8 FSP_S_CONFIG::PchCio2Enable

Offset 0x0030 - Enable CIO2 Controller Enable/disable SKYCAM CIO2 Controller.

$EN_DIS

Definition at line 137 of file FspsUpd.h.

8.6.2.30 UINT8 FSP_S_CONFIG::PchCrid

Offset 0x0365 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.

$EN_DIS

Definition at line 1192 of file FspsUpd.h.

8.6.2.31 UINT8 FSP_S_CONFIG::PchDisableComplianceMode

Offset 0x0704 - Disable XHCI Compliance Mode This policy will disable XHCI compliance mode on all ports.

Complicance Mode should be default enabled. $EN_DIS

Definition at line 1964 of file FspsUpd.h.

8.6.2.32 UINT8 FSP_S_CONFIG::PchDmiAspm

Offset 0x0316 - Enable DMI ASPM ASPM on PCH side of the DMI Link.

$EN_DIS

Definition at line 921 of file FspsUpd.h.

8.6.2.33 UINT8 FSP_S_CONFIG::PchDmiTsawEn

Offset 0x06E8 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.

$EN_DIS

Definition at line 1837 of file FspsUpd.h.

8.6.2.34 UINT8 FSP_S_CONFIG::PchHdaDspEnable

Offset 0x002E - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

$EN_DIS

Definition at line 121 of file FspsUpd.h.

8.6.2.35 UINT8 FSP_S_CONFIG::PchHdaDspEndpointBluetooth

Offset 0x033F - DSP Bluetooth enablement 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1003 of file FspsUpd.h.

8.6.2.36 UINT8 FSP_S_CONFIG::PchHdaDspEndpointI2s

Offset 0x0348 - DSP I2S enablement 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1023 of file FspsUpd.h.

8.6.2.37 UINT32 FSP_S_CONFIG::PchHdaDspFeatureMask

Offset 0x0340 - Bitmask of supported DSP features [BIT0] - WoV; [BIT1] - BT Sideband; [BIT2] - Codec VAD; [BIT5] - BT Intel HFP; [BIT6].

- BT Intel A2DP; [BIT7] - DSP based speech pre-processing disabled; [BIT8] - 0: Intel WoV, 1: Windows Voice Activation.

Definition at line 1010 of file FspsUpd.h.

8.6.2.38 UINT8 FSP_S_CONFIG::PchHdaDspUaaCompliance

Offset 0x033C - 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 986 of file FspsUpd.h.

8.6.2.39 UINT8 FSP_S_CONFIG::PchHdaEnable

Offset 0x002D - Enable Intel HD Audio (Azalia) Enable/disable Azalia controller.

$EN_DIS

Definition at line 115 of file FspsUpd.h.

8.6.2.40 UINT8 FSP_S_CONFIG::PchHdaIDispCodecDisconnect

Offset 0x033D - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.

$EN_DIS

Definition at line 992 of file FspsUpd.h.

8.6.2.41 UINT8 FSP_S_CONFIG::PchHdaIoBufferOwnership

Offset 0x002F - Select HDAudio IoBuffer Ownership Indicates the ownership of the I/O buffer between Intel HD Audio link vs I2S0 / I2S port.

0: Intel HD-Audio link owns all the I/O buffers. 1: Intel HD-Audio link owns 4 of the I/O buffers for 1 HD-Audio codec connection, and I2S1 port owns 4 of the I/O buffers for 1 I2S codec connection. 2: Reserved. 3: I2S0 and I2S1 ports own all the I/O buffers. 0:HD-A Link, 1:Shared HD-A Link and I2S Port, 3:I2S Ports

Definition at line 131 of file FspsUpd.h.

8.6.2.42 UINT8 FSP_S_CONFIG::PchHdaPme

Offset 0x0336 - Enable Pme Enable Azalia wake-on-ring.

$EN_DIS

Definition at line 954 of file FspsUpd.h.

8.6.2.43 UINT8 FSP_S_CONFIG::PchIoApicBdfValid

Offset 0x0349 - Enable PCH Io Apic Set to 1 if BDF value is valid.

$EN_DIS

Definition at line 1029 of file FspsUpd.h.

8.6.2.44 UINT8 FSP_S_CONFIG::PchIoApicBusNumber

Offset 0x034A - PCH Io Apic Bus Number Bus/Device/Function used as Requestor / Completer ID.

Default is 0xF0.

Definition at line 1034 of file FspsUpd.h.

8.6.2.45 UINT8 FSP_S_CONFIG::PchIoApicDeviceNumber

Offset 0x034B - PCH Io Apic Device Number Bus/Device/Function used as Requestor / Completer ID.

Default is 0x1F.

Definition at line 1039 of file FspsUpd.h.

8.6.2.46 UINT8 FSP_S_CONFIG::PchIoApicEntry24_119

Offset 0x034D - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1050 of file FspsUpd.h.

8.6.2.47 UINT8 FSP_S_CONFIG::PchIoApicFunctionNumber

Offset 0x034C - PCH Io Apic Function Number Bus/Device/Function used as Requestor / Completer ID.

Default is 0x00.

Definition at line 1044 of file FspsUpd.h.

8.6.2.48 UINT8 FSP_S_CONFIG::PchIoApicId

Offset 0x034E - PCH Io Apic ID This member determines IOAPIC ID.

Default is 0x02.

Definition at line 1055 of file FspsUpd.h.

8.6.2.49 UINT8 FSP_S_CONFIG::PchIoApicRangeSelect

Offset 0x034F - PCH Io Apic Range Select Define address bits 19:12 for the IOxAPIC range.

Default is 0.

Definition at line 1060 of file FspsUpd.h.

8.6.2.50 UINT8 FSP_S_CONFIG::PchIshEnable

Offset 0x0034 - Enable PCH ISH Controller Enable/disable ISH Controller.

$EN_DIS

Definition at line 161 of file FspsUpd.h.

8.6.2.51 UINT8 FSP_S_CONFIG::PchIshGp0GpioAssign

Offset 0x0356 - Enable PCH ISH GP_0 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1102 of file FspsUpd.h.

8.6.2.52 UINT8 FSP_S_CONFIG::PchIshGp1GpioAssign

Offset 0x0357 - Enable PCH ISH GP_1 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1108 of file FspsUpd.h.

8.6.2.53 UINT8 FSP_S_CONFIG::PchIshGp2GpioAssign

Offset 0x0358 - Enable PCH ISH GP_2 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1114 of file FspsUpd.h.

8.6.2.54 UINT8 FSP_S_CONFIG::PchIshGp3GpioAssign

Offset 0x0359 - Enable PCH ISH GP_3 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1120 of file FspsUpd.h.

8.6.2.55 UINT8 FSP_S_CONFIG::PchIshGp4GpioAssign

Offset 0x035A - Enable PCH ISH GP_4 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1126 of file FspsUpd.h.

8.6.2.56 UINT8 FSP_S_CONFIG::PchIshGp5GpioAssign

Offset 0x035B - Enable PCH ISH GP_5 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1132 of file FspsUpd.h.

8.6.2.57 UINT8 FSP_S_CONFIG::PchIshGp6GpioAssign

Offset 0x035C - Enable PCH ISH GP_6 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1138 of file FspsUpd.h.

8.6.2.58 UINT8 FSP_S_CONFIG::PchIshGp7GpioAssign

Offset 0x035D - Enable PCH ISH GP_7 GPIO pin assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1144 of file FspsUpd.h.

8.6.2.59 UINT8 FSP_S_CONFIG::PchIshI2c0GpioAssign

Offset 0x0353 - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1084 of file FspsUpd.h.

8.6.2.60 UINT8 FSP_S_CONFIG::PchIshI2c1GpioAssign

Offset 0x0354 - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1090 of file FspsUpd.h.

8.6.2.61 UINT8 FSP_S_CONFIG::PchIshI2c2GpioAssign

Offset 0x0355 - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1096 of file FspsUpd.h.

8.6.2.62 UINT8 FSP_S_CONFIG::PchIshPdtUnlock

Offset 0x035E - PCH ISH PDT Unlock Msg 0: False; 1: True.

$EN_DIS

Definition at line 1150 of file FspsUpd.h.

8.6.2.63 UINT8 FSP_S_CONFIG::PchIshSpiGpioAssign

Offset 0x0350 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1066 of file FspsUpd.h.

8.6.2.64 UINT8 FSP_S_CONFIG::PchIshUart0GpioAssign

Offset 0x0351 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1072 of file FspsUpd.h.

8.6.2.65 UINT8 FSP_S_CONFIG::PchIshUart1GpioAssign

Offset 0x0352 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1078 of file FspsUpd.h.

8.6.2.66 UINT8 FSP_S_CONFIG::PchLanClkReqSupported

Offset 0x0361 - Indicate whether dedicated CLKREQ# is supported 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1168 of file FspsUpd.h.

8.6.2.67 UINT8 FSP_S_CONFIG::PchLanEnable

Offset 0x00FB - Enable LAN Enable/disable LAN controller.

$EN_DIS

Definition at line 366 of file FspsUpd.h.

8.6.2.68 UINT8 FSP_S_CONFIG::PchLanK1OffEnable

Offset 0x0360 - Enable PCH Lan use CLKREQ for GbE power management 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1162 of file FspsUpd.h.

8.6.2.69 UINT8 FSP_S_CONFIG::PchLanLtrEnable

Offset 0x035F - Enable PCH Lan LTR capabilty of PCH internal LAN 0: Disable; 1: Enable.

$EN_DIS

Definition at line 1156 of file FspsUpd.h.

8.6.2.70 UINT8 FSP_S_CONFIG::PchLockDownBiosLock

Offset 0x0363 - 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 1180 of file FspsUpd.h.

8.6.2.71 UINT8 FSP_S_CONFIG::PchLockDownSpiEiss

Offset 0x0364 - Enable LOCKDOWN SPI Eiss Enable InSMM.STS (EISS) in SPI.

$EN_DIS

Definition at line 1186 of file FspsUpd.h.

8.6.2.72 UINT8 FSP_S_CONFIG::PchMemoryThrottlingEnable

Offset 0x06FB - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.

$EN_DIS

Definition at line 1937 of file FspsUpd.h.

8.6.2.73 UINT32 FSP_S_CONFIG::PchPcieDeviceOverrideTablePtr

Offset 0x0724 - 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_DE↩ VICE_OVERRIDE structure for the table. Last entry VendorId must be 0.

Definition at line 2006 of file FspsUpd.h.

8.6.2.74 UINT8 FSP_S_CONFIG::PchPmCapsuleResetType

Offset 0x0655 - PCH Pm Capsule Reset Type Deprecated: Determines type of reset issued during Update↩ Capsule().

Always Warm reset. $EN_DIS

Definition at line 1508 of file FspsUpd.h.

8.6.2.75 UINT8 FSP_S_CONFIG::PchPmDeepSxPol

Offset 0x0645 - PCH Pm Deep Sx Pol Deep Sx Policy.

$EN_DIS

Definition at line 1449 of file FspsUpd.h.

8.6.2.76 UINT8 FSP_S_CONFIG::PchPmDisableDsxAcPresentPulldown

Offset 0x0654 - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRE↩ SENT in deep SX and during G3 exit.

$EN_DIS

Definition at line 1502 of file FspsUpd.h.

8.6.2.77 UINT8 FSP_S_CONFIG::PchPmDisableNativePowerButton

Offset 0x0656 - PCH Pm Disable Native Power Button Power button native mode disable.

$EN_DIS

Definition at line 1514 of file FspsUpd.h.

8.6.2.78 UINT8 FSP_S_CONFIG::PchPmLanWakeFromDeepSx

Offset 0x0644 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.

$EN_DIS

Definition at line 1443 of file FspsUpd.h.

8.6.2.79 UINT8 FSP_S_CONFIG::PchPmLpcClockRun

Offset 0x0650 - PCH Pm Lpc Clock Run This member describes whether or not the LPC ClockRun feature of PCH should be enabled.

$EN_DIS

Definition at line 1479 of file FspsUpd.h.

8.6.2.80 UINT8 FSP_S_CONFIG::PchPmMeWakeSts

Offset 0x0658 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS) register.

$EN_DIS

Definition at line 1526 of file FspsUpd.h.

8.6.2.81 UINT8 FSP_S_CONFIG::PchPmPcieWakeFromDeepSx

Offset 0x0641 - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.

$EN_DIS

Definition at line 1424 of file FspsUpd.h.

8.6.2.82 UINT8 FSP_S_CONFIG::PchPmPmeB0S5Dis

Offset 0x0639 - 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 1402 of file FspsUpd.h.

8.6.2.83 UINT8 FSP_S_CONFIG::PchPmPwrBtnOverridePeriod

Offset 0x0653 - 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 1496 of file FspsUpd.h.

8.6.2.84 UINT8 FSP_S_CONFIG::PchPmPwrCycDur

Offset 0x065A - 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 1538 of file FspsUpd.h.

8.6.2.85 UINT8 FSP_S_CONFIG::PchPmSlpAMinAssert

Offset 0x0649 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.

Default is PchSlpA2s.

Definition at line 1469 of file FspsUpd.h.

8.6.2.86 UINT8 FSP_S_CONFIG::PchPmSlpLanLowDc

Offset 0x0652 - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.

$EN_DIS

Definition at line 1491 of file FspsUpd.h.

8.6.2.87 UINT8 FSP_S_CONFIG::PchPmSlpS0Enable

Offset 0x0657 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.

$EN_DIS

Definition at line 1520 of file FspsUpd.h.

8.6.2.88 UINT8 FSP_S_CONFIG::PchPmSlpS0VmEnable

Offset 0x063A - PCH Pm Slp S0 Voltage Margining Enable Indicates platform has support for VCCPrim_Core Voltage Margining in SLP_S0# asserted state.

$EN_DIS

Definition at line 1408 of file FspsUpd.h.

8.6.2.89 UINT8 FSP_S_CONFIG::PchPmSlpS3MinAssert

Offset 0x0646 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.

Default is PchSlpS350ms.

Definition at line 1454 of file FspsUpd.h.

8.6.2.90 UINT8 FSP_S_CONFIG::PchPmSlpS4MinAssert

Offset 0x0647 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.

Default is PchSlpS44s.

Definition at line 1459 of file FspsUpd.h.

8.6.2.91 UINT8 FSP_S_CONFIG::PchPmSlpStrchSusUp

Offset 0x0651 - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.

$EN_DIS

Definition at line 1485 of file FspsUpd.h.

8.6.2.92 UINT8 FSP_S_CONFIG::PchPmSlpSusMinAssert

Offset 0x0648 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.

Default is PchSlpSus4s.

Definition at line 1464 of file FspsUpd.h.

8.6.2.93 UINT8 FSP_S_CONFIG::PchPmWolEnableOverride

Offset 0x0640 - 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 1418 of file FspsUpd.h.

8.6.2.94 UINT8 FSP_S_CONFIG::PchPmWolOvrWkSts

Offset 0x0659 - 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 1532 of file FspsUpd.h.

8.6.2.95 UINT8 FSP_S_CONFIG::PchPmWoWlanDeepSxEnable

Offset 0x0643 - 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 1437 of file FspsUpd.h.

8.6.2.96 UINT8 FSP_S_CONFIG::PchPmWoWlanEnable

Offset 0x0642 - 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 1430 of file FspsUpd.h.

8.6.2.97 UINT8 FSP_S_CONFIG::PchPort61hEnable

Offset 0x065C - PCH Port 61h Config Enable/Disable Used for the emulation feature for Port61h read.

The port is trapped and the SMI handler will toggle bit4 according to the handler's internal state. $EN_DIS

Definition at line 1549 of file FspsUpd.h.

8.6.2.98 UINT8 FSP_S_CONFIG::PchPwrOptEnable

Offset 0x0317 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.

$EN_DIS

Definition at line 927 of file FspsUpd.h.

8.6.2.99 UINT8 FSP_S_CONFIG::PchScsEmmcHs400DllDataValid

Offset 0x06C6 - Set HS400 Tuning Data Valid Set if HS400 Tuning Data Valid.

$EN_DIS

Definition at line 1710 of file FspsUpd.h.

8.6.2.100 UINT8 FSP_S_CONFIG::PchScsEmmcHs400TuningRequired

Offset 0x06C5 - Enable eMMC HS400 Training Determine if HS400 Training is required.

$EN_DIS

Definition at line 1704 of file FspsUpd.h.

8.6.2.101 UINT8 FSP_S_CONFIG::PchSirqEnable

Offset 0x06D8 - Enable Serial IRQ Determines if enable Serial IRQ.

$EN_DIS

Definition at line 1762 of file FspsUpd.h.

8.6.2.102 UINT8 FSP_S_CONFIG::PchSirqMode

Offset 0x06D9 - Serial IRQ Mode Select Serial IRQ Mode Select, 0: quiet mode, 1: continuous mode.

$EN_DIS

Definition at line 1768 of file FspsUpd.h.

8.6.2.103 UINT8 FSP_S_CONFIG::PchSkyCamPortACtleEnable

Offset 0x0303 - Enable SkyCam PortA Ctle Enable/disable PortA Ctle.

$EN_DIS

Definition at line 838 of file FspsUpd.h.

8.6.2.104 UINT8 FSP_S_CONFIG::PchSkyCamPortATermOvrEnable

Offset 0x02FB - Enable SkyCam PortA Termination override Enable/disable PortA Termination override.

$EN_DIS

Definition at line 790 of file FspsUpd.h.

8.6.2.105 UINT8 FSP_S_CONFIG::PchSkyCamPortATrimEnable

Offset 0x02FF - Enable SkyCam PortA Clk Trim Enable/disable PortA Clk Trim.

$EN_DIS

Definition at line 814 of file FspsUpd.h.

8.6.2.106 UINT8 FSP_S_CONFIG::PchSkyCamPortBCtleEnable

Offset 0x0304 - Enable SkyCam PortB Ctle Enable/disable PortB Ctle.

$EN_DIS

Definition at line 844 of file FspsUpd.h.

8.6.2.107 UINT8 FSP_S_CONFIG::PchSkyCamPortBTermOvrEnable

Offset 0x02FC - Enable SkyCam PortB Termination override Enable/disable PortB Termination override.

$EN_DIS

Definition at line 796 of file FspsUpd.h.

8.6.2.108 UINT8 FSP_S_CONFIG::PchSkyCamPortBTrimEnable

Offset 0x0300 - Enable SkyCam PortB Clk Trim Enable/disable PortB Clk Trim.

$EN_DIS

Definition at line 820 of file FspsUpd.h.

8.6.2.109 UINT8 FSP_S_CONFIG::PchSkyCamPortCDCtleEnable

Offset 0x0305 - Enable SkyCam PortCD Ctle Enable/disable PortCD Ctle.

$EN_DIS

Definition at line 850 of file FspsUpd.h.

8.6.2.110 UINT8 FSP_S_CONFIG::PchSkyCamPortCTermOvrEnable

Offset 0x02FD - Enable SkyCam PortC Termination override Enable/disable PortC Termination override.

$EN_DIS

Definition at line 802 of file FspsUpd.h.

8.6.2.111 UINT8 FSP_S_CONFIG::PchSkyCamPortCTrimEnable

Offset 0x0301 - Enable SkyCam PortC Clk Trim Enable/disable PortC Clk Trim.

$EN_DIS

Definition at line 826 of file FspsUpd.h.

8.6.2.112 UINT8 FSP_S_CONFIG::PchSkyCamPortDTermOvrEnable

Offset 0x02FE - Enable SkyCam PortD Termination override Enable/disable PortD Termination override.

$EN_DIS

Definition at line 808 of file FspsUpd.h.

8.6.2.113 UINT8 FSP_S_CONFIG::PchSkyCamPortDTrimEnable

Offset 0x0302 - Enable SkyCam PortD Clk Trim Enable/disable PortD Clk Trim.

$EN_DIS

Definition at line 832 of file FspsUpd.h.

8.6.2.114 UINT16 FSP_S_CONFIG::PchSubSystemId

Offset 0x0368 - PCH Sub system ID Default Subsystem ID of the PCH devices.

Default is 0x7270.

Definition at line 1202 of file FspsUpd.h.

8.6.2.115 UINT16 FSP_S_CONFIG::PchSubSystemVendorId

Offset 0x0366 - PCH Sub system vendor ID Default Subsystem Vendor ID of the PCH devices.

Default is 0x8086.

Definition at line 1197 of file FspsUpd.h.

8.6.2.116 UINT8 FSP_S_CONFIG::PchThermalDeviceEnable

Offset 0x06DB - Enable Thermal Device Enable Thermal Device.

$EN_DIS

Definition at line 1779 of file FspsUpd.h.

8.6.2.117 UINT8 FSP_S_CONFIG::PchTsmicLock

Offset 0x06E2 - Thermal Device SMI Enable This locks down SMI Enable on Alert Thermal Sensor Trip.

$EN_DIS

Definition at line 1800 of file FspsUpd.h.

8.6.2.118 UINT8 FSP_S_CONFIG::PchTTEnable

Offset 0x06E3 - Enable The Thermal Throttle Enable the thermal throttle function.

$EN_DIS

Definition at line 1806 of file FspsUpd.h.

8.6.2.119 UINT8 FSP_S_CONFIG::PchTTLock

Offset 0x06E5 - Thermal Throttle Lock Thermal Throttle Lock.

$EN_DIS

Definition at line 1819 of file FspsUpd.h.

8.6.2.120 UINT8 FSP_S_CONFIG::PchTTState13Enable

Offset 0x06E4 - 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 1813 of file FspsUpd.h.

8.6.2.121 UINT8 FSP_S_CONFIG::PcieAllowNoLtrIccPllShutdown

Offset 0x0634 - PCIE Allow No Ltr Icc PLL Shutdown Allows BIOS to control ICC PLL Shutdown by determining PCIe devices are LTR capable or leaving untouched.

$EN_DIS

Definition at line 1377 of file FspsUpd.h.

8.6.2.122 UINT8 FSP_S_CONFIG::PcieComplianceTestMode

Offset 0x0635 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

$EN_DIS

Definition at line 1383 of file FspsUpd.h.

8.6.2.123 UINT8 FSP_S_CONFIG::PcieDisableRootPortClockGating

Offset 0x0632 - 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 1364 of file FspsUpd.h.

8.6.2.124 UINT8 FSP_S_CONFIG::PcieEnablePeerMemoryWrite

Offset 0x0633 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

$EN_DIS

Definition at line 1370 of file FspsUpd.h.

8.6.2.125 UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCm[24]

Offset 0x05F8 - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.

Coefficient C-1.

Definition at line 1342 of file FspsUpd.h.

8.6.2.126 UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCp[24]

Offset 0x0610 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.

Coefficient C+1.

Definition at line 1347 of file FspsUpd.h.

8.6.2.127 UINT8 FSP_S_CONFIG::PcieRpAspm[24]

Offset 0x0598 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 1321 of file FspsUpd.h.

8.6.2.128 UINT8 FSP_S_CONFIG::PcieRpClkReqNumber[24]

Offset 0x012C - Configure CLKREQ Number Configure Root Port CLKREQ Number if CLKREQ is supported.

Each value in arrary can be between 0-6. One byte for each port, byte0 for port1, byte1 for port2, and so on.

Definition at line 389 of file FspsUpd.h.

8.6.2.129 UINT8 FSP_S_CONFIG::PcieRpClkReqSupport[24]

Offset 0x0114 - Enable PCIE RP CLKREQ Support Enable/disable PCIE Root Port CLKREQ support.

0: disable, 1: enable. One byte for each port, byte0 for port1, byte1 for port2, and so on.

Definition at line 383 of file FspsUpd.h.

8.6.2.130 UINT8 FSP_S_CONFIG::PcieRpClkSrcNumber[24]

Offset 0x015D - Configure CLKSRC Number Configure Root Port CLKSRC Number.

Each value in arrary can be between 0-6 for valid clock numbers or 0x1F for an invalid number. One byte for each port, byte0 for port1, byte1 for port2, and so on.

Definition at line 460 of file FspsUpd.h.

8.6.2.131 UINT8 FSP_S_CONFIG::PcieRpCompletionTimeout[24]

Offset 0x0520 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETIO↩ N_TIMEOUT).

Default is PchPcieCompletionTO_Default.

Definition at line 1309 of file FspsUpd.h.

8.6.2.132 UINT32 FSP_S_CONFIG::PcieRpDeviceResetPad[24]

Offset 0x0538 - PCIE RP Device Reset Pad The PCH pin assigned to device PERST# signal if available, zero otherwise.

See also DeviceResetPadActiveHigh.

Definition at line 1315 of file FspsUpd.h.

8.6.2.133 UINT8 FSP_S_CONFIG::PcieRpFunctionSwap

Offset 0x0638 - 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 1396 of file FspsUpd.h.

8.6.2.134 UINT8 FSP_S_CONFIG::PcieRpGen3EqPh3Method[24]

Offset 0x04F0 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_M↩ ETHOD).

0: Default; 2: Software Search; 4: Fixed Coeficients.

Definition at line 1299 of file FspsUpd.h.

8.6.2.135 UINT8 FSP_S_CONFIG::PcieRpL1Substates[24]

Offset 0x05B0 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SU↩ BSTATES_CONTROL).

Default is PchPcieL1SubstatesL1_1_2.

Definition at line 1327 of file FspsUpd.h.

8.6.2.136 UINT8 FSP_S_CONFIG::PcieRpPcieSpeed[24]

Offset 0x04D8 - 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 1293 of file FspsUpd.h.

8.6.2.137 UINT8 FSP_S_CONFIG::PcieRpPhysicalSlotNumber[24]

Offset 0x0508 - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 1304 of file FspsUpd.h.

8.6.2.138 UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCm[5]

Offset 0x0628 - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.

Coefficient C-1.

Definition at line 1352 of file FspsUpd.h.

8.6.2.139 UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCp[5]

Offset 0x062D - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

Coefficient C+1.

Definition at line 1357 of file FspsUpd.h.

8.6.2.140 UINT8 FSP_S_CONFIG::PortUsb20Enable[16]

Offset 0x0052 - 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 218 of file FspsUpd.h.

8.6.2.141 UINT8 FSP_S_CONFIG::PortUsb30Enable[10]

Offset 0x0062 - 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 224 of file FspsUpd.h.

8.6.2.142 UINT16 FSP_S_CONFIG::Psi1Threshold[5]

Offset 0x02AC - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cuttof in 1/4 Amp increments.

Range is 0-128A. Default Value = 20A.

Definition at line 700 of file FspsUpd.h.

8.6.2.143 UINT16 FSP_S_CONFIG::Psi2Threshold[5]

Offset 0x02B6 - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cuttof in 1/4 Amp increments.

Range is 0-128A. Default Value = 5A.

Definition at line 706 of file FspsUpd.h.

8.6.2.144 UINT8 FSP_S_CONFIG::Psi3Enable[5]

Offset 0x024E - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; **1: Enable**.

For all VR Indexes

Definition at line 573 of file FspsUpd.h.

8.6.2.145 UINT16 FSP_S_CONFIG::Psi3Threshold[5]

Offset 0x02C0 - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cuttof in 1/4 Amp increments.

Range is 0-128A. Default Value = 1A.

Definition at line 712 of file FspsUpd.h.

8.6.2.146 UINT8 FSP_S_CONFIG::PsysOffset

Offset 0x0277 - 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 627 of file FspsUpd.h.

8.6.2.147 UINT8 FSP_S_CONFIG::PsysSlope

Offset 0x0276 - 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 621 of file FspsUpd.h.

8.6.2.148 UINT8 FSP_S_CONFIG::PxRcConfig[8]

Offset 0x007F - 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 265 of file FspsUpd.h.

8.6.2.149 UINT8 FSP_S_CONFIG::SataEnable

Offset 0x0091 - Enable SATA Enable/disable SATA controller.

$EN_DIS

Definition at line 306 of file FspsUpd.h.

8.6.2.150 UINT8 FSP_S_CONFIG::SataMode

Offset 0x0092 - SATA Mode Select SATA controller working mode.

0:AHCI, 1:RAID

Definition at line 312 of file FspsUpd.h.

8.6.2.151 UINT8 FSP_S_CONFIG::SataP0TDispFinit

Offset 0x06F7 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.

$EN_DIS

Definition at line 1914 of file FspsUpd.h.

8.6.2.152 UINT8 FSP_S_CONFIG::SataP1TDispFinit

Offset 0x06F9 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.

$EN_DIS

Definition at line 1925 of file FspsUpd.h.

8.6.2.153 UINT8 FSP_S_CONFIG::SataPortsDevSlp[8]

Offset 0x004A - 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 212 of file FspsUpd.h.

8.6.2.154 UINT8 FSP_S_CONFIG::SataPortsDmVal[8]

Offset 0x0690 - Enable SATA Port DmVal DITO multiplier.

Default is 15.

Definition at line 1601 of file FspsUpd.h.

8.6.2.155 UINT8 FSP_S_CONFIG::SataPortsEnable[8]

Offset 0x0042 - Enable SATA ports Enable/disable SATA ports.

One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 206 of file FspsUpd.h.

8.6.2.156 UINT8 FSP_S_CONFIG::SataPwrOptEnable

Offset 0x065D - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.

$EN_DIS

Definition at line 1555 of file FspsUpd.h.

8.6.2.157 UINT8 FSP_S_CONFIG::SataRstHddUnlock

Offset 0x06B8 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.

$EN_DIS

Definition at line 1664 of file FspsUpd.h.

8.6.2.158 UINT8 FSP_S_CONFIG::SataRstIrrt

Offset 0x06B5 - PCH Sata Rst Irrt Intel Rapid Recovery Technology.

$EN_DIS

Definition at line 1647 of file FspsUpd.h.

8.6.2.159 UINT8 FSP_S_CONFIG::SataRstIrrtOnly

Offset 0x06BA - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.

$EN_DIS

Definition at line 1677 of file FspsUpd.h.

8.6.2.160 UINT8 FSP_S_CONFIG::SataRstLedLocate

Offset 0x06B9 - 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 1671 of file FspsUpd.h.

8.6.2.161 UINT8 FSP_S_CONFIG::SataRstOromUiBanner

Offset 0x06B6 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.

$EN_DIS

Definition at line 1653 of file FspsUpd.h.

8.6.2.162 UINT8 FSP_S_CONFIG::SataRstPcieDeviceResetDelay[3]

Offset 0x06C2 - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.

Default value is 100ms

Definition at line 1698 of file FspsUpd.h.

8.6.2.163 UINT8 FSP_S_CONFIG::SataRstRaid0

Offset 0x06B1 - PCH Sata Rst Raid0 RAID0.

$EN_DIS

Definition at line 1623 of file FspsUpd.h.

8.6.2.164 UINT8 FSP_S_CONFIG::SataRstRaid1

Offset 0x06B2 - PCH Sata Rst Raid1 RAID1.

$EN_DIS

Definition at line 1629 of file FspsUpd.h.

8.6.2.165 UINT8 FSP_S_CONFIG::SataRstRaid10

Offset 0x06B3 - PCH Sata Rst Raid10 RAID10.

$EN_DIS

Definition at line 1635 of file FspsUpd.h.

8.6.2.166 UINT8 FSP_S_CONFIG::SataRstRaid5

Offset 0x06B4 - PCH Sata Rst Raid5 RAID5.

$EN_DIS

Definition at line 1641 of file FspsUpd.h.

8.6.2.167 UINT8 FSP_S_CONFIG::SataRstRaidAlternateId

Offset 0x06B0 - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.

0:Client, 1:Alternate, 2:Server

Definition at line 1617 of file FspsUpd.h.

8.6.2.168 UINT8 FSP_S_CONFIG::SataRstSmartStorage

Offset 0x06BB - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.

$EN_DIS

Definition at line 1683 of file FspsUpd.h.

8.6.2.169 UINT8 FSP_S_CONFIG::SataSalpSupport

Offset 0x0041 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.

$EN_DIS

Definition at line 200 of file FspsUpd.h.

8.6.2.170 UINT8 FSP_S_CONFIG::SataThermalSuggestedSetting

Offset 0x06FA - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.

$EN_DIS

Definition at line 1931 of file FspsUpd.h.

8.6.2.171 UINT8 FSP_S_CONFIG::SciIrqSelect

Offset 0x0088 - Select SciIrqSelect SCI IRQ Select.

The valid value is 9, 10, 11, and 20, 21, 22, 23 for APIC only.

Definition at line 275 of file FspsUpd.h.

8.6.2.172 UINT8 FSP_S_CONFIG::ScsEmmcEnabled

Offset 0x0031 - Enable eMMC Controller Enable/disable eMMC Controller.

$EN_DIS

Definition at line 143 of file FspsUpd.h.

8.6.2.173 UINT8 FSP_S_CONFIG::ScsEmmcHs400Enabled

Offset 0x0032 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.

$EN_DIS

Definition at line 149 of file FspsUpd.h.

8.6.2.174 UINT8 FSP_S_CONFIG::ScsSdCardEnabled

Offset 0x0033 - Enable SdCard Controller Enable/disable SD Card Controller.

$EN_DIS

Definition at line 155 of file FspsUpd.h.

8.6.2.175 UINT64 FSP_S_CONFIG::SendEcCmd

Offset 0x0730 - 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 2035 of file FspsUpd.h.

8.6.2.176 UINT8 FSP_S_CONFIG::SendVrMbxCmd

Offset 0x02E2 - 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 752 of file FspsUpd.h.

8.6.2.177 UINT8 FSP_S_CONFIG::SendVrMbxCmd1

Offset 0x02E3 - Select VR specific mailbox command to send VR specific mailbox commands.

000b - no VR specific command sent. 001b - VR mailbox command specifically for the MPS IMPV8 VR will be sent. 010b - VR specific command sent for PS4 exit issue. 100b - VR specific command sent for MPS VR decay issue.

Definition at line 759 of file FspsUpd.h.

8.6.2.178 UINT8 FSP_S_CONFIG::SerialIoDebugUartNumber

Offset 0x06D6 - UART Number For Debug Purpose UART number for debug purpose.

0:UART0, 1: UART1, 2:UART2.

Definition at line 1751 of file FspsUpd.h.

8.6.2.179 UINT8 FSP_S_CONFIG::SerialIoDevMode[11]

Offset 0x0074 - Enable SerialIo Device Mode 0:Disabled, 1:ACPI Mode, 2:PCI Mode, 3:Hidden mode, 4:Legacy UART mode - Enable/disable SerialIo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5,SPI0,SPI1,UART0,UART1,UART2 device mode respectively.

One byte for each controller, byte0 for I2C0, byte1 for I2C1, and so on.

Definition at line 258 of file FspsUpd.h.

8.6.2.180 UINT8 FSP_S_CONFIG::SerialIoGpio

Offset 0x06CA - Enable Pch Serial IO GPIO Determines if enable Serial IO GPIO.

$EN_DIS

Definition at line 1731 of file FspsUpd.h.

8.6.2.181 UINT8 FSP_S_CONFIG::ShowSpiController

Offset 0x0035 - Show SPI controller Enable/disable to show SPI controller.

$EN_DIS

Definition at line 167 of file FspsUpd.h.

8.6.2.182 UINT8 FSP_S_CONFIG::SlowSlewRateForGt

Offset 0x027B - 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 654 of file FspsUpd.h.

8.6.2.183 UINT8 FSP_S_CONFIG::SlowSlewRateForIa

Offset 0x027A - 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 647 of file FspsUpd.h.

8.6.2.184 UINT8 FSP_S_CONFIG::SlowSlewRateForSa

Offset 0x027C - 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 661 of file FspsUpd.h.

8.6.2.185 UINT8 FSP_S_CONFIG::SpiFlashCfgLockDown

Offset 0x0036 - 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 174 of file FspsUpd.h.

8.6.2.186 UINT8 FSP_S_CONFIG::SsicPortEnable

Offset 0x006D - Enable XHCI SSIC Enable Enable/disable XHCI SSIC port.

$EN_DIS

Definition at line 236 of file FspsUpd.h.

8.6.2.187 UINT8 FSP_S_CONFIG::TcoIrqSelect

Offset 0x0089 - Select TcoIrqSelect TCO IRQ Select.

The valid value is 9, 10, 11, 20, 21, 22, 23.

Definition at line 280 of file FspsUpd.h.

8.6.2.188 UINT16 FSP_S_CONFIG::TdcPowerLimit[5]

Offset 0x0286 - 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 671 of file FspsUpd.h.

8.6.2.189 UINT8 FSP_S_CONFIG::TdcTimeWindow[5]

Offset 0x026C - 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 609 of file FspsUpd.h.

8.6.2.190 UINT8 FSP_S_CONFIG::TTSuggestedSetting

Offset 0x06E6 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.

$EN_DIS

Definition at line 1825 of file FspsUpd.h.

8.6.2.191 UINT8 FSP_S_CONFIG::TurboMode

Offset 0x0040 - Turbo Mode Enable/Disable Turbo mode.

0: disable, 1: enable $EN_DIS

Definition at line 194 of file FspsUpd.h.

8.6.2.192 UINT8 FSP_S_CONFIG::Usb2AfePehalfbit[16]

Offset 0x00C3 - 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 336 of file FspsUpd.h.

8.6.2.193 UINT8 FSP_S_CONFIG::Usb2AfePetxiset[16]

Offset 0x0093 - 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 318 of file FspsUpd.h.

8.6.2.194 UINT8 FSP_S_CONFIG::Usb2AfePredeemp[16]

Offset 0x00B3 - 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 330 of file FspsUpd.h.

8.6.2.195 UINT8 FSP_S_CONFIG::Usb2AfeTxiset[16]

Offset 0x00A3 - 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 324 of file FspsUpd.h.

8.6.2.196 UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmph[10]

Offset 0x00DD - 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 348 of file FspsUpd.h.

8.6.2.197 UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmphEnable[10]

Offset 0x00D3 - 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 342 of file FspsUpd.h.

8.6.2.198 UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmp[10]

Offset 0x00F1 - 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 360 of file FspsUpd.h.

8.6.2.199 UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmpEnable[10]

Offset 0x00E7 - 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 354 of file FspsUpd.h.

8.6.2.200 UINT32 FSP_S_CONFIG::VrPowerDeliveryDesign

Offset 0x0290 - 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 678 of file FspsUpd.h.

8.6.2.201 UINT16 FSP_S_CONFIG::VrVoltageLimit[5]

Offset 0x02D4 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.

Range is 0-7999mV.

Definition at line 722 of file FspsUpd.h.

8.6.2.202 UINT8 FSP_S_CONFIG::WatchDog

Offset 0x0154 - WatchDog Timer Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable WatchDog timer. $EN_DIS

Definition at line 416 of file FspsUpd.h.

8.6.2.203 UINT16 FSP_S_CONFIG::WatchDogTimerBios

Offset 0x015A - BIOS Timer 16 bits Value, Set BIOS watchdog timer.

$EN_DIS

Definition at line 447 of file FspsUpd.h.

8.6.2.204 UINT16 FSP_S_CONFIG::WatchDogTimerOs

Offset 0x0158 - OS Timer 16 bits Value, Set OS watchdog timer.

$EN_DIS

Definition at line 441 of file FspsUpd.h.

8.6.2.205 UINT8 FSP_S_CONFIG::XdciEnable

Offset 0x006C - Enable xDCI controller Enable/disable to xDCI controller.

$EN_DIS

Definition at line 230 of file FspsUpd.h.

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

- FspsUpd.h

8.7 FSP_S_TEST_CONFIG Struct Reference

Fsp S Test Configuration.

`#include <FspsUpd.h>`

Public Attributes

- UINT32 Signature
  Offset 0x0780.
- UINT8 ChapDeviceEnable
  Offset 0x0784 - Enable/Disable Device 7 Enable: Device 7 enabled, Disable (Default): Device 7 disabled $EN_DIS.

- UINT8 SkipPamLock

  Offset 0x0785 - 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 0x0786 - 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 0x0787 - DMI Extended Sync Control Enable: Enable DMI Extended Sync Control, Disable(Default): Disable DMI Extended Sync Control $EN_DIS.
- UINT8 DmiIot

  Offset 0x0788 - DMI IOT Control Enable: Enable DMI IOT Control, Disable(Default): Disable DMI IOT Control $EN↩ _DIS.
- UINT8 PegMaxPayload [3]

  Offset 0x0789 - 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 0x078C - Enable/Disable IGFX RenderStandby Enable(Default): Enable IGFX RenderStandby, Disable: Disable IGFX RenderStandby $EN_DIS.
- UINT8 PmSupport

  Offset 0x078D - Enable/Disable IGFX PmSupport Enable(Default): Enable IGFX PmSupport, Disable: Disable IGFX PmSupport $EN_DIS.
- UINT8 CdynmaxClampEnable

  Offset 0x078E - Enable/Disable CdynmaxClamp Enable(Default): Enable CdynmaxClamp, Disable: Disable CdynmaxClamp $EN_DIS.
- UINT8 VtdDisable

  Offset 0x078F - Disable VT-d 0=Enable/FALSE(VT-d disabled), 1=Disable/TRUE (VT-d enabled) $EN_DIS.
- UINT8 GtFreqMax

  Offset 0x0790 - 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 SaPostMemTestRsvd [11]

  Offset 0x0791 - SaPostMemTestRsvd Reserved for SA Post-Mem Test $EN_DIS.
- UINT8 OneCoreRatioLimit

  Offset 0x079C - 1-Core Ratio Limit 1-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 TwoCoreRatioLimit

  Offset 0x079D - 2-Core Ratio Limit 2-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 ThreeCoreRatioLimit

  Offset 0x079E - 3-Core Ratio Limit 3-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 FourCoreRatioLimit

  Offset 0x079F - 4-Core Ratio Limit 4-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 UnusedUpdSpace22

  Offset 0x07A0.
- UINT8 Hwp

  Offset 0x07A1 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.
- UINT8 HdcControl

  Offset 0x07A2 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.
- UINT8 PowerLimit1Time

  Offset 0x07A3 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.
- UINT8 PowerLimit2

Offset 0x07A4 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

- UINT8 TurboPowerLimitLock

  *Offset 0x07A5 - Turbo settings Lock Lock all Turbo settings Enable/Disable; **0: Disable ,** 1: Enable $EN_DIS.*

- UINT8 PowerLimit3Time

  Offset 0x07A6 - Package PL3 time window Package PL3 time window range for this policy in milliseconds.

- UINT8 PowerLimit3DutyCycle

  Offset 0x07A7 - Package PL3 Duty Cycle Package PL3 Duty Cycle; Valid Range is 0 to 100.

- UINT8 PowerLimit3Lock

  *Offset 0x07A8 - Package PL3 Lock Package PL3 Lock Enable/Disable; **0: Disable ; 1: Enable $EN_DIS.***

- UINT8 PowerLimit4Lock

  *Offset 0x07A9 - Package PL4 Lock Package PL4 Lock Enable/Disable; **0: Disable ; 1: Enable $EN_DIS.***

- UINT8 TccActivationOffset

  Offset 0x07AA - TCC Activation Offset TCC Activation Offset.

- UINT8 TccOffsetClamp

  *Offset 0x07AB - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For SKL Y SKU, the recommended default for this policy is **1: Enabled**, For all other SKUs the recommended default are **0: Disabled**.*

- UINT8 TccOffsetLock

  *Offset 0x07AC - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; 1: Enabled.*

- UINT8 NumberOfEntries

  Offset 0x07AD - 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 0x07AE - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.

- UINT8 Custom1TurboActivationRatio

  Offset 0x07AF - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

- UINT8 Custom1ConfigTdpControl

  Offset 0x07B0 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

- UINT8 Custom2PowerLimit1Time

  Offset 0x07B1 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.

- UINT8 Custom2TurboActivationRatio

  Offset 0x07B2 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

- UINT8 Custom2ConfigTdpControl

  Offset 0x07B3 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

- UINT8 Custom3PowerLimit1Time

  Offset 0x07B4 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.

- UINT8 Custom3TurboActivationRatio

  Offset 0x07B5 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

- UINT8 Custom3ConfigTdpControl

  Offset 0x07B6 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

- UINT8 ConfigTdpLock

  *Offset 0x07B7 - ConfigTdp mode settings Lock Lock the ConfigTdp mode settings from runtime changes; **0: Disable**; 1: Enable $EN_DIS.*

- UINT8 ConfigTdpBios

  *Offset 0x07B8 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.*

- UINT8 PsysPowerLimit1

  Offset 0x07B9 - PL1 Enable value PL1 Enable value to limit average platform power.

- UINT8 PsysPowerLimit1Time

Offset 0x07BA - PL1 timewindow PL1 timewindow in seconds.Valid values(Unit in seconds) 0 to 8 , 10 , 12 ,14 , 16 , 20 , 24 , 28 , 32 , 40 , 48 , 56 , 64 , 80 , 96 , 112 , 128.

- UINT8 PsysPowerLimit2

  Offset 0x07BB - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

- UINT8 UnusedUpdSpace23 [2]

  Offset 0x07BC.

- UINT8 MlcStreamerPrefetcher

  *Offset 0x07BE - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0: Disable; **1: Enable**.*

- UINT8 MlcSpatialPrefetcher

  *Offset 0x07BF - Enable or Disable MLC Spatial Prefetcher Enable or Disable MLC Spatial Prefetcher; 0: Disable; **1: Enable** $EN_DIS.*

- UINT8 MonitorMwaitEnable

  *Offset 0x07C0 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable**.*

- UINT8 MachineCheckEnable

  *Offset 0x07C1 - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.*

- UINT8 DebugInterfaceEnable

  *Offset 0x07C2 - Enable or Disable processor debug features Enable or Disable processor debug features; **0: Disable**; 1: Enable.*

- UINT8 DebugInterfaceLockEnable

  *Offset 0x07C3 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; **1: Enable**.*

- UINT8 ApIdleManner

  *Offset 0x07C4 - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.*

- UINT8 ApHandoffManner

  *Offset 0x07C5 - Settings for AP Handoff to OS Settings for AP Handoff to OS; 1: HALT loop; **2: MWAIT loop**.*

- UINT8 UnusedUpdSpace24 [2]

  Offset 0x07C6.

- UINT8 ProcTraceOutputScheme

  *Offset 0x07C8 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.*

- UINT8 ProcTraceEnable

  *Offset 0x07C9 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.*

- UINT8 ProcTraceMemSize

  Offset 0x07CA - Memory region allocation for Processor Trace Memory region allocation for Processor Trace, Total Memory required is up to requested value ∗ 2 (for memory alignment) ∗ 8 active threads, to enable Processor Trace, PcdFspReservedMemoryLength must be increased by the total memory required, and PlatformMemorySize policy must also be increased by the total memory required over 32MB, Valid Values are 0 - 4KB , 0x1 - 8KB , 0x2 - 16KB , 0x3 - 32KB , 0x4 - 64KB , 0x5 - 128KB , 0x6 - 256KB , 0x7 - 512KB , 0x8 - 1MB , 0x9 - 2MB , 0xA - 4MB , 0xB - 8MB , 0xC - 16MB , 0xD - 32MB , 0xE - 64MB , 0xF - 128MB , 0xFF: Disable.

- UINT8 UnusedUpdSpace25

  Offset 0x07CB.

- UINT8 VoltageOptimization

  *Offset 0x07CC - Enable or Disable Voltage Optimization feature Enable or Disable Voltage Optimization feature 0: Disable; **1: Enable** $EN_DIS.*

- UINT8 Eist

  Offset 0x07CD - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

- UINT8 EnergyEfficientPState

  Offset 0x07CE - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.

- UINT8 EnergyEfficientTurbo

  Offset 0x07CF - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.
- UINT8 TStates

  *Offset 0x07D0 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.*
- UINT8 BiProcHot

  *Offset 0x07D1 - Enable or Disable Bi-Directional PROCHOT# Enable or Disable Bi-Directional PROCHOT#; 0: Disable; **1: Enable** $EN_DIS.*
- UINT8 DisableProcHotOut

  *Offset 0x07D2 - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; **1: Enable**.*
- UINT8 ProcHotResponse

  *Offset 0x07D3 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.*
- UINT8 DisableVrThermalAlert

  *Offset 0x07D4 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.*
- UINT8 AutoThermalReporting

  *Offset 0x07D5 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; **1: Enable**.*
- UINT8 ThermalMonitor

  *Offset 0x07D6 - Enable or Disable Thermal Monitor Enable or Disable Thermal Monitor; 0: Disable; **1: Enable** $EN_DIS.*
- UINT8 Cx

  Offset 0x07D7 - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).
- UINT8 PmgCstCfgCtrlLock

  *Offset 0x07D8 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; **1: Enable**.*
- UINT8 C1e

  Offset 0x07D9 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.
- UINT8 PkgCStateDemotion

  Offset 0x07DA - Enable or Disable Package C-State Demotion Enable or Disable Package C-State Demotion.
- UINT8 PkgCStateUnDemotion

  Offset 0x07DB - Enable or Disable Package C-State UnDemotion Enable or Disable Package C-State UnDemotion.
- UINT8 CStatePreWake

  Offset 0x07DC - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.
- UINT8 TimedMwait

  Offset 0x07DD - Enable or Disable TimedMwait Support.
- UINT8 CstCfgCtrIoMwaitRedirection

  *Offset 0x07DE - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.*
- UINT8 PkgCStateLimit

  Offset 0x07DF - Set the Max Pkg Cstate Set the Max Pkg Cstate.
- UINT8 CstateLatencyControl0TimeUnit

  Offset 0x07E0 - 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 0x07E1 - 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 0x07E2 - 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 0x07E3 - 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 0x07E4 - TimeUnit for C-State Latency Control4 TimeUnit for C-State Latency Control4;Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.
- UINT8 CstateLatencyControl5TimeUnit

  Offset 0x07E5 - 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 0x07E6 - 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 0x07E7 - Lock prochot configuration Lock prochot configuration Enable/Disable; **0: Disable**; 1: Enable $EN↩ _DIS.*
- UINT8 ConfigTdpLevel

  *Offset 0x07E8 - Configuration for boot TDP selection Configuration for boot TDP selection; **0: TDP Nominal**; 1: TDP Down; 2: TDP Up; 0xFF: Deactivate 0:TDP Nominal, 1:TDP Down, 2:TDP Up, 0xFF:Deactivate.*
- UINT8 RaceToHalt

  Offset 0x07E9 - Race To Halt Enable/Disable Race To Halt feature.
- UINT16 MaxRatio

  Offset 0x07EA - Max P-State Ratio Max P-State Ratio , Valid Range 0 to 0x7F.
- UINT16 StateRatio [40]

  Offset 0x07EC - Maximum P-state ratio to use in the custom P-state table Maximum P-state ratio to use in the custom P-state table.
- UINT16 CstateLatencyControl0Irtl

  Offset 0x083C - Interrupt Response Time Limit of C-State LatencyContol0 Interrupt Response Time Limit of C-State LatencyContol0.Range of value 0 to 0x3FF, Default is 0x4E, Server Platform is 0x4B.
- UINT16 CstateLatencyControl1Irtl

  Offset 0x083E - Interrupt Response Time Limit of C-State LatencyContol1 Interrupt Response Time Limit of C-State LatencyContol1.Range of value 0 to 0x3FF, Default is 0x76, Server Platform is 0x6B.
- UINT16 CstateLatencyControl2Irtl

  Offset 0x0840 - 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 0x0842 - 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 0x0844 - 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 0x0846 - Interrupt Response Time Limit of C-State LatencyContol5 Interrupt Response Time Limit of C-State LatencyContol5.Range of value 0 to 0x3FF.
- UINT32 PowerLimit1

  Offset 0x0848 - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.
- UINT32 PowerLimit2Power

  Offset 0x084C - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.
- UINT32 PowerLimit3

  Offset 0x0850 - Package PL3 power limit Package PL3 power limit.
- UINT32 PowerLimit4

  Offset 0x0854 - Package PL4 power limit Package PL4 power limit.
- UINT32 TccOffsetTimeWindowForRatl

  Offset 0x0858 - Tcc Offset Time Window for RATL Package PL4 power limit.
- UINT32 Custom1PowerLimit1

  Offset 0x085C - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.

- UINT32 Custom1PowerLimit2

  Offset 0x0860 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.
- UINT32 Custom2PowerLimit1

  Offset 0x0864 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.
- UINT32 Custom2PowerLimit2

  Offset 0x0868 - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.
- UINT32 Custom3PowerLimit1

  Offset 0x086C - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.
- UINT32 Custom3PowerLimit2

  Offset 0x0870 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.
- UINT32 PsysPowerLimit1Power

  Offset 0x0874 - Platform PL1 power Platform PL1 power.
- UINT32 PsysPowerLimit2Power

  Offset 0x0878 - Platform PL2 power Platform PL2 power.
- UINT16 PsysPmax

  Offset 0x087C - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.
- UINT16 CpuS3ResumeDataSize

  Offset 0x087E - CpuS3ResumeDataSize Size of CPU S3 Resume Data.
- UINT32 CpuS3ResumeData

  Offset 0x0880 - CpuS3ResumeData Pointer to CPU S3 Resume Data.
- UINT8 FiveCoreRatioLimit

  Offset 0x0884 - 5-Core Ratio Limit 5-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 SixCoreRatioLimit

  Offset 0x0885 - 6-Core Ratio Limit 6-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 SevenCoreRatioLimit

  Offset 0x0886 - 7-Core Ratio Limit 7-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 EightCoreRatioLimit

  Offset 0x0887 - 8-Core Ratio Limit 8-Core Ratio Limit: LFM to Fused max, For overclocking part: LFM to 255.
- UINT8 ThreeStrikeCounterDisable

  *Offset 0x0888 - 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 ReservedCpuPostMemTest [1]

  Offset 0x0889 - ReservedCpuPostMemTest Reserved for CPU Post-Mem Test $EN_DIS.
- UINT8 SgxSinitDataFromTpm

  Offset 0x088A - SgxSinitDataFromTpm SgxSinitDataFromTpm default values.
- UINT8 EndOfPostMessage

  Offset 0x088B - End of Post message Test, Send End of Post message.
- UINT8 DisableD0I3SettingForHeci

  Offset 0x088C - D0I3 Setting for HECI Disable Test, 0: disable, 1: enable, Setting this option disables setting D0I3 bit for all HECI devices $EN_DIS.
- UINT8 PchLockDownGlobalSmi

  Offset 0x088D - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.
- UINT16 PchHdaResetWaitTimer

  Offset 0x088E - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.
- UINT8 PchLockDownBiosInterface

  Offset 0x0890 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

- UINT8 PchLockDownRtcLock

  Offset 0x0891 - RTC CMOS RAM 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 PchSbiUnlock

  Offset 0x0892 - PCH Sbi lock bit This unlock the SBI lock bit to allow SBI after post time.
- UINT8 PchSbAccessUnlock

  Offset 0x0893 - PCH Psf lock bit The PSF registers will be locked before 3rd party code execution.
- UINT16 PcieRpLtrMaxSnoopLatency [24]

  Offset 0x0894 - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.
- UINT16 PcieRpLtrMaxNoSnoopLatency [24]

  Offset 0x08C4 - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.
- UINT8 PcieRpSnoopLatencyOverrideMode [24]

  Offset 0x08F4 - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.
- UINT8 PcieRpSnoopLatencyOverrideMultiplier [24]

  Offset 0x090C - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.
- UINT16 PcieRpSnoopLatencyOverrideValue [24]

  Offset 0x0924 - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.
- UINT8 PcieRpNonSnoopLatencyOverrideMode [24]

  Offset 0x0954 - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.
- UINT8 PcieRpNonSnoopLatencyOverrideMultiplier [24]

  Offset 0x096C - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.
- UINT16 PcieRpNonSnoopLatencyOverrideValue [24]

  Offset 0x0984 - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.
- UINT8 PcieRpSlotPowerLimitScale [24]

  Offset 0x09B4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.
- UINT16 PcieRpSlotPowerLimitValue [24]

  Offset 0x09CC - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.
- UINT8 PcieRpUptp [24]

  Offset 0x09FC - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.
- UINT8 PcieRpDptp [24]

  Offset 0x0A14 - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.
- UINT8 PcieEnablePort8xhDecode

  Offset 0x0A2C - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.
- UINT8 PchPciePort8xhDecodePortIndex

  Offset 0x0A2D - PCIE Port8xh Decode Port Index The Index of PCIe Port that is selected for Port8xh Decode (0 Based).
- UINT8 PchPmDisableEnergyReport

  Offset 0x0A2E - PCH Pm Disable Energy Report Disable/Enable PCH to CPU enery report feature.
- UINT8 PchPmPmcReadDisable

  Offset 0x0A2F - PCH Pm Pmc Read Disable Deprecated $EN_DIS.
- UINT8 SataTestMode

  Offset 0x0A30 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.
- UINT8 ReservedFspsTestUpd [15]

  Offset 0x0A31.

8.7.1 Detailed Description

Fsp S Test Configuration.

Definition at line 2096 of file FspsUpd.h.

8.7.2 Member Data Documentation

8.7.2.1 UINT8 FSP_S_TEST_CONFIG::ApHandoffManner

Offset 0x07C5 - Settings for AP Handoff to OS Settings for AP Handoff to OS; 1: HALT loop; **2: MWAIT loop**.

1:HALT loop, 2:MWAIT loop

Definition at line 2424 of file FspsUpd.h.

8.7.2.2 UINT8 FSP_S_TEST_CONFIG::ApIdleManner

Offset 0x07C4 - 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 2418 of file FspsUpd.h.

8.7.2.3 UINT8 FSP_S_TEST_CONFIG::AutoThermalReporting

Offset 0x07D5 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2517 of file FspsUpd.h.

8.7.2.4 UINT8 FSP_S_TEST_CONFIG::C1e

Offset 0x07D9 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

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

Definition at line 2541 of file FspsUpd.h.

8.7.2.5 UINT8 FSP_S_TEST_CONFIG::ConfigTdpBios

Offset 0x07B8 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2353 of file FspsUpd.h.

8.7.2.6 UINT8 FSP_S_TEST_CONFIG::CStatePreWake

Offset 0x07DC - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

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

Definition at line 2561 of file FspsUpd.h.

8.7.2.7 UINT8 FSP_S_TEST_CONFIG::CstCfgCtrIoMwaitRedirection

Offset 0x07DE - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2573 of file FspsUpd.h.

8.7.2.8 UINT8 FSP_S_TEST_CONFIG::Custom1ConfigTdpControl

Offset 0x07B0 - 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 2311 of file FspsUpd.h.

8.7.2.9 UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit1

Offset 0x085C - 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 2723 of file FspsUpd.h.

8.7.2.10 UINT8 FSP_S_TEST_CONFIG::Custom1PowerLimit1Time

Offset 0x07AE - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.

Valid Range 0 to 128

Definition at line 2301 of file FspsUpd.h.

8.7.2.11 UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit2

Offset 0x0860 - 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 2729 of file FspsUpd.h.

8.7.2.12 UINT8 FSP_S_TEST_CONFIG::Custom1TurboActivationRatio

Offset 0x07AF - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

Valid Range 0 to 255

Definition at line 2306 of file FspsUpd.h.

8.7.2.13 UINT8 FSP_S_TEST_CONFIG::Custom2ConfigTdpControl

Offset 0x07B3 - 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 2326 of file FspsUpd.h.

8.7.2.14 UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit1

Offset 0x0864 - 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 2735 of file FspsUpd.h.

8.7.2.15 UINT8 FSP_S_TEST_CONFIG::Custom2PowerLimit1Time

Offset 0x07B1 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.

Valid Range 0 to 128

Definition at line 2316 of file FspsUpd.h.

8.7.2.16 UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit2

Offset 0x0868 - 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 2741 of file FspsUpd.h.

8.7.2.17 UINT8 FSP_S_TEST_CONFIG::Custom2TurboActivationRatio

Offset 0x07B2 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

Valid Range 0 to 255

Definition at line 2321 of file FspsUpd.h.

8.7.2.18 UINT8 FSP_S_TEST_CONFIG::Custom3ConfigTdpControl

Offset 0x07B6 - 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 2341 of file FspsUpd.h.

8.7.2.19 UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit1

Offset 0x086C - 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 2747 of file FspsUpd.h.

8.7.2.20 UINT8 FSP_S_TEST_CONFIG::Custom3PowerLimit1Time

Offset 0x07B4 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.

Valid Range 0 to 128

Definition at line 2331 of file FspsUpd.h.

8.7.2.21 UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit2

Offset 0x0870 - 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 2753 of file FspsUpd.h.

8.7.2.22 UINT8 FSP_S_TEST_CONFIG::Custom3TurboActivationRatio

Offset 0x07B5 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

Valid Range 0 to 255

Definition at line 2336 of file FspsUpd.h.

8.7.2.23 UINT8 FSP_S_TEST_CONFIG::Cx

Offset 0x07D7 - 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 2529 of file FspsUpd.h.

8.7.2.24 UINT8 FSP_S_TEST_CONFIG::DebugInterfaceEnable

Offset 0x07C2 - Enable or Disable processor debug features Enable or Disable processor debug features; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2406 of file FspsUpd.h.

8.7.2.25 UINT8 FSP_S_TEST_CONFIG::DebugInterfaceLockEnable

Offset 0x07C3 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2412 of file FspsUpd.h.

8.7.2.26 UINT8 FSP_S_TEST_CONFIG::DisableProcHotOut

Offset 0x07D2 - 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 2499 of file FspsUpd.h.

8.7.2.27 UINT8 FSP_S_TEST_CONFIG::DisableVrThermalAlert

Offset 0x07D4 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2511 of file FspsUpd.h.

8.7.2.28 UINT8 FSP_S_TEST_CONFIG::EightCoreRatioLimit

Offset 0x0887 - 8-Core Ratio Limit 8-Core Ratio Limit: LFM to Fused max, 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

Definition at line 2805 of file FspsUpd.h.

8.7.2.29 UINT8 FSP_S_TEST_CONFIG::Eist

Offset 0x07CD - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

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

Definition at line 2467 of file FspsUpd.h.

8.7.2.30 UINT8 FSP_S_TEST_CONFIG::EndOfPostMessage

Offset 0x088B - End of Post message Test, Send End of Post message.

Disable(0x0): Disable EOP message, Send in PEI(0x1): EOP send in PEI, Send in DXE(0x2)(Default): EOP send in PEI 0:Disable, 1:Send in PEI, 2:Send in DXE, 3:Reserved

Definition at line 2830 of file FspsUpd.h.

8.7.2.31 UINT8 FSP_S_TEST_CONFIG::EnergyEfficientPState

Offset 0x07CE - 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 2474 of file FspsUpd.h.

8.7.2.32 UINT8 FSP_S_TEST_CONFIG::EnergyEfficientTurbo

Offset 0x07CF - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.

Disable; **1: Enable** $EN_DIS

Definition at line 2481 of file FspsUpd.h.

8.7.2.33 UINT8 FSP_S_TEST_CONFIG::FiveCoreRatioLimit

Offset 0x0884 - 5-Core Ratio Limit 5-Core Ratio Limit: LFM to Fused max, 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

Definition at line 2787 of file FspsUpd.h.

8.7.2.34 UINT8 FSP_S_TEST_CONFIG::FourCoreRatioLimit

Offset 0x079F - 4-Core Ratio Limit 4-Core Ratio Limit: LFM to Fused max, 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 2209 of file FspsUpd.h.

8.7.2.35 UINT8 FSP_S_TEST_CONFIG::HdcControl

Offset 0x07A2 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

0: Disabled; **1: Enabled** 2-3:Reserved $EN_DIS

Definition at line 2226 of file FspsUpd.h.

8.7.2.36 UINT8 FSP_S_TEST_CONFIG::Hwp

Offset 0x07A1 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

0: Disable; **1: Enable;** 2-3:Reserved $EN_DIS

Definition at line 2220 of file FspsUpd.h.

8.7.2.37 UINT8 FSP_S_TEST_CONFIG::MachineCheckEnable

Offset 0x07C1 - 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 2400 of file FspsUpd.h.

8.7.2.38 UINT8 FSP_S_TEST_CONFIG::MlcStreamerPrefetcher

Offset 0x07BE - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0↩ : Disable; **1: Enable**.

$EN_DIS

Definition at line 2382 of file FspsUpd.h.

8.7.2.39 UINT8 FSP_S_TEST_CONFIG::MonitorMwaitEnable

Offset 0x07C0 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2394 of file FspsUpd.h.

8.7.2.40 UINT8 FSP_S_TEST_CONFIG::NumberOfEntries

Offset 0x07AD - 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 2296 of file FspsUpd.h.

8.7.2.41 UINT8 FSP_S_TEST_CONFIG::OneCoreRatioLimit

Offset 0x079C - 1-Core Ratio Limit 1-Core Ratio Limit: LFM to Fused max, 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 2191 of file FspsUpd.h.

8.7.2.42 UINT16 FSP_S_TEST_CONFIG::PchHdaResetWaitTimer

Offset 0x088E - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.

Default is 600.

Definition at line 2848 of file FspsUpd.h.

8.7.2.43 UINT8 FSP_S_TEST_CONFIG::PchLockDownBiosInterface

Offset 0x0890 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

$EN_DIS

Definition at line 2854 of file FspsUpd.h.

8.7.2.44 UINT8 FSP_S_TEST_CONFIG::PchLockDownGlobalSmi

Offset 0x088D - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.

$EN_DIS

Definition at line 2843 of file FspsUpd.h.

8.7.2.45 UINT8 FSP_S_TEST_CONFIG::PchLockDownRtcLock

Offset 0x0891 - RTC CMOS RAM 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 2861 of file FspsUpd.h.

8.7.2.46 UINT8 FSP_S_TEST_CONFIG::PchPmDisableEnergyReport

Offset 0x0A2E - PCH Pm Disable Energy Report Disable/Enable PCH to CPU enery report feature.

$EN_DIS

Definition at line 2951 of file FspsUpd.h.

8.7.2.47 UINT8 FSP_S_TEST_CONFIG::PchSbAccessUnlock

Offset 0x0893 - PCH Psf lock bit The PSF registers will be locked before 3rd party code execution.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2873 of file FspsUpd.h.

8.7.2.48 UINT8 FSP_S_TEST_CONFIG::PchSbiUnlock

Offset 0x0892 - PCH Sbi lock bit This unlock the SBI lock bit to allow SBI after post time.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2867 of file FspsUpd.h.

8.7.2.49 UINT8 FSP_S_TEST_CONFIG::PcieEnablePort8xhDecode

Offset 0x0A2C - 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 2940 of file FspsUpd.h.

8.7.2.50 UINT8 FSP_S_TEST_CONFIG::PcieRpDptp[24]

Offset 0x0A14 - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 2933 of file FspsUpd.h.

8.7.2.51 UINT8 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitScale[24]

Offset 0x09B4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

Leave as 0 to set to default.

Definition at line 2918 of file FspsUpd.h.

8.7.2.52 UINT16 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitValue[24]

Offset 0x09CC - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.

Leave as 0 to set to default.

Definition at line 2923 of file FspsUpd.h.

8.7.2.53 UINT8 FSP_S_TEST_CONFIG::PcieRpUptp[24]

Offset 0x09FC - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 2928 of file FspsUpd.h.

8.7.2.54 UINT8 FSP_S_TEST_CONFIG::PkgCStateDemotion

Offset 0x07DA - Enable or Disable Package C-State Demotion Enable or Disable Package C-State Demotion.

0: Disable; 1: Enable; **2: Auto** (Auto: Enabled for Skylake; Disabled for Kabylake) 0:Disable, 1:Enable, 2:Auto

Definition at line 2548 of file FspsUpd.h.

8.7.2.55 UINT8 FSP_S_TEST_CONFIG::PkgCStateLimit

Offset 0x07DF - 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 2580 of file FspsUpd.h.

8.7.2.56 UINT8 FSP_S_TEST_CONFIG::PkgCStateUnDemotion

Offset 0x07DB - Enable or Disable Package C-State UnDemotion Enable or Disable Package C-State UnDemotion.

0: Disable; 1: Enable; **2: Auto** (Auto: Enabled for Skylake; Disabled for Kabylake) 0:Disable, 1:Enable, 2:Auto

Definition at line 2555 of file FspsUpd.h.

8.7.2.57 UINT8 FSP_S_TEST_CONFIG::PmgCstCfgCtrlLock

Offset 0x07D8 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; **1: Enable**.

$EN_DIS

Definition at line 2535 of file FspsUpd.h.

8.7.2.58 UINT32 FSP_S_TEST_CONFIG::PowerLimit1

Offset 0x0848 - 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 2693 of file FspsUpd.h.

8.7.2.59 UINT8 FSP_S_TEST_CONFIG::PowerLimit1Time

Offset 0x07A3 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.

Valid values(Unit in seconds) 0 to 8 , 10 , 12 ,14 , 16 , 20 , 24 , 28 , 32 , 40 , 48 , 56 , 64 , 80 , 96 , 112 , 128

Definition at line 2232 of file FspsUpd.h.

8.7.2.60 UINT8 FSP_S_TEST_CONFIG::PowerLimit2

Offset 0x07A4 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

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

Definition at line 2238 of file FspsUpd.h.

8.7.2.61 UINT32 FSP_S_TEST_CONFIG::PowerLimit2Power

Offset 0x084C - 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 2699 of file FspsUpd.h.

8.7.2.62 UINT32 FSP_S_TEST_CONFIG::PowerLimit3

Offset 0x0850 - 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 2705 of file FspsUpd.h.

8.7.2.63 UINT8 FSP_S_TEST_CONFIG::PowerLimit3Time

Offset 0x07A6 - Package PL3 time window Package PL3 time window range for this policy in milliseconds.

Valid values are 0, 3 to 8, 10, 12, 14, 16, 20 , 24, 28, 32, 40, 48, 55, 56, 64

Definition at line 2250 of file FspsUpd.h.

8.7.2.64 UINT32 FSP_S_TEST_CONFIG::PowerLimit4

Offset 0x0854 - Package PL4 power limit Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 2711 of file FspsUpd.h.

8.7.2.65 UINT8 FSP_S_TEST_CONFIG::ProcHotResponse

Offset 0x07D3 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2505 of file FspsUpd.h.

8.7.2.66 UINT8 FSP_S_TEST_CONFIG::ProcTraceEnable

Offset 0x07C9 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2440 of file FspsUpd.h.

8.7.2.67 UINT8 FSP_S_TEST_CONFIG::ProcTraceOutputScheme

Offset 0x07C8 - 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 2434 of file FspsUpd.h.

8.7.2.68 UINT16 FSP_S_TEST_CONFIG::PsysPmax

Offset 0x087C - 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 2771 of file FspsUpd.h.

8.7.2.69 UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit1

Offset 0x07B9 - PL1 Enable value PL1 Enable value to limit average platform power.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2359 of file FspsUpd.h.

8.7.2.70 UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit1Power

Offset 0x0874 - 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 2759 of file FspsUpd.h.

8.7.2.71 UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit2

Offset 0x07BB - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

0: Disable; 1: Enable. $EN_DIS

Definition at line 2372 of file FspsUpd.h.

8.7.2.72 UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit2Power

Offset 0x0878 - 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 2765 of file FspsUpd.h.

8.7.2.73 UINT8 FSP_S_TEST_CONFIG::RaceToHalt

Offset 0x07E9 - 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 2643 of file FspsUpd.h.

8.7.2.74 UINT8 FSP_S_TEST_CONFIG::SataTestMode

Offset 0x0A30 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

$EN_DIS

Definition at line 2963 of file FspsUpd.h.

8.7.2.75 UINT8 FSP_S_TEST_CONFIG::SevenCoreRatioLimit

Offset 0x0886 - 7-Core Ratio Limit 7-Core Ratio Limit: LFM to Fused max, 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

Definition at line 2799 of file FspsUpd.h.

8.7.2.76 UINT8 FSP_S_TEST_CONFIG::SixCoreRatioLimit

Offset 0x0885 - 6-Core Ratio Limit 6-Core Ratio Limit: LFM to Fused max, 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

Definition at line 2793 of file FspsUpd.h.

8.7.2.77 UINT16 FSP_S_TEST_CONFIG::StateRatio[40]

Offset 0x07EC - Maximum P-state ratio to use in the custom P-state table Maximum P-state ratio to use in the custom P-state table.

NumOfCustomPStates has valid range between 0 to 40. For no. of P-States supported(NumOfCustomPStates) , StateRatio[NumOfCustomPStates] are configurable. Valid Range of value is 0 to 0x7F

Definition at line 2655 of file FspsUpd.h.

8.7.2.78 UINT8 FSP_S_TEST_CONFIG::TccActivationOffset

Offset 0x07AA - 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 SKL Y SKU, the recommended default for this policy is **10**, For all other SKUs the recommended default are **0**

Definition at line 2275 of file FspsUpd.h.

8.7.2.79 UINT8 FSP_S_TEST_CONFIG::TccOffsetClamp

Offset 0x07AB - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For SKL 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 2283 of file FspsUpd.h.

8.7.2.80 UINT8 FSP_S_TEST_CONFIG::TccOffsetLock

Offset 0x07AC - 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 2290 of file FspsUpd.h.

8.7.2.81 UINT32 FSP_S_TEST_CONFIG::TccOffsetTimeWindowForRatl

Offset 0x0858 - Tcc Offset Time Window for RATL Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125

Definition at line 2717 of file FspsUpd.h.

8.7.2.82 UINT8 FSP_S_TEST_CONFIG::ThreeCoreRatioLimit

Offset 0x079E - 3-Core Ratio Limit 3-Core Ratio Limit: LFM to Fused max, 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 2203 of file FspsUpd.h.

8.7.2.83 UINT8 FSP_S_TEST_CONFIG::ThreeStrikeCounterDisable

Offset 0x0888 - 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 2812 of file FspsUpd.h.

8.7.2.84 UINT8 FSP_S_TEST_CONFIG::TimedMwait

Offset 0x07DD - Enable or Disable TimedMwait Support.

Enable or Disable TimedMwait Support. **0: Disable**; 1: Enable $EN_DIS

Definition at line 2567 of file FspsUpd.h.

8.7.2.85 UINT8 FSP_S_TEST_CONFIG::TStates

Offset 0x07D0 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.

$EN_DIS

Definition at line 2487 of file FspsUpd.h.

8.7.2.86 UINT8 FSP_S_TEST_CONFIG::TwoCoreRatioLimit

Offset 0x079D - 2-Core Ratio Limit 2-Core Ratio Limit: LFM to Fused max, 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 2197 of file FspsUpd.h.

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

- FspsUpd.h

8.8 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 Select SerialIo Uart Controller for debug.
- UINT8 UnusedUpdSpace0 [2]

  Offset 0x0042.
- UINT32 PcdSerialIoUartInputClock

  Offset 0x0044.
- 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 ReservedFsptUpd1 [12]

  Offset 0x0054.

8.8.1 Detailed Description

Fsp T Configuration.

Definition at line 69 of file FsptUpd.h.

8.8.2 Member Data Documentation

8.8.2.1 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 75 of file FsptUpd.h.

8.8.2.2 UINT8 FSP_T_CONFIG::PcdSerialIoUartNumber

Offset 0x0041 - PcdSerialIoUartNumber Select SerialIo Uart Controller for debug.

0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 81 of file FsptUpd.h.

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

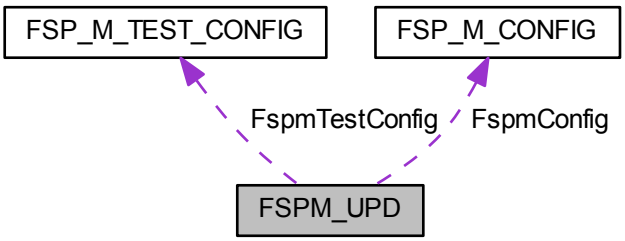
- FsptUpd.h

8.9 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 0x0520.
- UINT8 UnusedUpdSpace10 [134]
  Offset 0x05C0.

- UINT16 UpdTerminator
  Offset 0x0646.

8.9.1 Detailed Description

Fsp M UPD Configuration.

Definition at line 1685 of file FspmUpd.h.

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

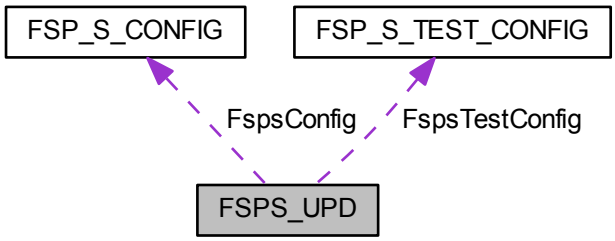
- FspmUpd.h

8.10 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 0x0780.
- UINT8 UnusedUpdSpace26 [470]
  Offset 0x0A40.
- UINT16 UpdTerminator
  Offset 0x0C16.

8.10.1 Detailed Description

Fsp S UPD Configuration.

Definition at line 2972 of file FspsUpd.h.

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

- FspsUpd.h

8.11 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.

8.11.1 Detailed Description

Fsp T Core UPD.

Definition at line 44 of file FsptUpd.h.

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

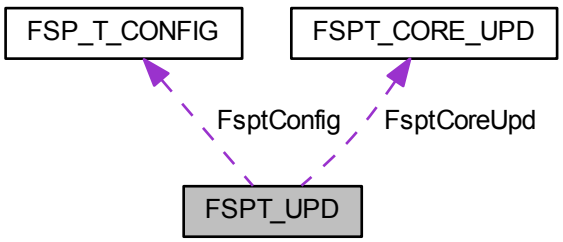
- FsptUpd.h

8.12 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.
- UINT8 UnusedUpdSpace1 [6]

  Offset 0x0060.
- UINT16 UpdTerminator

  Offset 0x0066.

8.12.1 Detailed Description

Fsp T UPD Configuration.

Definition at line 108 of file FsptUpd.h.

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

- FsptUpd.h

8.13 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.

8.13.1 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.

8.13.2 Member Data Documentation

8.13.2.1 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.

8.13.2.2 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.

8.13.2.3 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.

8.13.2.4 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.

8.13.2.5 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.

8.13.2.6 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.

8.13.2.7 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.

8.13.2.8 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

8.14 MEMORY_PLATFORM_DATA Struct Reference

Memory Platform Data Hob.

`#include <MemInfoHob.h>`

8.14.1 Detailed Description

Memory Platform Data Hob.

Revision 1:

- Initial version. **Revision 2:**
- Added TsegBase, PrmrrSize, PrmrrBase, Gttbase, MmioSize, PciEBaseAddress fields

Definition at line 259 of file MemInfoHob.h.

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

- MemInfoHob.h

8.15 SI_CHIPSET_INIT_INFO Struct Reference

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

`#include <FspmUpd.h>`

8.15.1 Detailed Description

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

Definition at line 47 of file FspmUpd.h.

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

- FspmUpd.h

8.16 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.

8.16.1 Detailed Description

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

Definition at line 76 of file FspsUpd.h.

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

- FspsUpd.h

8.17 SMBIOS_CACHE_INFO Struct Reference

SMBIOS Cache Info HOB Structure.

`#include <SmbiosCacheInfoHob.h>`

Public Attributes

- 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.

8.17.1 Detailed Description

SMBIOS Cache Info HOB Structure.

Definition at line 32 of file SmbiosCacheInfoHob.h.

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

- SmbiosCacheInfoHob.h

8.18 SMBIOS_PROCESSOR_INFO Struct Reference

SMBIOS Processor Info HOB Structure.

`#include <SmbiosProcessorInfoHob.h>`

Public Attributes

- UINT8 ProcessorType

  ENUM defined in SMBIOS Spec v3.0 Section 7.5.1.

- UINT16 ProcessorFamily

  This info is used for both ProcessorFamily and ProcessorFamily2 fields See ENUM defined in SMBIOS Spec v3.0 Section 7.5.2.

- 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.

- UINT16 CoreCount

  This info is used for both CoreCount & CoreCount2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.6.

- UINT16 EnabledCoreCount

  This info is used for both CoreEnabled & CoreEnabled2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.7.

- UINT16 ThreadCount

This info is used for both ThreadCount & ThreadCount2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.8.

- UINT16 ProcessorCharacteristics

  Format defined in SMBIOS Spec v3.0 Section 7.5.9.

8.18.1 Detailed Description

SMBIOS Processor Info HOB Structure.

Definition at line 32 of file SmbiosProcessorInfoHob.h.

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

- SmbiosProcessorInfoHob.h

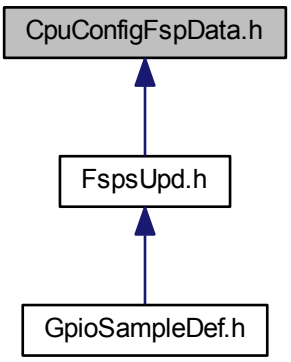
Chapter 9

File Documentation

9.1 CpuConfigFspData.h File Reference

FSP CPU Data Config Block.

This graph shows which files directly or indirectly include this file:



9.1.1 Detailed Description

FSP CPU Data Config Block.

Copyright

INTEL CONFIDENTIAL Copyright 2016 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon

you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

9.2 DoxygenFspIntegrationGuide.h File Reference

This file contains doxygen KabylakeFspIntegration Guide.

9.2.1 Detailed Description

This file contains doxygen KabylakeFspIntegration Guide.

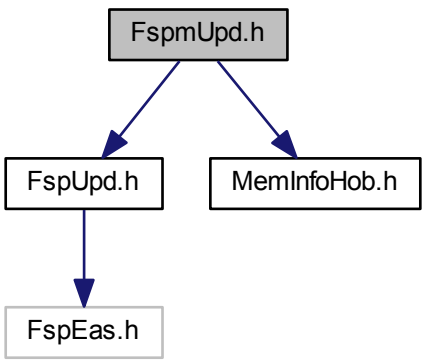
Copyright

Copyright (c) 2015 - 2018 Intel Corporation. All rights reserved This software and associated documentation (if any) is furnished under a license and may only be used or copied in accordance with the terms of the license. Except as permitted by such license, no part of this software or documentation may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation. This file contains an 'Intel Peripheral Driver' and uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement

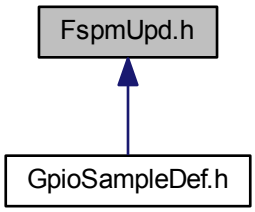
9.3 FspmUpd.h File Reference

```
#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 SI_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 FSPM_UPD

  Fsp M UPD Configuration.

9.3.1 Detailed Description

Copyright

Copyright (c) 2018, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

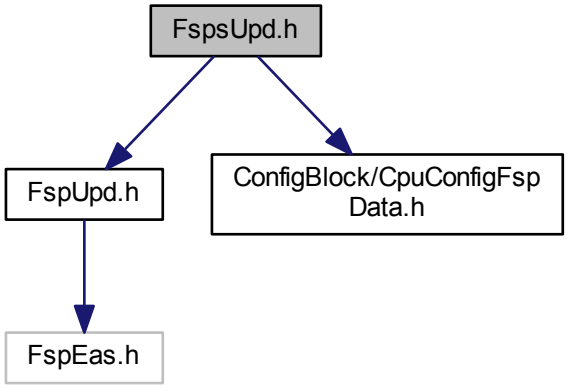
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH↩ ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE↩ MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT↩ ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

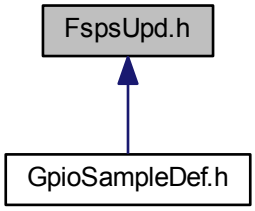
9.4 FspsUpd.h File Reference

```
#include <FspUpd.h>
#include <ConfigBlock/CpuConfigFspData.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 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.

9.4.1 Detailed Description

Copyright

Copyright (c) 2018, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH↩ ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE↩ MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT↩ ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

9.4.2 Enumeration Type Documentation

9.4.2.1 enum SI_PCH_INT_PIN

Refer to the definition of PCH_INT_PIN.

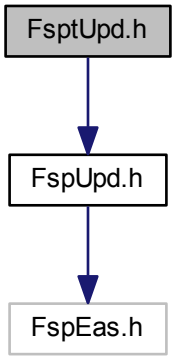
Enumerator

SiPchNoInt No Interrupt Pin.

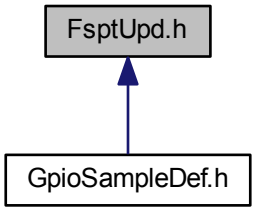
Definition at line 66 of file FspsUpd.h.

9.5 FsptUpd.h File Reference

`#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 FSPT_UPD

  Fsp T UPD Configuration.

9.5.1 Detailed Description

Copyright

Copyright (c) 2018, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

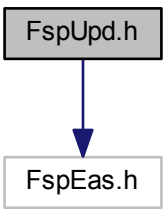
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH↩ ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE↩ MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT↩ ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

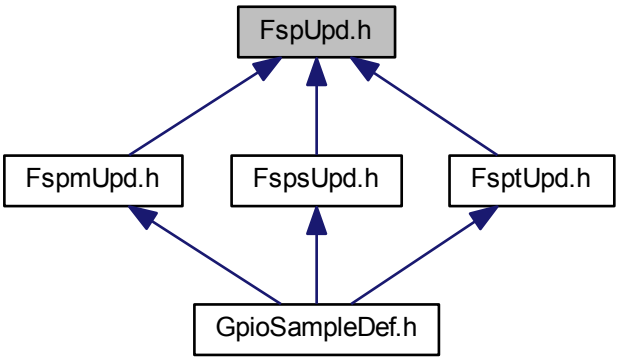
9.6 FspUpd.h File Reference

```
#include <FspEas.h>
```

Include dependency graph for FspUpd.h:



This graph shows which files directly or indirectly include this file:



9.6.1 Detailed Description

Copyright

Copyright (c) 2018, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH↩ ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE↩ MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT↩ ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

9.7 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:

9.7.1 Detailed Description

Header file for GpioConfig structure used by GPIO library.

Copyright

INTEL CONFIDENTIAL Copyright 2014 - 2016 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

9.7.2 Enumeration Type Documentation

9.7.2.1 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.

9.7.2.2 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.

9.7.2.3 enum GPIO_HARDWARE_DEFAULT

Enumerator

GpioHardwareDefault Leave setting unmodified.

Definition at line 118 of file GpioConfig.h.

9.7.2.4 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.

9.7.2.5 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 GpioIntNmi 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.IntSel) 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.

9.7.2.6 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.

9.7.2.7 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.

9.7.2.8 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.

9.7.2.9 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.

9.7.2.10 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:

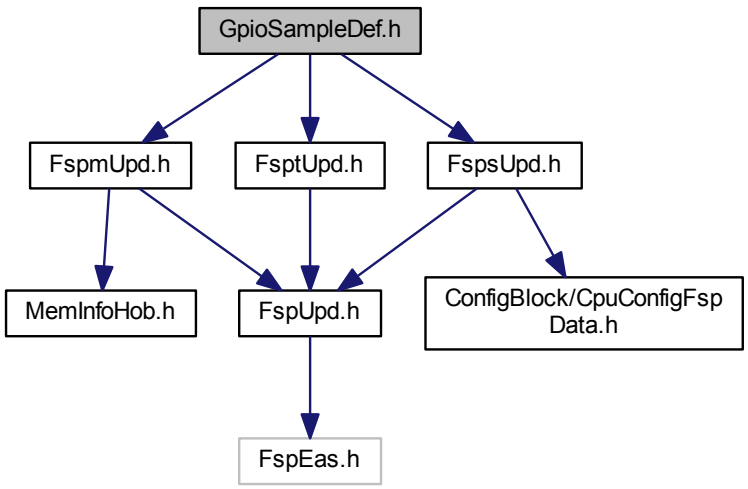
- G3 Pad settings will not reset on:
- S3/S4/S5 transition
- Warm/Cold/Global reset
- DeepSx transition

Definition at line 229 of file GpioConfig.h.

9.8 GpioSampleDef.h File Reference

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

Include dependency graph for GpioSampleDef.h:



9.8.1 Detailed Description

Copyright

Copyright (c) 2015, Intel Corporation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

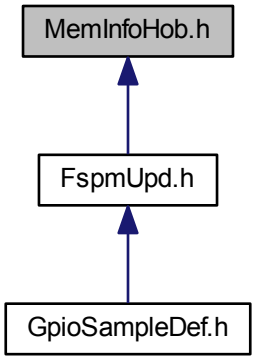
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SH↩ ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE↩ MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT↩ ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

9.9 MemInfoHob.h File Reference

This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs.

This graph shows which files directly or indirectly include this file:



Classes

- struct DIMM_INFO

  Memory SMBIOS & OC Memory Data Hob.
- struct MEMORY_PLATFORM_DATA

  Memory Platform Data Hob.

Macros

- #define WARM_BOOT 2

  Host reset states from MRC.
- #define MAX_SPD_SAVE 29

  Defines taken from MRC so avoid having to include MrcInterface.h.

9.9.1 Detailed Description

This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs.

Copyright

INTEL CONFIDENTIAL Copyright 1999 - 2018 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

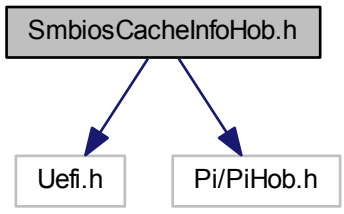
Specification Reference:

9.10 SmbiosCacheInfoHob.h File Reference

Header file for SMBIOS Cache Info HOB.

```
#include <Uefi.h>
#include <Pi/PiHob.h>
```

Include dependency graph for SmbiosCacheInfoHob.h:



Classes

- struct SMBIOS_CACHE_INFO

  SMBIOS Cache Info HOB Structure.

9.10.1 Detailed Description

Header file for SMBIOS Cache Info HOB.

Copyright

Copyright (c) 2015, 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.

Specification Reference:

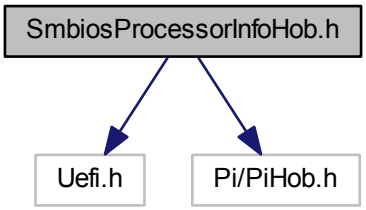
System Management BIOS (SMBIOS) Reference Specification v3.0.0 dated 2015-Feb-12 (DSP0134) http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.0.pdf

9.11 SmbiosProcessorInfoHob.h File Reference

Header file for SMBIOS Processor Info HOB.

```
#include <Uefi.h>
#include <Pi/PiHob.h>
```

Include dependency graph for SmbiosProcessorInfoHob.h:



Classes

- struct SMBIOS_PROCESSOR_INFO

  SMBIOS Processor Info HOB Structure.

9.11.1 Detailed Description

Header file for SMBIOS Processor Info HOB.

Copyright

Copyright (c) 2015, 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.

Specification Reference:

System Management BIOS (SMBIOS) Reference Specification v3.0.0 dated 2015-Feb-12 (DSP0134) http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.0.pdf

Index

AUDIO_AZALIA_VERB_TABLE, 23
AZALIA_HEADER, 24
AcLoadline
    FSP_S_CONFIG, 74
AcousticNoiseMitigation
    FSP_S_CONFIG, 74
ActiveCoreCount
    FSP_M_CONFIG, 35
AmtEnabled
    FSP_S_CONFIG, 74
AmtSolEnabled
    FSP_S_CONFIG, 74
ApHandoffManner
    FSP_S_TEST_CONFIG, 110
ApIdleManner
    FSP_S_TEST_CONFIG, 110
ApertureSize
    FSP_M_CONFIG, 35
AsfEnabled
    FSP_S_CONFIG, 74
AutoThermalReporting
    FSP_S_TEST_CONFIG, 110
Avx2RatioOffset
    FSP_M_CONFIG, 35
Avx3RatioOffset
    FSP_M_CONFIG, 36

BclkAdaptiveVoltage
    FSP_M_CONFIG, 36
BdatEnable
    FSP_M_TEST_CONFIG, 51
BiosAcmBase
    FSP_M_TEST_CONFIG, 51
BiosAcmSize
    FSP_M_TEST_CONFIG, 51
BiosGuard
    FSP_M_CONFIG, 36
BiosSize
    FSP_M_TEST_CONFIG, 51
BistOnReset
    FSP_M_CONFIG, 36
BootFrequency
    FSP_M_CONFIG, 36
BypassPhySyncReset
    FSP_M_TEST_CONFIG, 51

C1e
    FSP_S_TEST_CONFIG, 110
CStatePreWake
    FSP_S_TEST_CONFIG, 110
ChipsetInitMessage
    FSP_M_TEST_CONFIG, 51
CleanMemory
    FSP_M_CONFIG, 36
CmdTriStateDis
    FSP_M_CONFIG, 37
ConfigTdpBios
    FSP_S_TEST_CONFIG, 110
CoreMaxOcRatio
    FSP_M_CONFIG, 37
CorePllVoltageOffset
    FSP_M_CONFIG, 37
CoreVoltageAdaptive
    FSP_M_CONFIG, 37
CoreVoltageMode
    FSP_M_CONFIG, 37
CoreVoltageOverride
    FSP_M_CONFIG, 37
CpuConfigFspData.h, 133
CpuRatio
    FSP_M_CONFIG, 37
CpuRatioOverride
    FSP_M_CONFIG, 38
CstCfgCtrIoMwaitRedirection
    FSP_S_TEST_CONFIG, 110
Custom1ConfigTdpControl
    FSP_S_TEST_CONFIG, 111
Custom1PowerLimit1
    FSP_S_TEST_CONFIG, 111
Custom1PowerLimit1Time
    FSP_S_TEST_CONFIG, 111
Custom1PowerLimit2
    FSP_S_TEST_CONFIG, 111
Custom1TurboActivationRatio
    FSP_S_TEST_CONFIG, 111
Custom2ConfigTdpControl
    FSP_S_TEST_CONFIG, 111
Custom2PowerLimit1
    FSP_S_TEST_CONFIG, 111
Custom2PowerLimit1Time
    FSP_S_TEST_CONFIG, 112
Custom2PowerLimit2
    FSP_S_TEST_CONFIG, 112
Custom2TurboActivationRatio
    FSP_S_TEST_CONFIG, 112
Custom3ConfigTdpControl
    FSP_S_TEST_CONFIG, 112
Custom3PowerLimit1
    FSP_S_TEST_CONFIG, 112

Custom3PowerLimit1Time
FSP_S_TEST_CONFIG, 112
Custom3PowerLimit2
FSP_S_TEST_CONFIG, 112
Custom3TurboActivationRatio
FSP_S_TEST_CONFIG, 113
Cx
FSP_S_TEST_CONFIG, 113

DIMM_INFO, 24
DcLoadline
FSP_S_CONFIG, 74
DdrFreqLimit
FSP_M_CONFIG, 38
DebugInterfaceEnable
FSP_S_TEST_CONFIG, 113
DebugInterfaceLockEnable
FSP_S_TEST_CONFIG, 113
DelayUsbPdoProgramming
FSP_S_CONFIG, 74
DevIntConfigPtr
FSP_S_CONFIG, 74
Direction
GPIO_CONFIG, 127
DisableHeciRetry
FSP_M_TEST_CONFIG, 52
DisableMessageCheck
FSP_M_TEST_CONFIG, 52
DisableProcHotOut
FSP_S_TEST_CONFIG, 113
DisableVrThermalAlert
FSP_S_TEST_CONFIG, 113
DmiDeEmphasis
FSP_M_CONFIG, 38
DmiGen3EndPointHint
FSP_M_CONFIG, 38
DmiGen3EndPointPreset
FSP_M_CONFIG, 38
DmiGen3EqPh2Enable
FSP_M_TEST_CONFIG, 52
DmiGen3EqPh3Method
FSP_M_TEST_CONFIG, 52
DmiGen3ProgramStaticEq
FSP_M_CONFIG, 38
DmiGen3RootPortPreset
FSP_M_CONFIG, 38
DmiSuggestedSetting
FSP_S_CONFIG, 75
DmiVc1
FSP_M_TEST_CONFIG, 52
DmiVcm
FSP_M_TEST_CONFIG, 52
DoxygenFspIntegrationGuide.h, 134

Early8254ClockGatingEnable
FSP_S_CONFIG, 75
EcCmdLock
FSP_S_CONFIG, 75
EcCmdProvisionEav
FSP_S_CONFIG, 75
EightCoreRatioLimit
FSP_S_TEST_CONFIG, 113
Eist
FSP_S_TEST_CONFIG, 114
ElectricalConfig
GPIO_CONFIG, 127
EnableC6Dram
FSP_M_CONFIG, 39
EnableSgx
FSP_M_CONFIG, 39
EnableTcoTimer
FSP_S_CONFIG, 75
EnableTraceHub
FSP_M_CONFIG, 39
EndOfPostMessage
FSP_S_TEST_CONFIG, 114
EnergyEfficientPState
FSP_S_TEST_CONFIG, 114
EnergyEfficientTurbo
FSP_S_TEST_CONFIG, 114
EsataSpeedLimit
FSP_S_CONFIG, 75
EvLoader
FSP_M_CONFIG, 39

FClkFrequency
FSP_M_CONFIG, 39
FSP_M_CONFIG, 25
ActiveCoreCount, 35
ApertureSize, 35
Avx2RatioOffset, 35
Avx3RatioOffset, 36
BclkAdaptiveVoltage, 36
BiosGuard, 36
BistOnReset, 36
BootFrequency, 36
CleanMemory, 36
CmdTriStateDis, 37
CoreMaxOcRatio, 37
CorePllVoltageOffset, 37
CoreVoltageAdaptive, 37
CoreVoltageMode, 37
CoreVoltageOverride, 37
CpuRatio, 37
CpuRatioOverride, 38
DdrFreqLimit, 38
DmiDeEmphasis, 38
DmiGen3EndPointHint, 38
DmiGen3EndPointPreset, 38
DmiGen3ProgramStaticEq, 38
DmiGen3RootPortPreset, 38
EnableC6Dram, 39
EnableSgx, 39
EnableTraceHub, 39
EvLoader, 39
FClkFrequency, 39
FlashWearOutProtection, 39
GtPllVoltageOffset, 39

HeciTimeouts, 40
IgdDvmt50PreAlloc, 40
InitPcieAspmAfterOprom, 40
InternalGfx, 40
JtagC10PowerGateDisable, 40
McPllVoltageOffset, 40
MmioSize, 40
OcLock, 41
PcdDebugInterfaceFlags, 41
PcdIsaSerialUartBase, 41
PcdSerialDebugBaudRate, 41
PcdSerialDebugLevel, 41
PcdSerialIoUartNumber, 41
PchAcpiBase, 41
PchHpetBase, 42
PchHpetBdfValid, 42
PchHpetBusNumber, 42
PchHpetDeviceNumber, 42
PchHpetEnable, 42
PchHpetFunctionNumber, 42
PchLpcEnhancePort8xhDecoding, 42
PchNumRsvdSmbusAddresses, 43
PchPmPciePllSsc, 43
PchPort80Route, 43
PcieRpEnableMask, 43
PeciC10Reset, 43
PeciSxReset, 43
PegDataPtr, 43
PegDisableSpreadSpectrumClocking, 44
PrmrrSize, 44
ProbelessTrace, 44
RMT, 45
Ratio, 44
RealtimeMemoryTiming, 44
RefClk, 44
RingDownBin, 44
RingMaxOcRatio, 44
RingMinOcRatio, 45
RingPllVoltageOffset, 45
SaGv, 45
SaPllVoltageOffset, 45
SinitMemorySize, 45
SmbusArpEnable, 45
SmbusEnable, 46
SpdProfileSelected, 46
tRTP, 46
TjMaxOffset, 46
TsegSize, 46
TvbRatioClipping, 46
TvbVoltageOptimization, 46
Txt, 47
TxtDprMemoryBase, 47
TxtDprMemorySize, 47
TxtHeapMemorySize, 47
TxtImplemented, 47
VddVoltage, 47
VmxEnable, 47
FSP_M_TEST_CONFIG, 48
BdatEnable, 51
BiosAcmBase, 51
BiosAcmSize, 51
BiosSize, 51
BypassPhySyncReset, 51
ChipsetInitMessage, 51
DisableHeciRetry, 52
DisableMessageCheck, 52
DmiGen3EqPh2Enable, 52
DmiGen3EqPh3Method, 52
DmiVc1, 52
DmiVcm, 52
Gen3SwEqAlwaysAttempt, 52
Gen3SwEqEnableVocTest, 53
Gen3SwEqJitterDwellTime, 53
Gen3SwEqJitterErrorTarget, 53
Gen3SwEqNumberOfPresets, 53
Gen3SwEqVocDwellTime, 53
Gen3SwEqVocErrorTarget, 53
HeciCommunication2, 54
IderDeviceEnable, 54
KtDeviceEnable, 54
LockPTMregs, 54
PanelPowerEnable, 54
PchDciEn, 54
Peg0Gen3EqPh2Enable, 54
Peg0Gen3EqPh3Method, 55
Peg1Gen3EqPh2Enable, 55
Peg1Gen3EqPh3Method, 55
Peg2Gen3EqPh2Enable, 55
Peg2Gen3EqPh3Method, 55
PegGen3EndPointHint, 55
PegGen3EndPointPreset, 56
PegGen3ProgramStaticEq, 56
PegGen3RootPortPreset, 56
PegGenerateBdatMarginTable, 56
PegRxCemLoopbackLane, 56
PegRxCemNonProtocolAwareness, 56
ScanExtGfxForLegacyOpRom, 57
SkipMbpHob, 57
SmbusDynamicPowerGating, 57
SmbusSpdWriteDisable, 57
TgaSize, 57
TotalFlashSize, 57
TxtLcpPdBase, 57
TxtLcpPdSize, 58
WdtDisableAndLock, 58
FSP_S_CONFIG, 58
AcLoadline, 74
AcousticNoiseMitigation, 74
AmtEnabled, 74
AmtSolEnabled, 74
AsfEnabled, 74
DcLoadline, 74
DelayUsbPdoProgramming, 74
DevIntConfigPtr, 74
DmiSuggestedSetting, 75
Early8254ClockGatingEnable, 75

EcCmdLock, 75
EcCmdProvisionEav, 75
EnableTcoTimer, 75
EsataSpeedLimit, 75
FastPkgCRampDisableGt, 75
FastPkgCRampDisableIa, 76
FastPkgCRampDisableSa, 76
FwProgress, 76
GpioIrqRoute, 76
Heci3Enabled, 76
IccMax, 76
ImonOffset, 76
ImonSlope, 77
IslVrCmd, 77
ManageabilityMode, 77
MeUnconfigIsValid, 77
MicrocodePatchAddress, 77
NumOfDevIntConfig, 77
PchCio2Enable, 77
PchCrid, 78
PchDisableComplianceMode, 78
PchDmiAspm, 78
PchDmiTsawEn, 78
PchHdaDspEnable, 78
PchHdaDspEndpointBluetooth, 78
PchHdaDspEndpointI2s, 78
PchHdaDspFeatureMask, 79
PchHdaDspUaaCompliance, 79
PchHdaEnable, 79
PchHdaIDispCodecDisconnect, 79
PchHdaIoBufferOwnership, 79
PchHdaPme, 79
PchIoApicBdfValid, 79
PchIoApicBusNumber, 80
PchIoApicDeviceNumber, 80
PchIoApicEntry24_119, 80
PchIoApicFunctionNumber, 80
PchIoApicId, 80
PchIoApicRangeSelect, 80
PchIshEnable, 80
PchIshGp0GpioAssign, 81
PchIshGp1GpioAssign, 81
PchIshGp2GpioAssign, 81
PchIshGp3GpioAssign, 81
PchIshGp4GpioAssign, 81
PchIshGp5GpioAssign, 81
PchIshGp6GpioAssign, 81
PchIshGp7GpioAssign, 81
PchIshI2c0GpioAssign, 82
PchIshI2c1GpioAssign, 82
PchIshI2c2GpioAssign, 82
PchIshPdtUnlock, 82
PchIshSpiGpioAssign, 82
PchIshUart0GpioAssign, 82
PchIshUart1GpioAssign, 82
PchLanClkReqSupported, 83
PchLanEnable, 83
PchLanK1OffEnable, 83
PchLanLtrEnable, 83
PchLockDownBiosLock, 83
PchLockDownSpiEiss, 83
PchMemoryThrottlingEnable, 83
PchPcieDeviceOverrideTablePtr, 83
PchPmCapsuleResetType, 84
PchPmDeepSxPol, 84
PchPmDisableDsxAcPresentPulldown, 84
PchPmDisableNativePowerButton, 84
PchPmLanWakeFromDeepSx, 84
PchPmLpcClockRun, 84
PchPmMeWakeSts, 84
PchPmPcieWakeFromDeepSx, 85
PchPmPmeB0S5Dis, 85
PchPmPwrBtnOverridePeriod, 85
PchPmPwrCycDur, 85
PchPmSlpAMinAssert, 85
PchPmSlpLanLowDc, 85
PchPmSlpS0Enable, 85
PchPmSlpS0VmEnable, 86
PchPmSlpS3MinAssert, 86
PchPmSlpS4MinAssert, 86
PchPmSlpStrchSusUp, 86
PchPmSlpSusMinAssert, 86
PchPmWoWlanDeepSxEnable, 87
PchPmWoWlanEnable, 87
PchPmWolEnableOverride, 86
PchPmWolOvrWkSts, 86
PchPort61hEnable, 87
PchPwrOptEnable, 87
PchScsEmmcHs400DllDataValid, 87
PchScsEmmcHs400TuningRequired, 87
PchSirqEnable, 87
PchSirqMode, 88
PchSkyCamPortACtleEnable, 88
PchSkyCamPortATermOvrEnable, 88
PchSkyCamPortATrimEnable, 88
PchSkyCamPortBCtleEnable, 88
PchSkyCamPortBTermOvrEnable, 88
PchSkyCamPortBTrimEnable, 88
PchSkyCamPortCDCtleEnable, 89
PchSkyCamPortCTermOvrEnable, 89
PchSkyCamPortCTrimEnable, 89
PchSkyCamPortDTermOvrEnable, 89
PchSkyCamPortDTrimEnable, 89
PchSubSystemId, 89
PchSubSystemVendorId, 89
PchTTEnable, 90
PchTTLock, 90
PchTTState13Enable, 90
PchThermalDeviceEnable, 89
PchTsmicLock, 90
PcieAllowNoLtrIccPllShutdown, 90
PcieComplianceTestMode, 90
PcieDisableRootPortClockGating, 90
PcieEnablePeerMemoryWrite, 91
PcieEqPh3LaneParamCm, 91
PcieEqPh3LaneParamCp, 91

PcieRpAspm, 91
PcieRpClkReqNumber, 91
PcieRpClkReqSupport, 91
PcieRpClkSrcNumber, 91
PcieRpCompletionTimeout, 92
PcieRpDeviceResetPad, 92
PcieRpFunctionSwap, 92
PcieRpGen3EqPh3Method, 92
PcieRpL1Substates, 92
PcieRpPcieSpeed, 92
PcieRpPhysicalSlotNumber, 92
PcieSwEqCoeffListCm, 93
PcieSwEqCoeffListCp, 93
PortUsb20Enable, 93
PortUsb30Enable, 93
Psi1Threshold, 93
Psi2Threshold, 93
Psi3Enable, 93
Psi3Threshold, 94
PsysOffset, 94
PsysSlope, 94
PxRcConfig, 94
SataEnable, 94
SataMode, 94
SataP0TDispFinit, 94
SataP1TDispFinit, 95
SataPortsDevSlp, 95
SataPortsDmVal, 95
SataPortsEnable, 95
SataPwrOptEnable, 95
SataRstHddUnlock, 95
SataRstIrrt, 95
SataRstIrrtOnly, 96
SataRstLedLocate, 96
SataRstOromUiBanner, 96
SataRstPcieDeviceResetDelay, 96
SataRstRaid0, 96
SataRstRaid1, 96
SataRstRaid10, 96
SataRstRaid5, 96
SataRstRaidAlternateId, 97
SataRstSmartStorage, 97
SataSalpSupport, 97
SataThermalSuggestedSetting, 97
SciIrqSelect, 97
ScsEmmcEnabled, 97
ScsEmmcHs400Enabled, 97
ScsSdCardEnabled, 98
SendEcCmd, 98
SendVrMbxCmd, 98
SendVrMbxCmd1, 98
SerialIoDebugUartNumber, 98
SerialIoDevMode, 98
SerialIoGpio, 98
ShowSpiController, 99
SlowSlewRateForGt, 99
SlowSlewRateForIa, 99
SlowSlewRateForSa, 99
SpiFlashCfgLockDown, 99
SsicPortEnable, 99
TTSuggestedSetting, 100
TcoIrqSelect, 99
TdcPowerLimit, 100
TdcTimeWindow, 100
TurboMode, 100
Usb2AfePehalfbit, 100
Usb2AfePetxiset, 100
Usb2AfePredeemp, 100
Usb2AfeTxiset, 101
Usb3HsioTxDeEmph, 101
Usb3HsioTxDeEmphEnable, 101
Usb3HsioTxDownscaleAmp, 101
Usb3HsioTxDownscaleAmpEnable, 101
VrPowerDeliveryDesign, 101
VrVoltageLimit, 102
WatchDog, 102
WatchDogTimerBios, 102
WatchDogTimerOs, 102
XdciEnable, 102
FSP_S_TEST_CONFIG, 102
ApHandoffManner, 110
ApIdleManner, 110
AutoThermalReporting, 110
C1e, 110
CStatePreWake, 110
ConfigTdpBios, 110
CstCfgCtrIoMwaitRedirection, 110
Custom1ConfigTdpControl, 111
Custom1PowerLimit1, 111
Custom1PowerLimit1Time, 111
Custom1PowerLimit2, 111
Custom1TurboActivationRatio, 111
Custom2ConfigTdpControl, 111
Custom2PowerLimit1, 111
Custom2PowerLimit1Time, 112
Custom2PowerLimit2, 112
Custom2TurboActivationRatio, 112
Custom3ConfigTdpControl, 112
Custom3PowerLimit1, 112
Custom3PowerLimit1Time, 112
Custom3PowerLimit2, 112
Custom3TurboActivationRatio, 113
Cx, 113
DebugInterfaceEnable, 113
DebugInterfaceLockEnable, 113
DisableProcHotOut, 113
DisableVrThermalAlert, 113
EightCoreRatioLimit, 113
Eist, 114
EndOfPostMessage, 114
EnergyEfficientPState, 114
EnergyEfficientTurbo, 114
FiveCoreRatioLimit, 114
FourCoreRatioLimit, 114
HdcControl, 114
Hwp, 115

MachineCheckEnable, 115
MlcStreamerPrefetcher, 115
MonitorMwaitEnable, 115
NumberOfEntries, 115
OneCoreRatioLimit, 115
PchHdaResetWaitTimer, 115
PchLockDownBiosInterface, 116
PchLockDownGlobalSmi, 116
PchLockDownRtcLock, 116
PchPmDisableEnergyReport, 116
PchSbAccessUnlock, 116
PchSbiUnlock, 116
PcieEnablePort8xhDecode, 116
PcieRpDptp, 117
PcieRpSlotPowerLimitScale, 117
PcieRpSlotPowerLimitValue, 117
PcieRpUptp, 117
PkgCStateDemotion, 117
PkgCStateLimit, 117
PkgCStateUnDemotion, 117
PmgCstCfgCtrlLock, 118
PowerLimit1, 118
PowerLimit1Time, 118
PowerLimit2, 118
PowerLimit2Power, 118
PowerLimit3, 118
PowerLimit3Time, 118
PowerLimit4, 119
ProcHotResponse, 119
ProcTraceEnable, 119
ProcTraceOutputScheme, 119
PsysPmax, 119
PsysPowerLimit1, 119
PsysPowerLimit1Power, 119
PsysPowerLimit2, 120
PsysPowerLimit2Power, 120
RaceToHalt, 120
SataTestMode, 120
SevenCoreRatioLimit, 120
SixCoreRatioLimit, 120
StateRatio, 120
TStates, 121
TccActivationOffset, 120
TccOffsetClamp, 121
TccOffsetLock, 121
TccOffsetTimeWindowForRatl, 121
ThreeCoreRatioLimit, 121
ThreeStrikeCounterDisable, 121
TimedMwait, 121
TwoCoreRatioLimit, 122
FSP_T_CONFIG, 122
PcdSerialIoUartDebugEnable, 122
PcdSerialIoUartNumber, 123
FSPM_UPD, 123
FSPS_UPD, 124
FSPT_CORE_UPD, 125
FSPT_UPD, 125
FastPkgCRampDisableGt
FSP_S_CONFIG, 75
FastPkgCRampDisableIa
FSP_S_CONFIG, 76
FastPkgCRampDisableSa
FSP_S_CONFIG, 76
FiveCoreRatioLimit
FSP_S_TEST_CONFIG, 114
FlashWearOutProtection
FSP_M_CONFIG, 39
FourCoreRatioLimit
FSP_S_TEST_CONFIG, 114
FspUpd.h, 139
FspmUpd.h, 134
FspsUpd.h, 136
SI_PCH_INT_PIN, 137
SiPchNoInt, 137
FsptUpd.h, 138
FwProgress
FSP_S_CONFIG, 76

GPIO_CONFIG, 126
Direction, 127
ElectricalConfig, 127
HostSoftPadOwn, 127
InterruptConfig, 127
LockConfig, 127
OutputState, 127
PadMode, 127
PowerConfig, 128
GPIO_DIRECTION
GpioConfig.h, 142
GPIO_ELECTRICAL_CONFIG
GpioConfig.h, 142
GPIO_HARDWARE_DEFAULT
GpioConfig.h, 143
GPIO_HOSTSW_OWN
GpioConfig.h, 143
GPIO_INT_CONFIG
GpioConfig.h, 143
GPIO_LOCK_CONFIG
GpioConfig.h, 144
GPIO_OTHER_CONFIG
GpioConfig.h, 144
GPIO_OUTPUT_STATE
GpioConfig.h, 144
GPIO_PAD_MODE
GpioConfig.h, 145
GPIO_RESET_CONFIG
GpioConfig.h, 145
Gen3SwEqAlwaysAttempt
FSP_M_TEST_CONFIG, 52
Gen3SwEqEnableVocTest
FSP_M_TEST_CONFIG, 53
Gen3SwEqJitterDwellTime
FSP_M_TEST_CONFIG, 53
Gen3SwEqJitterErrorTarget
FSP_M_TEST_CONFIG, 53
Gen3SwEqNumberOfPresets
FSP_M_TEST_CONFIG, 53

Gen3SwEqVocDwellTime
FSP_M_TEST_CONFIG, 53
Gen3SwEqVocErrorTarget
FSP_M_TEST_CONFIG, 53
GpioConfig.h, 140
GPIO_DIRECTION, 142
GPIO_ELECTRICAL_CONFIG, 142
GPIO_HARDWARE_DEFAULT, 143
GPIO_HOSTSW_OWN, 143
GPIO_INT_CONFIG, 143
GPIO_LOCK_CONFIG, 144
GPIO_OTHER_CONFIG, 144
GPIO_OUTPUT_STATE, 144
GPIO_PAD_MODE, 145
GPIO_RESET_CONFIG, 145
GpioDirDefault, 142
GpioDirIn, 142
GpioDirInInv, 142
GpioDirInInvOut, 142
GpioDirInOut, 142
GpioDirNone, 142
GpioDirOut, 142
GpioDswReset, 146
GpioHardwareDefault, 143
GpioHostDeepReset, 145
GpioHostOwnAcpi, 143
GpioHostOwnDefault, 143
GpioHostOwnGpio, 143
GpioIntApic, 144
GpioIntBothEdge, 144
GpioIntDefault, 144
GpioIntDis, 144
GpioIntEdge, 144
GpioIntLevel, 144
GpioIntLvlEdgDis, 144
GpioIntNmi, 144
GpioIntSci, 144
GpioIntSmi, 144
GpioLockDefault, 144
GpioNoTolerance1v8, 143
GpioOutDefault, 145
GpioOutHigh, 145
GpioOutLow, 145
GpioOutputStateLock, 144
GpioPadConfigLock, 144
GpioPlatformReset, 145
GpioResetDeep, 145
GpioResetDefault, 145
GpioResetNormal, 145
GpioResetPwrGood, 145
GpioResetResume, 145
GpioResumeReset, 145
GpioRxRaw1Default, 144
GpioRxRaw1Dis, 144
GpioRxRaw1En, 144
GpioTermDefault, 142
GpioTermNative, 143
GpioTermNone, 142
GpioTermWpd20K, 143
GpioTermWpd5K, 142
GpioTermWpu1K, 143
GpioTermWpu1K2K, 143
GpioTermWpu20K, 143
GpioTermWpu2K, 143
GpioTermWpu5K, 143
GpioTolerance1v8, 143
GpioDirDefault
GpioConfig.h, 142
GpioDirIn
GpioConfig.h, 142
GpioDirInInv
GpioConfig.h, 142
GpioDirInInvOut
GpioConfig.h, 142
GpioDirInOut
GpioConfig.h, 142
GpioDirNone
GpioConfig.h, 142
GpioDirOut
GpioConfig.h, 142
GpioDswReset
GpioConfig.h, 146
GpioHardwareDefault
GpioConfig.h, 143
GpioHostDeepReset
GpioConfig.h, 145
GpioHostOwnAcpi
GpioConfig.h, 143
GpioHostOwnDefault
GpioConfig.h, 143
GpioHostOwnGpio
GpioConfig.h, 143
GpioIntApic
GpioConfig.h, 144
GpioIntBothEdge
GpioConfig.h, 144
GpioIntDefault
GpioConfig.h, 144
GpioIntDis
GpioConfig.h, 144
GpioIntEdge
GpioConfig.h, 144
GpioIntLevel
GpioConfig.h, 144
GpioIntLvlEdgDis
GpioConfig.h, 144
GpioIntNmi
GpioConfig.h, 144
GpioIntSci
GpioConfig.h, 144
GpioIntSmi
GpioConfig.h, 144
GpioIrqRoute
FSP_S_CONFIG, 76
GpioLockDefault
GpioConfig.h, 144

GpioNoTolerance1v8
GpioConfig.h, 143
GpioOutDefault
GpioConfig.h, 145
GpioOutHigh
GpioConfig.h, 145
GpioOutLow
GpioConfig.h, 145
GpioOutputStateLock
GpioConfig.h, 144
GpioPadConfigLock
GpioConfig.h, 144
GpioPlatformReset
GpioConfig.h, 145
GpioResetDeep
GpioConfig.h, 145
GpioResetDefault
GpioConfig.h, 145
GpioResetNormal
GpioConfig.h, 145
GpioResetPwrGood
GpioConfig.h, 145
GpioResetResume
GpioConfig.h, 145
GpioResumeReset
GpioConfig.h, 145
GpioRxRaw1Default
GpioConfig.h, 144
GpioRxRaw1Dis
GpioConfig.h, 144
GpioRxRaw1En
GpioConfig.h, 144
GpioSampleDef.h, 146
GpioTermDefault
GpioConfig.h, 142
GpioTermNative
GpioConfig.h, 143
GpioTermNone
GpioConfig.h, 142
GpioTermWpd20K
GpioConfig.h, 143
GpioTermWpd5K
GpioConfig.h, 142
GpioTermWpu1K
GpioConfig.h, 143
GpioTermWpu1K2K
GpioConfig.h, 143
GpioTermWpu20K
GpioConfig.h, 143
GpioTermWpu2K
GpioConfig.h, 143
GpioTermWpu5K
GpioConfig.h, 143
GpioTolerance1v8
GpioConfig.h, 143
GtPllVoltageOffset
FSP_M_CONFIG, 39

HdcControl
FSP_S_TEST_CONFIG, 114
Heci3Enabled
FSP_S_CONFIG, 76
HeciCommunication2
FSP_M_TEST_CONFIG, 54
HeciTimeouts
FSP_M_CONFIG, 40
HostSoftPadOwn
GPIO_CONFIG, 127
Hwp
FSP_S_TEST_CONFIG, 115

IccMax
FSP_S_CONFIG, 76
IderDeviceEnable
FSP_M_TEST_CONFIG, 54
IgdDvmt50PreAlloc
FSP_M_CONFIG, 40
ImonOffset
FSP_S_CONFIG, 76
ImonSlope
FSP_S_CONFIG, 77
InitPcieAspmAfterOprom
FSP_M_CONFIG, 40
InternalGfx
FSP_M_CONFIG, 40
InterruptConfig
GPIO_CONFIG, 127
IslVrCmd
FSP_S_CONFIG, 77

JtagC10PowerGateDisable
FSP_M_CONFIG, 40

KtDeviceEnable
FSP_M_TEST_CONFIG, 54

LockConfig
GPIO_CONFIG, 127
LockPTMregs
FSP_M_TEST_CONFIG, 54

MEMORY_PLATFORM_DATA, 128
MachineCheckEnable
FSP_S_TEST_CONFIG, 115
ManageabilityMode
FSP_S_CONFIG, 77
McPllVoltageOffset
FSP_M_CONFIG, 40
MeUnconfigIsValid
FSP_S_CONFIG, 77
MemInfoHob.h, 147
MicrocodePatchAddress
FSP_S_CONFIG, 77
MlcStreamerPrefetcher
FSP_S_TEST_CONFIG, 115
MmioSize
FSP_M_CONFIG, 40
MonitorMwaitEnable

FSP_S_TEST_CONFIG, 115

NumOfDevIntConfig
FSP_S_CONFIG, 77
NumberOfEntries
FSP_S_TEST_CONFIG, 115

OcLock
FSP_M_CONFIG, 41
OneCoreRatioLimit
FSP_S_TEST_CONFIG, 115
OutputState
GPIO_CONFIG, 127

PadMode
GPIO_CONFIG, 127
PanelPowerEnable
FSP_M_TEST_CONFIG, 54
PcdDebugInterfaceFlags
FSP_M_CONFIG, 41
PcdIsaSerialUartBase
FSP_M_CONFIG, 41
PcdSerialDebugBaudRate
FSP_M_CONFIG, 41
PcdSerialDebugLevel
FSP_M_CONFIG, 41
PcdSerialIoUartDebugEnable
FSP_T_CONFIG, 122
PcdSerialIoUartNumber
FSP_M_CONFIG, 41
FSP_T_CONFIG, 123
PchAcpiBase
FSP_M_CONFIG, 41
PchCio2Enable
FSP_S_CONFIG, 77
PchCrid
FSP_S_CONFIG, 78
PchDciEn
FSP_M_TEST_CONFIG, 54
PchDisableComplianceMode
FSP_S_CONFIG, 78
PchDmiAspm
FSP_S_CONFIG, 78
PchDmiTsawEn
FSP_S_CONFIG, 78
PchHdaDspEnable
FSP_S_CONFIG, 78
PchHdaDspEndpointBluetooth
FSP_S_CONFIG, 78
PchHdaDspEndpointI2s
FSP_S_CONFIG, 78
PchHdaDspFeatureMask
FSP_S_CONFIG, 79
PchHdaDspUaaCompliance
FSP_S_CONFIG, 79
PchHdaEnable
FSP_S_CONFIG, 79
PchHdaIDispCodecDisconnect
FSP_S_CONFIG, 79
PchHdaIoBufferOwnership
FSP_S_CONFIG, 79
PchHdaPme
FSP_S_CONFIG, 79
PchHdaResetWaitTimer
FSP_S_TEST_CONFIG, 115
PchHpetBase
FSP_M_CONFIG, 42
PchHpetBdfValid
FSP_M_CONFIG, 42
PchHpetBusNumber
FSP_M_CONFIG, 42
PchHpetDeviceNumber
FSP_M_CONFIG, 42
PchHpetEnable
FSP_M_CONFIG, 42
PchHpetFunctionNumber
FSP_M_CONFIG, 42
PchIoApicBdfValid
FSP_S_CONFIG, 79
PchIoApicBusNumber
FSP_S_CONFIG, 80
PchIoApicDeviceNumber
FSP_S_CONFIG, 80
PchIoApicEntry24_119
FSP_S_CONFIG, 80
PchIoApicFunctionNumber
FSP_S_CONFIG, 80
PchIoApicId
FSP_S_CONFIG, 80
PchIoApicRangeSelect
FSP_S_CONFIG, 80
PchIshEnable
FSP_S_CONFIG, 80
PchIshGp0GpioAssign
FSP_S_CONFIG, 81
PchIshGp1GpioAssign
FSP_S_CONFIG, 81
PchIshGp2GpioAssign
FSP_S_CONFIG, 81
PchIshGp3GpioAssign
FSP_S_CONFIG, 81
PchIshGp4GpioAssign
FSP_S_CONFIG, 81
PchIshGp5GpioAssign
FSP_S_CONFIG, 81
PchIshGp6GpioAssign
FSP_S_CONFIG, 81
PchIshGp7GpioAssign
FSP_S_CONFIG, 81
PchIshI2c0GpioAssign
FSP_S_CONFIG, 82
PchIshI2c1GpioAssign
FSP_S_CONFIG, 82
PchIshI2c2GpioAssign
FSP_S_CONFIG, 82
PchIshPdtUnlock
FSP_S_CONFIG, 82

PchIshSpiGpioAssign
FSP_S_CONFIG, 82
PchIshUart0GpioAssign
FSP_S_CONFIG, 82
PchIshUart1GpioAssign
FSP_S_CONFIG, 82
PchLanClkReqSupported
FSP_S_CONFIG, 83
PchLanEnable
FSP_S_CONFIG, 83
PchLanK1OffEnable
FSP_S_CONFIG, 83
PchLanLtrEnable
FSP_S_CONFIG, 83
PchLockDownBiosInterface
FSP_S_TEST_CONFIG, 116
PchLockDownBiosLock
FSP_S_CONFIG, 83
PchLockDownGlobalSmi
FSP_S_TEST_CONFIG, 116
PchLockDownRtcLock
FSP_S_TEST_CONFIG, 116
PchLockDownSpiEiss
FSP_S_CONFIG, 83
PchLpcEnhancePort8xhDecoding
FSP_M_CONFIG, 42
PchMemoryThrottlingEnable
FSP_S_CONFIG, 83
PchNumRsvdSmbusAddresses
FSP_M_CONFIG, 43
PchPcieDeviceOverrideTablePtr
FSP_S_CONFIG, 83
PchPmCapsuleResetType
FSP_S_CONFIG, 84
PchPmDeepSxPol
FSP_S_CONFIG, 84
PchPmDisableDsxAcPresentPulldown
FSP_S_CONFIG, 84
PchPmDisableEnergyReport
FSP_S_TEST_CONFIG, 116
PchPmDisableNativePowerButton
FSP_S_CONFIG, 84
PchPmLanWakeFromDeepSx
FSP_S_CONFIG, 84
PchPmLpcClockRun
FSP_S_CONFIG, 84
PchPmMeWakeSts
FSP_S_CONFIG, 84
PchPmPciePllSsc
FSP_M_CONFIG, 43
PchPmPcieWakeFromDeepSx
FSP_S_CONFIG, 85
PchPmPmeB0S5Dis
FSP_S_CONFIG, 85
PchPmPwrBtnOverridePeriod
FSP_S_CONFIG, 85
PchPmPwrCycDur
FSP_S_CONFIG, 85
PchPmSlpAMinAssert
FSP_S_CONFIG, 85
PchPmSlpLanLowDc
FSP_S_CONFIG, 85
PchPmSlpS0Enable
FSP_S_CONFIG, 85
PchPmSlpS0VmEnable
FSP_S_CONFIG, 86
PchPmSlpS3MinAssert
FSP_S_CONFIG, 86
PchPmSlpS4MinAssert
FSP_S_CONFIG, 86
PchPmSlpStrchSusUp
FSP_S_CONFIG, 86
PchPmSlpSusMinAssert
FSP_S_CONFIG, 86
PchPmWoWlanDeepSxEnable
FSP_S_CONFIG, 87
PchPmWoWlanEnable
FSP_S_CONFIG, 87
PchPmWolEnableOverride
FSP_S_CONFIG, 86
PchPmWolOvrWkSts
FSP_S_CONFIG, 86
PchPort61hEnable
FSP_S_CONFIG, 87
PchPort80Route
FSP_M_CONFIG, 43
PchPwrOptEnable
FSP_S_CONFIG, 87
PchSbAccessUnlock
FSP_S_TEST_CONFIG, 116
PchSbiUnlock
FSP_S_TEST_CONFIG, 116
PchScsEmmcHs400DllDataValid
FSP_S_CONFIG, 87
PchScsEmmcHs400TuningRequired
FSP_S_CONFIG, 87
PchSirqEnable
FSP_S_CONFIG, 87
PchSirqMode
FSP_S_CONFIG, 88
PchSkyCamPortACtleEnable
FSP_S_CONFIG, 88
PchSkyCamPortATermOvrEnable
FSP_S_CONFIG, 88
PchSkyCamPortATrimEnable
FSP_S_CONFIG, 88
PchSkyCamPortBCtleEnable
FSP_S_CONFIG, 88
PchSkyCamPortBTermOvrEnable
FSP_S_CONFIG, 88
PchSkyCamPortBTrimEnable
FSP_S_CONFIG, 88
PchSkyCamPortCDCtleEnable
FSP_S_CONFIG, 89
PchSkyCamPortCTermOvrEnable
FSP_S_CONFIG, 89

PchSkyCamPortCTrimEnable
FSP_S_CONFIG, 89
PchSkyCamPortDTermOvrEnable
FSP_S_CONFIG, 89
PchSkyCamPortDTrimEnable
FSP_S_CONFIG, 89
PchSubSystemId
FSP_S_CONFIG, 89
PchSubSystemVendorId
FSP_S_CONFIG, 89
PchTTEnable
FSP_S_CONFIG, 90
PchTTLock
FSP_S_CONFIG, 90
PchTTState13Enable
FSP_S_CONFIG, 90
PchThermalDeviceEnable
FSP_S_CONFIG, 89
PchTsmicLock
FSP_S_CONFIG, 90
PcieAllowNoLtrIccPllShutdown
FSP_S_CONFIG, 90
PcieComplianceTestMode
FSP_S_CONFIG, 90
PcieDisableRootPortClockGating
FSP_S_CONFIG, 90
PcieEnablePeerMemoryWrite
FSP_S_CONFIG, 91
PcieEnablePort8xhDecode
FSP_S_TEST_CONFIG, 116
PcieEqPh3LaneParamCm
FSP_S_CONFIG, 91
PcieEqPh3LaneParamCp
FSP_S_CONFIG, 91
PcieRpAspm
FSP_S_CONFIG, 91
PcieRpClkReqNumber
FSP_S_CONFIG, 91
PcieRpClkReqSupport
FSP_S_CONFIG, 91
PcieRpClkSrcNumber
FSP_S_CONFIG, 91
PcieRpCompletionTimeout
FSP_S_CONFIG, 92
PcieRpDeviceResetPad
FSP_S_CONFIG, 92
PcieRpDptp
FSP_S_TEST_CONFIG, 117
PcieRpEnableMask
FSP_M_CONFIG, 43
PcieRpFunctionSwap
FSP_S_CONFIG, 92
PcieRpGen3EqPh3Method
FSP_S_CONFIG, 92
PcieRpL1Substates
FSP_S_CONFIG, 92
PcieRpPcieSpeed
FSP_S_CONFIG, 92
PcieRpPhysicalSlotNumber
FSP_S_CONFIG, 92
PcieRpSlotPowerLimitScale
FSP_S_TEST_CONFIG, 117
PcieRpSlotPowerLimitValue
FSP_S_TEST_CONFIG, 117
PcieRpUptp
FSP_S_TEST_CONFIG, 117
PcieSwEqCoeffListCm
FSP_S_CONFIG, 93
PcieSwEqCoeffListCp
FSP_S_CONFIG, 93
PeciC10Reset
FSP_M_CONFIG, 43
PeciSxReset
FSP_M_CONFIG, 43
Peg0Gen3EqPh2Enable
FSP_M_TEST_CONFIG, 54
Peg0Gen3EqPh3Method
FSP_M_TEST_CONFIG, 55
Peg1Gen3EqPh2Enable
FSP_M_TEST_CONFIG, 55
Peg1Gen3EqPh3Method
FSP_M_TEST_CONFIG, 55
Peg2Gen3EqPh2Enable
FSP_M_TEST_CONFIG, 55
Peg2Gen3EqPh3Method
FSP_M_TEST_CONFIG, 55
PegDataPtr
FSP_M_CONFIG, 43
PegDisableSpreadSpectrumClocking
FSP_M_CONFIG, 44
PegGen3EndPointHint
FSP_M_TEST_CONFIG, 55
PegGen3EndPointPreset
FSP_M_TEST_CONFIG, 56
PegGen3ProgramStaticEq
FSP_M_TEST_CONFIG, 56
PegGen3RootPortPreset
FSP_M_TEST_CONFIG, 56
PegGenerateBdatMarginTable
FSP_M_TEST_CONFIG, 56
PegRxCemLoopbackLane
FSP_M_TEST_CONFIG, 56
PegRxCemNonProtocolAwareness
FSP_M_TEST_CONFIG, 56
PkgCStateDemotion
FSP_S_TEST_CONFIG, 117
PkgCStateLimit
FSP_S_TEST_CONFIG, 117
PkgCStateUnDemotion
FSP_S_TEST_CONFIG, 117
PmgCstCfgCtrlLock
FSP_S_TEST_CONFIG, 118
PortUsb20Enable
FSP_S_CONFIG, 93
PortUsb30Enable
FSP_S_CONFIG, 93

PowerConfig
GPIO_CONFIG, 128
PowerLimit1
FSP_S_TEST_CONFIG, 118
PowerLimit1Time
FSP_S_TEST_CONFIG, 118
PowerLimit2
FSP_S_TEST_CONFIG, 118
PowerLimit2Power
FSP_S_TEST_CONFIG, 118
PowerLimit3
FSP_S_TEST_CONFIG, 118
PowerLimit3Time
FSP_S_TEST_CONFIG, 118
PowerLimit4
FSP_S_TEST_CONFIG, 119
PrmrrSize
FSP_M_CONFIG, 44
ProbelessTrace
FSP_M_CONFIG, 44
ProcHotResponse
FSP_S_TEST_CONFIG, 119
ProcTraceEnable
FSP_S_TEST_CONFIG, 119
ProcTraceOutputScheme
FSP_S_TEST_CONFIG, 119
Psi1Threshold
FSP_S_CONFIG, 93
Psi2Threshold
FSP_S_CONFIG, 93
Psi3Enable
FSP_S_CONFIG, 93
Psi3Threshold
FSP_S_CONFIG, 94
PsysOffset
FSP_S_CONFIG, 94
PsysPmax
FSP_S_TEST_CONFIG, 119
PsysPowerLimit1
FSP_S_TEST_CONFIG, 119
PsysPowerLimit1Power
FSP_S_TEST_CONFIG, 119
PsysPowerLimit2
FSP_S_TEST_CONFIG, 120
PsysPowerLimit2Power
FSP_S_TEST_CONFIG, 120
PsysSlope
FSP_S_CONFIG, 94
PxRcConfig
FSP_S_CONFIG, 94

RMT
FSP_M_CONFIG, 45
RaceToHalt
FSP_S_TEST_CONFIG, 120
Ratio
FSP_M_CONFIG, 44
RealtimeMemoryTiming
FSP_M_CONFIG, 44
RefClk
FSP_M_CONFIG, 44
RingDownBin
FSP_M_CONFIG, 44
RingMaxOcRatio
FSP_M_CONFIG, 44
RingMinOcRatio
FSP_M_CONFIG, 45
RingPllVoltageOffset
FSP_M_CONFIG, 45

SI_CHIPSET_INIT_INFO, 128
SI_PCH_DEVICE_INTERRUPT_CONFIG, 129
SI_PCH_INT_PIN
FspsUpd.h, 137
SMBIOS_CACHE_INFO, 129
SMBIOS_PROCESSOR_INFO, 130
SaGv
FSP_M_CONFIG, 45
SaPllVoltageOffset
FSP_M_CONFIG, 45
SataEnable
FSP_S_CONFIG, 94
SataMode
FSP_S_CONFIG, 94
SataP0TDispFinit
FSP_S_CONFIG, 94
SataP1TDispFinit
FSP_S_CONFIG, 95
SataPortsDevSlp
FSP_S_CONFIG, 95
SataPortsDmVal
FSP_S_CONFIG, 95
SataPortsEnable
FSP_S_CONFIG, 95
SataPwrOptEnable
FSP_S_CONFIG, 95
SataRstHddUnlock
FSP_S_CONFIG, 95
SataRstIrrt
FSP_S_CONFIG, 95
SataRstIrrtOnly
FSP_S_CONFIG, 96
SataRstLedLocate
FSP_S_CONFIG, 96
SataRstOromUiBanner
FSP_S_CONFIG, 96
SataRstPcieDeviceResetDelay
FSP_S_CONFIG, 96
SataRstRaid0
FSP_S_CONFIG, 96
SataRstRaid1
FSP_S_CONFIG, 96
SataRstRaid10
FSP_S_CONFIG, 96
SataRstRaid5
FSP_S_CONFIG, 96
SataRstRaidAlternateId
FSP_S_CONFIG, 97

SataRstSmartStorage
FSP_S_CONFIG, 97
SataSalpSupport
FSP_S_CONFIG, 97
SataTestMode
FSP_S_TEST_CONFIG, 120
SataThermalSuggestedSetting
FSP_S_CONFIG, 97
ScanExtGfxForLegacyOpRom
FSP_M_TEST_CONFIG, 57
SciIrqSelect
FSP_S_CONFIG, 97
ScsEmmcEnabled
FSP_S_CONFIG, 97
ScsEmmcHs400Enabled
FSP_S_CONFIG, 97
ScsSdCardEnabled
FSP_S_CONFIG, 98
SendEcCmd
FSP_S_CONFIG, 98
SendVrMbxCmd
FSP_S_CONFIG, 98
SendVrMbxCmd1
FSP_S_CONFIG, 98
SerialIoDebugUartNumber
FSP_S_CONFIG, 98
SerialIoDevMode
FSP_S_CONFIG, 98
SerialIoGpio
FSP_S_CONFIG, 98
SevenCoreRatioLimit
FSP_S_TEST_CONFIG, 120
ShowSpiController
FSP_S_CONFIG, 99
SiPchNoInt
FspsUpd.h, 137
SinitMemorySize
FSP_M_CONFIG, 45
SixCoreRatioLimit
FSP_S_TEST_CONFIG, 120
SkipMbpHob
FSP_M_TEST_CONFIG, 57
SlowSlewRateForGt
FSP_S_CONFIG, 99
SlowSlewRateForIa
FSP_S_CONFIG, 99
SlowSlewRateForSa
FSP_S_CONFIG, 99
SmbiosCacheInfoHob.h, 148
SmbiosProcessorInfoHob.h, 149
SmbusArpEnable
FSP_M_CONFIG, 45
SmbusDynamicPowerGating
FSP_M_TEST_CONFIG, 57
SmbusEnable
FSP_M_CONFIG, 46
SmbusSpdWriteDisable
FSP_M_TEST_CONFIG, 57
SpdProfileSelected
FSP_M_CONFIG, 46
SpiFlashCfgLockDown
FSP_S_CONFIG, 99
SsicPortEnable
FSP_S_CONFIG, 99
StateRatio
FSP_S_TEST_CONFIG, 120

tRTP
FSP_M_CONFIG, 46
TStates
FSP_S_TEST_CONFIG, 121
TTSuggestedSetting
FSP_S_CONFIG, 100
TccActivationOffset
FSP_S_TEST_CONFIG, 120
TccOffsetClamp
FSP_S_TEST_CONFIG, 121
TccOffsetLock
FSP_S_TEST_CONFIG, 121
TccOffsetTimeWindowForRatl
FSP_S_TEST_CONFIG, 121
TcoIrqSelect
FSP_S_CONFIG, 99
TdcPowerLimit
FSP_S_CONFIG, 100
TdcTimeWindow
FSP_S_CONFIG, 100
TgaSize
FSP_M_TEST_CONFIG, 57
ThreeCoreRatioLimit
FSP_S_TEST_CONFIG, 121
ThreeStrikeCounterDisable
FSP_S_TEST_CONFIG, 121
TimedMwait
FSP_S_TEST_CONFIG, 121
TjMaxOffset
FSP_M_CONFIG, 46
TotalFlashSize
FSP_M_TEST_CONFIG, 57
TsegSize
FSP_M_CONFIG, 46
TurboMode
FSP_S_CONFIG, 100
TvbRatioClipping
FSP_M_CONFIG, 46
TvbVoltageOptimization
FSP_M_CONFIG, 46
TwoCoreRatioLimit
FSP_S_TEST_CONFIG, 122
Txt
FSP_M_CONFIG, 47
TxtDprMemoryBase
FSP_M_CONFIG, 47
TxtDprMemorySize
FSP_M_CONFIG, 47
TxtHeapMemorySize
FSP_M_CONFIG, 47

TxtImplemented
FSP_M_CONFIG, 47
TxtLcpPdBase
FSP_M_TEST_CONFIG, 57
TxtLcpPdSize
FSP_M_TEST_CONFIG, 58

Usb2AfePehalfbit
FSP_S_CONFIG, 100
Usb2AfePetxiset
FSP_S_CONFIG, 100
Usb2AfePredeemp
FSP_S_CONFIG, 100
Usb2AfeTxiset
FSP_S_CONFIG, 101
Usb3HsioTxDeEmph
FSP_S_CONFIG, 101
Usb3HsioTxDeEmphEnable
FSP_S_CONFIG, 101
Usb3HsioTxDownscaleAmp
FSP_S_CONFIG, 101
Usb3HsioTxDownscaleAmpEnable
FSP_S_CONFIG, 101

VddVoltage
FSP_M_CONFIG, 47
VmxEnable
FSP_M_CONFIG, 47
VrPowerDeliveryDesign
FSP_S_CONFIG, 101
VrVoltageLimit
FSP_S_CONFIG, 102

WatchDog
FSP_S_CONFIG, 102
WatchDogTimerBios
FSP_S_CONFIG, 102
WatchDogTimerOs
FSP_S_CONFIG, 102
WdtDisableAndLock
FSP_M_TEST_CONFIG, 58

XdciEnable
FSP_S_CONFIG, 102