

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

Mon Nov 26 2018 13:53:37

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 PORTING RECOMMENDATION 11**
- 5 UPD PORTING GUIDE 13**
- 6 FSP OUTPUT 15**
- 7 FSP POSTCODE 19**
- 8 Class Index 27**
 - 8.1 Class List 27
- 9 File Index 29**
 - 9.1 File List 29
- 10 Class Documentation 31**
 - 10.1 AUDIO_AZALIA_VERB_TABLE Struct Reference 31
 - 10.1.1 Detailed Description 31
 - 10.2 AZALIA_HEADER Struct Reference 32
 - 10.2.1 Detailed Description 32
 - 10.3 CHIPSET_INIT_INFO Struct Reference 32
 - 10.3.1 Detailed Description 33
 - 10.4 DIMM_INFO Struct Reference 33
 - 10.4.1 Detailed Description 33
 - 10.5 FIRMWARE_VERSION Struct Reference 33
 - 10.5.1 Detailed Description 34
 - 10.6 FIRMWARE_VERSION_INFO Struct Reference 34
 - 10.6.1 Detailed Description 34
 - 10.7 FIRMWARE_VERSION_INFO_HOB Struct Reference 34
 - 10.7.1 Detailed Description 35

10.7.2	Member Data Documentation	35
10.7.2.1	Count	35
10.8	FSP_M_CONFIG Struct Reference	35
10.8.1	Detailed Description	53
10.8.2	Member Data Documentation	53
10.8.2.1	ActiveCoreCount	53
10.8.2.2	ApertureSize	53
10.8.2.3	ApStartupBase	53
10.8.2.4	Avx2RatioOffset	53
10.8.2.5	Avx3RatioOffset	54
10.8.2.6	BclkAdaptiveVoltage	54
10.8.2.7	BclkRfiFreq	54
10.8.2.8	BiosAcmBase	54
10.8.2.9	BiosAcmSize	54
10.8.2.10	BiosGuard	55
10.8.2.11	BistOnReset	55
10.8.2.12	BootFrequency	55
10.8.2.13	ChHashEnable	55
10.8.2.14	ChHashInterleaveBit	55
10.8.2.15	ChHashMask	56
10.8.2.16	CkeRankMapping	56
10.8.2.17	CleanMemory	56
10.8.2.18	CmdRanksTerminated	56
10.8.2.19	CoreMaxOcRatio	56
10.8.2.20	CorePIIVoltageOffset	57
10.8.2.21	CoreVoltageAdaptive	57
10.8.2.22	CoreVoltageMode	57
10.8.2.23	CoreVoltageOverride	57
10.8.2.24	CpuRatio	57
10.8.2.25	CpuRatioOverride	57
10.8.2.26	CpuTraceHubMemReg0Size	58
10.8.2.27	CpuTraceHubMemReg1Size	58
10.8.2.28	CpuTraceHubMode	58
10.8.2.29	CridEnable	58
10.8.2.30	DciUsb3TypecUfpDbg	58
10.8.2.31	DdrFreqLimit	59
10.8.2.32	DdrSpeedControl	59
10.8.2.33	DisableDimmChannel0	59
10.8.2.34	DisableDimmChannel1	59
10.8.2.35	DmiDeEmphasis	59

10.8.2.36 DmiGen3EndPointHint	60
10.8.2.37 DmiGen3EndPointPreset	60
10.8.2.38 DmiGen3ProgramStaticEq	60
10.8.2.39 DmiGen3RootPortPreset	60
10.8.2.40 EnableC6Dram	60
10.8.2.41 EnableSgx	61
10.8.2.42 EnCmdRate	61
10.8.2.43 EpgEnable	61
10.8.2.44 FClkFrequency	61
10.8.2.45 FivrEfficiency	61
10.8.2.46 FivrFaults	62
10.8.2.47 ForceOltmOrRefresh2x	62
10.8.2.48 FreqSaGvLow	62
10.8.2.49 FreqSaGvMid	62
10.8.2.50 GmAdr	62
10.8.2.51 GtPllVoltageOffset	63
10.8.2.52 GtPsmiSupport	63
10.8.2.53 GttMmAdr	63
10.8.2.54 HobBufferSize	63
10.8.2.55 HotThresholdCh0Dimm0	63
10.8.2.56 HotThresholdCh0Dimm1	64
10.8.2.57 HotThresholdCh1Dimm0	64
10.8.2.58 HotThresholdCh1Dimm1	64
10.8.2.59 Idd3n	64
10.8.2.60 Idd3p	64
10.8.2.61 IgdDvmt50PreAlloc	65
10.8.2.62 ImgUclkOutEn	65
10.8.2.63 ImrRpSelection	65
10.8.2.64 InitPcieAspmAfterOprom	65
10.8.2.65 InternalGfx	65
10.8.2.66 IsvtloPort	66
10.8.2.67 JtagC10PowerGateDisable	66
10.8.2.68 McPllVoltageOffset	66
10.8.2.69 MmioSize	66
10.8.2.70 OcLock	66
10.8.2.71 PcdDebugInterfaceFlags	66
10.8.2.72 PcdIsaSerialUartBase	67
10.8.2.73 PcdSerialDebugBaudRate	67
10.8.2.74 PcdSerialDebugLevel	67
10.8.2.75 PcdSerialUartNumber	67

10.8.2.76 PchLpcEnhancePort8xhDecoding	67
10.8.2.77 PchNumRsvdSmbusAddresses	68
10.8.2.78 PchPort80Route	68
10.8.2.79 PchSmbAlertEnable	68
10.8.2.80 PchTraceHubMemReg0Size	68
10.8.2.81 PchTraceHubMemReg1Size	68
10.8.2.82 PchTraceHubMode	69
10.8.2.83 PcieImrSize	69
10.8.2.84 PcieMultipleSegmentEnabled	69
10.8.2.85 PcieRpEnableMask	69
10.8.2.86 PlatformDebugConsent	69
10.8.2.87 PrmrrSize	70
10.8.2.88 ProbelessTrace	70
10.8.2.89 PwdwnIdleCounter	70
10.8.2.90 RankInterleave	70
10.8.2.91 Ratio	70
10.8.2.92 RealtimeMemoryTiming	71
10.8.2.93 RefClk	71
10.8.2.94 RhSolution	71
10.8.2.95 RingDownBin	71
10.8.2.96 RingMaxOcRatio	71
10.8.2.97 RingPIIVoltageOffset	72
10.8.2.98 RingVoltageAdaptive	72
10.8.2.99 RingVoltageMode	72
10.8.2.100RingVoltageOffset	72
10.8.2.101RingVoltageOverride	72
10.8.2.102RMT	72
10.8.2.103RMTLoopCount	73
10.8.2.104RmtPerTask	73
10.8.2.105SafeMode	73
10.8.2.106SaGv	73
10.8.2.107SaPcieRpEnableMask	73
10.8.2.108SaPcieRpLinkDownGpios	74
10.8.2.109SaPIIVoltageOffset	74
10.8.2.110ScramblerSupport	74
10.8.2.111SinitMemorySize	74
10.8.2.112SmbusArpEnable	74
10.8.2.113SmbusEnable	75
10.8.2.114SpdAddressTable	75
10.8.2.115SpdProfileSelected	75

10.8.2.116TcssDma0En	75
10.8.2.117TcssDma1En	75
10.8.2.118TcssDma2En	75
10.8.2.119TcssltbtPcie0En	76
10.8.2.120TcssltbtPcie1En	76
10.8.2.121TcssltbtPcie2En	76
10.8.2.122TcssltbtPcie3En	76
10.8.2.123TcssltbtPcie4En	76
10.8.2.124TcssltbtPcie5En	77
10.8.2.125TcssXhciEn	77
10.8.2.126TcssXhciEn	77
10.8.2.127TgaSize	77
10.8.2.128ThrtCkeMinTmr	77
10.8.2.129TjMaxOffset	77
10.8.2.130TmeEnable	78
10.8.2.131TrainTrace	78
10.8.2.132RTP	78
10.8.2.133TsegSize	78
10.8.2.134TsocAlarmwindowLockBit	78
10.8.2.135TsocCriticalEventOnly	79
10.8.2.136TsocCriticaltripLockBit	79
10.8.2.137TsocEventMode	79
10.8.2.138TsocEventOutputControl	79
10.8.2.139TsocEventPolarity	79
10.8.2.140TsocManualEnable	80
10.8.2.141TsocShutdownMode	80
10.8.2.142TsocTcritMax	80
10.8.2.143Txt	80
10.8.2.144TxDprMemoryBase	80
10.8.2.145TxDprMemorySize	81
10.8.2.146TxDprHeapMemorySize	81
10.8.2.147TxDprImplemented	81
10.8.2.148TxDprLcpPdBase	81
10.8.2.149TxDprLcpPdSize	81
10.8.2.150TxDprUserBudgetEnable	82
10.8.2.151TxDprUserThresholdEnable	82
10.8.2.152TxDprVddVoltage	82
10.8.2.153TxDprVmxEnable	82
10.8.2.154TxDprWarmThresholdCh0Dimm0	82
10.8.2.155TxDprWarmThresholdCh0Dimm1	83

10.8.2.156WarmThresholdCh1Dimm0	83
10.8.2.157WarmThresholdCh1Dimm1	83
10.9 FSP_M_TEST_CONFIG Struct Reference	83
10.9.1 Detailed Description	85
10.9.2 Member Data Documentation	85
10.9.2.1 BdatEnable	85
10.9.2.2 BdatTestType	85
10.9.2.3 BiosSize	85
10.9.2.4 BypassPhySyncReset	85
10.9.2.5 ChipsetInitMessage	86
10.9.2.6 DisableMessageCheck	86
10.9.2.7 DmiGen3EqPh2Enable	86
10.9.2.8 DmiGen3EqPh3Method	86
10.9.2.9 HeciCommunication2	86
10.9.2.10 KtDeviceEnable	87
10.9.2.11 LockPTMregs	87
10.9.2.12 PanelPowerEnable	87
10.9.2.13 ScanExtGfxForLegacyOpRom	87
10.9.2.14 SkipMbpHob	87
10.9.2.15 SmbusDynamicPowerGating	87
10.9.2.16 SmbusSpdWriteDisable	88
10.9.2.17 TotalFlashSize	88
10.9.2.18 TxtAcheckRequest	88
10.9.2.19 WdtDisableAndLock	88
10.10FSP_S_CONFIG Struct Reference	88
10.10.1 Detailed Description	112
10.10.2 Member Data Documentation	112
10.10.2.1 AcLoadline	112
10.10.2.2 AcousticNoiseMitigation	113
10.10.2.3 AmtEnabled	113
10.10.2.4 AmtKvmEnabled	113
10.10.2.5 AmtSolEnabled	113
10.10.2.6 AsfEnabled	113
10.10.2.7 CnviBtAudioOffload	113
10.10.2.8 CnviBtCore	114
10.10.2.9 CnviClkreqPinMux	114
10.10.2.10CnviMode	114
10.10.2.11CnviRfResetPinMux	114
10.10.2.12DcLoadline	114
10.10.2.13DevIntConfigPtr	115

10.10.2.14DmiSuggestedSetting	115
10.10.2.15DmiTS0TW	115
10.10.2.16DmiTS1TW	115
10.10.2.17DmiTS2TW	115
10.10.2.18DmiTS3TW	116
10.10.2.19EcCmdLock	116
10.10.2.20EcCmdProvisionEav	116
10.10.2.21Enable8254ClockGating	116
10.10.2.22EnableMinVoltageOverride	116
10.10.2.23EnableTcoTimer	116
10.10.2.24EnableTimedGPIO0	117
10.10.2.25EnableTimedGPIO1	117
10.10.2.26EsataSpeedLimit	117
10.10.2.27FastPkgCRampDisableFivr	117
10.10.2.28FastPkgCRampDisableGt	118
10.10.2.29FastPkgCRampDisableIa	118
10.10.2.30FastPkgCRampDisableSa	118
10.10.2.31FivrRfiFrequency	118
10.10.2.32FivrSpreadSpectrum	118
10.10.2.33ForcMebxSyncUp	119
10.10.2.34FwProgress	119
10.10.2.35GpioIrqRoute	119
10.10.2.36Heci3Enabled	119
10.10.2.37ccMax	119
10.10.2.38monOffset	119
10.10.2.39monSlope	120
10.10.2.40omTypeCPortPadCfg	120
10.10.2.41ITbtConnectTopologyTimeoutInMs	120
10.10.2.42TbtForcePowerOnTimeoutInMs	120
10.10.2.43ManageabilityMode	120
10.10.2.44MeUnconfigOnRtcClear	121
10.10.2.45MinVoltageC8	121
10.10.2.46MinVoltageRuntime	121
10.10.2.47NumOfDevIntConfig	121
10.10.2.48PchCrid	121
10.10.2.49PchDmiAspmCtrl	122
10.10.2.50PchDmiTsawEn	122
10.10.2.51PchEnableComplianceMode	122
10.10.2.52PchEnableDbcObs	122
10.10.2.53PchEspHostC10ReportEnable	122

10.10.2.54PchFivrDynPm	123
10.10.2.55PchFivrExtVnnRailSxEnabledStates	123
10.10.2.56PchFivrExtVnnRailSxlccMax	123
10.10.2.57PchFivrExtVnnRailSxVoltage	123
10.10.2.58PchFivrVccinAuxLowToHighCurModeVolTranTime	123
10.10.2.59PchFivrVccinAuxOffToHighCurModeVolTranTime	124
10.10.2.60PchFivrVccinAuxRetToHighCurModeVolTranTime	124
10.10.2.61PchFivrVccinAuxRetToLowCurModeVolTranTime	124
10.10.2.62PchHdaAudioLinkDmic0ClkAPinMux	124
10.10.2.63PchHdaAudioLinkDmic0ClkBPinMux	124
10.10.2.64PchHdaAudioLinkDmic0DataPinMux	125
10.10.2.65PchHdaAudioLinkDmic0Enable	125
10.10.2.66PchHdaAudioLinkDmic1ClkAPinMux	125
10.10.2.67PchHdaAudioLinkDmic1ClkBPinMux	125
10.10.2.68PchHdaAudioLinkDmic1DataPinMux	125
10.10.2.69PchHdaAudioLinkDmic1Enable	125
10.10.2.70PchHdaAudioLinkHdaEnable	126
10.10.2.71PchHdaAudioLinkSndw1Enable	126
10.10.2.72PchHdaAudioLinkSndw2Enable	126
10.10.2.73PchHdaAudioLinkSndw3Enable	126
10.10.2.74PchHdaAudioLinkSndw4Enable	126
10.10.2.75PchHdaAudioLinkSsp0Enable	127
10.10.2.76PchHdaAudioLinkSsp1Enable	127
10.10.2.77PchHdaAudioLinkSsp2Enable	127
10.10.2.78PchHdaAudioLinkSsp3Enable	127
10.10.2.79PchHdaAudioLinkSsp4Enable	127
10.10.2.80PchHdaAudioLinkSsp5Enable	127
10.10.2.81PchHdaDspEnable	128
10.10.2.82PchHdaDspUaaCompliance	128
10.10.2.83PchHdaDispCodecDisconnect	128
10.10.2.84PchHdaDispLinkFrequency	128
10.10.2.85PchHdaLinkFrequency	128
10.10.2.86PchHdaPme	129
10.10.2.87PchHdaVcType	129
10.10.2.88PchHotEnable	129
10.10.2.89PchIoApicEntry24_119	129
10.10.2.90PchIoApicId	129
10.10.2.91PchIshGpEnable	130
10.10.2.92PchIshI2cEnable	130
10.10.2.93PchIshPdtUnlock	130

10.10.2.94PchIshSpiCs0Enable	130
10.10.2.95PchIshSpiEnable	130
10.10.2.96PchIshUartEnable	130
10.10.2.97PchLanEnable	131
10.10.2.98PchLanLtrEnable	131
10.10.2.99PchLockDownBiosLock	131
10.10.2.100PchMemoryThrottlingEnable	131
10.10.2.101PchOseAdcEnable	131
10.10.2.102PchOseCanEnable	132
10.10.2.103PchOseHsuartEnable	132
10.10.2.104PchOsel2cEnable	132
10.10.2.105PchOsel2sEnable	132
10.10.2.106PchOsePwmEnable	132
10.10.2.107PchOseQepEnable	132
10.10.2.108PchOseSpiCs0Enable	133
10.10.2.109PchOseSpiEnable	133
10.10.2.110PchOseTimedGpioEnable	133
10.10.2.111PchOseTimedGpioPinAllocation	133
10.10.2.112PchOseTimedGpioPinEnable	133
10.10.2.113PchOseUartEnable	134
10.10.2.114PchPcieDeviceOverrideTablePtr	134
10.10.2.115PchPmDeepSxPol	134
10.10.2.116PchPmDisableDsxAcPresentPulldown	134
10.10.2.117PchPmDisableNativePowerButton	134
10.10.2.118PchPmLanWakeFromDeepSx	135
10.10.2.119PchPmMeWakeSts	135
10.10.2.120PchPmPciePllSsc	135
10.10.2.121PchPmPcieWakeFromDeepSx	135
10.10.2.122PchPmPmeB0S5Dis	135
10.10.2.123PchPmPwrBtnOverridePeriod	135
10.10.2.124PchPmPwrCycDur	136
10.10.2.125PchPmSlpAMinAssert	136
10.10.2.126PchPmSlpLanLowDc	136
10.10.2.127PchPmSlpS0Enable	136
10.10.2.128PchPmSlpS0Vm070VSupport	136
10.10.2.129PchPmSlpS0Vm075VSupport	137
10.10.2.130PchPmSlpS0VmRuntimeControl	137
10.10.2.131PchPmSlpS3MinAssert	137
10.10.2.132PchPmSlpS4MinAssert	137
10.10.2.133PchPmSlpStrchSusUp	137

10.10.2.134	chPmSlpSusMinAssert	137
10.10.2.135	chPmVrAlert	138
10.10.2.136	chPmWolEnableOverride	138
10.10.2.137	chPmWolOvrWkSts	138
10.10.2.138	chPmWoWlanDeepSxEnable	138
10.10.2.139	chPmWoWlanEnable	138
10.10.2.140	chPwrOptEnable	139
10.10.2.141	chS0ixAutoDemotion	139
10.10.2.142	chSeriallol2cPadsTermination	139
10.10.2.143	chSeriallol2cSciPinMux	139
10.10.2.144	chSeriallol2cSdaPinMux	139
10.10.2.145	chStartFramePulse	140
10.10.2.146	chTsnEnable	140
10.10.2.147	chTTEnable	140
10.10.2.148	chTTLock	140
10.10.2.149	chTTState13Enable	140
10.10.2.150	cieComplianceTestMode	141
10.10.2.151	cieDisableRootPortClockGating	141
10.10.2.152	cieEnablePeerMemoryWrite	141
10.10.2.153	cieEqPh3LaneParamCm	141
10.10.2.154	cieEqPh3LaneParamCp	141
10.10.2.155	cieRpAspm	142
10.10.2.156	cieRpCompletionTimeout	142
10.10.2.157	cieRpDpcExtensionsMask	142
10.10.2.158	cieRpDpcMask	142
10.10.2.159	cieRpFunctionSwap	142
10.10.2.160	cieRpGen3EqPh3Method	142
10.10.2.161	cieRpImrEnabled	143
10.10.2.162	cieRpL1Substates	143
10.10.2.163	cieRpPcieSpeed	143
10.10.2.164	cieRpPhysicalSlotNumber	143
10.10.2.165	cieRpPtmMask	143
10.10.2.166	cieSwEqCoeffListCm	144
10.10.2.167	cieSwEqCoeffListCp	144
10.10.2.168	mcCpuC10GatePinEnable	144
10.10.2.169	mcDbgMsgEn	144
10.10.2.170	mcGrTscEnable	144
10.10.2.171	mcModPhySusPgEnable	145
10.10.2.172	mcPowerButtonDebounce	145
10.10.2.173	mcV1p05IsExtFetControlEn	145

10.10.2.174	mcV1p05PhyExtFetControlEn	145
10.10.2.175	PortUsb20Enable	145
10.10.2.176	PortUsb30Enable	146
10.10.2.177	PinSupport	146
10.10.2.178	Psi1Threshold	146
10.10.2.179	Psi2Threshold	146
10.10.2.180	Psi3Enable	146
10.10.2.181	Psi3Threshold	147
10.10.2.182	PsOnEnable	147
10.10.2.183	PsysOffset	147
10.10.2.184	PsysSlope	147
10.10.2.185	RcConfig	147
10.10.2.186	RemoteAssistance	148
10.10.2.187	RtcBiosInterfaceLock	148
10.10.2.188	RtcMemoryLock	148
10.10.2.189	SaPcieComplianceTestMode	148
10.10.2.190	SaPcieDeviceOverrideTablePtr	148
10.10.2.191	SaPcieDisableRootPortClockGating	149
10.10.2.192	SaPcieDisableRootPortPowerGating	149
10.10.2.193	SaPcieEnablePeerMemoryWrite	149
10.10.2.194	SaPcieEqPh3LaneParamCm	149
10.10.2.195	SaPcieEqPh3LaneParamCp	149
10.10.2.196	SaPcieGen3EndPointHint	150
10.10.2.197	SaPcieGen3EndPointPreset	150
10.10.2.198	SaPcieGen3ProgramStaticEq	150
10.10.2.199	SaPcieGen3RootPortPreset	150
10.10.2.200	SaPcieGen4EndPointHint	150
10.10.2.201	SaPcieGen4EndPointPreset	151
10.10.2.202	SaPcieGen4ProgramStaticEq	151
10.10.2.203	SaPcieGen4RootPortPreset	151
10.10.2.204	SaPcieHwEqGen3CoeffListCm	151
10.10.2.205	SaPcieHwEqGen3CoeffListCp	151
10.10.2.206	SaPcieHwEqGen4CoeffListCm	152
10.10.2.207	SaPcieHwEqGen4CoeffListCp	152
10.10.2.208	SaPcieRpAspm	152
10.10.2.209	SaPcieRpDpcEnabled	152
10.10.2.210	SaPcieRpDpcExtensionsEnabled	152
10.10.2.211	SaPcieRpFunctionSwap	152
10.10.2.212	SaPcieRpGen3EqPh23Enable	153
10.10.2.213	SaPcieRpGen3EqPh3Enable	153

10.10.2.213aPcieRpGen3EqPh3Method	153
10.10.2.215aPcieRpGen4EqPh23Enable	153
10.10.2.216aPcieRpGen4EqPh3Enable	153
10.10.2.217aPcieRpGen4EqPh3Method	154
10.10.2.218aPcieRpL1Substates	154
10.10.2.219aPcieRpPcieSpeed	154
10.10.2.220aPcieRpPhysicalSlotNumber	154
10.10.2.223aPcieRpPtmEnabled	154
10.10.2.222aPcieRpVcEnabled	155
10.10.2.223aataEnable	155
10.10.2.223aataLedEnable	155
10.10.2.225aataMode	155
10.10.2.226aataP0TDispFinit	155
10.10.2.227aataP1TDispFinit	156
10.10.2.228aataPortsDevSlp	156
10.10.2.229aataPortsDmVal	156
10.10.2.230aataPortsEnable	156
10.10.2.233aataPwrOptEnable	156
10.10.2.232aataRstHddUnlock	156
10.10.2.233aataRstInterrupt	157
10.10.2.233aataRstIrrt	157
10.10.2.235aataRstIrrtOnly	157
10.10.2.236aataRstLedLocate	157
10.10.2.237aataRstOromUiBanner	157
10.10.2.238aataRstPcieDeviceResetDelay	158
10.10.2.239aataRstRaid0	158
10.10.2.240aataRstRaid1	158
10.10.2.243aataRstRaid10	158
10.10.2.242aataRstRaid5	158
10.10.2.243aataRstRaidDeviceld	159
10.10.2.244aataRstSmartStorage	159
10.10.2.245aataSalpSupport	159
10.10.2.246aataThermalSuggestedSetting	159
10.10.2.247aataCilrqSelect	159
10.10.2.248aataCsEmmcEnabled	159
10.10.2.249aataCsEmmcHs400Enabled	160
10.10.2.250aataCsSdCardEnabled	160
10.10.2.253aataEndEcCmd	160
10.10.2.252aataEndVrMbxCmd	160
10.10.2.253aataSerialIoDebugUartNumber	160

10.10.2.253	SerialIoI2cMode	161
10.10.2.255	SerialIoSpi0CsEnable	161
10.10.2.256	SerialIoSpi0CsPolarity	161
10.10.2.257	SerialIoSpi1CsEnable	161
10.10.2.258	SerialIoSpi1CsPolarity	161
10.10.2.259	SerialIoSpi2CsEnable	162
10.10.2.260	SerialIoSpi2CsPolarity	162
10.10.2.263	SerialIoSpi3CsEnable	162
10.10.2.262	SerialIoSpi3CsPolarity	162
10.10.2.263	SerialIoSpi4CsEnable	162
10.10.2.264	SerialIoSpi4CsPolarity	163
10.10.2.265	SerialIoSpi5CsEnable	163
10.10.2.266	SerialIoSpi5CsPolarity	163
10.10.2.267	SerialIoSpi6CsEnable	163
10.10.2.268	SerialIoSpi6CsPolarity	163
10.10.2.269	SerialIoSpiDefaultCsOutput	163
10.10.2.270	SerialIoSpiMode	164
10.10.2.273	SerialIoUartCtsPinMuxPolicy	164
10.10.2.272	SerialIoUartDataBits	164
10.10.2.273	SerialIoUartDmaEnable	164
10.10.2.274	SerialIoUartMode	164
10.10.2.275	SerialIoUartParity	165
10.10.2.276	SerialIoUartPowerGating	165
10.10.2.277	SerialIoUartRtsPinMuxPolicy	165
10.10.2.278	SerialIoUartRxPinMuxPolicy	165
10.10.2.279	SerialIoUartStopBits	165
10.10.2.280	SerialIoUartTxPinMuxPolicy	166
10.10.2.283	ShowSpiController	166
10.10.2.282	SiCsmFlag	166
10.10.2.283	SkipMplnit	166
10.10.2.284	SlowSlewRateForFivr	166
10.10.2.285	SlowSlewRateForGt	166
10.10.2.286	SlowSlewRateForIa	167
10.10.2.287	SlowSlewRateForSa	167
10.10.2.288	SpS0DisQForDebug	167
10.10.2.289	SpS0Override	167
10.10.2.290	UcolrqSelect	167
10.10.2.291	TcssAuxOri	168
10.10.2.292	TcssHslOri	168
10.10.2.293	TdcPowerLimit	168

10.10.2.297	AdcTimeWindow	168
10.10.2.295	EncPort0InterruptPinMuxing	168
10.10.2.296	EncPort1InterruptPinMuxing	169
10.10.2.297	TSuggestedSetting	169
10.10.2.298	BurboMode	169
10.10.2.299	ExtEnable	169
10.10.2.300	fsEnable	169
10.10.2.301	sb2PhyPehalfbit	170
10.10.2.302	sb2PhyPetxiset	170
10.10.2.303	sb2PhyPredeemp	170
10.10.2.304	sb2PhyTxiset	170
10.10.2.305	sb3HsioTxDeEmph	170
10.10.2.306	sb3HsioTxDeEmphEnable	171
10.10.2.307	sb3HsioTxDownscaleAmp	171
10.10.2.308	sb3HsioTxDownscaleAmpEnable	171
10.10.2.309	sbPdoProgramming	171
10.10.2.310	sbTcPortEn	171
10.10.2.311	mdEnable	172
10.10.2.312	mdPortA	172
10.10.2.313	mdPortB	172
10.10.2.314	mdPortC	172
10.10.2.315	mdPortD	172
10.10.2.316	rVoltageLimit	172
10.10.2.317	WatchDog	173
10.10.2.318	WatchDogTimerBios	173
10.10.2.319	WatchDogTimerOs	173
10.10.2.320	dcieEnable	173
10.11	FSP_S_TEST_CONFIG Struct Reference	173
10.11.1	Detailed Description	182
10.11.2	Member Data Documentation	182
10.11.2.1	ApldleManner	182
10.11.2.2	AutoThermalReporting	182
10.11.2.3	C1e	183
10.11.2.4	C1StateAutoDemotion	183
10.11.2.5	C1StateUnDemotion	183
10.11.2.6	ConfigTdpBios	183
10.11.2.7	CoreCStateLimit	183
10.11.2.8	CStatePreWake	183
10.11.2.9	CstCfgCtrlIoMwaitRedirection	184
10.11.2.10	Custom1ConfigTdpControl	184

10.11.2.11Custom1PowerLimit1	184
10.11.2.12Custom1PowerLimit1Time	184
10.11.2.13Custom1PowerLimit2	184
10.11.2.14Custom1TurboActivationRatio	185
10.11.2.15Custom2ConfigTdpControl	185
10.11.2.16Custom2PowerLimit1	185
10.11.2.17Custom2PowerLimit1Time	185
10.11.2.18Custom2PowerLimit2	185
10.11.2.19Custom2TurboActivationRatio	186
10.11.2.20Custom3ConfigTdpControl	186
10.11.2.21Custom3PowerLimit1	186
10.11.2.22Custom3PowerLimit1Time	186
10.11.2.23Custom3PowerLimit2	186
10.11.2.24Custom3TurboActivationRatio	187
10.11.2.25Cx	187
10.11.2.26DebugInterfaceLockEnable	187
10.11.2.27DisableProcHotOut	187
10.11.2.28DisableVrThermalAlert	187
10.11.2.29Eist	187
10.11.2.30EnableEpbPeciOverride	188
10.11.2.31EnableFastMsrHwpReq	188
10.11.2.32EnableHwpAutoEppGrouping	188
10.11.2.33EnableHwpAutoPerCorePstate	188
10.11.2.34EnableIbmi	188
10.11.2.35EnablePerCorePState	189
10.11.2.36EndOfPostMessage	189
10.11.2.37EnergyEfficientPState	189
10.11.2.38EnergyEfficientTurbo	189
10.11.2.39HdcControl	189
10.11.2.40Hwp	190
10.11.2.41HwpInterruptControl	190
10.11.2.42MachineCheckEnable	190
10.11.2.43MaxRingRatioLimit	190
10.11.2.44MctpBroadcastCycle	190
10.11.2.45MinRingRatioLimit	191
10.11.2.46MlcStreamerPrefetcher	191
10.11.2.47MonitorMwaitEnable	191
10.11.2.48NumberOfEntries	191
10.11.2.49OneCoreRatioLimit	191
10.11.2.50PchHdaResetWaitTimer	192

10.11.2.51PchLockDownBiosInterface	192
10.11.2.52PchLockDownGlobalSmi	192
10.11.2.53PchPmDisableEnergyReport	192
10.11.2.54PchSbAccessUnlock	192
10.11.2.55PchUnlockGpioPads	192
10.11.2.56PchXhciOcLock	193
10.11.2.57PcieEnablePort8xhDecode	193
10.11.2.58PcieRpDptp	193
10.11.2.59PcieRpSlotPowerLimitScale	193
10.11.2.60PcieRpSlotPowerLimitValue	193
10.11.2.61PcieRpUptp	194
10.11.2.62PkgCStateDemotion	194
10.11.2.63PkgCStateLimit	194
10.11.2.64PkgCStateUnDemotion	194
10.11.2.65PmcLpmS0ixSubStateEnableMask	194
10.11.2.66PmgCstCfgCtrlLock	195
10.11.2.67PowerLimit1	195
10.11.2.68PowerLimit1Time	195
10.11.2.69PowerLimit2	195
10.11.2.70PowerLimit2Power	195
10.11.2.71PowerLimit3	196
10.11.2.72PowerLimit4	196
10.11.2.73ProcessorTraceEnable	196
10.11.2.74ProcessorTraceMemBase	196
10.11.2.75ProcessorTraceMemLength	196
10.11.2.76ProcessorTraceOutputScheme	197
10.11.2.77ProcHotResponse	197
10.11.2.78PsysPmax	197
10.11.2.79PsysPowerLimit1	197
10.11.2.80PsysPowerLimit1Power	197
10.11.2.81PsysPowerLimit2	197
10.11.2.82PsysPowerLimit2Power	198
10.11.2.83RaceToHalt	198
10.11.2.84SaPcieRpGen3Dptp	198
10.11.2.85SaPcieRpGen3Uptp	198
10.11.2.86SaPcieRpGen4Dptp	198
10.11.2.87SaPcieRpGen4Uptp	199
10.11.2.88SataTestMode	199
10.11.2.89SkipPostBootSai	199
10.11.2.90StateRatio	199

10.11.2.91StateRatioMax16	199
10.11.2.92TccActivationOffset	200
10.11.2.93TccOffsetClamp	200
10.11.2.94TccOffsetLock	200
10.11.2.95TccOffsetTimeWindowForRatl	200
10.11.2.96ThreeStrikeCounterDisable	200
10.11.2.97TimedMwait	201
10.11.2.98TStates	201
10.12FSP_T_CONFIG Struct Reference	201
10.12.1 Detailed Description	202
10.12.2 Member Data Documentation	202
10.12.2.1 PcdSerialloUartAutoFlow	202
10.12.2.2 PcdSerialloUartCtsPinMux	202
10.12.2.3 PcdSerialloUartDataBits	202
10.12.2.4 PcdSerialloUartDebugEnabled	203
10.12.2.5 PcdSerialloUartNumber	203
10.12.2.6 PcdSerialloUartParity	203
10.12.2.7 PcdSerialloUartRtsPinMux	203
10.12.2.8 PcdSerialloUartStopBits	203
10.13FSP_T_TEST_CONFIG Struct Reference	204
10.13.1 Detailed Description	204
10.14FSPM_UPD Struct Reference	204
10.14.1 Detailed Description	205
10.15FSPS_UPD Struct Reference	205
10.15.1 Detailed Description	206
10.16FSPT_CORE_UPD Struct Reference	206
10.16.1 Detailed Description	206
10.17FSPT_UPD Struct Reference	206
10.17.1 Detailed Description	207
10.18GPIO_CONFIG Struct Reference	207
10.18.1 Detailed Description	208
10.18.2 Member Data Documentation	208
10.18.2.1 Direction	208
10.18.2.2 ElectricalConfig	209
10.18.2.3 HostSoftPadOwn	209
10.18.2.4 InterruptConfig	209
10.18.2.5 LockConfig	209
10.18.2.6 OutputState	209
10.18.2.7 PadMode	210
10.18.2.8 PowerConfig	210

10.19	HOB_USAGE_DATA_HOB Struct Reference	210
10.19.1	Detailed Description	210
10.20	MEMORY_PLATFORM_DATA Struct Reference	210
10.20.1	Detailed Description	210
10.21	SI_PCH_DEVICE_INTERRUPT_CONFIG Struct Reference	211
10.21.1	Detailed Description	211
10.22	SMBIOS_CACHE_INFO Struct Reference	211
10.22.1	Detailed Description	212
10.23	SMBIOS_PROCESSOR_INFO Struct Reference	212
10.23.1	Detailed Description	213
10.24	SMBIOS_STRUCTURE Struct Reference	213
10.24.1	Detailed Description	213
11	File Documentation	215
11.1	FirmwareVersionInfoHob.h File Reference	215
11.1.1	Detailed Description	215
11.2	FspFixedPcds.h File Reference	216
11.2.1	Detailed Description	216
11.3	FspInfoHob.h File Reference	216
11.3.1	Detailed Description	217
11.4	FspmUpd.h File Reference	217
11.4.1	Detailed Description	218
11.5	FspsUpd.h File Reference	219
11.5.1	Detailed Description	220
11.5.2	Enumeration Type Documentation	220
11.5.2.1	SI_PCH_INT_PIN	220
11.6	FsptUpd.h File Reference	221
11.6.1	Detailed Description	222
11.7	FspUpd.h File Reference	222
11.7.1	Detailed Description	223
11.8	GpioConfig.h File Reference	223
11.8.1	Detailed Description	225
11.8.2	Enumeration Type Documentation	225
11.8.2.1	GPIO_DIRECTION	225
11.8.2.2	GPIO_ELECTRICAL_CONFIG	225
11.8.2.3	GPIO_HARDWARE_DEFAULT	226
11.8.2.4	GPIO_HOSTSW_OWN	226
11.8.2.5	GPIO_INT_CONFIG	227
11.8.2.6	GPIO_LOCK_CONFIG	227
11.8.2.7	GPIO_OTHER_CONFIG	228

11.8.2.8	GPIO_OUTPUT_STATE	228
11.8.2.9	GPIO_PAD_MODE	228
11.8.2.10	GPIO_RESET_CONFIG	229
11.9	GpioSampleDef.h File Reference	230
11.9.1	Detailed Description	230
11.10	HobUsageDataHob.h File Reference	231
11.10.1	Detailed Description	231
11.11	MemInfoHob.h File Reference	231
11.11.1	Detailed Description	232
11.11.2	Enumeration Type Documentation	233
11.11.2.1	MRC_BOOT_MODE	233
11.12	SmbiosCacheInfoHob.h File Reference	233
11.12.1	Detailed Description	234
11.13	SmbiosProcessorInfoHob.h File Reference	234
11.13.1	Detailed Description	234
Index		237

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 ElkhartLake platforms with ElkhartLake processor and ElkhartLake 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>
- *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

Acronym	Definition
FSP	Firmware Support Package
FSP API	Firmware Support Package Interface
FW	Firmware
PCH	Platform Controller Hub
PMC	Power Management Controller
SBSP	System BSP
SMI	System Management Interrupt
SMM	System Management Mode
SPI	Serial Peripheral Interface
TSEG	Memory Reserved at the Top of Memory to be used as SMRAM
UPD	Updatable Product Data
IED	Intel Enhanced Debug
GTT	Graphics Translation Table
BDSM	Base Data Of Stolen Memory
PMRR	Protected Memory Range Reporting
IOT	Internal Observation Trace
MOT	Memory Observation Trace
DPR	DMA Protected Range
REMAP	Remapped Memory Area
TOLUD	Top of Low Usable Memory
TOUUD	Top of Upper Usable Memory

Chapter 2

FSP OVERVIEW

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

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

3.2 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-P-S) must have same FSP Image ID and revision number, using FV segments with different revision numbers in a single FSP image is not valid. The FSP API parameters documented in this integration guide are applicable for the Image ID and Revision specified as below.

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

3.5 FSP Global Data

FSP uses some amount of TempRam area to store FSP global data which contains some critical data like pointers to FSP information headers and UPD configuration regions, FSP/Bootloader stack pointers required for stack switching

etc. HPET Timer register(2) [PcdGlobalDataPointerAddress](#) is reserved to store address of this global data, and hence boot loader should not use this register for any other purpose. If TempRAM initialization is done by boot loader, then HPET has to be initialized to the base so that access to the register will work fine.

3.6 FSP APIs

This release of the ElkhartLake 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 given by [PcdTemporaryRamSize](#) starting from the base address of [PcdTemporaryRamBase](#). Out of total temporary memory available, last [PcdFspReservedBufferSize](#) bytes of space reserved by FSP for TempRamInit if temporary RAM initialization is done by FSP and remaining space from **TemporaryRamBase**(ECX) to **TemporaryRamBase+TemporaryRamSize-FspReservedBufferSize** (EDX) is available for both bootloader and FSP binary.

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

Note

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

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

FSPT_UPD.MicrocodeRegionBase** and **FSPT_UPD.MicrocodeRegionLength** are input parameters to 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
0xFEFE0000 - 0x00080000	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 0xFEFE17F00 by default.

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

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

3.6.3 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 boot-loader must skip calling this API and bootloader will tear down the temporary memory area setup in the cache and bring the cache to normal mode of operation.

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

At the end of *TempRamExit* the original code and data caching are disabled. FSP will reconfigure all MTRRs as described in the table below for performance optimization.

Memory range	Cache Attribute
0x00000000 - 0x0009FFFF	Write back
0x000C0000 - Top of Low Memory	Write back
0xFF000000 - 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 *FspUpdPtr* is pointer to **FSPS_UPD** structure which is described in header file [FspUpd.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 FspSiliconInit for starting APs. If this data is important to bootloader, then bootloader needs to preserve it before calling FspSiliconInit.

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

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

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

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

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

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

Programs SA Bars: MchBar, DmiBar, EpBar, GdxcBar, EDRAM (if supported). Please refer to section 2.↔

8 (MemoryMap) for the corresponding Bar values. GttMmadr (0xDF000000) and GmAdr(0xC0000000) are temporarily programmed and cleared after use in FSP.

3.6.5 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.

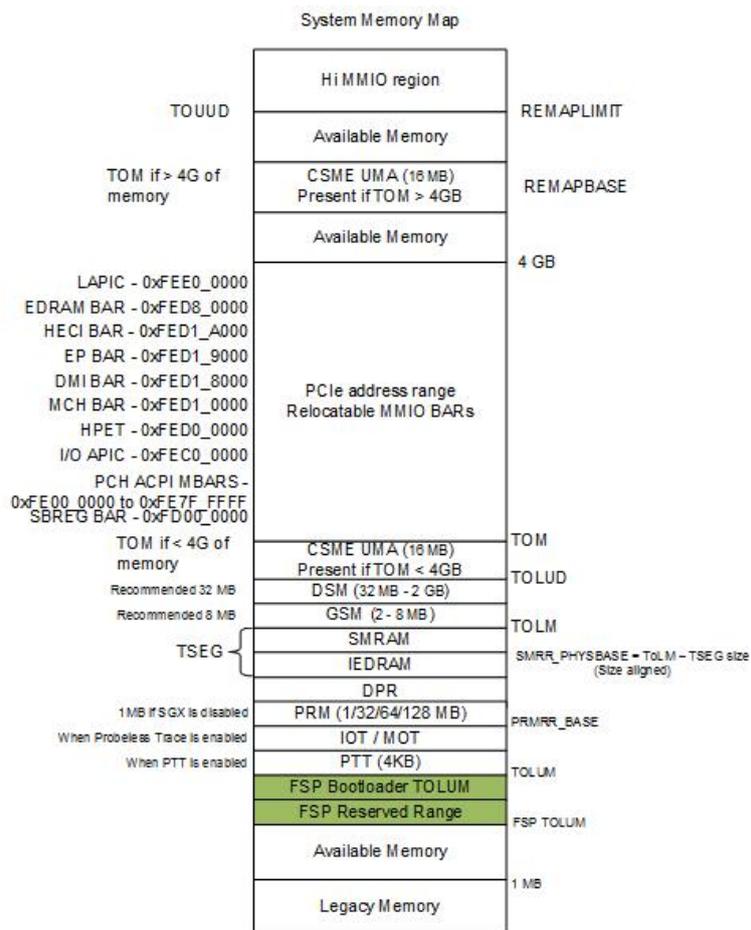


Figure 3.1: System Memory Map

/**

Chapter 4

FSP PORTING RECOMMENDATION

4 FSP Porting Recommendation

Here listed some notes or recommendation when porting with FSP.

4.1 Locking PAM register

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

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

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

4.2 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 party OpRom execution (and should be locked in S3 resume right before OS waking vector).

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

4.3 Locking SMI register

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

4.4 Verify below settings are correct for your platforms

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

Register	Values
ABASE	0x1800
PWRMBASE	0xFE000000
PCIEXBAR_BASE_ADDRESS	0xE0000000

Note

:

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

4.5 FSP_STATUS_RESET_REQUIRED

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

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

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

Chapter 5

UPD PORTING GUIDE

5 UPD porting guide

UPD porting guide:

UPD	Dependency	Description	Value
EnableSgx	ElkhartLake Platform	Temporary workaround	2
CstateLatencyControl1Irtl	Server platform	Server platform should has different setting	0x6B
PchPcieHsioRxSetCtleEnable	Board design	Different board requires different value	tune
PchPcieHsioRxSetCtle	Board design	Different board requires different value	tune
PchSataHsioRxGen3EqBoostMag↔ Enable	Board design	Different board requires different value	tune
PchSataHsioRxGen3EqBoostMag	Board design	Different board requires different value	tune
PchSataHsioTxGen1Downscale↔ AmpEnable	Board design	Different board requires different value	tune
PchSataHsioTxGen1DownscaleAmp	Board design	Different board requires different value	tune
PchSataHsioTxGen2Downscale↔ AmpEnable	Board design	Different board requires different value	tune
PchSataHsioTxGen2DownscaleAmp	Board design	Different board requires different value	tune
PchNumRsvdSmbusAddresses	Board design	Different board requires different value	tune
RsvdSmbusAddressTablePtr	Board design	Different board requires different value	tune
BiosSize	Board design	Different board requires different value	tune

Chapter 6

FSP OUTPUT

6 FSP Output

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

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

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

6.1 SMRAM Resource Descriptor HOB

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

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

6.2 SMBIOS INFO HOB

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

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

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

typedef struct {
    UINT8 Status;                 ///< Indicates whether this channel should be used.
    UINT8 ChannelId;
```

```

    UINT8          DimmCount;                ///< Number of valid DIMMs that exist in the channel.
    MRC_CH_TIMING Timing[MAX_PROFILE];      ///< The channel timing values.
    DIMM_INFO      Dimm[MAX_DIMM];          ///< Save the DIMM output characteristics.
} CHANNEL_INFO;

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

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

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

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

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

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

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

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

```

```

///
typedef struct {
    UINT16    TotalNumberOfSockets;
    UINT16    CurrentSocketNumber;
    UINT8     ProcessorType;          ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.1
    ///

```

6.3 CHIPSETINIT INFO HOB

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

```

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

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

```

```
} CHIPSET_INIT_INFO;
```

6.4 HOB USAGE INFO HOB

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

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

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

Chapter 7

FSP POSTCODE

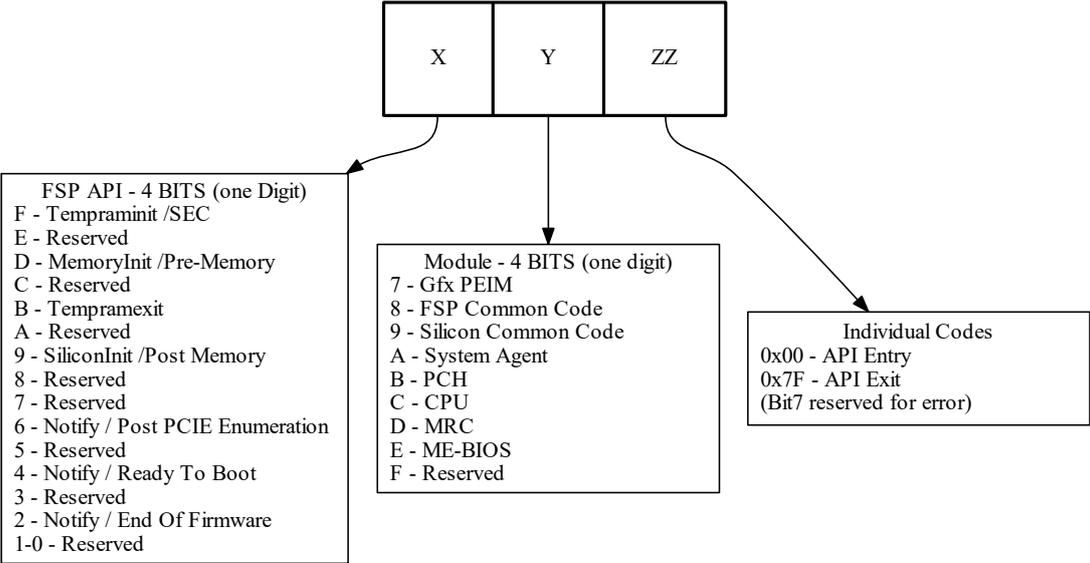
7 FSP PostCode

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

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

7.1 PostCode Info

Below diagram represents the 16 bit PostCode usage in FSP.



7.1.1 TempRamInit API Status Codes (0xFxxx)

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

7.1.2 FspMemoryInit API Status Codes (0xDxxx)

PostCode	Module	Description
0xD800	FSP	FspMemoryInit API Entry
0xD87F	FSP	FSpMemoryInit API Exit
0xDA00	SA	Pre-Mem Salnit Entry
0xDA02	SA	OverrideDev0Did Start
0xDA04	SA	OverrideDev2Did Start
0xDA06	SA	Programming SA Bars
0xDA08	SA	Install SA HOBs
0xDA0A	SA	Reporting SA PCIe code version
0xDA0C	SA	SaSvInit Start
0xDA10	SA	Initializing DMI
0xDA15	SA	Initialize TCSS PreMem
0xDA1F	SA	Initializing DMI/OPI Max Payload Size
0xDA20	SA	Initializing SwitchableGraphics
0xDA30	SA	Initializing SA PCIe
0xDA3F	SA	Programming PEG credit values Start
0xDA40	SA	Initializing DMI Tc/Vc mapping
0xDA42	SA	CheckOffboardPcieVga
0xDA44	SA	CheckAndInitializePegVga
0xDA50	SA	Initializing Graphics
0xDA52	SA	Initializing System Agent Overclocking
0xDA7F	SA	Pre-Mem Salnit Exit
0xDB00	PCH	Pre-Mem PchInit Entry
0xDB02	PCH	Pre-Mem Disable PCH fused controllers
0xDB15	PCH	Pre-Mem SMBUS configuration
0xDB48	PCH	Pre-Mem PchOnPolicyInstalled Entry
0xDB49	PCH	Pre-Mem Program HSIO
0xDB4A	PCH	Pre-Mem DCI configuration
0xDB4C	PCH	Pre-Mem Host DCI enabled
0xDB4D	PCH	Pre-Mem Trace Hub - Early configuration
0xDB4E	PCH	Pre-Mem Trace Hub - Device disabled
0xDB4F	PCH	Pre-Mem TraceHub - Programming MSR
0xDB50	PCH	Pre-Mem Trace Hub - Power gating configuration
0xDB51	PCH	Pre-Mem Trace Hub - Power gating Trace Hub device and locking HSWPGCR1 register
0xDB52	PCH	Pre-Mem Initialize HPET timer
0xDB55	PCH	Pre-Mem PchOnPolicyInstalled Exit
0xDB7F	PCH	Pre-Mem PchInit Exit
0xDC00	CPU	CPU Pre-Mem Entry
0xDC0F	CPU	CpuAddPreMemConfigBlocks Done
0xDC20	CPU	CpuOnPolicyInstalled Start
0xDC2F	CPU	XmmInit Start
0xDC3F	CPU	TxtInit Start
0xDC4F	CPU	Init CPU Straps

PostCode	Module	Description
0xDC5F	CPU	Init Overclocking
0xDC6F	CPU	CPU Pre-Mem Exit
0x**55	SA	MRC_MEM_INIT_DONE
0x**D5	SA	MRC_MEM_INIT_DONE_WITH_ERRORS
0xDD00	SA	MRC_INITIALIZATION_START
0xDD10	SA	MRC_CMD_PLOT_2D
0xDD1B	SA	MRC_FAST_BOOT_PERMITTED
0xDD1C	SA	MRC_RESTORE_NON_TRAINING
0xDD1D	SA	MRC_PRINT_INPUT_PARAMS
0xDD1E	SA	MRC_SET_OVERRIDES_PSPD
0xDD20	SA	MRC_SPD_PROCESSING
0xDD21	SA	MRC_SET_OVERRIDES
0xDD22	SA	MRC_MC_CAPABILITY
0xDD23	SA	MRC_MC_CONFIG
0xDD24	SA	MRC_MC_MEMORY_MAP
0xDD25	SA	MRC_JEDEC_INIT_LPDDR3
0xDD26	SA	MRC_RESET_SEQUENCE
0xDD27	SA	MRC_PRE_TRAINING
0xDD28	SA	MRC_EARLY_COMMAND
0xDD29	SA	MRC_SENSE_AMP_OFFSET
0xDD2A	SA	MRC_READ_MPR
0xDD2B	SA	MRC_RECEIVE_ENABLE
0xDD2C	SA	MRC_JEDEC_WRITE_LEVELING
0xDD2D	SA	MRC_LPDDR_LATENCY_SET_B
0xDD2E	SA	MRC_WRITE_TIMING_1D
0xDD2F	SA	MRC_READ_TIMING_1D
0xDD30	SA	MRC_DIMM_ODT
0xDD31	SA	MRC_EARLY_WRITE_TIMING_2D
0xDD32	SA	MRC_WRITE_DS
0xDD33	SA	MRC_WRITE_EQ
0xDD34	SA	MRC_EARLY_READ_TIMING_2D
0xDD35	SA	MRC_READ_ODT
0xDD36	SA	MRC_READ_EQ
0xDD37	SA	MRC_READ_AMP_POWER
0xDD38	SA	MRC_WRITE_TIMING_2D
0xDD39	SA	MRC_READ_TIMING_2D
0xDD3A	SA	MRC_CMD_VREF
0xDD3B	SA	MRC_WRITE_VREF_2D
0xDD3C	SA	MRC_READ_VREF_2D
0xDD3D	SA	MRC_POST_TRAINING
0xDD3E	SA	MRC_LATE_COMMAND
0xDD3F	SA	MRC_ROUND_TRIP_LAT
0xDD40	SA	MRC_TURN_AROUND
0xDD41	SA	MRC_CMP_OPT
0xDD42	SA	MRC_SAVE_MC_VALUES
0xDD43	SA	MRC_RESTORE_TRAINING
0xDD44	SA	MRC_RMT_TOOL
0xDD45	SA	MRC_WRITE_SR
0xDD46	SA	MRC_DIMM_RON
0xDD47	SA	MRC_RCVEN_TIMING_1D
0xDD48	SA	MRC_MR_FILL

PostCode	Module	Description
0xDD49	SA	MRC_PWR_MTR
0xDD4A	SA	MRC_DDR4_MAPPING
0xDD4B	SA	MRC_WRITE_VOLTAGE_1D
0xDD4C	SA	MRC_EARLY_RDMPR_TIMING_2D
0xDD4D	SA	MRC_FORCE_OLTM
0xDD50	SA	MRC_MC_ACTIVATE
0xDD51	SA	MRC_RH_PREVENTION
0xDD52	SA	MRC_GET_MRC_DATA
0xDD53	SA	Reserved
0xDD58	SA	MRC_RETRAIN_CHECK
0xDD5A	SA	MRC_SA_GV_SWITCH
0xDD5B	SA	MRC_ALIAS_CHECK
0xDD5C	SA	MRC_ECC_CLEAN_START
0xDD5D	SA	MRC_DONE
0xDD5F	SA	MRC_CPGC_MEMORY_TEST
0xDD60	SA	MRC_TXT_ALIAS_CHECK
0xDD61	SA	MRC_ENG_PERF_GAIN
0xDD68	SA	MRC_MEMORY_TEST
0xDD69	SA	MRC_FILL_RMT_STRUCTURE
0xDD70	SA	MRC_SELF_REFRESH_EXIT
0xDD71	SA	MRC_NORMAL_MODE
0xDD7D	SA	MRC_SSA_PRE_STOP_POINT
0xDD7F	SA	MRC_SSA_STOP_POINT, MRC_INITIALIZATION_END
0xDD90	SA	MRC_CMD_PLOT_2D_ERROR
0xDD9B	SA	MRC_FAST_BOOT_PERMITTED_ERROR
0xDD9C	SA	MRC_RESTORE_NON_TRAINING_ERROR
0xDD9D	SA	MRC_PRINT_INPUT_PARAMS_ERROR
0xDD9E	SA	MRC_SET_OVERRIDES_PSPD_ERROR
0xDDA0	SA	MRC_SPD_PROCESSING_ERROR
0xDDA1	SA	MRC_SET_OVERRIDES_ERROR
0xDDA2	SA	MRC_MC_CAPABILITY_ERROR
0xDDA3	SA	MRC_MC_CONFIG_ERROR
0xDDA4	SA	MRC_MC_MEMORY_MAP_ERROR
0xDDA5	SA	MRC_JEDEC_INIT_LPDDR3_ERROR
0xDDA6	SA	MRC_RESET_ERROR
0xDDA7	SA	MRC_PRE_TRAINING_ERROR
0xDDA8	SA	MRC_EARLY_COMMAND_ERROR
0xDDA9	SA	MRC_SENSE_AMP_OFFSET_ERROR
0xDDAA	SA	MRC_READ_MPR_ERROR
0xDDAB	SA	MRC_RECEIVE_ENABLE_ERROR
0xDDAC	SA	MRC_JEDEC_WRITE_LEVELING_ERROR
0xDDAD	SA	MRC_LPDDR_LATENCY_SET_B_ERROR
0xDDAE	SA	MRC_WRITE_TIMING_1D_ERROR
0xDDAF	SA	MRC_READ_TIMING_1D_ERROR
0xDDB0	SA	MRC_DIMM_ODT_ERROR
0xDDB1	SA	MRC_EARLY_WRITE_TIMING_ERROR
0xDDB2	SA	MRC_WRITE_DS_ERROR
0xDDB3	SA	MRC_WRITE_EQ_ERROR
0xDDB4	SA	MRC_EARLY_READ_TIMING_ERROR
0xDDB5	SA	MRC_READ_ODT_ERROR
0xDDB6	SA	MRC_READ_EQ_ERROR

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

7.1.3 TempRamExit API Status Codes (0xBxxx)

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

7.1.4 FspSiliconInit API Status Codes (0x9xxx)

PostCode	Module	Description
0x9800	FSP	FspSiliconInit API Entry
0x987F	FSP	FspSiliconInit API Exit
0x9A00	SA	PostMem Salnit Entry
0x9A01	SA	DeviceConfigure Start
0x9A02	SA	UpdateSaHobPostMem Start
0x9A03	SA	Initializing Pei Display
0x9A04	SA	PeiGraphicsNotifyCallback Entry
0x9A05	SA	CallPpiAndFillFrameBuffer
0x9A06	SA	GraphicsPpiInit
0x9A07	SA	GraphicsPpiGetMode
0x9A08	SA	FillFrameBufferAndShowLogo
0x9A0F	SA	PeiGraphicsNotifyCallback Exit
0x9A14	SA	Initializing SA IPU device
0x9A16	SA	Initializing SA GNA device
0x9A1A	SA	SaProgramLlcWays Start
0x9A20	SA	Initializing PciExpressInitPostMem
0x9A22	SA	Initializing ConfigureNorthIntelTraceHub
0x9A30	SA	Initializing Vtd
0x9A31	SA	Initializing TCSS
0x9A32	SA	Initializing Pavp
0x9A34	SA	PeiInstallSmmAccessPpi Start
0x9A36	SA	EdramWa Start
0x9A4F	SA	Post-Mem Salnit Exit
0x9A50	SA	SaSecurityLock Start
0x9A5F	SA	SaSecurityLock End
0x9A60	SA	SaSResetComplete Entry
0x9A61	SA	Set BIOS_RESET_CPL to indicate all configurations complete
0x9A62	SA	SaSvInit2 Start
0x9A63	SA	GraphicsPmInit Start
0x9A64	SA	SaPciPrint Start
0x9A6F	SA	SaSResetComplete Exit
0x9A70	SA	SaS3ResumeAtEndOfPei Callback Entry
0x9A7F	SA	SaS3ResumeAtEndOfPei Callback Exit
0x9B00	PCH	Post-Mem PchInit Entry
0x9B03	PCH	Post-Mem Tune the USB 2.0 high-speed signals quality
0x9B04	PCH	Post-Mem Tune the USB 3.0 signals quality
0x9B05	PCH	Post-Mem Configure PCH xHCI
0x9B06	PCH	Post-Mem Performs configuration of PCH xHCI SSIC
0x9B07	PCH	Post-Mem Configure PCH xHCI after init
0x9B08	PCH	Post-Mem Configures PCH USB device (xDCI)
0x9B0A	PCH	Post-Mem DMI/OP-DMI configuration
0x9B0B	PCH	Post-Mem Initialize P2SB controller
0x9B0C	PCH	Post-Mem IOAPIC initialization
0x9B0D	PCH	Post-Mem PCH devices interrupt configuration
0x9B0E	PCH	Post-Mem HD Audio initialization
0x9B0F	PCH	Post-Mem HD Audio Codec enumeration
0x9B10	PCH	Post-Mem HD Audio Codec not detected
0x9B13	PCH	Post-Mem SCS initialization
0x9B14	PCH	Post-Mem ISH initialization

PostCode	Module	Description
0x9B15	PCH	Post-Mem Configure SMBUS power management
0x9B16	PCH	Post-Mem Reserved
0x9B17	PCH	Post-Mem Performing global reset
0x9B18	PCH	Post-Mem Reserved
0x9B19	PCH	Post-Mem Reserved
0x9B40	PCH	Post-Mem OnEndOfPEI Entry
0x9B41	PCH	Post-Mem Initialize Thermal controller
0x9B42	PCH	Post-Mem Configure Memory Throttling
0x9B47	PCH	Post-Mem OnEndOfPEI Exit
0x9B4D	PCH	Post-Mem Trace Hub - Memory configuration
0x9B4E	PCH	Post-Mem Trace Hub - MSC0 configured
0x9B4F	PCH	Post-Mem Trace Hub - MSC1 configured
0x9B7F	PCH	Post-Mem PchInit Exit
0x9C00	CPU	CPU Post-Mem Entry
0x9C09	CPU	CpuAddConfigBlocks Done
0x9C0A	CPU	SetCpuStrapAndEarlyPowerOnConfig Start
0x9C13	CPU	SetCpuStrapAndEarlyPowerOnConfig Reset
0x9C14	CPU	SetCpuStrapAndEarlyPowerOnConfig Done
0x9C15	CPU	Cpulnit Start
0x9C16	CPU	SgxInitializationPrePatchLoad Start
0x9C17	CPU	CollectProcessorFeature Start
0x9C18	CPU	ProgramProcessorFeature Start
0x9C19	CPU	ProgramProcessorFeature Done
0x9C20	CPU	CpulnitPreResetCpl Start
0x9C21	CPU	ProcessorsPrefetcherInitialization Start
0x9C22	CPU	InitRatl Start
0x9C23	CPU	ConfigureSvidVrs Start
0x9C24	CPU	ConfigurePidSettings Start
0x9C25	CPU	SetBootFrequency Start
0x9C26	CPU	CpuOclnitPreMem Start
0x9C27	CPU	CpuOclnit Reset
0x9C28	CPU	BiosGuardInit Start
0x9C29	CPU	BiosGuardInit Reset
0x9C3F	CPU	CpulnitPreResetCpl Done
0x9C42	CPU	SgxActivation Start
0x9C43	CPU	InitializeCpuDataHob Start
0x9C44	CPU	InitializeCpuDataHob Done
0x9C4F	CPU	Cpulnit Done
0x9C50	CPU	S3InitializeCpu Start
0x9C55	CPU	MpRendezvousProcedure Start
0x9C56	CPU	MpRendezvousProcedure Done
0x9C69	CPU	S3InitializeCpu Done
0x9C6A	CPU	CpuPowerMgmtInit Start
0x9C71	CPU	InitPpm
0x9C7F	CPU	CPU Post-Mem Exit
0x9C80	CPU	ReloadMicrocodePatch Start
0x9C81	CPU	ReloadMicrocodePatch Done
0x9C82	CPU	ApSafePostMicrocodePatchInit Start
0x9C83	CPU	ApSafePostMicrocodePatchInit Done

7.1.5 NotifyPhase API Status Codes (0x6xxx)

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

Chapter 8

Class Index

8.1 Class List

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

AUDIO_AZALIA_VERB_TABLE	Audio Azalia Verb Table structure	31
AZALIA_HEADER	Azalia Header structure	32
CHIPSET_INIT_INFO	The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC	32
DIMM_INFO	Memory SMBIOS & OC Memory Data Hob	33
FIRMWARE_VERSION	Firmware Version Structure	33
FIRMWARE_VERSION_INFO	Firmware Version Information Structure	34
FIRMWARE_VERSION_INFO_HOB	Firmware Version Information HOB Structure	34
FSP_M_CONFIG	Fsp M Configuration	35
FSP_M_TEST_CONFIG	Fsp M Test Configuration	83
FSP_S_CONFIG	Fsp S Configuration	88
FSP_S_TEST_CONFIG	Fsp S Test Configuration	173
FSP_T_CONFIG	Fsp T Configuration	201
FSP_T_TEST_CONFIG	Fsp T Test Configuration	204
FSPM_UPD	Fsp M UPD Configuration	204
FSPS_UPD	Fsp S UPD Configuration	205
FSPT_CORE_UPD	Fsp T Core UPD	206
FSPT_UPD	Fsp T UPD Configuration	206
GPIO_CONFIG	GPIO configuration structure used for pin programming	207

HOB_USAGE_DATA_HOB	
Hob Usage Data Hob	210
MEMORY_PLATFORM_DATA	
Memory Platform Data Hob	210
SI_PCH_DEVICE_INTERRUPT_CONFIG	
The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device	211
SMBIOS_CACHE_INFO	
SMBIOS Cache Info HOB Structure	211
SMBIOS_PROCESSOR_INFO	
SMBIOS Processor Info HOB Structure	212
SMBIOS_STRUCTURE	
The Smbios structure header	213

Chapter 9

File Index

9.1 File List

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

FirmwareVersionInfoHob.h	Header file for Firmware Version Information	215
FspFixedPcds.h	This file lists all FixedAtBuild PCDs referenced in FSP integration guide	216
FspInfoHob.h	Header file for FSP Information HOB	216
FspmUpd.h	Copyright (c) 2018, Intel Corporation	217
FspUpd.h	Copyright (c) 2018, Intel Corporation	219
FspTUpd.h	Copyright (c) 2018, Intel Corporation	221
FspUpd.h	Copyright (c) 2018, Intel Corporation	222
GpioConfig.h	Header file for GpioConfig structure used by GPIO library	223
GpioSampleDef.h	Copyright (c) 2015 - 2017, Intel Corporation	230
HobUsageDataHob.h	Definitions for Hob Usage data HOB	231
MemInfoHob.h	This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs	231
SmbiosCacheInfoHob.h	Header file for SMBIOS Cache Info HOB	233
SmbiosProcessorInfoHob.h	Header file for SMBIOS Processor Info HOB	234

Chapter 10

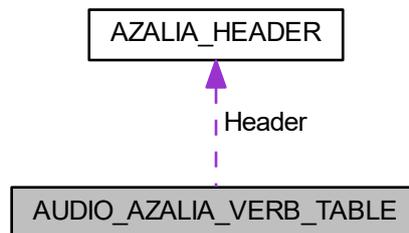
Class Documentation

10.1 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.

10.1.1 Detailed Description

Audio Azalia Verb Table structure.

Definition at line 56 of file `FspsUpd.h`.

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

- [FspsUpd.h](#)

10.2 AZALIA_HEADER Struct Reference

Azalia Header structure.

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

Public Attributes

- [UINT16 VendorId](#)
Codec Vendor ID.
- [UINT16 Deviceld](#)
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.

10.2.1 Detailed Description

Azalia Header structure.

Definition at line 44 of file FspsUpd.h.

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

- [FspsUpd.h](#)

10.3 CHIPSET_INIT_INFO Struct Reference

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

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

Public Attributes

- [UINT8 Revision](#)
Chipset Init Info Revision.
 - [UINT8 Rsvd](#) [3]
Reserved.
 - [UINT16 MeChipInitCrc](#)
16 bit CRC value of MeChipInit Table
 - [UINT16 BiosChipInitCrc](#)
16 bit CRC value of PchChipInit Table
-

10.3.1 Detailed Description

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

Definition at line 46 of file FspmUpd.h.

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

- [FspmUpd.h](#)

10.4 DIMM_INFO Struct Reference

Memory SMBIOS & OC Memory Data Hob.

```
#include <MemInfoHob.h>
```

Public Attributes

- UIN8 [Status](#)
See MrcDimmStatus for the definition of this field.
- UIN32 [DimmCapacity](#)
DIMM size in MBytes.
- UIN8 [ModulePartNum](#) [20]
Module part number for DDR3 is 18 bytes however for DRR4 20 bytes as per JEDEC Spec, so reserving 20 bytes.
- UIN8 [RankInDimm](#)
The number of ranks in this DIMM.
- UIN8 [SpdDramDeviceType](#)
Save SPD DramDeviceType information needed for SMBIOS structure creation.
- UIN8 [SpdModuleType](#)
Save SPD ModuleType information needed for SMBIOS structure creation.
- UIN8 [SpdModuleMemoryBusWidth](#)
Save SPD ModuleMemoryBusWidth information needed for SMBIOS structure creation.
- UIN8 [SpdSave](#) [MAX_SPD_SAVE]
Save SPD Manufacturing information needed for SMBIOS structure creation.
- UIN16 [Speed](#)
The maximum capable speed of the device, in MHz.

10.4.1 Detailed Description

Memory SMBIOS & OC Memory Data Hob.

Definition at line 191 of file MemInfoHob.h.

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

- [MemInfoHob.h](#)

10.5 FIRMWARE_VERSION Struct Reference

Firmware Version Structure.

```
#include <FirmwareVersionInfoHob.h>
```

10.5.1 Detailed Description

Firmware Version Structure.

Definition at line 28 of file FirmwareVersionInfoHob.h.

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

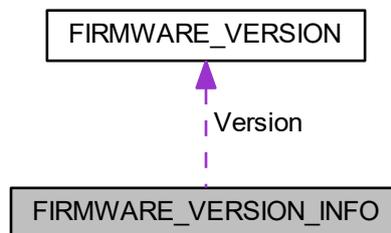
- [FirmwareVersionInfoHob.h](#)

10.6 FIRMWARE_VERSION_INFO Struct Reference

Firmware Version Information Structure.

```
#include <FirmwareVersionInfoHob.h>
```

Collaboration diagram for FIRMWARE_VERSION_INFO:



Public Attributes

- [UINT8 ComponentNameIndex](#)
Offset 0 Index of Component Name.
- [UINT8 VersionStringIndex](#)
Offset 1 Index of Version String.
- [FIRMWARE_VERSION Version](#)
Offset 2-6 Firmware version.

10.6.1 Detailed Description

Firmware Version Information Structure.

Definition at line 38 of file FirmwareVersionInfoHob.h.

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

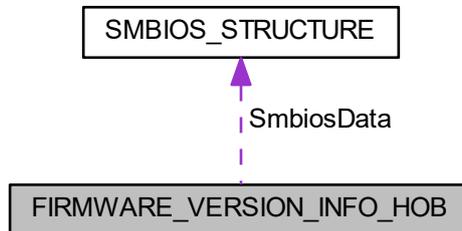
- [FirmwareVersionInfoHob.h](#)

10.7 FIRMWARE_VERSION_INFO_HOB Struct Reference

Firmware Version Information HOB Structure.

```
#include <FirmwareVersionInfoHob.h>
```

Collaboration diagram for FIRMWARE_VERSION_INFO_HOB:



Public Attributes

- [EFI_HOB_GUID_TYPE Header](#)
Offset 0-23 The header of FVI HOB.
- [SMBIOS_STRUCTURE SmbiosData](#)
Offset 24-27 The SMBIOS header of FVI HOB.
- [UINT8 Count](#)
Offset 28 Number of FVI elements included.

10.7.1 Detailed Description

Firmware Version Information HOB Structure.

Definition at line 58 of file FirmwareVersionInfoHob.h.

10.7.2 Member Data Documentation

10.7.2.1 Count

```
UINT8 FIRMWARE_VERSION_INFO_HOB::Count
```

Offset 28 Number of FVI elements included.

Definition at line 61 of file FirmwareVersionInfoHob.h.

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

- [FirmwareVersionInfoHob.h](#)

10.8 FSP_M_CONFIG Struct Reference

Fsp M Configuration.

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

Public Attributes

- UUINT64 [PlatformMemorySize](#)
Offset 0x0040 - Platform Reserved Memory Size The minimum platform memory size required to pass control into DXE.
 - UUINT16 [MemorySpdDataLen](#)
Offset 0x0048 - SPD Data Length Length of SPD Data 0x100:256 Bytes, 0x200:512 Bytes.
 - UUINT8 [UnusedUpdSpace0](#) [2]
Offset 0x004A.
 - UUINT32 [MemorySpdPtr00](#)
Offset 0x004C - Memory SPD Pointer Channel 0 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.
 - UUINT32 [MemorySpdPtr01](#)
Offset 0x0050 - Memory SPD Pointer Channel 0 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.
 - UUINT32 [MemorySpdPtr10](#)
Offset 0x0054 - Memory SPD Pointer Channel 1 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.
 - UUINT32 [MemorySpdPtr11](#)
Offset 0x0058 - Memory SPD Pointer Channel 1 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.
 - UUINT8 [DqByteMapCh0](#) [12]
Offset 0x005C - Dq Byte Map CH0 Dq byte mapping between CPU and DRAM, Channel 0: board-dependent.
 - UUINT8 [DqByteMapCh1](#) [12]
Offset 0x0068 - Dq Byte Map CH1 Dq byte mapping between CPU and DRAM, Channel 1: board-dependent.
 - UUINT8 [DqsMapCpu2DramCh0](#) [8]
Offset 0x0074 - Dqs Map CPU to DRAM CH 0 Set Dqs mapping relationship between CPU and DRAM, Channel 0: board-dependent.
 - UUINT8 [DqsMapCpu2DramCh1](#) [8]
Offset 0x007C - Dqs Map CPU to DRAM CH 1 Set Dqs mapping relationship between CPU and DRAM, Channel 1: board-dependent.
 - UUINT16 [RcompResistor](#) [3]
Offset 0x0084 - RcompResister settings Indicates RcompReister settings: Board-dependent.
 - UUINT16 [RcompTarget](#) [5]
Offset 0x008A - RcompTarget settings RcompTarget settings: board-dependent.
 - UUINT8 [DqPinsInterleaved](#)
Offset 0x0094 - Dqs Pins Interleaved Setting Indicates DqPinsInterleaved setting: board-dependent \$EN_DIS.
 - UUINT8 [CaVrefConfig](#)
Offset 0x0095 - 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.
 - UUINT8 [SmramMask](#)
Offset 0x0096 - Smram Mask The SMM Regions AB-SEG and/or H-SEG reserved 0: Neither, 1:AB-SEG, 2:H-SEG, 3: Both.
 - UUINT8 [MrcFastBoot](#)
Offset 0x0097 - MRC Fast Boot Enables/Disable the MRC fast path thru the MRC \$EN_DIS.
 - UUINT8 [Ibecc](#)
Offset 0x0098 - Ibecc Enables/Disable Ibecc \$EN_DIS.
 - UUINT8 [RmtPerTask](#)
Offset 0x0099 - Rank Margin Tool per Task This option enables the user to execute Rank Margin Tool per major training step in the MRC.
 - UUINT8 [TrainTrace](#)
Offset 0x009A - Training Trace This option enables the trained state tracing feature in MRC.
 - UUINT8 [UnusedUpdSpace1](#)
-

- Offset 0x009B.
- UUINT32 [IedSize](#)
 - Offset 0x009C - Intel Enhanced Debug Intel Enhanced Debug (IED): 0=Disabled, 0x400000=Enabled and 4MB S←MRAM occupied 0 : Disable, 0x400000 : Enable.
- UUINT32 [TsegSize](#)
 - Offset 0x00A0 - Tseg Size Size of SMRAM memory reserved.
- UUINT16 [MmioSize](#)
 - Offset 0x00A4 - MMIO Size Size of MMIO space reserved for devices.
- UUINT8 [ProbelessTrace](#)
 - Offset 0x00A6 - Probeless Trace Probeless Trace: 0=Disabled, 1=Enable.
- UUINT8 [SmbusEnable](#)
 - Offset 0x00A7 - Enable SMBus Enable/disable SMBus controller.
- UUINT8 [SpdAddressTable](#) [4]
 - Offset 0x00A8 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.
- UUINT8 [PlatformDebugConsent](#)
 - Offset 0x00AC - Platform Debug Consent To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type.
- UUINT8 [DciEn](#)
 - Offset 0x00AD - DCI Enable Determine if to enable DCI debug from host \$EN_DIS.
- UUINT8 [DciDbcMode](#)
 - Offset 0x00AE - DCI Dbc Mode Disabled: Clear both USB2/3DBCEN; USB2: set USB2DBCEN; USB3: set USB3←DBCEN; Both: Set both USB2/3DBCEN; No Change: Comply with HW value 0:Disabled, 1:USB2 Dbc, 2:USB3 Dbc, 3:Both, 4:No Change.
- UUINT8 [DciUsb3TypecUfpDbg](#)
 - Offset 0x00AF - USB3 Type-C UFP2DFP Kernel/Platform Debug Support This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting.
- UUINT8 [PchTraceHubMode](#)
 - Offset 0x00B0 - PCH Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.
- UUINT8 [PchTraceHubMemReg0Size](#)
 - Offset 0x00B1 - PCH Trace Hub Memory Region 0 buffer Size Specify size of Pch trace memory region 0 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.
- UUINT8 [PchTraceHubMemReg1Size](#)
 - Offset 0x00B2 - PCH Trace Hub Memory Region 1 buffer Size Specify size of Pch trace memory region 1 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.
- UUINT8 [PchPreMemRsvd](#) [7]
 - Offset 0x00B3 - PchPreMemRsvd Reserved for PCH Pre-Mem Reserved \$EN_DIS.
- UUINT8 [IgdDvmt50PreAlloc](#)
 - Offset 0x00BA - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.
- UUINT8 [InternalGfx](#)
 - Offset 0x00BB - Internal Graphics Enable/disable internal graphics.
- UUINT8 [ApertureSize](#)
 - Offset 0x00BC - Aperture Size Select the Aperture Size.
- UUINT8 [UserBd](#)
 - Offset 0x00BD - 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.
- UUINT16 [DdrFreqLimit](#)
 - Offset 0x00BE - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.
- UUINT8 [SaGv](#)
 - Offset 0x00C0 - SA GV System Agent dynamic frequency support and when enabled memory will be training at three different frequencies.
- UUINT8 [DdrSpeedControl](#)
 - Offset 0x00C1 - DDR Speed Control DDR Frequency and Gear control for all SAGV points.

- UINT16 [FreqSaGvLow](#)
Offset 0x00C2 - Low Frequency SAGV Low Frequency Selections in Mhz.
 - UINT16 [FreqSaGvMid](#)
Offset 0x00C4 - Mid Frequency SAGV Mid Frequency Selections in Mhz.
 - UINT8 [RMT](#)
Offset 0x00C6 - Rank Margin Tool Enable/disable Rank Margin Tool.
 - UINT8 [DisableDimmChannel0](#)
Offset 0x00C7 - Channel A DIMM Control Channel A DIMM Control Support - Enable or Disable Dimms on Channel A.
 - UINT8 [DisableDimmChannel1](#)
Offset 0x00C8 - Channel B DIMM Control Channel B DIMM Control Support - Enable or Disable Dimms on Channel B.
 - UINT8 [ScramblerSupport](#)
Offset 0x00C9 - Scrambler Support This option enables data scrambling in memory.
 - UINT8 [UnusedUpdSpace2](#) [2]
Offset 0x00CA.
 - UINT32 [MmaTestContentPtr](#)
Offset 0x00CC - MMA Test Content Pointer Pointer to MMA Test Content in Memory.
 - UINT32 [MmaTestContentSize](#)
Offset 0x00D0 - MMA Test Content Size Size of MMA Test Content in Memory.
 - UINT32 [MmaTestConfigPtr](#)
Offset 0x00D4 - MMA Test Config Pointer Pointer to MMA Test Config in Memory.
 - UINT32 [MmaTestConfigSize](#)
Offset 0x00D8 - MMA Test Config Size Size of MMA Test Config in Memory.
 - UINT8 [SpdProfileSelected](#)
Offset 0x00DC - SPD Profile Selected Select DIMM timing profile.
 - UINT8 [RefClk](#)
Offset 0x00DD - Memory Reference Clock 100MHz, 133MHz.
 - UINT16 [VddVoltage](#)
Offset 0x00DE - Memory Voltage Memory Voltage Override (Vddq).
 - UINT8 [Ratio](#)
Offset 0x00E0 - Memory Ratio Automatic or the frequency will equal ratio times reference clock.
 - UINT8 [OddRatioMode](#)
Offset 0x00E1 - QCLK Odd Ratio Adds 133 or 100 MHz to QCLK frequency, depending on RefClk \$EN_DIS.
 - UINT8 [tCL](#)
Offset 0x00E2 - tCL CAS Latency, 0: AUTO, max: 31.
 - UINT8 [tCWL](#)
Offset 0x00E3 - tCWL Min CAS Write Latency Delay Time, 0: AUTO, max: 34.
 - UINT16 [tFAW](#)
Offset 0x00E4 - tFAW Min Four Activate Window Delay Time, 0: AUTO, max: 63.
 - UINT16 [tRAS](#)
Offset 0x00E6 - tRAS RAS Active Time, 0: AUTO, max: 64.
 - UINT8 [tRCDtRP](#)
Offset 0x00E8 - tRCD/tRP RAS to CAS delay time and Row Precharge delay time, 0: AUTO, max: 63.
 - UINT8 [SaGvLowGear2](#)
Offset 0x00E9 - SA GV Low Gear Gear Selection for SAGV Low point 0:Gear1, 1:Gear2.
 - UINT16 [tREFI](#)
Offset 0x00EA - tREFI Refresh Interval, 0: AUTO, max: 65535.
 - UINT16 [tRFC](#)
Offset 0x00EC - tRFC Min Refresh Recovery Delay Time, 0: AUTO, max: 1023.
 - UINT8 [tRRD](#)
-

- Offset 0x00EE - tRRD Min Row Active to Row Active Delay Time, 0: AUTO, max: 15.*

 - UUINT8 [tRTP](#)
 - Offset 0x00EF - tRTP Min Internal Read to Precharge Command Delay Time, 0: AUTO, max: 15.*
 - UUINT8 [tWR](#)
 - Offset 0x00F0 - tWR Min Write Recovery Time, 0: AUTO, legal values: 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 24, 30, 34, 40 0:Auto, 5:5, 6:6, 7:7, 8:8, 10:10, 12:12, 14:14, 16:16, 18:18, 20:20, 24:24, 30:30, 34:34, 40:40.*
 - UUINT8 [tWTR](#)
 - Offset 0x00F1 - tWTR Min Internal Write to Read Command Delay Time, 0: AUTO, max: 28.*
 - UUINT8 [NModeSupport](#)
 - Offset 0x00F2 - NMode System command rate, range 0-2, 0 means auto, 1 = 1N, 2 = 2N.*
 - UUINT8 [DlIBwEn0](#)
 - Offset 0x00F3 - DlIBwEn[0] DlIBwEn[0], for 1067 (0..7)*
 - UUINT8 [DlIBwEn1](#)
 - Offset 0x00F4 - DlIBwEn[1] DlIBwEn[1], for 1333 (0..7)*
 - UUINT8 [DlIBwEn2](#)
 - Offset 0x00F5 - DlIBwEn[2] DlIBwEn[2], for 1600 (0..7)*
 - UUINT8 [DlIBwEn3](#)
 - Offset 0x00F6 - DlIBwEn[3] DlIBwEn[3], for 1867 and up (0..7)*
 - UUINT8 [IsvtIoPort](#)
 - Offset 0x00F7 - ISVT IO Port Address ISVT IO Port Address.*
 - UUINT8 [PchHdaEnable](#)
 - Offset 0x00F8 - Enable Intel HD Audio (Azalia) 0: Disable, 1: Enable (Default) Azalia controller \$EN_DIS.*
 - UUINT8 [PchIshEnable](#)
 - Offset 0x00F9 - Enable PCH ISH Controller 0: Disable, 1: Enable (Default) ISH Controller \$EN_DIS.*
 - UUINT8 [PchOseEnable](#)
 - Offset 0x00FA - Enable PCH OSE Controller 0: Disable, 1: Enable (Default) OSE Controller \$EN_DIS.*
 - UUINT8 [CpuTraceHubMode](#)
 - Offset 0x00FB - CPU Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.*
 - UUINT8 [CpuTraceHubMemReg0Size](#)
 - Offset 0x00FC - CPU Trace Hub Memory Region 0 CPU Trace Hub Memory Region 0, The available memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.*
 - UUINT8 [CpuTraceHubMemReg1Size](#)
 - Offset 0x00FD - CPU Trace Hub Memory Region 1 CPU Trace Hub Memory Region 1.*
 - UUINT8 [SaGvMidGear2](#)
 - Offset 0x00FE - SA GV Mid Gear Gear Selection for SAGV Mid point 0:Gear1, 1:Gear2.*
 - UUINT8 [SaGvHighGear2](#)
 - Offset 0x00FF - SA GV High Gear Gear Selection for SAGV High point, or when SAGV is disabled 0:Gear1, 1:Gear2.*
 - UUINT8 [HeciTimeouts](#)
 - Offset 0x0100 - HECI Timeouts 0: Disable, 1: Enable (Default) timeout check for HECI \$EN_DIS.*
 - UUINT8 [UnusedUpdSpace3](#) [3]
 - Offset 0x0101.*
 - UUINT32 [Heci1BarAddress](#)
 - Offset 0x0104 - HECI1 BAR address BAR address of HECI1.*
 - UUINT32 [Heci2BarAddress](#)
 - Offset 0x0108 - HECI2 BAR address BAR address of HECI2.*
 - UUINT32 [Heci3BarAddress](#)
 - Offset 0x010C - HECI3 BAR address BAR address of HECI3.*
 - UUINT32 [Heci4BarAddress](#)
 - Offset 0x0110 - HECI4 BAR address BAR address of HECI4.*
 - UUINT16 [SgDelayAfterPwrEn](#)
-

- Offset 0x0114 - SG dGPU Power Delay SG dGPU delay interval after power enabling: 0=Minimal, 1000=Maximum, default is 300=300 microseconds.
- UINT16 [SgDelayAfterHoldReset](#)
Offset 0x0116 - SG dGPU Reset Delay SG dGPU delay interval for Reset complete: 0=Minimal, 1000=Maximum, default is 100=100 microseconds.
 - UINT16 [MmioSizeAdjustment](#)
Offset 0x0118 - 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 0x011A - Enable/Disable DMI GEN3 Static EQ Phase1 programming Program DMI Gen3 EQ Phase1 Static Presets.
 - UINT8 [InitPcieAspmAfterOprom](#)
Offset 0x011B - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.
 - UINT8 [DmiGen3RootPortPreset](#) [8]
Offset 0x011C - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.
 - UINT8 [DmiGen3EndPointPreset](#) [8]
Offset 0x0124 - DMI Gen3 End port preset values per lane Used for programming DMI Gen3 preset values per lane.
 - UINT8 [DmiGen3EndPointHint](#) [8]
Offset 0x012C - DMI Gen3 End port Hint values per lane Used for programming DMI Gen3 Hint values per lane.
 - UINT8 [DmiGen3RxCtlePeaking](#) [4]
Offset 0x0134 - DMI Gen3 RxCTLEp per-Bundle control Range: 0-15, 0 is default for each bundle, must be specified based upon platform design.
 - UINT8 [DmiDeEmphasis](#)
Offset 0x0138 - DeEmphasis control for DMI DeEmphasis control for DMI.
 - UINT8 [PrimaryDisplay](#)
Offset 0x0139 - 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 [PsmiRegionSize](#)
Offset 0x013A - Selection of PSMI Region size 0=32MB, 1=288MB, 2=544MB, 3=800MB, 4=1024MB Default is 0 0:32MB, 1:288MB, 2:544MB, 3:800MB, 4:1024MB.
 - UINT8 [UnusedUpdSpace4](#)
Offset 0x013B.
 - UINT32 [GmAdr](#)
Offset 0x013C - Temporary MMIO address for GMADR The reference code will use this as Temporary MMIO address space to access GMADR Registers.Platform should provide conflict free Temporary MMIO Range: GmAdr to (GmAdr + ApertureSize).
 - UINT32 [GttMmAdr](#)
Offset 0x0140 - Temporary MMIO address for GTTMMADR The reference code will use this as Temporary MMIO address space to access GTTMMADR Registers.Platform should provide conflict free Temporary MMIO Range: GttMmAdr to (GttMmAdr + 2MB MMIO + 6MB Reserved + GttSize).
 - UINT16 [GttSize](#)
Offset 0x0144 - Selection of iGFX GTT Memory size 1=2MB, 2=4MB, 3=8MB, Default is 3 1:2MB, 2:4MB, 3:8MB.
 - UINT8 [SaRtd3Pcie0Gpio](#) [24]
Offset 0x0146 - Switchable Graphics GPIO information for PEG 0 Switchable Graphics GPIO information for PEG 0, for Reset, power and wake GPIOs.
 - UINT8 [TxtImplemented](#)
Offset 0x015E - Enable/Disable MRC TXT dependency When enabled MRC execution will wait for TXT initialization to be done first.
 - UINT8 [SaOcSupport](#)
Offset 0x015F - Enable/Disable SA OcSupport Enable: Enable SA OcSupport, Disable(Default): Disable SA OcSupport \$EN_DIS.
 - UINT8 [GtVoltageMode](#)
Offset 0x0160 - GT slice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.
-

- UINT8 [GtMaxOcRatio](#)
Offset 0x0161 - Maximum GTs turbo ratio override 0(Default)=Minimal/Auto, 60=Maximum.
- UINT16 [GtVoltageOffset](#)
Offset 0x0162 - The voltage offset applied to GT slice 0(Default)=Minimal, 1000=Maximum.
- UINT16 [GtVoltageOverride](#)
Offset 0x0164 - The GT slice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.
- UINT16 [GtExtraTurboVoltage](#)
Offset 0x0166 - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.
- UINT16 [SaVoltageOffset](#)
Offset 0x0168 - voltage offset applied to the SA 0(Default)=Minimal, 1000=Maximum.
- UINT8 [RootPortIndex](#)
Offset 0x016A - PCIe root port Function number for Switchable Graphics dGPU Root port Index number to indicate which PCIe root port has dGPU.
- UINT8 [RealtimeMemoryTiming](#)
Offset 0x016B - Realtime Memory Timing 0(Default): Disabled, 1: Enabled.
- UINT8 [PcieMultipleSegmentEnabled](#)
Offset 0x016C - This is policy to control iTBT PCIe Multiple Segment setting.
- UINT8 [SalpuEnable](#)
Offset 0x016D - Enable/Disable SA IPU Enable(Default): Enable SA IPU, Disable: Disable SA IPU \$EN_DIS.
- UINT8 [SalpulmrConfiguration](#)
Offset 0x016E - IPU IMR Configuration 0:IPU Camera, 1:IPU Gen Default is 0 0:IPU Camera, 1:IPU Gen.
- UINT8 [ImguClkOutEn](#) [5]
*Offset 0x016F - IMGU CLKOUT Configuration The configuration of IMGU CLKOUT, 0: Disable;1: **Enable**.*
- UINT8 [SalpuFusaConfigEnable](#)
Offset 0x0174 - IPU FUSA Configuration 0:FUSA Disable, 1:FUSA Enable Default is 0 0:FUSA Disable, 1:FUSA Enable.
- UINT8 [AcSplitLock](#)
Offset 0x0175 - AC Split Lock Enables/Disable the AC Split Lock Bit \$EN_DIS.
- UINT8 [UnusedUpdSpace5](#) [2]
Offset 0x0176.
- UINT32 [SaPcieRpEnableMask](#)
Offset 0x0178 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.
- UINT8 [SaPcieRpLinkDownGpios](#)
Offset 0x017C - Assertion on Link Down GPIOs GPIO Assertion on Link Down.
- UINT8 [GtPsmiSupport](#)
Offset 0x017D - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.
- UINT8 [DismSize](#)
Offset 0x017E - Selection of DiSM Region Size DiSM Size to be allocated for 2LM Sku Default is 0 0:0GB, 1:1GB, 2:2GB, 3:3GB, 4:4GB, 5:5GB, 6:6GB, 7:7GB.
- UINT8 [SaPreMemProductionRsvd](#) [138]
Offset 0x017F - SaPreMemProductionRsvd Reserved for SA Pre-Mem Production \$EN_DIS.
- UINT8 [BistOnReset](#)
*Offset 0x0209 - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.*
- UINT8 [SkipStopPbet](#)
*Offset 0x020A - Skip Stop PBET Timer Enable/Disable Skip Stop PBET Timer; **0: Disable**; 1: Enable \$EN_DIS.*
- UINT8 [EnableC6Dram](#)
Offset 0x020B - C6DRAM power gating feature This policy indicates whether or not BIOS should allocate PRMRR memory for C6DRAM power gating feature.
- UINT8 [OcSupport](#)
*Offset 0x020C - Over clocking support Over clocking support; **0: Disable**; 1: Enable \$EN_DIS.*
- UINT8 [OcLock](#)

- Offset 0x020D - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.
 - UINT8 [CoreMaxOcRatio](#)

Offset 0x020E - 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 0x020F - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.
 - UINT8 [RingMaxOcRatio](#)

Offset 0x0210 - 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 0x0211 - Hyper Threading Enable/Disable Enable or Disable Hyper Threading; 0: Disable; **1: Enable** \$EN_↔DIS.
 - UINT8 [CpuRatioOverride](#)

Offset 0x0212 - Enable or Disable CPU Ratio Override Enable or Disable CPU Ratio Override; **0: Disable**; 1: Enable.
 - UINT8 [CpuRatio](#)

Offset 0x0213 - CPU ratio value CPU ratio value.
 - UINT8 [BootFrequency](#)

Offset 0x0214 - Boot frequency Sets the boot frequency starting from reset vector.
 - UINT8 [ActiveCoreCount](#)

Offset 0x0215 - Number of active cores Number of active cores(Depends on Number of cores).
 - UINT8 [FClkFrequency](#)

Offset 0x0216 - Processor Early Power On Configuration FCLK setting **0: 800 MHz (ULT/ULX)**.
 - UINT8 [JtagC10PowerGateDisable](#)

Offset 0x0217 - Set JTAG power in C10 and deeper power states False: JTAG is power gated in C10 state.
 - UINT8 [VmxEnable](#)

Offset 0x0218 - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.
 - UINT8 [Avx2RatioOffset](#)

Offset 0x0219 - AVX2 Ratio Offset 0(Default)= No Offset.
 - UINT8 [Avx3RatioOffset](#)

Offset 0x021A - AVX3 Ratio Offset 0(Default)= No Offset.
 - UINT8 [BclkAdaptiveVoltage](#)

Offset 0x021B - BCLK Adaptive Voltage Enable When enabled, the CPU V/F curves are aware of BCLK frequency when calculated.
 - UINT16 [CoreVoltageOverride](#)

Offset 0x021C - core voltage override The core voltage override which is applied to the entire range of cpu core frequencies.
 - UINT16 [CoreVoltageAdaptive](#)

Offset 0x021E - Core Turbo voltage Adaptive Extra Turbo voltage applied to the cpu core when the cpu is operating in turbo mode.
 - UINT16 [CoreVoltageOffset](#)

Offset 0x0220 - Core Turbo voltage Offset The voltage offset applied to the core while operating in turbo mode. Valid Range 0 to 1000.
 - UINT8 [CorePllVoltageOffset](#)

Offset 0x0222 - Core PLL voltage offset Core PLL voltage offset.
 - UINT8 [RingDownBin](#)

Offset 0x0223 - Ring Downbin Ring Downbin enable/disable.
 - UINT8 [RingVoltageMode](#)

Offset 0x0224 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.
 - UINT8 [TjMaxOffset](#)

Offset 0x0225 - 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.
 - UINT16 [RingVoltageOverride](#)
-

- Offset 0x0226 - Ring voltage override The ring voltage override which is applied to the entire range of cpu ring frequencies.
- UINT16 [RingVoltageAdaptive](#)
Offset 0x0228 - Ring Turbo voltage Adaptive Extra Turbo voltage applied to the cpu ring when the cpu is operating in turbo mode.
 - UINT16 [RingVoltageOffset](#)
Offset 0x022A - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.
 - UINT8 [TmeEnable](#)
Offset 0x022C - Enable or Disable TME Enable or Disable TME; **0: Disable**; 1: Enable.
 - UINT8 [UnusedUpdSpace6](#) [3]
Offset 0x022D.
 - UINT32 [ElixirSpringsPatchAddr](#)
Offset 0x0230 - ElixirSpringsPatchAddr Address of Elixir Springs Patches.
 - UINT32 [ElixirSpringsPatchSize](#)
Offset 0x0234 - ElixirSpringsPatchSize Size of Elixir Springs Patches.
 - UINT8 [BiosGuard](#)
Offset 0x0238 - BiosGuard Enable/Disable.
 - UINT8 [BiosGuardToolsInterface](#)
Offset 0x0239.
 - UINT8 [EnableSgx](#)
Offset 0x023A - EnableSgx Enable/Disable.
 - UINT8 [Txt](#)
Offset 0x023B - Txt Enable/Disable.
 - UINT32 [PrmrrSize](#)
Offset 0x023C - PrmrrSize Enable/Disable.
 - UINT32 [SinitMemorySize](#)
Offset 0x0240 - SinitMemorySize Enable/Disable.
 - UINT8 [UnusedUpdSpace7](#) [4]
Offset 0x0244.
 - UINT64 [TxtDprMemoryBase](#)
Offset 0x0248 - TxtDprMemoryBase Enable/Disable.
 - UINT32 [TxtHeapMemorySize](#)
Offset 0x0250 - TxtHeapMemorySize Enable/Disable.
 - UINT32 [TxtDprMemorySize](#)
Offset 0x0254 - TxtDprMemorySize Enable/Disable.
 - UINT32 [BiosAcmBase](#)
Offset 0x0258 - BiosAcmBase Enable/Disable.
 - UINT32 [BiosAcmSize](#)
Offset 0x025C - BiosAcmSize Enable/Disable.
 - UINT32 [ApStartupBase](#)
Offset 0x0260 - ApStartupBase Enable/Disable.
 - UINT32 [TgaSize](#)
Offset 0x0264 - TgaSize Enable/Disable.
 - UINT64 [TxtLcpPdBase](#)
Offset 0x0268 - TxtLcpPdBase Enable/Disable.
 - UINT64 [TxtLcpPdSize](#)
Offset 0x0270 - TxtLcpPdSize Enable/Disable.
 - UINT8 [IsTPMPresence](#)
Offset 0x0278 - IsTPMPresence IsTPMPresence default values.
 - UINT8 [ReservedSecurityPreMem](#) [6]
Offset 0x0279 - ReservedSecurityPreMem Reserved for Security Pre-Mem \$EN_DIS.
-

- UINT8 [PchPcieHsioRxSetCtleEnable](#) [24]
Offset 0x027F - Enable PCH HSIO PCIE Rx Set Ctle Enable PCH PCIe Gen 3 Set CTLE Value.
 - UINT8 [PchPcieHsioRxSetCtle](#) [24]
Offset 0x0297 - PCH HSIO PCIE Rx Set Ctle Value PCH PCIe Gen 3 Set CTLE Value.
 - UINT8 [PchPcieHsioTxGen1DownscaleAmpEnable](#) [24]
Offset 0x02AF - Enable PCH HSIO PCIE TX Gen 1 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen1DownscaleAmp](#) [24]
Offset 0x02C7 - 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 0x02DF - Enable PCH HSIO PCIE TX Gen 2 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen2DownscaleAmp](#) [24]
Offset 0x02F7 - 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 0x030F - Enable PCH HSIO PCIE TX Gen 3 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen3DownscaleAmp](#) [24]
Offset 0x0327 - 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 0x033F - Enable PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen1DeEmph](#) [24]
Offset 0x0357 - 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 0x036F - Enable PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen2DeEmph3p5](#) [24]
Offset 0x0387 - 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 0x039F - Enable PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchPcieHsioTxGen2DeEmph6p0](#) [24]
Offset 0x03B7 - 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 0x03CF - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↔ : Disable; 1: Enable.
 - UINT8 [PchSataHsioRxGen1EqBoostMag](#) [8]
Offset 0x03D7 - 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 0x03DF - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↔ : Disable; 1: Enable.
 - UINT8 [PchSataHsioRxGen2EqBoostMag](#) [8]
Offset 0x03E7 - 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 0x03EF - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0: Disable; 1: Enable.
- UINT8 [PchSataHsioRxGen3EqBoostMag](#) [8]

Offset 0x03F7 - 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 0x03FF - Enable PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen1DownscaleAmp](#) [8]

Offset 0x0407 - 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 0x040F - Enable PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen2DownscaleAmp](#) [8]

Offset 0x0417 - 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 0x041F - Enable PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen3DownscaleAmp](#) [8]

Offset 0x0427 - 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 0x042F - Enable PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen1DeEmph](#) [8]

Offset 0x0437 - 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 0x043F - Enable PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen2DeEmph](#) [8]

Offset 0x0447 - 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 0x044F - Enable PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.
 - UINT8 [PchSataHsioTxGen3DeEmph](#) [8]

Offset 0x0457 - 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 0x045F - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.
 - UINT8 [PchPort80Route](#)

Offset 0x0460 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.
 - UINT8 [SmbusArpEnable](#)

Offset 0x0461 - Enable SMBus ARP support Enable SMBus ARP support.
 - UINT8 [PchNumRsvdSmbusAddresses](#)

Offset 0x0462 - Number of RsvdSmbusAddressTable.
 - UINT8 [UnusedUpdSpace8](#)

Offset 0x0463.
 - UINT16 [PchSmbusIoBase](#)

Offset 0x0464 - SMBUS Base Address SMBUS Base Address (IO space).
 - UINT16 [PciImrSize](#)
-

- Offset 0x0466 - Size of PCIe IMR.*

 - UINT8 [PcieImrEnabled](#)
 - Offset 0x0468 - Enable PCIe IMR 0:Disable, 1:Enable \$EN_DIS.*
 - UINT8 [PchSmbAlertEnable](#)
 - Offset 0x0469 - Enable SMBus Alert Pin Enable SMBus Alert Pin.*
 - UINT8 [ImrRpSelection](#)
 - Offset 0x046A - Root port number for IMR.*
 - UINT8 [UnusedUpdSpace9](#)
 - Offset 0x046B.*
 - UINT32 [RsvdSmbusAddressTablePtr](#)
 - Offset 0x046C - Point of RsvdSmbusAddressTable Array of addresses reserved for non-ARP-capable SMBus devices.*
 - UINT32 [PcieRpEnableMask](#)
 - Offset 0x0470 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.*
 - UINT8 [PcdDebugInterfaceFlags](#)
 - Offset 0x0474 - Debug Interfaces Debug Interfaces.*
 - UINT8 [PcdSerialIoUartNumber](#)
 - Offset 0x0475 - PcdSerialIoUartNumber Select SerialIoUart Controller for debug.*
 - UINT8 [PcdIsaSerialUartBase](#)
 - Offset 0x0476 - ISA Serial Base selection Select ISA Serial Base address.*
 - UINT8 [GtPllVoltageOffset](#)
 - Offset 0x0477 - GT PLL voltage offset Core PLL voltage offset.*
 - UINT8 [RingPllVoltageOffset](#)
 - Offset 0x0478 - Ring PLL voltage offset Core PLL voltage offset.*
 - UINT8 [SaPllVoltageOffset](#)
 - Offset 0x0479 - System Agent PLL voltage offset Core PLL voltage offset.*
 - UINT8 [McPllVoltageOffset](#)
 - Offset 0x047A - Memory Controller PLL voltage offset Core PLL voltage offset.*
 - UINT8 [MrcSafeConfig](#)
 - Offset 0x047B - MRC Safe Config Enables/Disable MRC Safe Config \$EN_DIS.*
 - UINT8 [TcssltbtPcie0En](#)
 - Offset 0x047C - TCSS Thunderbolt PCIe Root Port 0 Enable Set TCSS Thunderbolt PCIe Root Port 0.*
 - UINT8 [TcssltbtPcie1En](#)
 - Offset 0x047D - TCSS Thunderbolt PCIe Root Port 1 Enable Set TCSS Thunderbolt PCIe Root Port 1.*
 - UINT8 [TcssltbtPcie2En](#)
 - Offset 0x047E - TCSS Thunderbolt PCIe Root Port 2 Enable Set TCSS Thunderbolt PCIe Root Port 2.*
 - UINT8 [TcssltbtPcie3En](#)
 - Offset 0x047F - TCSS Thunderbolt PCIe Root Port 3 Enable Set TCSS Thunderbolt PCIe Root Port 3.*
 - UINT8 [TcssltbtPcie4En](#)
 - Offset 0x0480 - TCSS Thunderbolt PCIe Root Port 4 Enable Set TCSS Thunderbolt PCIe Root Port 4.*
 - UINT8 [TcssltbtPcie5En](#)
 - Offset 0x0481 - TCSS Thunderbolt PCIe Root Port 5 Enable Set TCSS Thunderbolt PCIe Root Port 5.*
 - UINT8 [TcssXhciEn](#)
 - Offset 0x0482 - TCSS USB HOST (xHCI) Enable Set TCSS XHCI.*
 - UINT8 [TcssXdcIEn](#)
 - Offset 0x0483 - TCSS USB DEVICE (xDCI) Enable Set TCSS XDCI.*
 - UINT8 [TcssDma0En](#)
 - Offset 0x0484 - TCSS DMA0 Enable Set TCSS DMA0.*
 - UINT8 [TcssDma1En](#)
 - Offset 0x0485 - TCSS DMA1 Enable Set TCSS DMA1.*
 - UINT8 [TcssDma2En](#)
 - Offset 0x0486 - TCSS DMA2 Enable Set TCSS DMA2.*
-

- UINT8 [PcdSerialDebugBaudRate](#)
Offset 0x0487 - PcdSerialDebugBaudRate Baud Rate for Serial Debug Messages.
 - UINT8 [HobBufferSize](#)
Offset 0x0488 - HobBufferSize Size to set HOB Buffer.
 - UINT8 [ECT](#)
Offset 0x0489 - Early Command Training Enables/Disable Early Command Training \$EN_DIS.
 - UINT8 [SOT](#)
Offset 0x048A - SenseAmp Offset Training Enables/Disable SenseAmp Offset Training \$EN_DIS.
 - UINT8 [ERDMPRTC2D](#)
Offset 0x048B - Early ReadMPR Timing Centering 2D Enables/Disable Early ReadMPR Timing Centering 2D \$EN_←_DIS.
 - UINT8 [RDMPRT](#)
Offset 0x048C - Read MPR Training Enables/Disable Read MPR Training \$EN_DIS.
 - UINT8 [RCVET](#)
Offset 0x048D - Receive Enable Training Enables/Disable Receive Enable Training \$EN_DIS.
 - UINT8 [JWRL](#)
Offset 0x048E - Jedec Write Leveling Enables/Disable Jedec Write Leveling \$EN_DIS.
 - UINT8 [EWRTC2D](#)
Offset 0x048F - Early Write Time Centering 2D Enables/Disable Early Write Time Centering 2D \$EN_DIS.
 - UINT8 [ERDTC2D](#)
Offset 0x0490 - Early Read Time Centering 2D Enables/Disable Early Read Time Centering 2D \$EN_DIS.
 - UINT8 [WRTC1D](#)
Offset 0x0491 - Write Timing Centering 1D Enables/Disable Write Timing Centering 1D \$EN_DIS.
 - UINT8 [WRVC1D](#)
Offset 0x0492 - Write Voltage Centering 1D Enables/Disable Write Voltage Centering 1D \$EN_DIS.
 - UINT8 [RDTC1D](#)
Offset 0x0493 - Read Timing Centering 1D Enables/Disable Read Timing Centering 1D \$EN_DIS.
 - UINT8 [DIMMODTT](#)
Offset 0x0494 - Dimm ODT Training Enables/Disable Dimm ODT Training \$EN_DIS.
 - UINT8 [DIMMFRONT](#)
Offset 0x0495 - DIMM RON Training Enables/Disable DIMM RON Training \$EN_DIS.
 - UINT8 [WRDSEQT](#)
Offset 0x0496 - Write Drive Strength/Equalization 2D Enables/Disable Write Drive Strength/Equalization 2D \$EN_←_DIS.
 - UINT8 [WRSRT](#)
Offset 0x0497 - Write Slew Rate Training Enables/Disable Write Slew Rate Training \$EN_DIS.
 - UINT8 [RDODTT](#)
Offset 0x0498 - Read ODT Training Enables/Disable Read ODT Training \$EN_DIS.
 - UINT8 [RDEQT](#)
Offset 0x0499 - Read Equalization Training Enables/Disable Read Equalization Training \$EN_DIS.
 - UINT8 [RDAPT](#)
Offset 0x049A - Read Amplifier Training Enables/Disable Read Amplifier Training \$EN_DIS.
 - UINT8 [WRTC2D](#)
Offset 0x049B - Write Timing Centering 2D Enables/Disable Write Timing Centering 2D \$EN_DIS.
 - UINT8 [RDTC2D](#)
Offset 0x049C - Read Timing Centering 2D Enables/Disable Read Timing Centering 2D \$EN_DIS.
 - UINT8 [WRVC2D](#)
Offset 0x049D - Write Voltage Centering 2D Enables/Disable Write Voltage Centering 2D \$EN_DIS.
 - UINT8 [RDVC2D](#)
Offset 0x049E - Read Voltage Centering 2D Enables/Disable Read Voltage Centering 2D \$EN_DIS.
 - UINT8 [CMDVC](#)
-

- Offset 0x049F - Command Voltage Centering Enables/Disable Command Voltage Centering \$EN_DIS.*

 - UINT8 [LCT](#)
 - Offset 0x04A0 - Late Command Training Enables/Disable Late Command Training \$EN_DIS.*

 - UINT8 [RTL](#)
 - Offset 0x04A1 - Round Trip Latency Training Enables/Disable Round Trip Latency Training \$EN_DIS.*

 - UINT8 [TAT](#)
 - Offset 0x04A2 - Turn Around Timing Training Enables/Disable Turn Around Timing Training \$EN_DIS.*

 - UINT8 [MEMTST](#)
 - Offset 0x04A3 - Memory Test Enables/Disable Memory Test \$EN_DIS.*

 - UINT8 [ALIASCHK](#)
 - Offset 0x04A4 - DIMM SPD Alias Test Enables/Disable DIMM SPD Alias Test \$EN_DIS.*

 - UINT8 [RCVENC1D](#)
 - Offset 0x04A5 - Receive Enable Centering 1D Enables/Disable Receive Enable Centering 1D \$EN_DIS.*

 - UINT8 [RMC](#)
 - Offset 0x04A6 - Retrain Margin Check Enables/Disable Retrain Margin Check \$EN_DIS.*

 - UINT8 [WRDSUDT](#)
 - Offset 0x04A7 - Write Drive Strength Up/Dn independently Enables/Disable Write Drive Strength Up/Dn independently \$EN_DIS.*

 - UINT8 [EccSupport](#)
 - Offset 0x04A8 - ECC Support Enables/Disable ECC Support \$EN_DIS.*

 - UINT8 [RemapEnable](#)
 - Offset 0x04A9 - Memory Remap Enables/Disable Memory Remap \$EN_DIS.*

 - UINT8 [RankInterleave](#)
 - Offset 0x04AA - Rank Interleave support Enables/Disable Rank Interleave support.*

 - UINT8 [EnhancedInterleave](#)
 - Offset 0x04AB - Enhanced Interleave support Enables/Disable Enhanced Interleave support \$EN_DIS.*

 - UINT8 [ChHashEnable](#)
 - Offset 0x04AC - Ch Hash Support Enable/Disable Channel Hash Support.*

 - UINT8 [EnableExtts](#)
 - Offset 0x04AD - Extern Therm Status Enables/Disable Extern Therm Status \$EN_DIS.*

 - UINT8 [EnableCltm](#)
 - Offset 0x04AE - Closed Loop Therm Manage Enables/Disable Closed Loop Therm Manage \$EN_DIS.*

 - UINT8 [EnableOltn](#)
 - Offset 0x04AF - Open Loop Therm Manage Enables/Disable Open Loop Therm Manage \$EN_DIS.*

 - UINT8 [EnablePwrDn](#)
 - Offset 0x04B0 - DDR PowerDown and idle counter Enables/Disable DDR PowerDown and idle counter(For LPDDR Only) \$EN_DIS.*

 - UINT8 [EnablePwrDnLpddr](#)
 - Offset 0x04B1 - DDR PowerDown and idle counter Enables/Disable DDR PowerDown and idle counter(For LPDDR Only) \$EN_DIS.*

 - UINT8 [UserPowerWeightsEn](#)
 - Offset 0x04B2 - Use user provided power weights, scale factor, and channel power floor values Enables/Disable Use user provided power weights, scale factor, and channel power floor values \$EN_DIS.*

 - UINT8 [RapLim2Lock](#)
 - Offset 0x04B3 - RAPL PL Lock Enables/Disable RAPL PL Lock \$EN_DIS.*

 - UINT8 [RapLim2Ena](#)
 - Offset 0x04B4 - RAPL PL 2 enable Enables/Disable RAPL PL 2 enable \$EN_DIS.*

 - UINT8 [RapLim1Ena](#)
 - Offset 0x04B5 - RAPL PL 1 enable Enables/Disable RAPL PL 1 enable \$EN_DIS.*

 - UINT8 [SrefCfgEna](#)
 - Offset 0x04B6 - SelfRefresh Enable Enables/Disable SelfRefresh Enable \$EN_DIS.*
-

- UINT8 [ThrtCkeMinDefeatLpddr](#)
Offset 0x04B7 - Throttler CKEMin Defeature Enables/Disable Throttler CKEMin Defeature(For LPDDR Only) \$EN←_DIS.
 - UINT8 [ThrtCkeMinDefeat](#)
Offset 0x04B8 - Throttler CKEMin Defeature Enables/Disable Throttler CKEMin Defeature \$EN_DIS.
 - UINT8 [RhPrevention](#)
Offset 0x04B9 - Enable RH Prevention Enables/Disable RH Prevention \$EN_DIS.
 - UINT8 [ExitOnFailure](#)
Offset 0x04BA - Exit On Failure (MRC) Enables/Disable Exit On Failure (MRC) \$EN_DIS.
 - UINT8 [DdrThermalSensor](#)
Offset 0x04BB - LPDDR Thermal Sensor Enables/Disable LPDDR Thermal Sensor \$EN_DIS.
 - UINT8 [EvLoader](#)
Offset 0x04BC - EV Loader Enable/Disable EV Loader Functionality \$EN_DIS.
 - UINT8 [EvLoaderDelay](#)
Offset 0x04BD - EV Loader Delay Enable/Disable EV Loader 2 Second Delay \$EN_DIS.
 - UINT8 [Ddr4DdpSharedClock](#)
Offset 0x04BE - Select if CLK0 is shared between Rank0 and Rank1 in DDR4 DDP Select if CLK0 is shared between Rank0 and Rank1 in DDR4 DDP \$EN_DIS.
 - UINT8 [Ddr4DdpSharedZq](#)
Offset 0x04BF - Select if ZQ pin is shared between Rank0 and Rank1 in DDR4 DDP ESelect if ZQ pin is shared between Rank0 and Rank1 in DDR4 DDP \$EN_DIS.
 - UINT8 [ChHashInterleaveBit](#)
Offset 0x04C0 - Ch Hash Interleaved Bit Select the BIT to be used for Channel Interleaved mode.
 - UINT8 [UnusedUpdSpace10](#)
Offset 0x04C1.
 - UINT16 [ChHashMask](#)
Offset 0x04C2 - Ch Hash Mask Set the BIT(s) to be included in the XOR function.
 - UINT32 [BClkFrequency](#)
Offset 0x04C4 - Base reference clock value Base reference clock value, in Hertz(Default is 125Hz) 100000000:100Hz, 125000000:125Hz, 167000000:167Hz, 250000000:250Hz.
 - UINT8 [EnergyScaleFact](#)
Offset 0x04C8 - Energy Scale Factor Energy Scale Factor, Default is 4.
 - UINT8 [CMDSR](#)
Offset 0x04C9 - CMD Slew Rate Training Enable/Disable CMD Slew Rate Training \$EN_DIS.
 - UINT16 [Idd3n](#)
Offset 0x04CA - EPG DIMM Idd3N Active standby current (Idd3N) in milliamps from datasheet.
 - UINT16 [Idd3p](#)
Offset 0x04CC - EPG DIMM Idd3P Active power-down current (Idd3P) in milliamps from datasheet.
 - UINT8 [CMDNSEQ](#)
Offset 0x04CE - CMD Drive Strength and Tx Equalization Enable/Disable CMD Drive Strength and Tx Equalization \$EN_DIS.
 - UINT8 [CMDNORM](#)
Offset 0x04CF - CMD Normalization Enable/Disable CMD Normalization \$EN_DIS.
 - UINT8 [EWRDSEQ](#)
Offset 0x04D0 - Early DQ Write Drive Strength and Equalization Training Enable/Disable Early DQ Write Drive Strength and Equalization Training \$EN_DIS.
 - UINT8 [RhActProbability](#)
Offset 0x04D1 - RH Activation Probability RH Activation Probability, Probability value is $1/2^{\wedge}$ (inputvalue)
 - UINT8 [RapLim2WindX](#)
Offset 0x04D2 - RAPL PL 2 WindowX Power PL 2 time window X value, $(1/1024)(1+(x/4))*(2^{\wedge}y)$ (0=Def)*
 - UINT8 [RapLim2WindY](#)
Offset 0x04D3 - RAPL PL 2 WindowY Power PL 2 time window Y value, $(1/1024)(1+(x/4))*(2^{\wedge}y)$ (0=Def)*
-

- UINT8 [RaplLim1WindX](#)
*Offset 0x04D4 - RAPL PL 1 WindowX Power PL 1 time window X value, $(1/1024) * (1+(x/4)) * (2^y)$ (0=Def)*
 - UINT8 [RaplLim1WindY](#)
*Offset 0x04D5 - RAPL PL 1 WindowY Power PL 1 time window Y value, $(1/1024) * (1+(x/4)) * (2^y)$ (0=Def)*
 - UINT16 [RaplLim2Pwr](#)
Offset 0x04D6 - RAPL PL 2 Power range[0;2¹⁴-1]= [2047.875;0]in W, (224= Def)
 - UINT16 [RaplLim1Pwr](#)
Offset 0x04D8 - RAPL PL 1 Power range[0;2¹⁴-1]= [2047.875;0]in W, (224= Def)
 - UINT8 [WarmThresholdCh0Dimm0](#)
Offset 0x04DA - Warm Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmThresholdCh0Dimm1](#)
Offset 0x04DB - Warm Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmThresholdCh1Dimm0](#)
Offset 0x04DC - Warm Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmThresholdCh1Dimm1](#)
Offset 0x04DD - Warm Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotThresholdCh0Dimm0](#)
Offset 0x04DE - Hot Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotThresholdCh0Dimm1](#)
Offset 0x04DF - Hot Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotThresholdCh1Dimm0](#)
Offset 0x04E0 - Hot Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotThresholdCh1Dimm1](#)
Offset 0x04E1 - Hot Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmBudgetCh0Dimm0](#)
Offset 0x04E2 - Warm Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmBudgetCh0Dimm1](#)
Offset 0x04E3 - Warm Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmBudgetCh1Dimm0](#)
Offset 0x04E4 - Warm Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [WarmBudgetCh1Dimm1](#)
Offset 0x04E5 - Warm Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotBudgetCh0Dimm0](#)
Offset 0x04E6 - Hot Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotBudgetCh0Dimm1](#)
Offset 0x04E7 - Hot Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotBudgetCh1Dimm0](#)
Offset 0x04E8 - Hot Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [HotBudgetCh1Dimm1](#)
Offset 0x04E9 - Hot Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.
 - UINT8 [IdleEnergyCh0Dimm0](#)
Offset 0x04EA - Idle Energy Ch0Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
 - UINT8 [IdleEnergyCh0Dimm1](#)
Offset 0x04EB - Idle Energy Ch0Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
 - UINT8 [IdleEnergyCh1Dimm0](#)
Offset 0x04EC - Idle Energy Ch1Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
 - UINT8 [IdleEnergyCh1Dimm1](#)
Offset 0x04ED - Idle Energy Ch1Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)
 - UINT8 [PdEnergyCh0Dimm0](#)
Offset 0x04EE - PowerDown Energy Ch0Dimm0 Power-Down Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
-

- UINT8 [PdEnergyCh0Dimm1](#)
Offset 0x04EF - PowerDown Energy Ch0Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
 - UINT8 [PdEnergyCh1Dimm0](#)
Offset 0x04F0 - PowerDown Energy Ch1Dimm0 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
 - UINT8 [PdEnergyCh1Dimm1](#)
Offset 0x04F1 - PowerDown Energy Ch1Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)
 - UINT8 [ActEnergyCh0Dimm0](#)
Offset 0x04F2 - Activate Energy Ch0Dimm0 Activate Energy Contribution, range[255;0],(172= Def)
 - UINT8 [ActEnergyCh0Dimm1](#)
Offset 0x04F3 - Activate Energy Ch0Dimm1 Activate Energy Contribution, range[255;0],(172= Def)
 - UINT8 [ActEnergyCh1Dimm0](#)
Offset 0x04F4 - Activate Energy Ch1Dimm0 Activate Energy Contribution, range[255;0],(172= Def)
 - UINT8 [ActEnergyCh1Dimm1](#)
Offset 0x04F5 - Activate Energy Ch1Dimm1 Activate Energy Contribution, range[255;0],(172= Def)
 - UINT8 [RdEnergyCh0Dimm0](#)
Offset 0x04F6 - Read Energy Ch0Dimm0 Read Energy Contribution, range[255;0],(212= Def)
 - UINT8 [RdEnergyCh0Dimm1](#)
Offset 0x04F7 - Read Energy Ch0Dimm1 Read Energy Contribution, range[255;0],(212= Def)
 - UINT8 [RdEnergyCh1Dimm0](#)
Offset 0x04F8 - Read Energy Ch1Dimm0 Read Energy Contribution, range[255;0],(212= Def)
 - UINT8 [RdEnergyCh1Dimm1](#)
Offset 0x04F9 - Read Energy Ch1Dimm1 Read Energy Contribution, range[255;0],(212= Def)
 - UINT8 [WrEnergyCh0Dimm0](#)
Offset 0x04FA - Write Energy Ch0Dimm0 Write Energy Contribution, range[255;0],(221= Def)
 - UINT8 [WrEnergyCh0Dimm1](#)
Offset 0x04FB - Write Energy Ch0Dimm1 Write Energy Contribution, range[255;0],(221= Def)
 - UINT8 [WrEnergyCh1Dimm0](#)
Offset 0x04FC - Write Energy Ch1Dimm0 Write Energy Contribution, range[255;0],(221= Def)
 - UINT8 [WrEnergyCh1Dimm1](#)
Offset 0x04FD - Write Energy Ch1Dimm1 Write Energy Contribution, range[255;0],(221= Def)
 - UINT8 [ThrtCkeMinTmr](#)
Offset 0x04FE - Throttler CKEMin Timer Timer value for CKEMin, range[255;0].
 - UINT8 [CkeRankMapping](#)
Offset 0x04FF - Cke Rank Mapping Bits [7:4] - Channel 1, bits [3:0] - Channel 0.
 - UINT8 [RaplPwrFICh0](#)
Offset 0x0500 - Rapl Power Floor Ch0 Power budget ,range[255;0],(0= 5.3W Def)
 - UINT8 [RaplPwrFICh1](#)
Offset 0x0501 - Rapl Power Floor Ch1 Power budget ,range[255;0],(0= 5.3W Def)
 - UINT8 [EnCmdRate](#)
Offset 0x0502 - Command Rate Support CMD Rate and Limit Support Option.
 - UINT8 [Refresh2X](#)
Offset 0x0503 - REFRESH_2X_MODE 0- (Default)Disabled 1-iMC enables 2xRef when Warm and Hot 2- iMC enables 2xRef when Hot 0:Disable, 1:Enabled for WARM or HOT, 2:Enabled HOT only.
 - UINT8 [EpgEnable](#)
Offset 0x0504 - Energy Performance Gain Enable/disable(default) Energy Performance Gain.
 - UINT8 [RhSolution](#)
Offset 0x0505 - Row Hammer Solution Type of method used to prevent Row Hammer.
 - UINT8 [UserThresholdEnable](#)
-

- Offset 0x0506 - User Manual Threshold Disabled: Predefined threshold will be used.*
 - UINT8 [UserBudgetEnable](#)
 - Offset 0x0507 - User Manual Budget Disabled: Configuration of memories will defined the Budget value.*
 - UINT8 [TsodTcritMax](#)
 - Offset 0x0508 - TcritMax Maximum Critical Temperature in Centigrade of the On-DIMM Thermal Sensor.*
 - UINT8 [TsodEventMode](#)
 - Offset 0x0509 - Event mode Disable:Comparator mode.*
 - UINT8 [TsodEventPolarity](#)
 - Offset 0x050A - EVENT polarity Disable:Active LOW.*
 - UINT8 [TsodCriticalEventOnly](#)
 - Offset 0x050B - Critical event only Disable:Trips on alarm or critical.*
 - UINT8 [TsodEventOutputControl](#)
 - Offset 0x050C - Event output control Disable:Event output disable.*
 - UINT8 [TsodAlarmwindowLockBit](#)
 - Offset 0x050D - Alarm window lock bit Disable:Alarm trips are not locked and can be changed.*
 - UINT8 [TsodCriticaltripLockBit](#)
 - Offset 0x050E - Critical trip lock bit Disable:Critical trip is not locked and can be changed.*
 - UINT8 [TsodShutdownMode](#)
 - Offset 0x050F - Shutdown mode Disable:Temperature sensor enable.*
 - UINT8 [TsodThigMax](#)
 - Offset 0x0510 - ThighMax Thigh = ThighMax (Default is 93)*
 - UINT8 [TsodManualEnable](#)
 - Offset 0x0511 - User Manual Thig and Tcrit Disabled(Default): Temperature will be given by the configuration of memories and 1x or 2xrefresh rate.*
 - UINT8 [ForceOltmOrRefresh2x](#)
 - Offset 0x0512 - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.*
 - UINT8 [PwrdwnIdleCounter](#)
 - Offset 0x0513 - Pwr Down Idle Timer The minimum value should = to the worst case Roundtrip delay + Burst_Length.*
 - UINT8 [CmdRanksTerminated](#)
 - Offset 0x0514 - Bitmask of ranks that have CA bus terminated Offset 225 LPDDR4: Bitmask of ranks that have CA bus terminated.*
 - UINT8 [PcdSerialDebugLevel](#)
 - Offset 0x0515 - PcdSerialDebugLevel Serial Debug Message Level.*
 - UINT8 [FivrFaults](#)
 - Offset 0x0516 - Fivr Faults Fivr Faults; 0: Disabled; 1: **Enabled**.*
 - UINT8 [FivrEfficiency](#)
 - Offset 0x0517 - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; 1: **Enabled**.*
 - UINT8 [SafeMode](#)
 - Offset 0x0518 - Safe Mode Support This option configures the varous items in the IO and MC to be more conservative.*
 - UINT8 [CleanMemory](#)
 - Offset 0x0519 - Ask MRC to clear memory content Ask MRC to clear memory content 0: **Do not Clear Memory**; 1: Clear Memory.*
 - UINT8 [LpDdrDqDqsReTraining](#)
 - Offset 0x051A - LpDdrDqDqsReTraining Enables/Disable LpDdrDqDqsReTraining \$EN_DIS.*
 - UINT8 [UsbTcPortEnPreMem](#)
 - Offset 0x051B - TCSS USB Port Enable Bitmap for per port enabling.*
 - UINT16 [PostCodeOutputPort](#)
 - Offset 0x051C - Post Code Output Port This option configures Post Code Output Port.*
 - UINT8 [RMTLoopCount](#)
 - Offset 0x051E - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.*
 - UINT8 [CridEnable](#)
-

- *Offset 0x051F - TCSS Compatible Revision ID Enable Set TCSS Crid .*
- UIN32 [BclkRfiFreq](#) [4]
 - *Offset 0x0520 - BCLK RFI Frequency Bclk RFI Frequency for each SAGV point in Hz units.*
- UIN8 [UnusedUpdSpace11](#) [1]
 - *Offset 0x0530.*
- UIN8 [ReservedFspmUpd](#) [15]
 - *Offset 0x0531.*

10.8.1 Detailed Description

Fsp M Configuration.

Definition at line 56 of file FspmUpd.h.

10.8.2 Member Data Documentation

10.8.2.1 ActiveCoreCount

UIN8 FSP_M_CONFIG::ActiveCoreCount

Offset 0x0215 - 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 894 of file FspmUpd.h.

10.8.2.2 ApertureSize

UIN8 FSP_M_CONFIG::ApertureSize

Offset 0x00BC - Aperture Size Select the Aperture Size.

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

Definition at line 284 of file FspmUpd.h.

10.8.2.3 ApStartupBase

UIN32 FSP_M_CONFIG::ApStartupBase

Offset 0x0260 - ApStartupBase Enable/Disable.

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

Definition at line 1077 of file FspmUpd.h.

10.8.2.4 Avx2RatioOffset

UIN8 FSP_M_CONFIG::Avx2RatioOffset

Offset 0x0219 - 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 920 of file FspmUpd.h.

10.8.2.5 Avx3RatioOffset

UINT8 FSP_M_CONFIG::Avx3RatioOffset

Offset 0x021A - 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 926 of file FspmUpd.h.

10.8.2.6 BclkAdaptiveVoltage

UINT8 FSP_M_CONFIG::BclkAdaptiveVoltage

Offset 0x021B - 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 933 of file FspmUpd.h.

10.8.2.7 BclkRfiFreq

UINT32 FSP_M_CONFIG::BclkRfiFreq[4]

Offset 0x0520 - BCLK RFI Frequency Bclk RFI Frequency for each SAGV point in Hz units.

98000000Hz = 98MHz **0 - No RFI Tuning**. Range is 98Mhz-100Mhz.

Definition at line 2280 of file FspmUpd.h.

10.8.2.8 BiosAcmBase

UINT32 FSP_M_CONFIG::BiosAcmBase

Offset 0x0258 - BiosAcmBase Enable/Disable.

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

Definition at line 1067 of file FspmUpd.h.

10.8.2.9 BiosAcmSize

UINT32 FSP_M_CONFIG::BiosAcmSize

Offset 0x025C - BiosAcmSize Enable/Disable.

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

Definition at line 1072 of file FspmUpd.h.

10.8.2.10 BiosGuard

UINT8 FSP_M_CONFIG::BiosGuard

Offset 0x0238 - BiosGuard Enable/Disable.

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

Definition at line 1017 of file FspmUpd.h.

10.8.2.11 BistOnReset

UINT8 FSP_M_CONFIG::BistOnReset

Offset 0x0209 - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 818 of file FspmUpd.h.

10.8.2.12 BootFrequency

UINT8 FSP_M_CONFIG::BootFrequency

Offset 0x0214 - 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 887 of file FspmUpd.h.

10.8.2.13 ChHashEnable

UINT8 FSP_M_CONFIG::ChHashEnable

Offset 0x04AC - Ch Hash Support Enable/Disable Channel Hash Support.

NOTE: ONLY if Memory interleaved Mode \$EN_DIS

Definition at line 1672 of file FspmUpd.h.

10.8.2.14 ChHashInterleaveBit

UINT8 FSP_M_CONFIG::ChHashInterleaveBit

Offset 0x04C0 - Ch Hash Interleaved Bit Select the BIT to be used for Channel Interleaved mode.

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

Definition at line 1794 of file FspmUpd.h.

10.8.2.15 ChHashMask

UINT16 FSP_M_CONFIG::ChHashMask

Offset 0x04C2 - Ch Hash Mask Set the BIT(s) to be included in the XOR function.

NOTE BIT mask corresponds to BITS [19:6] Default is 0x30CC

Definition at line 1804 of file FspmUpd.h.

10.8.2.16 CkeRankMapping

UINT8 FSP_M_CONFIG::CkeRankMapping

Offset 0x04FF - Cke Rank Mapping Bits [7:4] - Channel 1, bits [3:0] - Channel 0.

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

Definition at line 2078 of file FspmUpd.h.

10.8.2.17 CleanMemory

UINT8 FSP_M_CONFIG::CleanMemory

Offset 0x0519 - 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 2247 of file FspmUpd.h.

10.8.2.18 CmdRanksTerminated

UINT8 FSP_M_CONFIG::CmdRanksTerminated

Offset 0x0514 - Bitmask of ranks that have CA bus terminated Offset 225 LPDDR4: Bitmask of ranks that have CA bus terminated.

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

Definition at line 2214 of file FspmUpd.h.

10.8.2.19 CoreMaxOcRatio

UINT8 FSP_M_CONFIG::CoreMaxOcRatio

Offset 0x020E - 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: 0-85

Definition at line 850 of file FspmUpd.h.

10.8.2.20 CorePllVoltageOffset

UINT8 FSP_M_CONFIG::CorePllVoltageOffset

Offset 0x0222 - Core PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 955 of file FspmUpd.h.

10.8.2.21 CoreVoltageAdaptive

UINT16 FSP_M_CONFIG::CoreVoltageAdaptive

Offset 0x021E - 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 945 of file FspmUpd.h.

10.8.2.22 CoreVoltageMode

UINT8 FSP_M_CONFIG::CoreVoltageMode

Offset 0x020F - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.

\$EN_DIS

Definition at line 856 of file FspmUpd.h.

10.8.2.23 CoreVoltageOverride

UINT16 FSP_M_CONFIG::CoreVoltageOverride

Offset 0x021C - 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 939 of file FspmUpd.h.

10.8.2.24 CpuRatio

UINT8 FSP_M_CONFIG::CpuRatio

Offset 0x0213 - CPU ratio value CPU ratio value.

Valid Range 0 to 63

Definition at line 879 of file FspmUpd.h.

10.8.2.25 CpuRatioOverride

UINT8 FSP_M_CONFIG::CpuRatioOverride

Offset 0x0212 - Enable or Disable CPU Ratio Override Enable or Disable CPU Ratio Override; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 874 of file FspmUpd.h.

10.8.2.26 CpuTraceHubMemReg0Size

UINT8 FSP_M_CONFIG::CpuTraceHubMemReg0Size

Offset 0x00FC - CPU Trace Hub Memory Region 0 CPU Trace Hub Memory Region 0, The available memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

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

Definition at line 533 of file FspmUpd.h.

10.8.2.27 CpuTraceHubMemReg1Size

UINT8 FSP_M_CONFIG::CpuTraceHubMemReg1Size

Offset 0x00FD - CPU Trace Hub Memory Region 1 CPU Trace Hub Memory Region 1.

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

Definition at line 540 of file FspmUpd.h.

10.8.2.28 CpuTraceHubMode

UINT8 FSP_M_CONFIG::CpuTraceHubMode

Offset 0x00FB - CPU Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

0: Disable, 1:Target Debugger Mode, 2:Host Debugger Mode

Definition at line 526 of file FspmUpd.h.

10.8.2.29 CridEnable

UINT8 FSP_M_CONFIG::CridEnable

Offset 0x051F - TCSS Compatible Revision ID Enable Set TCSS Crid .

0:Stepping Revision ID 1:Compatible Revision ID \$EN_DIS

Definition at line 2274 of file FspmUpd.h.

10.8.2.30 DciUsb3TypecUfpDbg

UINT8 FSP_M_CONFIG::DciUsb3TypecUfpDbg

Offset 0x00AF - USB3 Type-C UFP2DFP Kernel/Platform Debug Support This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting.

0:Disabled, 1:Enabled, 2:No Change

Definition at line 237 of file FspmUpd.h.

10.8.2.31 DdrFreqLimit

UINT16 FSP_M_CONFIG::DdrFreqLimit

Offset 0x00BE - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.

Options are 1067, 1333, 1600, 1867, 2133, 2400, 2667, 2933 and 0 for Auto. 1067:1067, 1333:1333, 1600:1600, 1867:1867, 2133:2133, 2400:2400, 2667:2667, 2933:2933, 0:Auto

Definition at line 298 of file FspmUpd.h.

10.8.2.32 DdrSpeedControl

UINT8 FSP_M_CONFIG::DdrSpeedControl

Offset 0x00C1 - DDR Speed Control DDR Frequency and Gear control for all SAGV points.

0:Auto, 1:Manual

Definition at line 311 of file FspmUpd.h.

10.8.2.33 DisableDimmChannel0

UINT8 FSP_M_CONFIG::DisableDimmChannel0

Offset 0x00C7 - Channel A DIMM Control Channel A DIMM Control Support - Enable or Disable Dimms on Channel A.

0:Enable both DIMMs, 1:Disable DIMM0, 2:Disable DIMM1, 3:Disable both DIMMs

Definition at line 337 of file FspmUpd.h.

10.8.2.34 DisableDimmChannel1

UINT8 FSP_M_CONFIG::DisableDimmChannel1

Offset 0x00C8 - Channel B DIMM Control Channel B DIMM Control Support - Enable or Disable Dimms on Channel B.

0:Enable both DIMMs, 1:Disable DIMM0, 2:Disable DIMM1, 3:Disable both DIMMs

Definition at line 343 of file FspmUpd.h.

10.8.2.35 DmiDeEmphasis

UINT8 FSP_M_CONFIG::DmiDeEmphasis

Offset 0x0138 - DeEmphasis control for DMI DeEmphasis control for DMI.

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

Definition at line 641 of file FspmUpd.h.

10.8.2.36 DmiGen3EndPointHint

UINT8 FSP_M_CONFIG::DmiGen3EndPointHint [8]

Offset 0x012C - 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 630 of file FspmUpd.h.

10.8.2.37 DmiGen3EndPointPreset

UINT8 FSP_M_CONFIG::DmiGen3EndPointPreset [8]

Offset 0x0124 - 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 625 of file FspmUpd.h.

10.8.2.38 DmiGen3ProgramStaticEq

UINT8 FSP_M_CONFIG::DmiGen3ProgramStaticEq

Offset 0x011A - 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 607 of file FspmUpd.h.

10.8.2.39 DmiGen3RootPortPreset

UINT8 FSP_M_CONFIG::DmiGen3RootPortPreset [8]

Offset 0x011C - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.

Range: 0-9, 8 is default for each lane

Definition at line 620 of file FspmUpd.h.

10.8.2.40 EnableC6Dram

UINT8 FSP_M_CONFIG::EnableC6Dram

Offset 0x020B - C6DRAM power gating feature This policy indicates whether or not BIOS should allocate PRMRR memory for C6DRAM power gating feature.

- 0: Don't allocate any PRMRR memory for C6DRAM power gating feature.- **1: Allocate PRMRR memory for C6DRAM power gating feature.** \$EN_DIS

Definition at line 832 of file FspmUpd.h.

10.8.2.41 EnableSgx

UINT8 FSP_M_CONFIG::EnableSgx

Offset 0x023A - EnableSgx Enable/Disable.

0: Disable, Enable/Disable SGX feature, 1: enable, 2: Software Control 0: Disable, 1: Enable, 2: Software Control

Definition at line 1027 of file FspmUpd.h.

10.8.2.42 EnCmdRate

UINT8 FSP_M_CONFIG::EnCmdRate

Offset 0x0502 - Command Rate Support CMD Rate and Limit Support Option.

NOTE: ONLY supported in 1N Mode, Default is 3 CMDs 0:Disable, 5:2 CMDS, 7:3 CMDS, 9:4 CMDS, 11:5 CMDS, 13:6 CMDS, 15:7 CMDS

Definition at line 2094 of file FspmUpd.h.

10.8.2.43 EpgEnable

UINT8 FSP_M_CONFIG::EpgEnable

Offset 0x0504 - Energy Performance Gain Enable/disable(default) Energy Performance Gain.

\$EN_DIS

Definition at line 2106 of file FspmUpd.h.

10.8.2.44 FClkFrequency

UINT8 FSP_M_CONFIG::FClkFrequency

Offset 0x0216 - 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 901 of file FspmUpd.h.

10.8.2.45 FivrEfficiency

UINT8 FSP_M_CONFIG::FivrEfficiency

Offset 0x0517 - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; **1: Enabled.**

\$EN_DIS

Definition at line 2235 of file FspmUpd.h.

10.8.2.46 FivrFaults

UINT8 FSP_M_CONFIG::FivrFaults

Offset 0x0516 - Fivr Faults Fivr Faults; 0: Disabled; 1: **Enabled**.

\$EN_DIS

Definition at line 2229 of file FspmUpd.h.

10.8.2.47 ForceOltmOrRefresh2x

UINT8 FSP_M_CONFIG::ForceOltmOrRefresh2x

Offset 0x0512 - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.

Enabled: = Force 2x Refresh. \$EN_DIS

Definition at line 2202 of file FspmUpd.h.

10.8.2.48 FreqSaGvLow

UINT16 FSP_M_CONFIG::FreqSaGvLow

Offset 0x00C2 - Low Frequency SAGV Low Frequency Selections in Mhz.

Options are 1067, 1333, 1600, 1867, 2133, 2400, 2667, 2933 and 0 for Auto. 1067:1067, 1333:1333, 1600:1600, 1867:1867, 2133:2133, 2400:2400, 2667:2667, 2933:2933, 0:Auto

Definition at line 318 of file FspmUpd.h.

10.8.2.49 FreqSaGvMid

UINT16 FSP_M_CONFIG::FreqSaGvMid

Offset 0x00C4 - Mid Frequency SAGV Mid Frequency Selections in Mhz.

Options are 1067, 1333, 1600, 1867, 2133, 2400, 2667, 2933 and 0 for Auto. 1067:1067, 1333:1333, 1600:1600, 1867:1867, 2133:2133, 2400:2400, 2667:2667, 2933:2933, 0:Auto

Definition at line 325 of file FspmUpd.h.

10.8.2.50 GmAdr

UINT32 FSP_M_CONFIG::GmAdr

Offset 0x013C - Temporary MMIO address for GMADR The reference code will use this as Temporary MMIO address space to access GMADR Registers. Platform should provide conflict free Temporary MMIO Range: GmAdr to (GmAdr + ApertureSize).

Default is (PciExpressBaseAddress - ApertureSize) to (PciExpressBaseAddress

- 0x1) (Where ApertureSize = 256MB)

Definition at line 665 of file FspmUpd.h.

10.8.2.51 GtPllVoltageOffset

UINT8 FSP_M_CONFIG::GtPllVoltageOffset

Offset 0x0477 - GT PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1355 of file FspmUpd.h.

10.8.2.52 GtPsmiSupport

UINT8 FSP_M_CONFIG::GtPsmiSupport

Offset 0x017D - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.

When TRUE, it will allow the PSMI Support \$EN_DIS

Definition at line 800 of file FspmUpd.h.

10.8.2.53 GttMmAdr

UINT32 FSP_M_CONFIG::GttMmAdr

Offset 0x0140 - Temporary MMIO address for GTTMMADR The reference code will use this as Temporary MMIO address space to access GTTMMADR Registers. Platform should provide conflict free Temporary MMIO Range: GttMmAdr to (GttMmAdr + 2MB MMIO + 6MB Reserved + GttSize).

Default is (GmAdr - (2MB MMIO

- 6MB Reserved + GttSize)) to (GmAdr - 0x1) (Where GttSize = 8MB)

Definition at line 673 of file FspmUpd.h.

10.8.2.54 HobBufferSize

UINT8 FSP_M_CONFIG::HobBufferSize

Offset 0x0488 - HobBufferSize Size to set HOB Buffer.

0:Default, 1: 1 Byte, 2: 1 KB, 3: Max value(assuming 63KB total HOB size). 0:Default, 1: 1 Byte, 2: 1 KB, 3: Max value

Definition at line 1455 of file FspmUpd.h.

10.8.2.55 HotThresholdCh0Dimm0

UINT8 FSP_M_CONFIG::HotThresholdCh0Dimm0

Offset 0x04DE - Hot Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 1911 of file FspmUpd.h.

10.8.2.56 HotThresholdCh0Dimm1

UINT8 FSP_M_CONFIG::HotThresholdCh0Dimm1

Offset 0x04DF - Hot Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 1916 of file FspmUpd.h.

10.8.2.57 HotThresholdCh1Dimm0

UINT8 FSP_M_CONFIG::HotThresholdCh1Dimm0

Offset 0x04E0 - Hot Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 1921 of file FspmUpd.h.

10.8.2.58 HotThresholdCh1Dimm1

UINT8 FSP_M_CONFIG::HotThresholdCh1Dimm1

Offset 0x04E1 - Hot Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Default is 255

Definition at line 1926 of file FspmUpd.h.

10.8.2.59 Idd3n

UINT16 FSP_M_CONFIG::Idd3n

Offset 0x04CA - EPG DIMM Idd3N Active standby current (Idd3N) in milliamps from datasheet.

Must be calculated on a per DIMM basis. Default is 26

Definition at line 1827 of file FspmUpd.h.

10.8.2.60 Idd3p

UINT16 FSP_M_CONFIG::Idd3p

Offset 0x04CC - EPG DIMM Idd3P Active power-down current (Idd3P) in milliamps from datasheet.

Must be calculated on a per DIMM basis. Default is 11

Definition at line 1833 of file FspmUpd.h.

10.8.2.61 IgdDvmt50PreAlloc

UINT8 FSP_M_CONFIG::IgdDvmt50PreAlloc

Offset 0x00BA - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.

0x00:0MB, 0x01:32MB, 0x02:64MB, 0x03:96MB, 0x04:128MB, 0x05:160MB, 0xF0:4MB, 0xF1:8MB, 0xF2:12MB, 0xF3:16MB, 0xF4:20MB, 0xF5:24MB, 0xF6:28MB, 0xF7:32MB, 0xF8:36MB, 0xF9:40MB, 0xFA:44MB, 0xFB:48MB, 0xFC:52MB, 0xFD:56MB, 0xFE:60MB

Definition at line 272 of file FspmUpd.h.

10.8.2.62 ImguClkOutEn

UINT8 FSP_M_CONFIG::ImguClkOutEn[5]

Offset 0x016F - IMGU CLKOUT Configuration The configuration of IMGU CLKOUT, 0: Disable;1: **Enable**.

\$EN_DIS

Definition at line 765 of file FspmUpd.h.

10.8.2.63 ImrRpSelection

UINT8 FSP_M_CONFIG::ImrRpSelection

Offset 0x046A - Root port number for IMR.

Root port number for IMR.

Definition at line 1317 of file FspmUpd.h.

10.8.2.64 InitPcieAspmAfterOprom

UINT8 FSP_M_CONFIG::InitPcieAspmAfterOprom

Offset 0x011B - 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 615 of file FspmUpd.h.

10.8.2.65 InternalGfx

UINT8 FSP_M_CONFIG::InternalGfx

Offset 0x00BB - Internal Graphics Enable/disable internal graphics.

\$EN_DIS

Definition at line 278 of file FspmUpd.h.

10.8.2.66 IsvtIoPort

UINT8 FSP_M_CONFIG::IsvtIoPort

Offset 0x00F7 - ISVT IO Port Address ISVT IO Port Address.

0=Minimal, 0xFF=Maximum, 0x99=Default

Definition at line 501 of file FspmUpd.h.

10.8.2.67 JtagC10PowerGateDisable

UINT8 FSP_M_CONFIG::JtagC10PowerGateDisable

Offset 0x0217 - Set JTAG power in C10 and deeper power states False: JTAG is power gated in C10 state.

True: keeps the JTAG power up during C10 and deeper power states for debug purpose. **0: False**; 1: True. 0: False, 1: True

Definition at line 908 of file FspmUpd.h.

10.8.2.68 McPllVoltageOffset

UINT8 FSP_M_CONFIG::McPllVoltageOffset

Offset 0x047A - Memory Controller PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1370 of file FspmUpd.h.

10.8.2.69 MmioSize

UINT16 FSP_M_CONFIG::MmioSize

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

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

Definition at line 187 of file FspmUpd.h.

10.8.2.70 OcLock

UINT8 FSP_M_CONFIG::OcLock

Offset 0x020D - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 844 of file FspmUpd.h.

10.8.2.71 PcdDebugInterfaceFlags

UINT8 FSP_M_CONFIG::PcdDebugInterfaceFlags

Offset 0x0474 - Debug Interfaces Debug Interfaces.

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

Definition at line 1338 of file FspmUpd.h.

10.8.2.72 PcdIsaSerialUartBase

UINT8 FSP_M_CONFIG::PcdIsaSerialUartBase

Offset 0x0476 - ISA Serial Base selection Select ISA Serial Base address.

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

Definition at line 1350 of file FspmUpd.h.

10.8.2.73 PcdSerialDebugBaudRate

UINT8 FSP_M_CONFIG::PcdSerialDebugBaudRate

Offset 0x0487 - 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 1448 of file FspmUpd.h.

10.8.2.74 PcdSerialDebugLevel

UINT8 FSP_M_CONFIG::PcdSerialDebugLevel

Offset 0x0515 - 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 2223 of file FspmUpd.h.

10.8.2.75 PcdSerialIoUartNumber

UINT8 FSP_M_CONFIG::PcdSerialIoUartNumber

Offset 0x0475 - PcdSerialIoUartNumber Select SerialIo Uart Controller for debug.

0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 1344 of file FspmUpd.h.

10.8.2.76 PchLpcEnhancePort8xhDecoding

UINT8 FSP_M_CONFIG::PchLpcEnhancePort8xhDecoding

Offset 0x045F - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.

\$EN_DIS

Definition at line 1269 of file FspmUpd.h.

10.8.2.77 PchNumRsvdSmbusAddresses

UINT8 FSP_M_CONFIG::PchNumRsvdSmbusAddresses

Offset 0x0462 - Number of RsvdSmbusAddressTable.

The number of elements in the RsvdSmbusAddressTable.

Definition at line 1286 of file FspmUpd.h.

10.8.2.78 PchPort80Route

UINT8 FSP_M_CONFIG::PchPort80Route

Offset 0x0460 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.

\$EN_DIS

Definition at line 1275 of file FspmUpd.h.

10.8.2.79 PchSmbAlertEnable

UINT8 FSP_M_CONFIG::PchSmbAlertEnable

Offset 0x0469 - Enable SMBus Alert Pin Enable SMBus Alert Pin.

\$EN_DIS

Definition at line 1312 of file FspmUpd.h.

10.8.2.80 PchTraceHubMemReg0Size

UINT8 FSP_M_CONFIG::PchTraceHubMemReg0Size

Offset 0x00B1 - PCH Trace Hub Memory Region 0 buffer Size Specify size of Pch trace memory region 0 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

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

Definition at line 251 of file FspmUpd.h.

10.8.2.81 PchTraceHubMemReg1Size

UINT8 FSP_M_CONFIG::PchTraceHubMemReg1Size

Offset 0x00B2 - PCH Trace Hub Memory Region 1 buffer Size Specify size of Pch trace memory region 1 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.

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

Definition at line 258 of file FspmUpd.h.

10.8.2.82 PchTraceHubMode

UINT8 FSP_M_CONFIG::PchTraceHubMode

Offset 0x00B0 - PCH Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.

0: Disable, 1: Target Debugger Mode, 2: Host Debugger Mode

Definition at line 244 of file FspmUpd.h.

10.8.2.83 PcieImrSize

UINT16 FSP_M_CONFIG::PcieImrSize

Offset 0x0466 - Size of PCIe IMR.

Size of PCIe IMR in megabytes

Definition at line 1300 of file FspmUpd.h.

10.8.2.84 PcieMultipleSegmentEnabled

UINT8 FSP_M_CONFIG::PcieMultipleSegmentEnabled

Offset 0x016C - This is policy to control iTBT PCIe Multiple Segment setting.

When Disabled all the TBT PCIe RP are located at Segment0, When Enabled all the TBT PCIe RP are located at Segment1. **0: Disable**; 1: Enable. \$EN_DIS

Definition at line 747 of file FspmUpd.h.

10.8.2.85 PcieRpEnableMask

UINT32 FSP_M_CONFIG::PcieRpEnableMask

Offset 0x0470 - 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 1332 of file FspmUpd.h.

10.8.2.86 PlatformDebugConsent

UINT8 FSP_M_CONFIG::PlatformDebugConsent

Offset 0x00AC - Platform Debug Consent To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type.

Enabling this BIOS option may alter the default value of other debug-related BIOS options.: Do not use Platform Debug Consent to override other debug-relevant policies, but the user must set each debug option manually, aimed at advanced users.

Note: DCI OOB (aka BSSB) uses CCA probe;[DCI OOB+DbC] and [USB2 DbC] have the same setting. 0:Disabled,

1:Enabled (DCI OOB+[DbC]), 2:Enabled (DCI OOB), 3:Enabled (USB3 DbC), 4:Enabled (XDP/MIPI60), 5:Enabled (USB2 DbC), 6:Enable (2-wire DCI OOB), 7:Manual

Definition at line 217 of file FspmUpd.h.

10.8.2.87 PrmrrSize

UINT32 FSP_M_CONFIG::PrmrrSize

Offset 0x023C - PrmrrSize Enable/Disable.

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

Definition at line 1038 of file FspmUpd.h.

10.8.2.88 ProbelessTrace

UINT8 FSP_M_CONFIG::ProbelessTrace

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

Enabling Probeless Trace will reserve 128MB. This also requires IED to be enabled. \$EN_DIS

Definition at line 194 of file FspmUpd.h.

10.8.2.89 PwdwnIdleCounter

UINT8 FSP_M_CONFIG::PwdownIdleCounter

Offset 0x0513 - Pwr Down Idle Timer The minimum value should = to the worst case Roundtrip delay + Burst_↔ Length.

0 means AUTO: 64 for ULX/ULT, 128 for DT/Halo

Definition at line 2208 of file FspmUpd.h.

10.8.2.90 RankInterleave

UINT8 FSP_M_CONFIG::RankInterleave

Offset 0x04AA - Rank Interleave support Enables/Disable Rank Interleave support.

NOTE: RI and HORI can not be enabled at the same time. \$EN_DIS

Definition at line 1660 of file FspmUpd.h.

10.8.2.91 Ratio

UINT8 FSP_M_CONFIG::Ratio

Offset 0x00E0 - 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 400 of file FspmUpd.h.

10.8.2.92 RealtimeMemoryTiming

UINT8 FSP_M_CONFIG::RealtimeMemoryTiming

Offset 0x016B - 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 740 of file FspmUpd.h.

10.8.2.93 RefClk

UINT8 FSP_M_CONFIG::RefClk

Offset 0x00DD - Memory Reference Clock 100MHz, 133MHz.

0:133MHz, 1:100MHz

Definition at line 386 of file FspmUpd.h.

10.8.2.94 RhSolution

UINT8 FSP_M_CONFIG::RhSolution

Offset 0x0505 - Row Hammer Solution Type of method used to prevent Row Hammer.

Default is Hardware RHP 0:Hardware RHP, 1:2x Refresh

Definition at line 2112 of file FspmUpd.h.

10.8.2.95 RingDownBin

UINT8 FSP_M_CONFIG::RingDownBin

Offset 0x0223 - 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 962 of file FspmUpd.h.

10.8.2.96 RingMaxOcRatio

UINT8 FSP_M_CONFIG::RingMaxOcRatio

Offset 0x0210 - 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: 0-85

Definition at line 862 of file FspmUpd.h.

10.8.2.97 RingPllVoltageOffset

UINT8 FSP_M_CONFIG::RingPllVoltageOffset

Offset 0x0478 - Ring PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1360 of file FspmUpd.h.

10.8.2.98 RingVoltageAdaptive

UINT16 FSP_M_CONFIG::RingVoltageAdaptive

Offset 0x0228 - Ring Turbo voltage Adaptive Extra Turbo voltage applied to the cpu ring when the cpu is operating in turbo mode.

Valid Range 0 to 2000

Definition at line 986 of file FspmUpd.h.

10.8.2.99 RingVoltageMode

UINT8 FSP_M_CONFIG::RingVoltageMode

Offset 0x0224 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.

\$EN_DIS

Definition at line 968 of file FspmUpd.h.

10.8.2.100 RingVoltageOffset

UINT16 FSP_M_CONFIG::RingVoltageOffset

Offset 0x022A - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.

Valid Range 0 to 1000

Definition at line 991 of file FspmUpd.h.

10.8.2.101 RingVoltageOverride

UINT16 FSP_M_CONFIG::RingVoltageOverride

Offset 0x0226 - Ring voltage override The ring voltage override which is applied to the entire range of cpu ring frequencies.

Valid Range 0 to 2000

Definition at line 980 of file FspmUpd.h.

10.8.2.102 RMT

UINT8 FSP_M_CONFIG::RMT

Offset 0x00C6 - Rank Margin Tool Enable/disable Rank Margin Tool.

\$EN_DIS

Definition at line 331 of file FspmUpd.h.

10.8.2.103 RMTLoopCount

UINT8 FSP_M_CONFIG::RMTLoopCount

Offset 0x051E - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.

0 - AUTO

Definition at line 2268 of file FspmUpd.h.

10.8.2.104 RmtPerTask

UINT8 FSP_M_CONFIG::RmtPerTask

Offset 0x0099 - Rank Margin Tool per Task This option enables the user to execute Rank Margin Tool per major training step in the MRC.

\$EN_DIS

Definition at line 159 of file FspmUpd.h.

10.8.2.105 SafeMode

UINT8 FSP_M_CONFIG::SafeMode

Offset 0x0518 - Safe Mode Support This option configures the various items in the IO and MC to be more conservative.

(def=Disable) \$EN_DIS

Definition at line 2241 of file FspmUpd.h.

10.8.2.106 SaGv

UINT8 FSP_M_CONFIG::SaGv

Offset 0x00C0 - SA GV System Agent dynamic frequency support and when enabled memory will be training at three different frequencies.

0:Disabled, 1:FixedLow, 2:FixedMid, 3:FixedHigh, 4:Enabled

Definition at line 305 of file FspmUpd.h.

10.8.2.107 SaPcieRpEnableMask

UINT32 FSP_M_CONFIG::SaPcieRpEnableMask

Offset 0x0178 - 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 787 of file FspmUpd.h.

10.8.2.108 SaPcieRpLinkDownGpios

UINT8 FSP_M_CONFIG::SaPcieRpLinkDownGpios

Offset 0x017C - Assertion on Link Down GPIOs GPIO Assertion on Link Down.

Disabled(0x0)(Default): Disable assertion on Link Down GPIOs, Enabled(0x1): Enable assertion on Link Down GPIOs 0:Disable, 1:Enable

Definition at line 794 of file FspmUpd.h.

10.8.2.109 SaPllVoltageOffset

UINT8 FSP_M_CONFIG::SaPllVoltageOffset

Offset 0x0479 - System Agent PLL voltage offset Core PLL voltage offset.

0: No offset. Range 0-63

Definition at line 1365 of file FspmUpd.h.

10.8.2.110 ScramblerSupport

UINT8 FSP_M_CONFIG::ScramblerSupport

Offset 0x00C9 - Scrambler Support This option enables data scrambling in memory.

\$EN_DIS

Definition at line 349 of file FspmUpd.h.

10.8.2.111 SinitMemorySize

UINT32 FSP_M_CONFIG::SinitMemorySize

Offset 0x0240 - SinitMemorySize Enable/Disable.

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

Definition at line 1043 of file FspmUpd.h.

10.8.2.112 SmbusArpEnable

UINT8 FSP_M_CONFIG::SmbusArpEnable

Offset 0x0461 - Enable SMBus ARP support Enable SMBus ARP support.

\$EN_DIS

Definition at line 1281 of file FspmUpd.h.

10.8.2.113 SmbusEnable

UINT8 FSP_M_CONFIG::SmbusEnable

Offset 0x00A7 - Enable SMBus Enable/disable SMBus controller.

\$EN_DIS

Definition at line 200 of file FspmUpd.h.

10.8.2.114 SpdAddressTable

UINT8 FSP_M_CONFIG::SpdAddressTable[4]

Offset 0x00A8 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.

MemorySpdPtr will be used if SPD Address is 00

Definition at line 206 of file FspmUpd.h.

10.8.2.115 SpdProfileSelected

UINT8 FSP_M_CONFIG::SpdProfileSelected

Offset 0x00DC - 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 380 of file FspmUpd.h.

10.8.2.116 TcssDma0En

UINT8 FSP_M_CONFIG::TcssDma0En

Offset 0x0484 - TCSS DMA0 Enable Set TCSS DMA0.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1430 of file FspmUpd.h.

10.8.2.117 TcssDma1En

UINT8 FSP_M_CONFIG::TcssDma1En

Offset 0x0485 - TCSS DMA1 Enable Set TCSS DMA1.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1436 of file FspmUpd.h.

10.8.2.118 TcssDma2En

UINT8 FSP_M_CONFIG::TcssDma2En

Offset 0x0486 - TCSS DMA2 Enable Set TCSS DMA2.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1442 of file FspmUpd.h.

10.8.2.119 TcssItbtPcie0En

UINT8 FSP_M_CONFIG::TcssItbtPcie0En

Offset 0x047C - TCSS Thunderbolt PCIE Root Port 0 Enable Set TCSS Thunderbolt PCIE Root Port 0.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1382 of file FspmUpd.h.

10.8.2.120 TcssItbtPcie1En

UINT8 FSP_M_CONFIG::TcssItbtPcie1En

Offset 0x047D - TCSS Thunderbolt PCIE Root Port 1 Enable Set TCSS Thunderbolt PCIE Root Port 1.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1388 of file FspmUpd.h.

10.8.2.121 TcssItbtPcie2En

UINT8 FSP_M_CONFIG::TcssItbtPcie2En

Offset 0x047E - TCSS Thunderbolt PCIE Root Port 2 Enable Set TCSS Thunderbolt PCIE Root Port 2.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1394 of file FspmUpd.h.

10.8.2.122 TcssItbtPcie3En

UINT8 FSP_M_CONFIG::TcssItbtPcie3En

Offset 0x047F - TCSS Thunderbolt PCIE Root Port 3 Enable Set TCSS Thunderbolt PCIE Root Port 3.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1400 of file FspmUpd.h.

10.8.2.123 TcssItbtPcie4En

UINT8 FSP_M_CONFIG::TcssItbtPcie4En

Offset 0x0480 - TCSS Thunderbolt PCIE Root Port 4 Enable Set TCSS Thunderbolt PCIE Root Port 4.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1406 of file FspmUpd.h.

10.8.2.124 TcssItbtPcie5En

UINT8 FSP_M_CONFIG::TcssItbtPcie5En

Offset 0x0481 - TCSS Thunderbolt PCIE Root Port 5 Enable Set TCSS Thunderbolt PCIE Root Port 5.

0:Disabled 1:Enabled \$EN_DIS

Definition at line 1412 of file FspmUpd.h.

10.8.2.125 TcssXdcieEn

UINT8 FSP_M_CONFIG::TcssXdcieEn

Offset 0x0483 - TCSS USB DEVICE (xDCI) Enable Set TCSS XDCI.

0:Disabled 1:Enabled - xHCI must be enabled if xDCI is enabled \$EN_DIS

Definition at line 1424 of file FspmUpd.h.

10.8.2.126 TcssXhciEn

UINT8 FSP_M_CONFIG::TcssXhciEn

Offset 0x0482 - TCSS USB HOST (xHCI) Enable Set TCSS XHCI.

0:Disabled 1:Enabled - Must be enabled if xDCI is enabled below \$EN_DIS

Definition at line 1418 of file FspmUpd.h.

10.8.2.127 TgaSize

UINT32 FSP_M_CONFIG::TgaSize

Offset 0x0264 - TgaSize Enable/Disable.

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

Definition at line 1082 of file FspmUpd.h.

10.8.2.128 ThrtCkeMinTmr

UINT8 FSP_M_CONFIG::ThrtCkeMinTmr

Offset 0x04FE - Throttler CKEMin Timer Timer value for CKEMin, range[255;0].

Req'd min of SC_ROUND_T + BYTE_LENGTH (4). Dfault is 0x30

Definition at line 2072 of file FspmUpd.h.

10.8.2.129 TjMaxOffset

UINT8 FSP_M_CONFIG::TjMaxOffset

Offset 0x0225 - TjMax Offset TjMax offset. Specified value here is clipped by pCode (125 - TjMax Offset) to support TjMax in the range of 62 to 115 deg Celsius.

Valid Range 10 - 63

Definition at line 974 of file FspmUpd.h.

10.8.2.130 TmeEnable

UINT8 FSP_M_CONFIG::TmeEnable

Offset 0x022C - Enable or Disable TME Enable or Disable TME; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 997 of file FspmUpd.h.

10.8.2.131 TrainTrace

UINT8 FSP_M_CONFIG::TrainTrace

Offset 0x009A - Training Trace This option enables the trained state tracing feature in MRC.

This feature will print out the key training parameters state across major training steps. \$EN_DIS

Definition at line 166 of file FspmUpd.h.

10.8.2.132 tRTP

UINT8 FSP_M_CONFIG::tRTP

Offset 0x00EF - 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 458 of file FspmUpd.h.

10.8.2.133 TsegSize

UINT32 FSP_M_CONFIG::TsegSize

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

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

Definition at line 182 of file FspmUpd.h.

10.8.2.134 TsodAlarmwindowLockBit

UINT8 FSP_M_CONFIG::TsodAlarmwindowLockBit

Offset 0x050D - Alarm window lock bit Disable:Alarm trips are not locked and can be changed.

Enable:Alarm trips are locked and cannot be changed \$EN_DIS

Definition at line 2168 of file FspmUpd.h.

10.8.2.135 TsodCriticalEventOnly

UINT8 FSP_M_CONFIG::TsodCriticalEventOnly

Offset 0x050B - Critical event only Disable:Trips on alarm or critical.

Enable:Trips only if criticaal temperature is reached \$EN_DIS

Definition at line 2154 of file FspmUpd.h.

10.8.2.136 TsodCriticaltripLockBit

UINT8 FSP_M_CONFIG::TsodCriticaltripLockBit

Offset 0x050E - Critical trip lock bit Disable:Critical trip is not locked and can be changed.

Enable:Critical trip is locked and cannot be changed \$EN_DIS

Definition at line 2175 of file FspmUpd.h.

10.8.2.137 TsodEventMode

UINT8 FSP_M_CONFIG::TsodEventMode

Offset 0x0509 - Event mode Disable:Comparator mode.

Enable:Interrupt mode \$EN_DIS

Definition at line 2140 of file FspmUpd.h.

10.8.2.138 TsodEventOutputControl

UINT8 FSP_M_CONFIG::TsodEventOutputControl

Offset 0x050C - Event output control Disable:Event output disable.

Enable:Event output enabled \$EN_DIS

Definition at line 2161 of file FspmUpd.h.

10.8.2.139 TsodEventPolarity

UINT8 FSP_M_CONFIG::TsodEventPolarity

Offset 0x050A - EVENT polarity Disable:Active LOW.

Enable:Active HIGH \$EN_DIS

Definition at line 2147 of file FspmUpd.h.

10.8.2.140 TsodManualEnable

UINT8 FSP_M_CONFIG::TsodManualEnable

Offset 0x0511 - User Manual Thig and Tcrit Disabled(Default): Temperature will be given by the configuration of memories and 1x or 2xrefresh rate.

Enabled: User Input will define for Thigh and Tcrit. \$EN_DIS

Definition at line 2195 of file FspmUpd.h.

10.8.2.141 TsodShutdownMode

UINT8 FSP_M_CONFIG::TsodShutdownMode

Offset 0x050F - Shutdown mode Disable:Temperature sensor enable.

Enable:Temperature sensor disable \$EN_DIS

Definition at line 2182 of file FspmUpd.h.

10.8.2.142 TsodTcritMax

UINT8 FSP_M_CONFIG::TsodTcritMax

Offset 0x0508 - TcritMax Maximum Critical Temperature in Centigrade of the On-DIMM Thermal Sensor.

TCRITMax has to be greater than THIGHMax .

Critical temperature will be TcritMax

Definition at line 2133 of file FspmUpd.h.

10.8.2.143 Txt

UINT8 FSP_M_CONFIG::Txt

Offset 0x023B - Txt Enable/Disable.

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

Definition at line 1033 of file FspmUpd.h.

10.8.2.144 TxtDprMemoryBase

UINT64 FSP_M_CONFIG::TxtDprMemoryBase

Offset 0x0248 - TxtDprMemoryBase Enable/Disable.

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

Definition at line 1052 of file FspmUpd.h.

10.8.2.145 TxtDprMemorySize

UINT32 FSP_M_CONFIG::TxtDprMemorySize

Offset 0x0254 - TxtDprMemorySize Enable/Disable.

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

Definition at line 1062 of file FspmUpd.h.

10.8.2.146 TxtHeapMemorySize

UINT32 FSP_M_CONFIG::TxtHeapMemorySize

Offset 0x0250 - TxtHeapMemorySize Enable/Disable.

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

Definition at line 1057 of file FspmUpd.h.

10.8.2.147 TxtImplemented

UINT8 FSP_M_CONFIG::TxtImplemented

Offset 0x015E - 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 691 of file FspmUpd.h.

10.8.2.148 TxtLcpPdBase

UINT64 FSP_M_CONFIG::TxtLcpPdBase

Offset 0x0268 - TxtLcpPdBase Enable/Disable.

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

Definition at line 1087 of file FspmUpd.h.

10.8.2.149 TxtLcpPdSize

UINT64 FSP_M_CONFIG::TxtLcpPdSize

Offset 0x0270 - TxtLcpPdSize Enable/Disable.

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

Definition at line 1092 of file FspmUpd.h.

10.8.2.150 UserBudgetEnable

UINT8 FSP_M_CONFIG::UserBudgetEnable

Offset 0x0507 - User Manual Budget Disabled: Configuration of memories will defined the Budget value.

Enabled: User Input will be used. \$EN_DIS

Definition at line 2126 of file FspmUpd.h.

10.8.2.151 UserThresholdEnable

UINT8 FSP_M_CONFIG::UserThresholdEnable

Offset 0x0506 - User Manual Threshold Disabled: Predefined threshold will be used.

Enabled: User Input will be used. \$EN_DIS

Definition at line 2119 of file FspmUpd.h.

10.8.2.152 VddVoltage

UINT16 FSP_M_CONFIG::VddVoltage

Offset 0x00DE - Memory Voltage Memory Voltage Override (Vddq).

Default = no override 0:Default, 1200:1.20 Volts, 1250:1.25 Volts, 1300:1.30 Volts, 1350:1.35 Volts, 1400:1.40 Volts, 1450:1.45 Volts, 1500:1.50 Volts, 1550:1.55 Volts, 1600:1.60 Volts, 1650:1.65 Volts

Definition at line 393 of file FspmUpd.h.

10.8.2.153 VmxEnable

UINT8 FSP_M_CONFIG::VmxEnable

Offset 0x0218 - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable.**

\$EN_DIS

Definition at line 914 of file FspmUpd.h.

10.8.2.154 WarmThresholdCh0Dimm0

UINT8 FSP_M_CONFIG::WarmThresholdCh0Dimm0

Offset 0x04DA - Warm Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Fefault is 255

Definition at line 1891 of file FspmUpd.h.

10.8.2.155 WarmThresholdCh0Dimm1

UINT8 FSP_M_CONFIG::WarmThresholdCh0Dimm1

Offset 0x04DB - Warm Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Fefault is 255

Definition at line 1896 of file FspmUpd.h.

10.8.2.156 WarmThresholdCh1Dimm0

UINT8 FSP_M_CONFIG::WarmThresholdCh1Dimm0

Offset 0x04DC - Warm Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Fefault is 255

Definition at line 1901 of file FspmUpd.h.

10.8.2.157 WarmThresholdCh1Dimm1

UINT8 FSP_M_CONFIG::WarmThresholdCh1Dimm1

Offset 0x04DD - Warm Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.

Fefault is 255

Definition at line 1906 of file FspmUpd.h.

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

- [FspmUpd.h](#)

10.9 FSP_M_TEST_CONFIG Struct Reference

Fsp M Test Configuration.

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

Public Attributes

- [UINT32 Signature](#)
Offset 0x0540.
- [UINT8 SkipExtGfxScan](#)
Offset 0x0544 - Skip external display device scanning Enable: Do not scan for external display device, Disable (Default): Scan external display devices \$EN_DIS.
- [UINT8 BdatEnable](#)
Offset 0x0545 - Generate BIOS Data ACPI Table Enable: Generate BDAT for MRC RMT or SA PCIe data.
- [UINT8 ScanExtGfxForLegacyOpRom](#)
Offset 0x0546 - 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 0x0547 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.
- [UINT8 DmiMaxLinkSpeed](#)

Offset 0x0548 - 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 0x0549 - DMI Equalization Phase 2 DMI Equalization Phase 2.
 - UINT8 [DmiGen3EqPh3Method](#)
Offset 0x054A - DMI Gen3 Equalization Phase3 DMI Gen3 Equalization Phase3.
 - UINT8 [PegGen3Rsvd](#)
Offset 0x054B - 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 0x054C - Panel Power Enable Control for enabling/disabling VDD force bit (Required only for early enabling of eDP panel).
 - UINT8 [BdatTestType](#)
Offset 0x054D - BdatTestType Indicates the type of Memory Training data to populate into the BDAT ACPI table.
 - UINT8 [SaPreMemTestRsvd](#) [98]
Offset 0x054E - SaPreMemTestRsvd Reserved for SA Pre-Mem Test \$EN_DIS.
 - UINT16 [TotalFlashSize](#)
Offset 0x05B0 - TotalFlashSize Enable/Disable.
 - UINT16 [BiosSize](#)
Offset 0x05B2 - BiosSize Enable/Disable.
 - UINT8 [TxtAcheckRequest](#)
Offset 0x05B4 - TxtAcheckRequest Enable/Disable.
 - UINT8 [SecurityTestRsvd](#) [11]
Offset 0x05B5 - SecurityTestRsvd Reserved for SA Pre-Mem Test \$EN_DIS.
 - UINT8 [SmbusDynamicPowerGating](#)
Offset 0x05C0 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.
 - UINT8 [WdtDisableAndLock](#)
Offset 0x05C1 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.
 - UINT8 [SmbusSpdWriteDisable](#)
Offset 0x05C2 - SMBUS SPD Write Disable Set/Clear Smbus SPD Write Disable.
 - UINT8 [ChipsetInitMessage](#)
Offset 0x05C3 - ChipsetInit HECI message Enable/Disable.
 - UINT8 [BypassPhySyncReset](#)
Offset 0x05C4 - Bypass ChipsetInit sync reset.
 - UINT8 [DidInitStat](#)
Offset 0x05C5 - Force ME DID Init Status Test, 0: disable, 1: Success, 2: No Memory in Channels, 3: Memory Init Error, Set ME DID init stat value \$EN_DIS.
 - UINT8 [DisableCpuReplacedPolling](#)
Offset 0x05C6 - CPU Replaced Polling Disable Test, 0: disable, 1: enable, Setting this option disables CPU replacement polling loop \$EN_DIS.
 - UINT8 [SendDidMsg](#)
Offset 0x05C7 - ME DID Message Test, 0: disable, 1: enable, Enable/Disable ME DID Message (disable will prevent the DID message from being sent) \$EN_DIS.
 - UINT8 [DisableMessageCheck](#)
Offset 0x05C8 - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.
 - UINT8 [SkipMbpHob](#)
Offset 0x05C9 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.
 - UINT8 [HeciCommunication2](#)
Offset 0x05CA - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.
 - UINT8 [KiDeviceEnable](#)
-

Offset 0x05CB - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

- UIN8 ReservedFspmTestUpd [20]

Offset 0x05CC.

10.9.1 Detailed Description

Fsp M Test Configuration.

Definition at line 2293 of file FspmUpd.h.

10.9.2 Member Data Documentation

10.9.2.1 BdatEnable

UIN8 FSP_M_TEST_CONFIG::BdatEnable

Offset 0x0545 - 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 2310 of file FspmUpd.h.

10.9.2.2 BdatTestType

UIN8 FSP_M_TEST_CONFIG::BdatTestType

Offset 0x054D - BdatTestType Indicates the type of Memory Training data to populate into the BDAT ACPI table.

0:RMT per Rank, 1:RMT per Bit, 2:Margin2D

Definition at line 2368 of file FspmUpd.h.

10.9.2.3 BiosSize

UIN16 FSP_M_TEST_CONFIG::BiosSize

Offset 0x05B2 - BiosSize Enable/Disable.

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

Definition at line 2384 of file FspmUpd.h.

10.9.2.4 BypassPhySyncReset

UIN8 FSP_M_TEST_CONFIG::BypassPhySyncReset

Offset 0x05C4 - Bypass ChipsetInit sync reset.

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

Definition at line 2428 of file FspmUpd.h.

10.9.2.5 ChipsetInitMessage

UINT8 FSP_M_TEST_CONFIG::ChipsetInitMessage

Offset 0x05C3 - 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 2422 of file FspmUpd.h.

10.9.2.6 DisableMessageCheck

UINT8 FSP_M_TEST_CONFIG::DisableMessageCheck

Offset 0x05C8 - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.

\$EN_DIS

Definition at line 2454 of file FspmUpd.h.

10.9.2.7 DmiGen3EqPh2Enable

UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh2Enable

Offset 0x0549 - 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 2337 of file FspmUpd.h.

10.9.2.8 DmiGen3EqPh3Method

UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh3Method

Offset 0x054A - 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 2347 of file FspmUpd.h.

10.9.2.9 HeciCommunication2

UINT8 FSP_M_TEST_CONFIG::HeciCommunication2

Offset 0x05CA - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.

\$EN_DIS

Definition at line 2466 of file FspmUpd.h.

10.9.2.10 KtDeviceEnable

UINT8 FSP_M_TEST_CONFIG::KtDeviceEnable

Offset 0x05CB - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

\$EN_DIS

Definition at line 2472 of file FspmUpd.h.

10.9.2.11 LockPTMregs

UINT8 FSP_M_TEST_CONFIG::LockPTMregs

Offset 0x0547 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.

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

Definition at line 2323 of file FspmUpd.h.

10.9.2.12 PanelPowerEnable

UINT8 FSP_M_TEST_CONFIG::PanelPowerEnable

Offset 0x054C - 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 2362 of file FspmUpd.h.

10.9.2.13 ScanExtGfxForLegacyOpRom

UINT8 FSP_M_TEST_CONFIG::ScanExtGfxForLegacyOpRom

Offset 0x0546 - 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 2317 of file FspmUpd.h.

10.9.2.14 SkipMbpHob

UINT8 FSP_M_TEST_CONFIG::SkipMbpHob

Offset 0x05C9 - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.

\$EN_DIS

Definition at line 2460 of file FspmUpd.h.

10.9.2.15 SmbusDynamicPowerGating

UINT8 FSP_M_TEST_CONFIG::SmbusDynamicPowerGating

Offset 0x05C0 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.

\$EN_DIS

Definition at line 2402 of file FspmUpd.h.

10.9.2.16 SmbusSpdWriteDisable

UINT8 FSP_M_TEST_CONFIG::SmbusSpdWriteDisable

Offset 0x05C2 - 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 2415 of file FspmUpd.h.

10.9.2.17 TotalFlashSize

UINT16 FSP_M_TEST_CONFIG::TotalFlashSize

Offset 0x05B0 - TotalFlashSize Enable/Disable.

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

Definition at line 2379 of file FspmUpd.h.

10.9.2.18 TxtAcheckRequest

UINT8 FSP_M_TEST_CONFIG::TxtAcheckRequest

Offset 0x05B4 - TxtAcheckRequest Enable/Disable.

When Enabled, it will forcing calling TXT Acheck once. \$EN_DIS

Definition at line 2390 of file FspmUpd.h.

10.9.2.19 WdtDisableAndLock

UINT8 FSP_M_TEST_CONFIG::WdtDisableAndLock

Offset 0x05C1 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.

\$EN_DIS

Definition at line 2408 of file FspmUpd.h.

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

- [FspmUpd.h](#)

10.10 FSP_S_CONFIG Struct Reference

Fsp S Configuration.

```
#include <FspUpd.h>
```

Public Attributes

- UUINT32 [LogoPtr](#)
Offset 0x0020 - Logo Pointer Points to PEI Display Logo Image.
- UUINT32 [LogoSize](#)
Offset 0x0024 - Logo Size Size of PEI Display Logo Image.
- UUINT32 [BltBufferAddress](#)
Offset 0x0028 - Blt Buffer Address Address of Blt buffer.
- UUINT32 [BltBufferSize](#)
*Offset 0x002C - Blt Buffer Size Size of Blt Buffer, is equal to PixelWidth * PixelHeight * 4 bytes (the size of EFI_GRAPHICS_OUTPUT_BLT_PIXEL)*
- UUINT32 [GraphicsConfigPtr](#)
Offset 0x0030 - Graphics Configuration Ptr Points to VBT.
- UUINT8 [Device4Enable](#)
Offset 0x0034 - Enable Device 4 Enable/disable Device 4 \$EN_DIS.
- UUINT8 [PchHdaDspEnable](#)
Offset 0x0035 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.
- UUINT8 [ScsEmmcEnabled](#)
Offset 0x0036 - Enable eMMC Controller Enable/disable eMMC Controller.
- UUINT8 [ScsEmmcHs400Enabled](#)
Offset 0x0037 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.
- UUINT8 [ScsSdCardEnabled](#)
Offset 0x0038 - Enable SdCard Controller Enable/disable SD Card Controller.
- UUINT8 [ShowSpiController](#)
Offset 0x0039 - Show SPI controller Enable/disable to show SPI controller.
- UUINT8 [UnusedUpdSpace0](#) [2]
Offset 0x003A.
- UUINT32 [MicrocodeRegionBase](#)
Offset 0x003C - MicrocodeRegionBase Memory Base of Microcode Updates.
- UUINT32 [MicrocodeRegionSize](#)
Offset 0x0040 - MicrocodeRegionSize Size of Microcode Updates.
- UUINT8 [TurboMode](#)
Offset 0x0044 - Turbo Mode Enable/Disable Turbo mode.
- UUINT8 [SataSalpSupport](#)
Offset 0x0045 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.
- UUINT8 [SataPortMultiplier](#)
Offset 0x0046 - PCH Sata Port Multiplier Enable / Disable SATA Port Multiplier \$EN_DIS.
- UUINT8 [SataPortsEnable](#) [8]
Offset 0x0047 - Enable SATA ports Enable/disable SATA ports.
- UUINT8 [SataPortsDevSlp](#) [8]
Offset 0x004F - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.
- UUINT8 [PortUsb20Enable](#) [16]
Offset 0x0057 - Enable USB2 ports Enable/disable per USB2 ports.
- UUINT8 [PortUsb30Enable](#) [10]
Offset 0x0067 - Enable USB3 ports Enable/disable per USB3 ports.
- UUINT8 [XdcEnable](#)
Offset 0x0071 - Enable xDCI controller Enable/disable to xDCI controller.
- UUINT8 [UnusedUpdSpace1](#) [2]
Offset 0x0072.

- UINT32 [DevIntConfigPtr](#)
Offset 0x0074 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.
 - UINT8 [NumOfDevIntConfig](#)
Offset 0x0078 - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.
 - UINT8 [PxRcConfig](#) [8]
Offset 0x0079 - PIRQx to IRQx Map Config PIRQx to IRQx mapping.
 - UINT8 [GpioIrqRoute](#)
Offset 0x0081 - Select GPIO IRQ Route GPIO IRQ Select.
 - UINT8 [ScilrqSelect](#)
Offset 0x0082 - Select ScilrqSelect SCI IRQ Select.
 - UINT8 [TcolrqSelect](#)
Offset 0x0083 - Select TcolrqSelect TCO IRQ Select.
 - UINT8 [TcolrqEnable](#)
Offset 0x0084 - Enable/Disable Tco IRQ Enable/disable TCO IRQ \$EN_DIS.
 - UINT8 [PchHdaVerbTableEntryNum](#)
Offset 0x0085 - PCH HDA Verb Table Entry Number Number of Entries in Verb Table.
 - UINT8 [UnusedUpdSpace2](#) [2]
Offset 0x0086.
 - UINT32 [PchHdaVerbTablePtr](#)
Offset 0x0088 - PCH HDA Verb Table Pointer Pointer to Array of pointers to Verb Table.
 - UINT8 [PchHdaCodecSxWakeCapability](#)
Offset 0x008C - PCH HDA Codec Sx Wake Capability Capability to detect wake initiated by a codec in Sx.
 - UINT8 [SataEnable](#)
Offset 0x008D - Enable SATA Enable/disable SATA controller.
 - UINT8 [SataMode](#)
Offset 0x008E - SATA Mode Select SATA controller working mode.
 - UINT8 [SerialloSpiMode](#) [7]
Offset 0x008F - SPIIn Device Mode Selects SPI operation mode.
 - UINT8 [SerialloSpi0CsPolarity](#) [2]
Offset 0x0096 - SPI0 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi1CsPolarity](#) [2]
Offset 0x0098 - SPI1 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi2CsPolarity](#) [2]
Offset 0x009A - SPI2 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi3CsPolarity](#) [2]
Offset 0x009C - SPI3 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi4CsPolarity](#) [2]
Offset 0x009E - SPI4 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi5CsPolarity](#) [2]
Offset 0x00A0 - SPI5 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi6CsPolarity](#) [2]
Offset 0x00A2 - SPI6 Chip Select Polarity Sets polarity for each chip Select.
 - UINT8 [SerialloSpi0CsEnable](#) [2]
Offset 0x00A4 - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.
 - UINT8 [SerialloSpi1CsEnable](#) [2]
Offset 0x00A6 - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.
 - UINT8 [SerialloSpi2CsEnable](#) [2]
Offset 0x00A8 - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.
 - UINT8 [SerialloSpi3CsEnable](#) [2]
Offset 0x00AA - SPI3 Chip Select Enable 0:Disabled, 1:Enabled.
 - UINT8 [SerialloSpi4CsEnable](#) [2]
-

- Offset 0x00AC - SPI4 Chip Select Enable 0:Disabled, 1:Enabled.*

 - UINT8 [SerialloSpi5CsEnable](#) [2]
 - Offset 0x00AE - SPI5 Chip Select Enable 0:Disabled, 1:Enabled.*

 - UINT8 [SerialloSpi6CsEnable](#) [2]
 - Offset 0x00B0 - SPI6 Chip Select Enable 0:Disabled, 1:Enabled.*

 - UINT8 [SerialloSpiDefaultCsOutput](#) [7]
 - Offset 0x00B2 - SPIn Default Chip Select Output Sets Default CS as Output.*

 - UINT8 [SerialloUartMode](#) [7]
 - Offset 0x00B9 - UARTn Device Mode Selects Uart operation mode.*

 - UINT32 [SerialloUartBaudRate](#) [7]
 - Offset 0x00C0 - Default BaudRate for each Serial IO UART Set default BaudRate Supported from 0 - default to 6000000.*

 - UINT8 [SerialloUartParity](#) [7]
 - Offset 0x00DC - Default ParityType for each Serial IO UART Set default Parity.*

 - UINT8 [SerialloUartDataBits](#) [7]
 - Offset 0x00E3 - Default DataBits for each Serial IO UART Set default word length.*

 - UINT8 [SerialloUartStopBits](#) [7]
 - Offset 0x00EA - Default StopBits for each Serial IO UART Set default stop bits.*

 - UINT8 [SerialloUartPowerGating](#) [7]
 - Offset 0x00F1 - Power Gating mode for each Serial IO UART that works in COM mode Set Power Gating.*

 - UINT8 [SerialloUartDmaEnable](#) [7]
 - Offset 0x00F8 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.*

 - UINT8 [SerialloUartAutoFlow](#) [7]
 - Offset 0x00FF - Enables UART hardware flow control, CTS and RTS lines Enables UART hardware flow control, CTS and RTS lines.*

 - UINT8 [UnusedUpdSpace3](#) [2]
 - Offset 0x0106.*

 - UINT32 [SerialloUartRtsPinMuxPolicy](#) [7]
 - Offset 0x0108 - SerialloUartRtsPinMuxPolicy Select Seriallo Uart Rts pin muxing.*

 - UINT32 [SerialloUartCtsPinMuxPolicy](#) [7]
 - Offset 0x0124 - SerialloUartCtsPinMuxPolicy Select Seriallo Uart Cts pin muxing.*

 - UINT32 [SerialloUartRxPinMuxPolicy](#) [7]
 - Offset 0x0140 - SerialloUartRxPinMuxPolicy Select Seriallo Uart Rx pin muxing.*

 - UINT32 [SerialloUartTxPinMuxPolicy](#) [7]
 - Offset 0x015C - SerialloUartTxPinMuxPolicy Select Seriallo Uart Tx pin muxing.*

 - UINT8 [SerialloDebugUartNumber](#)
 - Offset 0x0178 - UART Number For Debug Purpose UART number for debug purpose.*

 - UINT8 [SerialloI2cMode](#) [8]
 - Offset 0x0179 - I2Cn Device Mode Selects I2c operation mode.*

 - UINT8 [UnusedUpdSpace4](#) [3]
 - Offset 0x0181.*

 - UINT32 [PchSerialloI2cSdaPinMux](#) [8]
 - Offset 0x0184 - Serial IO I2C SDA Pin Muxing Select Seriallo I2c Sda pin muxing.*

 - UINT32 [PchSerialloI2cSclPinMux](#) [8]
 - Offset 0x01A4 - Serial IO I2C SCL Pin Muxing Select Seriallo I2c Scl pin muxing.*

 - UINT8 [PchSerialloI2cPadsTermination](#) [8]
 - Offset 0x01C4 - PCH Seriallo I2C Pads Termination 0x0: Hardware default, 0x1: None, 0x13: 1kOhm weak pull-up, 0x15: 5kOhm weak pull-up, 0x19: 20kOhm weak pull-up - Enable/disable Seriallo I2C0,I2C1,...*

 - UINT8 [Usb2PhyPetxiset](#) [16]
 - Offset 0x01CC - USB Per Port HS Preemphasis Bias USB Per Port HS Preemphasis Bias.*

 - UINT8 [Usb2PhyTxiset](#) [16]
-

- Offset 0x01DC - USB Per Port HS Transmitter Bias USB Per Port HS Transmitter Bias.*

 - UINT8 [Usb2PhyPredeemp](#) [16]
- Offset 0x01EC - USB Per Port HS Transmitter Emphasis USB Per Port HS Transmitter Emphasis.*

 - UINT8 [Usb2PhyPehalfbit](#) [16]
- Offset 0x01FC - USB Per Port Half Bit Pre-emphasis USB Per Port Half Bit Pre-emphasis.*

 - UINT8 [Usb3HsioTxDeEmphEnable](#) [10]
- Offset 0x020C - 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 0x0216 - 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 0x0220 - 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 array can be between 0-1.*

 - UINT8 [Usb3HsioTxDownscaleAmp](#) [10]
- Offset 0x022A - 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 0x0234 - Enable LAN Enable/disable LAN controller.*

 - UINT8 [PchTsnEnable](#)
- Offset 0x0235 - Enable PCH TSN Enable/disable TSN on the PCH.*

 - UINT8 [PchHdaAudioLinkHdaEnable](#)
- Offset 0x0236 - Enable HD Audio Link Enable/disable HD Audio Link.*

 - UINT8 [PchHdaAudioLinkDmic0Enable](#)
- Offset 0x0237 - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.*

 - UINT8 [PchHdaAudioLinkDmic1Enable](#)
- Offset 0x0238 - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.*

 - UINT8 [PchHdaAudioLinkSsp0Enable](#)
- Offset 0x0239 - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.*

 - UINT8 [PchHdaAudioLinkSsp1Enable](#)
- Offset 0x023A - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.*

 - UINT8 [PchHdaAudioLinkSsp2Enable](#)
- Offset 0x023B - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.*

 - UINT8 [PchHdaAudioLinkSsp3Enable](#)
- Offset 0x023C - Enable HD Audio SSP3 Link Enable/disable HD Audio SSP3/I2S link.*

 - UINT8 [PchHdaAudioLinkSsp4Enable](#)
- Offset 0x023D - Enable HD Audio SSP4 Link Enable/disable HD Audio SSP4/I2S link.*

 - UINT8 [PchHdaAudioLinkSsp5Enable](#)
- Offset 0x023E - Enable HD Audio SSP5 Link Enable/disable HD Audio SSP5/I2S link.*

 - UINT8 [PchHdaAudioLinkSndw1Enable](#)
- Offset 0x023F - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.*

 - UINT8 [PchHdaAudioLinkSndw2Enable](#)
- Offset 0x0240 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.*

 - UINT8 [PchHdaAudioLinkSndw3Enable](#)
- Offset 0x0241 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.*

 - UINT8 [PchHdaAudioLinkSndw4Enable](#)
- Offset 0x0242 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.*

 - UINT8 [UnusedUpdSpace5](#)
- Offset 0x0243.*

 - UINT32 [PcieRpPtmMask](#)
- Offset 0x0244 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.*

- UINT32 [PcieRpDpcMask](#)
Offset 0x0248 - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.
 - UINT32 [PcieRpDpcExtensionsMask](#)
Offset 0x024C - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.
 - UINT8 [UsbPdoProgramming](#)
Offset 0x0250 - USB PDO Programming Enable/disable PDO programming for USB in PEI phase.
 - UINT8 [UnusedUpdSpace6](#) [3]
Offset 0x0251.
 - UINT32 [PmcPowerButtonDebounce](#)
Offset 0x0254 - Power button debounce configuration Debounce time for PWRBTN in microseconds.
 - UINT8 [PchEspIbmeMasterSlaveEnabled](#)
Offset 0x0258 - PCH eSPI Master and Slave BME enabled PCH eSPI Master and Slave BME enabled \$EN_DIS.
 - UINT8 [SataRstLegacyOrom](#)
Offset 0x0259 - PCH SATA use RST Legacy OROM Use PCH SATA RST Legacy OROM when CSM is Enabled \$EN_DIS.
 - UINT8 [PchFivrExtV1p05RailEnabledStates](#)
Offset 0x025A - Mask to enable the usage of external V1p05 VR rail in specific S0ix or Sx states Enable External V1P05 Rail in: BIT0:S0i1/S0i2, BIT1:S0i3, BIT2:S3, BIT3:S4, BIT5:S5.
 - UINT8 [UnusedUpdSpace7](#)
Offset 0x025B.
 - UINT16 [PchFivrExtV1p05RailVoltage](#)
Offset 0x025C - External V1P05 Voltage Value that will be used in S0i2/S0i3 states Value is given in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...)
 - UINT8 [PchFivrExtV1p05RailIccMax](#)
Offset 0x025E - External V1P05 Icc Max Value Granularity of this setting is 1mA and maximal possible value is 200mA.
 - UINT8 [PchFivrExtVnnRailEnabledStates](#)
Offset 0x025F - Mask to enable the usage of external Vnn VR rail in specific S0ix or Sx states Enable External Vnn Rail in: BIT0:S0i1/S0i2, BIT1:S0i3, BIT2:S3, BIT3:S4, BIT5:S5.
 - UINT16 [PchFivrExtVnnRailVoltage](#)
Offset 0x0260 - External Vnn Voltage Value that will be used in S0ix/Sx states Value is given in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...)
 - UINT8 [PchFivrExtVnnRailIccMax](#)
Offset 0x0262 - External Vnn Icc Max Value that will be used in S0ix/Sx states Granularity of this setting is 1mA and maximal possible value is 200mA.
 - UINT8 [PchFivrExtVnnRailSxEnabledStates](#)
Offset 0x0263 - Mask to enable the usage of external Vnn VR rail in Sx states Use only if Ext Vnn Rail config is different in Sx.
 - UINT16 [PchFivrExtVnnRailSxVoltage](#)
Offset 0x0264 - External Vnn Voltage Value that will be used in Sx states Use only if Ext Vnn Rail config is different in Sx.
 - UINT8 [PchFivrExtVnnRailSxIccMax](#)
Offset 0x0266 - External Vnn Icc Max Value that will be used in Sx states Use only if Ext Vnn Rail config is different in Sx.
 - UINT8 [PchFivrVccinAuxLowToHighCurModeVolTranTime](#)
Offset 0x0267 - Transition time in microseconds from Low Current Mode Voltage to High Current Mode Voltage This field has 1us resolution.
 - UINT8 [PchFivrVccinAuxRetToHighCurModeVolTranTime](#)
Offset 0x0268 - Transition time in microseconds from Retention Mode Voltage to High Current Mode Voltage This field has 1us resolution.
 - UINT8 [PchFivrVccinAuxRetToLowCurModeVolTranTime](#)
Offset 0x0269 - Transition time in microseconds from Retention Mode Voltage to Low Current Mode Voltage This field has 1us resolution.
-

- UINT16 [PchFivrVccinAuxOffToHighCurModeVolTranTime](#)
Offset 0x026A - Transition time in microseconds from Off (0V) to High Current Mode Voltage This field has 1us resolution.
 - UINT32 [TraceHubMemBase](#)
Offset 0x026C - Trace Hub Memory Base If Trace Hub is enabled and trace to memory is desired, BootLoader needs to allocate trace hub memory as reserved and uncacheable, set the base to ensure Trace Hub memory is configured properly.
 - UINT8 [PmcDbgMsgEn](#)
Offset 0x0270 - PMC Debug Message Enable When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug meesages to trace hub.
 - UINT8 [PchFivrDynPm](#)
Offset 0x0271 - FIVR Dynamic Power Management Enable/Disable FIVR Dynamic Power Management.
 - UINT8 [SdCardOverrideDefaultDll](#)
Offset 0x0272 - SdCard override default DLL Enable/Disable override on default DLL values \$EN_DIS.
 - UINT8 [SdCardSdr50RxDelay125ps](#)
Offset 0x0273 - SdCard SDR50 delay Value of the delay for SDR50 speed in 125ps multiple.
 - UINT8 [SdCardDdr50RxDelay125ps](#)
Offset 0x0274 - SdCard DDR50 delay Value of the delay for DDR50 speed in 125ps multiple.
 - UINT8 [UnusedUpdSpace8](#) [3]
Offset 0x0275.
 - UINT32 [PchHdaAudioLinkDmic0ClkAPinMux](#)
Offset 0x0278 - DMIC0 ClkA Pin Muxing Determines DMIC0 ClkA Pin muxing.
 - UINT8 [PchPostMemRsvd](#) [2]
Offset 0x027C - PchPostMemRsvd Reserved for PCH Post-Mem \$EN_DIS.
 - UINT8 [CnviMode](#)
Offset 0x027E - CNVi Configuration This option allows for automatic detection of Connectivity Solution.
 - UINT8 [CnviBtCore](#)
Offset 0x027F - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.
 - UINT8 [CnviBtAudioOffload](#)
Offset 0x0280 - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.
 - UINT8 [UnusedUpdSpace9](#) [3]
Offset 0x0281.
 - UINT32 [CnviRfResetPinMux](#)
Offset 0x0284 - CNVi RF_RESET pin muxing Select CNVi RF_RESET# pin depending on board routing.
 - UINT32 [CnviClkreqPinMux](#)
Offset 0x0288 - CNVi CLKREQ pin muxing Select CNVi CLKREQ pin depending on board routing.
 - UINT8 [PchEspIHostC10ReportEnable](#)
Offset 0x028C - Enable Host C10 reporting through eSPI Enable/disable Host C10 reporting to Slave via eSPI Virtual Wire.
 - UINT8 [PmcUsb2PhySusPgEnable](#)
Offset 0x028D - PCH USB2 PHY Power Gating enable 1: Will enable USB2 PHY SUS Well Power Gating, 0: Will not enable PG of USB2 PHY Sus Well PG \$EN_DIS.
 - UINT8 [PchUsbOverCurrentEnable](#)
Offset 0x028E - PCH USB OverCurrent mapping enable 1: Will program USB OC pin mapping in xHCI controller memory, 0: Will clear OC pin mapping allow for NOA usage of OC pins \$EN_DIS.
 - UINT8 [CnviMfUart1Type](#)
Offset 0x028F - CNVi MfUart1 Type This option configures Uart type which connects to MfUart1 0:ISH Uart0, 1↔:SerialIO Uart2, 2:Uart over external pads.
 - UINT8 [PchEspILgmrEnable](#)
Offset 0x0290 - Espi Lgmr Memory Range decode This option enables or disables espi lgmr \$EN_DIS.
 - UINT8 [UnusedUpdSpace10](#) [3]
Offset 0x0291.
-

- UINT32 [PchHdaAudioLinkDmic0ClkBPinMux](#)
Offset 0x0294 - DMIC0 ClkB Pin Muxing Determines DMIC0 ClkA Pin muxing.
 - UINT8 [PchFivrExtV1p05RailCtrlRampTmr](#)
Offset 0x0298 - External V1P05 Control Ramp Timer value Hold off time to be used when changing the v1p05_ctrl for external bypass value in us.
 - UINT8 [PchFivrExtVnnRailCtrlRampTmr](#)
Offset 0x0299 - External VNN Control Ramp Timer value Hold off time to be used when changing the vnn_ctrl for external bypass value in us.
 - UINT8 [Heci3Enabled](#)
Offset 0x029A - HECI3 state The HECI3 state from Mbp for reference in S3 path or when MbpHob is not installed.
 - UINT8 [PchHotEnable](#)
Offset 0x029B - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.
 - UINT8 [SataLedEnable](#)
Offset 0x029C - SATA LED SATA LED indicating SATA controller activity.
 - UINT8 [PchPmVrAlert](#)
Offset 0x029D - VRAAlert# Pin When VRAAlert# feature pin is enabled and its state is '0', the PMC requests throttling to a T3 Tstate to the PCH throttling unit.
 - UINT8 [PchPmSlpS0VmRuntimeControl](#)
Offset 0x029E - SLP_S0 VM Dynamic Control SLP_S0 Voltage Margining Runtime Control Policy.
 - UINT8 [PchPmSlpS0Vm070VSupport](#)
Offset 0x029F - SLP_S0 VM 0.70V Support SLP_S0 Voltage Margining 0.70V Support Policy.
 - UINT8 [PchPmSlpS0Vm075VSupport](#)
Offset 0x02A0 - SLP_S0 VM 0.75V Support SLP_S0 Voltage Margining 0.75V Support Policy.
 - UINT8 [AmtEnabled](#)
Offset 0x02A1 - AMT Switch Enable/Disable.
 - UINT8 [WatchDog](#)
Offset 0x02A2 - WatchDog Timer Switch Enable/Disable.
 - UINT8 [AsfEnabled](#)
Offset 0x02A3 - ASF Switch Enable/Disable.
 - UINT8 [ManageabilityMode](#)
Offset 0x02A4 - Manageability Mode set by Mebx Enable/Disable.
 - UINT8 [FwProgress](#)
Offset 0x02A5 - PET Progress Enable/Disable.
 - UINT8 [AmtSolEnabled](#)
Offset 0x02A6 - SOL Switch Enable/Disable.
 - UINT8 [UnusedUpdSpace11](#)
Offset 0x02A7.
 - UINT16 [WatchDogTimerOs](#)
Offset 0x02A8 - OS Timer 16 bits Value, Set OS watchdog timer.
 - UINT16 [WatchDogTimerBios](#)
Offset 0x02AA - BIOS Timer 16 bits Value, Set BIOS watchdog timer.
 - UINT8 [RemoteAssistance](#)
Offset 0x02AC - Remote Assistance Trigger Availabilty Enable/Disable.
 - UINT8 [AmtKvmEnabled](#)
Offset 0x02AD - KVM Switch Enable/Disable.
 - UINT8 [ForcMebxSyncUp](#)
Offset 0x02AE - KVM Switch Enable/Disable.
 - UINT8 [PcieRpSlotImplemented](#) [24]
Offset 0x02AF - PCH PCIe root port connection type 0: built-in device, 1:slot.
 - UINT8 [PcieClkSrcUsage](#) [16]
-

- Offset 0x02C7 - Usage type for ClkSrc 0-23: PCH rootport, 0x40-0x43: PEG port, 0x70:LAN, 0x80: unspecified but in use (free running), 0xFF: not used.
- UINT8 [PcieClkSrcClkReq](#) [16]

Offset 0x02D7 - ClkReq-to-ClkSrc mapping Number of ClkReq signal assigned to ClkSrc.
 - UINT8 [PcieRpAcsEnabled](#) [24]

Offset 0x02E7 - PCIE RP Access Control Services Extended Capability Enable/Disable PCIE RP Access Control Services Extended Capability.
 - UINT8 [PcieRpEnableCpm](#) [24]

Offset 0x02FF - PCIE RP Clock Power Management Enable/Disable PCIE RP Clock Power Management, even if disabled, CLKREQ# signal can still be controlled by L1 PM substates mechanism.
 - UINT8 [UnusedUpdSpace12](#) [1]

Offset 0x0317.
 - UINT16 [PcieRpDetectTimeoutMs](#) [24]

Offset 0x0318 - PCIE RP Detect Timeout Ms The number of milliseconds within 0~65535 in reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
 - UINT8 [PmcModPhySusPgEnable](#)

Offset 0x0348 - ModPHY SUS Power Domain Dynamic Gating Enable/Disable ModPHY SUS Power Domain Dynamic Gating.
 - UINT8 [PmcV1p05PhyExtFetControlEn](#)

Offset 0x0349 - V1p05-PHY supply external FET control Enable/Disable control using EXT_PWR_GATE# pin of external FET to power gate v1p05-PHY supply.
 - UINT8 [PmcV1p05IsExtFetControlEn](#)

Offset 0x034A - V1p05-IS supply external FET control Enable/Disable control using EXT_PWR_GATE2# pin of external FET to power gate v1p05-IS supply.
 - UINT8 [CridEnable](#)

Offset 0x034B - Enable/Disable SA CRID Enable: SA CRID, Disable (Default): SA CRID \$EN_DIS.
 - UINT8 [PavpEnable](#)

Offset 0x034C - Enable/Disable PavpEnable Enable(Default): Enable PavpEnable, Disable: Disable PavpEnable \$EN_DIS.
 - UINT8 [CdClock](#)

Offset 0x034D - CdClock Frequency selection 0 (Default) Auto (Max based on reference clock frequency), 0: 307.2, 1: 312 Mhz, 2: 552 Mhz, 3: 556.8 Mhz, 4: 648 Mhz, 5: 652.8 Mhz 0xFF: Auto (Max based on reference clock frequency), 0: 307.2, 1: 312 Mhz, 2: 552 Mhz, 3: 556.8 Mhz, 4: 648 Mhz, 5: 652.8 Mhz.
 - UINT8 [PeiGraphicsPeimInit](#)

Offset 0x034E - Enable/Disable PeiGraphicsPeimInit Enable: Enable PeiGraphicsPeimInit, Disable(Default): Disable PeiGraphicsPeimInit \$EN_DIS.
 - UINT8 [D3HotEnable](#)

Offset 0x034F - Enable D3 Hot in TCSS This policy will enable/disable D3 hot support in IOM \$EN_DIS.
 - UINT8 [GnaEnable](#)

Offset 0x0350 - Enable or disable GNA device 0=Disable, 1(Default)=Enable \$EN_DIS.
 - UINT8 [X2ApicOptOut](#)

Offset 0x0351 - State of X2APIC_OPT_OUT bit in the DMAR table 0=Disable/Clear, 1=Enable/Set \$EN_DIS.
 - UINT8 [UnusedUpdSpace13](#) [2]

Offset 0x0352.
 - UINT32 [VtdBaseAddress](#) [2]

Offset 0x0354 - Base addresses for VT-d function MMIO access Base addresses for VT-d MMIO access per VT-d engine.
 - UINT8 [DdiPortAConfig](#)

Offset 0x035C - Enable or disable HPD of DDI port-A device 0=Disabled,1(Default)=eDP, 2=MIPI DSI 0:Disabled, 1:eDP, 2:MIPI DSI.
 - UINT8 [DdiPortBHpd](#)

Offset 0x035D - Enable or disable HPD of DDI port B 0=Disable, 1(Default)=Enable \$EN_DIS.
 - UINT8 [DdiPortCHpd](#)
-

- Offset 0x035E - Enable or disable HPD of DDI port C 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPort1Hpd](#)
- Offset 0x035F - Enable or disable HPD of DDI port 1 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPort2Hpd](#)
- Offset 0x0360 - Enable or disable HPD of DDI port 2 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPort3Hpd](#)
- Offset 0x0361 - Enable or disable HPD of DDI port 3 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPort4Hpd](#)
- Offset 0x0362 - Enable or disable HPD of DDI port 4 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPortBDdc](#)
- Offset 0x0363 - Enable or disable DDC of DDI port B 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPortCDdc](#)
- Offset 0x0364 - Enable or disable DDC of DDI port C 0=Disable, 1(Default)=Enable \$EN_DIS.*

 - UINT8 [DdiPort1Ddc](#)
- Offset 0x0365 - Enable DDC setting of DDI Port 1 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.*

 - UINT8 [DdiPort2Ddc](#)
- Offset 0x0366 - Enable DDC setting of DDI Port 2 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.*

 - UINT8 [DdiPort3Ddc](#)
- Offset 0x0367 - Enable DDC setting of DDI Port 3 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.*

 - UINT8 [DdiPort4Ddc](#)
- Offset 0x0368 - Enable DDC setting of DDI Port 4 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.*

 - UINT8 [UnusedUpdSpace14](#) [3]
- Offset 0x0369.*

 - UINT32 [IomTypeCPortPadCfg](#) [12]
- Offset 0x036C - TypeC port GPIO setting GPIO Ping number for Type C Aux Orientation setting, use the GpioPad that is defined in GpioPinsXXXH.h and GpioPinsXXXLp.h as argument.*

 - UINT8 [CpuUsb3OverCurrentPin](#) [8]
- Offset 0x039C - CPU USB3 Port Over Current Pin Describe the specific over current pin number of USBC Port N.*

 - UINT8 [D3ColdEnable](#)
- Offset 0x03A4 - Enable D3 Cold in TCSS This policy will enable/disable D3 cold support in IOM \$EN_DIS.*

 - UINT8 [UnusedUpdSpace15](#) [3]
- Offset 0x03A5.*

 - UINT32 [PchHdaAudioLinkDmic0DataPinMux](#)
- Offset 0x03A8 - DMIC0 Data Pin Muxing Determines DMIC0 Data Pin muxing.*

 - UINT8 [VmdEnable](#)
- Offset 0x03AC - Enable VMD controller Enable/disable to VMD controller.*

 - UINT8 [VmdPortA](#)
- Offset 0x03AD - Enable VMD portA Support Enable/disable to VMD portA Support.*

 - UINT8 [VmdPortB](#)
- Offset 0x03AE - Enable VMD portB Support Enable/disable to VMD portB Support.*

 - UINT8 [VmdPortC](#)
- Offset 0x03AF - Enable VMD portC Support Enable/disable to VMD portC Support.*

 - UINT8 [VmdPortD](#)
- Offset 0x03B0 - Enable VMD portD Support Enable/disable to VMD portD Support.*

 - UINT8 [VmdCfgBarSz](#)
- Offset 0x03B1 - VMD Config Bar size Set The VMD Config Bar Size.*

 - UINT8 [VmdCfgBarAttr](#)
- Offset 0x03B2 - VMD Config Bar Attributes 0: VMD_32BIT_NONPREFETCH, 1: VMD_64BIT_NONPREFETCH, 2: VMD_64BIT_PREFETCH(Default) 0: VMD_32BIT_NONPREFETCH, 1: VMD_64BIT_NONPREFETCH, 2: VMD_↔64BIT_PREFETCH.*

 - UINT8 [VmdMemBarSz1](#)

- Offset 0x03B3 - VMD Mem Bar1 size Set The VMD Mem Bar1 Size.*

 - UINT8 [VmdMemBar1Attr](#)

Offset 0x03B4 - VMD Mem Bar1 Attributes 0: VMD_32BIT_NONPREFETCH(Default), 1: VMD_64BIT_NONPREFETCH, 2: VMD_64BIT_PREFETCH 0: VMD_32BIT_NONPREFETCH, 1: VMD_64BIT_NONPREFETCH, 2: VMD_64BIT_PREFETCH.
 - UINT8 [VmdMemBarSz2](#)

Offset 0x03B5 - VMD Mem Bar2 size Set The VMD Mem Bar2 Size.
 - UINT8 [VmdMemBar2Attr](#)

Offset 0x03B6 - VMD Mem Bar2 Attributes 0: VMD_32BIT_NONPREFETCH, 1: VMD_64BIT_NONPREFETCH(Default), 2: VMD_64BIT_PREFETCH 0: VMD_32BIT_NONPREFETCH, 1: VMD_64BIT_NONPREFETCH, 2: VMD_64BIT_PREFETCH.
 - UINT8 [PmcPdEnable](#)

Offset 0x03B7 - Enable/Disable PMC-PD Solution This policy will enable/disable PMC-PD Solution vs EC-TCPC Solution \$EN_DIS.
 - UINT16 [TcssAuxOri](#)

Offset 0x03B8 - TCSS Aux Orientation Override Enable Bits 0, 2, ...
 - UINT16 [TcssHslOri](#)

Offset 0x03BA - TCSS HSL Orientation Override Enable Bits 0, 2, ...
 - UINT8 [UsbOverride](#)

Offset 0x03BC - USB override in IOM This policy will enable/disable USB Connect override in IOM \$EN_DIS.
 - UINT8 [UsbTcPortEn](#)

Offset 0x03BD - TCSS USB Port Enable Bits 0, 1, ...
 - UINT8 [ITbtPcieRootPortEn](#) [6]

Offset 0x03BE - ITBT Root Port Enable ITBT Root Port Enable, 0:Disable, 1:Enable 0:Disable, 1:Enable.
 - UINT16 [ITbtForcePowerOnTimeoutInMs](#)

Offset 0x03C4 - ITBTForcePowerOn Timeout value ITBTForcePowerOn value.
 - UINT16 [ITbtConnectTopologyTimeoutInMs](#)

Offset 0x03C6 - ITbtConnectTopology Timeout value ITbtConnectTopologyTimeout value.
 - UINT8 [VccSt](#)

Offset 0x03C8 - VCCST request for IOM This policy will enable/disable VCCST and also decides if message would be replayed in S4/S5 \$EN_DIS.
 - UINT8 [CpuCrashLogEnable](#)

Offset 0x03C9 - Enable/Disable CrashLog Enable(Default): Enable CPU CrashLog, Disable: Disable CPU CrashLog \$EN_DIS.
 - UINT8 [AesEnable](#)

*Offset 0x03CA - Advanced Encryption Standard (AES) feature Enable or Disable Advanced Encryption Standard (AES) feature; 0: Disable; 1: **Enable** \$EN_DIS.*
 - UINT8 [Psi3Enable](#) [5]

*Offset 0x03CB - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; 1: **Enable**.*
 - UINT8 [Psi4Enable](#) [5]

*Offset 0x03D0 - 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 0x03D5 - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.
 - UINT8 [ImonOffset](#) [5]

Offset 0x03DA - Imon offset correction PCODE MMIO Mailbox: Imon offset correction.
 - UINT8 [VrConfigEnable](#) [5]

*Offset 0x03DF - Enable/Disable BIOS configuration of VR Enable/Disable BIOS configuration of VR; 0: **Disable**; 1: **Enable**.For all VR Indexes.*
 - UINT8 [TdcEnable](#) [5]

*Offset 0x03E4 - 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 0x03E9 - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.
 - UINT8 [TdcLock](#) [5]
*Offset 0x03EE - Thermal Design Current Lock PCODE MMIO Mailbox: Thermal Design Current Lock; **0: Disable**; 1: Enable.* For all VR Indexes.
 - UINT8 [PsysSlope](#)
Offset 0x03F3 - Platform Psys slope correction PCODE MMIO Mailbox: Platform Psys slope correction.
 - UINT8 [PsysOffset](#)
Offset 0x03F4 - Platform Psys offset correction PCODE MMIO Mailbox: Platform Psys offset correction.
 - UINT8 [AcousticNoiseMitigation](#)
Offset 0x03F5 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.
 - UINT8 [FastPkgCRampDisableIa](#)
Offset 0x03F6 - 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 0x03F7 - 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 0x03F8 - 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 0x03F9 - 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.
 - UINT16 [TdcPowerLimit](#) [5]
Offset 0x03FA - Thermal Design Current current limit PCODE MMIO Mailbox: Thermal Design Current current limit.
 - UINT16 [AcLoadline](#) [5]
Offset 0x0404 - AcLoadline PCODE MMIO Mailbox: AcLoadline in 1/100 mOhms (ie.
 - UINT16 [DcLoadline](#) [5]
Offset 0x040E - DcLoadline PCODE MMIO Mailbox: DcLoadline in 1/100 mOhms (ie.
 - UINT16 [Psi1Threshold](#) [5]
Offset 0x0418 - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cutoff in 1/4 Amp increments.
 - UINT16 [Psi2Threshold](#) [5]
Offset 0x0422 - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cutoff in 1/4 Amp increments.
 - UINT16 [Psi3Threshold](#) [5]
Offset 0x042C - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cutoff in 1/4 Amp increments.
 - UINT16 [IccMax](#) [5]
Offset 0x0436 - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.
 - UINT16 [VrVoltageLimit](#) [5]
Offset 0x0440 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.
 - UINT8 [FastPkgCRampDisableGt](#)
Offset 0x044A - 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 0x044B - Disable Fast Slew Rate for Deep Package C States for VR SA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.
 - UINT8 [SendVrMbxCmd](#)
Offset 0x044C - Enable VR specific mailbox command VR specific mailbox commands.
 - UINT8 [Reserved2](#)
Offset 0x044D - Reserved Reserved.
 - UINT8 [TxtEnable](#)
-

- Offset 0x044E - Enable or Disable TXT Enable or Disable TXT; 0: Disable; 1: **Enable**.*
 - UINT8 [SkipMplInit](#)
 - Offset 0x044F - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SilicionInit API.*
 - UINT16 [FivrRfiFrequency](#)
 - Offset 0x0450 - FIVR RFI Frequency PCODE MMIO Mailbox: Set the desired RFI frequency, in increments of 100KHz.*
 - UINT8 [FivrSpreadSpectrum](#)
 - Offset 0x0452 - FIVR RFI Spread Spectrum PCODE MMIO Mailbox: FIVR RFI Spread Spectrum, in 0.1% increments.*
 - UINT8 [FastPkgCRampDisableFivr](#)
 - Offset 0x0453 - Disable Fast Slew Rate for Deep Package C States for VR FIVR domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.*
 - UINT8 [SlowSlewRateForFivr](#)
 - Offset 0x0454 - Slew Rate configuration for Deep Package C States for VR FIVR domain Slew Rate configuration for Deep Package C States for VR FIVR domain based on Acoustic Noise Mitigation feature enabled.*
 - UINT8 [UnusedUpdSpace16](#) [3]
 - Offset 0x0455.*
 - UINT32 [CpuBistData](#)
 - Offset 0x0458 - CpuBistData Pointer CPU BIST Data.*
 - UINT8 [PpinSupport](#)
 - Offset 0x045C - PpinSupport to view Protected Processor Inventory Number Enable or Disable or Auto (Based on End of Manufacturing flag.*
 - UINT8 [EnableMinVoltageOverride](#)
 - Offset 0x045D - Enable or Disable Minimum Voltage Override Enable or disable Minimum Voltage overrides ; 0: **Disable**; 1: Enable.*
 - UINT16 [MinVoltageRuntime](#)
 - Offset 0x045E - Min Voltage for Runtime PCODE MMIO Mailbox: Minimum voltage for runtime.*
 - UINT16 [MinVoltageC8](#)
 - Offset 0x0460 - Min Voltage for C8 PCODE MMIO Mailbox: Minimum voltage for C8.*
 - UINT8 [ReservedCpuPostMemProduction](#) [8]
 - Offset 0x0462 - ReservedCpuPostMemProduction Reserved for CPU Post-Mem Production \$EN_DIS.*
 - UINT8 [PchPwrOptEnable](#)
 - Offset 0x046A - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.*
 - UINT8 [PchWriteProtectionEnable](#) [5]
 - Offset 0x046B - PCH Flash Protection Ranges Write Enble Write or erase is blocked by hardware.*
 - UINT8 [PchReadProtectionEnable](#) [5]
 - Offset 0x0470 - PCH Flash Protection Ranges Read Enble Read is blocked by hardware.*
 - UINT8 [UnusedUpdSpace17](#) [1]
 - Offset 0x0475.*
 - UINT16 [PchProtectedRangeLimit](#) [5]
 - Offset 0x0476 - 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 0x0480 - PCH Protect Range Base Left shifted address by 12 bits with address bits 11:0 are assumed to be 0.*
 - UINT8 [PchHdaPme](#)
 - Offset 0x048A - Enable Pme Enable Azalia wake-on-ring.*
 - UINT8 [PchHdaVcType](#)
 - Offset 0x048B - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.*
 - UINT8 [PchHdaLinkFrequency](#)
 - Offset 0x048C - HD Audio Link Frequency HDA Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 0: 6MHz, 1: 12MHz, 2: 24MHz.*
 - UINT8 [PchHdaIDisplinkFrequency](#)
-

- Offset 0x048D - *iDisp-Link Frequency iDisp-Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 4: 96MHz, 3: 48MHz.*
- UINT8 [PchHdaDispLinkTmode](#)
Offset 0x048E - *iDisp-Link T-mode iDisp-Link T-Mode (PCH_HDAUDIO_IDISP_TMODE enum): 0: 2T, 2: 4T, 3: 8T, 4: 16T 0: 2T, 2: 4T, 3: 8T, 4: 16T.*
 - UINT8 [PchHdaDspUaaCompliance](#)
Offset 0x048F - *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 [PchHdaDispCodecDisconnect](#)
Offset 0x0490 - *iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.*
 - UINT8 [PchIshSpiCs0Enable](#) [1]
Offset 0x0491 - *Enable PCH ISH SPI Cs0 pins assigned Set if ISH SPI Cs0 pins are to be enabled by BIOS.*
 - UINT8 [UnusedUpdSpace18](#) [2]
Offset 0x0492.
 - UINT32 [PchHdaAudioLinkDmic1ClkAPinMux](#)
Offset 0x0494 - *DMIC1 ClkA Pin Muxing Determines DMIC1 ClkA RstA Pin muxing.*
 - UINT32 [PchHdaAudioLinkDmic1ClkBPinMux](#)
Offset 0x0498 - *DMIC1 Data Pin Muxing Determines DMIC1 Data Pin muxing.*
 - UINT32 [PchHdaAudioLinkDmic1DataPinMux](#)
Offset 0x049C - *DMIC1 Data Pin Muxing Determines DMIC0 Data Pin muxing.*
 - UINT8 [PchIoApicEntry24_119](#)
Offset 0x04A0 - *Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.*
 - UINT8 [PchIoApicId](#)
Offset 0x04A1 - *PCH Io Apic ID This member determines IOAPIC ID.*
 - UINT8 [PchIshSpiEnable](#) [1]
Offset 0x04A2 - *Enable PCH ISH SPI pins assigned Set if ISH SPI native pins are to be enabled by BIOS.*
 - UINT8 [PchIshUartEnable](#) [2]
Offset 0x04A3 - *Enable PCH ISH UART pins assigned Set if ISH UART native pins are to be enabled by BIOS.*
 - UINT8 [PchIshI2cEnable](#) [3]
Offset 0x04A5 - *Enable PCH ISH I2C pins assigned Set if ISH I2C native pins are to be enabled by BIOS.*
 - UINT8 [PchIshGpEnable](#) [8]
Offset 0x04A8 - *Enable PCH ISH GP pins assigned Set if ISH GP native pins are to be enabled by BIOS.*
 - UINT8 [PchIshPdtUnlock](#)
Offset 0x04B0 - *PCH ISH PDT Unlock Msg 0: False; 1: True.*
 - UINT8 [PchOseI2sEnable](#) [2]
Offset 0x04B1 - *Enable PCH OSE I2S pins assigned Set if OSE I2S native pins are to be enabled by BIOS.*
 - UINT8 [PchOsePwmEnable](#)
Offset 0x04B3 - *Enable PCH OSE PWM pins assigned Set if OSE PWM native pins are to be enabled by BIOS.*
 - UINT8 [PchOseUartEnable](#) [6]
Offset 0x04B4 - *Enable PCH OSE UART pins assigned Set if OSE UART native pins are to be enabled by BIOS.*
 - UINT8 [PchOseHsuartEnable](#) [4]
Offset 0x04BA - *Enable PCH OSE HSUART pins assigned Set if OSE HSUART native pins are to be enabled by BIOS.*
 - UINT8 [PchOseQepEnable](#) [4]
Offset 0x04BE - *Enable PCH OSE QEP pins assigned Set if OSE QEP native pins are to be enabled by BIOS.*
 - UINT8 [PchOseI2cEnable](#) [8]
Offset 0x04C2 - *Enable PCH OSE I2C pins assigned Set if OSE I2C native pins are to be enabled by BIOS.*
 - UINT8 [PchOseSpiEnable](#) [4]
Offset 0x04CA - *Enable PCH OSE SPI pins assigned Set if OSE SPI native pins are to be enabled by BIOS.*
 - UINT8 [PchOseSpiCs0Enable](#) [4]
Offset 0x04CE - *Enable PCH OSE SPI CS0 pins assigned Set if OSE SPI CS0 pins are to be enabled by BIOS.*
-

- UINT8 [PchOseAdcEnable](#)
Offset 0x04D2 - Enable PCH OSE ADC pins assigned Set if OSE ADC native pins are to be enabled by BIOS.
 - UINT8 [PchOseCanEnable](#) [2]
Offset 0x04D3 - Enable PCH OSE CAN pins assigned Set if OSE CAN native pins are to be enabled by BIOS.
 - UINT8 [PchOseTimedGpioEnable](#) [2]
Offset 0x04D5 - Enable PCH OSE Timed GPIO pins assigned Set if OSE Timed GPIO native pins are to be enabled by BIOS.
 - UINT8 [PchOseTimedGpioPinAllocation](#) [2]
Offset 0x04D7 - Enable PCH OSE Timed GPIO 20 pins allocation Allocate 20 pins for PCH OSE Timed GPIO.
 - UINT8 [PchOseTimedGpioPinEnable](#) [60]
Offset 0x04D9 - Enable PCH OSE Timed GPIO Pin to OSE TGPIO native function Set TGPIO pin to OSE TGPIO native function.
 - UINT8 [PchLanLtrEnable](#)
Offset 0x0515 - Enable PCH Lan LTR capability of PCH internal LAN 0: Disable; 1: Enable.
 - UINT8 [PchLockDownBiosLock](#)
Offset 0x0516 - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:RegD←→ Ch[5]) for the BIOS region protection.
 - UINT8 [PchCrid](#)
Offset 0x0517 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.
 - UINT8 [RtcBiosInterfaceLock](#)
Offset 0x0518 - RTC BIOS Interface Lock Enable RTC BIOS interface lock.
 - UINT8 [RtcMemoryLock](#)
Offset 0x0519 - RTC Cmos Memory Lock Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.
 - UINT8 [PcieRpHotPlug](#) [24]
Offset 0x051A - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.
 - UINT8 [PcieRpPmSci](#) [24]
Offset 0x0532 - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.
 - UINT8 [PcieRpExtSync](#) [24]
Offset 0x054A - Enable PCIE RP Ext Sync Indicate whether the extended synch is enabled.
 - UINT8 [PcieRpTransmitterHalfSwing](#) [24]
Offset 0x0562 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.
 - UINT8 [PcieRpClkReqDetect](#) [24]
Offset 0x057A - Enable PCIE RP Clk Req Detect Probe CLKREQ# signal before enabling CLKREQ# based power management.
 - UINT8 [PcieRpAdvancedErrorReporting](#) [24]
Offset 0x0592 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.
 - UINT8 [PcieRpUnsupportedRequestReport](#) [24]
Offset 0x05AA - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.
 - UINT8 [PcieRpFatalErrorReport](#) [24]
Offset 0x05C2 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.
 - UINT8 [PcieRpNoFatalErrorReport](#) [24]
Offset 0x05DA - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.
 - UINT8 [PcieRpCorrectableErrorReport](#) [24]
Offset 0x05F2 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.
 - UINT8 [PcieRpSystemErrorOnFatalError](#) [24]
Offset 0x060A - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.
 - UINT8 [PcieRpSystemErrorOnNonFatalError](#) [24]
Offset 0x0622 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.
-

- UINTE8 [PcieRpSystemErrorOnCorrectableError](#) [24]

Offset 0x063A - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.
- UINTE8 [PcieRpMaxPayload](#) [24]

Offset 0x0652 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH_PCIE_MAX_PAYLOAD.
- UINTE8 [ThcPort0Assignment](#)

Offset 0x066A - Touch Host Controller Port 0 Assignment Assign THC Port 0 0x0:ThcAssignmentNone, 0x1:ThcAssignmentThc0.
- UINTE8 [ThcPort0ReadFrequency](#)

Offset 0x066B - Touch Host Controller Port 0 ReadFrequency Set THC Port 0 Read Frequency (THC_PORT_FREQUENCY enum): 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz.
- UINTE8 [ThcPort0WriteFrequency](#)

Offset 0x066C - Touch Host Controller Port 0 WriteFrequency Set THC Port 0 Write Frequency (THC_PORT_FREQUENCY enum): 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz.
- UINTE8 [UnusedUpdSpace19](#) [3]

Offset 0x066D.
- UINTE32 [ThcPort0InterruptPinMuxing](#)

Offset 0x0670 - THC Port 0 Interrupt Pin Mux Set THC Port 0 Pin Muxing Value if signal can be enabled on multiple pads.
- UINTE8 [ThcPort1Assignment](#)

Offset 0x0674 - Touch Host Controller Port 1 Assignment Assign THC Port 1 0x0:ThcAssignmentNone, 0x1:ThcAssignmentThc0, 0x2:ThcAssignmentThc1.
- UINTE8 [ThcPort1ReadFrequency](#)

Offset 0x0675 - Touch Host Controller Port 1 ReadFrequency Set THC Port 1 Read Frequency (THC_PORT_FREQUENCY enum): 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz.
- UINTE8 [ThcPort1WriteFrequency](#)

Offset 0x0676 - Touch Host Controller Port 1 WriteFrequency Set THC Port 1 Write Frequency (THC_PORT_FREQUENCY enum): 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz 0:2p1MHz,1:2p5Mz,2:3Mz,3:3p75Mz,4:5MHz,5:7p5MHz,6:15MHz,7:17MHz,8:20MHz,9:24MHz,10:30MHz.
- UINTE8 [UnusedUpdSpace20](#)

Offset 0x0677.
- UINTE32 [ThcPort1InterruptPinMuxing](#)

Offset 0x0678 - THC Port 1 Interrupt Pin Mux Set THC Port 1 Pin Muxing Value if signal can be enabled on multiple pads.
- UINTE8 [PcieRpPcieSpeed](#) [24]

Offset 0x067C - PCIE RP Pcie Speed Determines each PCIE Port speed capability.
- UINTE8 [PcieRpGen3EqPh3Method](#) [24]

Offset 0x0694 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_METHOD).
- UINTE8 [PcieRpPhysicalSlotNumber](#) [24]

Offset 0x06AC - PCIE RP Physical Slot Number Indicates the slot number for the root port.
- UINTE8 [PcieRpCompletionTimeout](#) [24]

Offset 0x06C4 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_TIMEOUT).
- UINTE8 [PcieRpAspm](#) [24]

Offset 0x06DC - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).
- UINTE8 [PcieRpL1Substates](#) [24]

- Offset 0x06F4 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUB← STATES_CONTROL).*
- UINT8 [PcieRpLtrEnable](#) [24]
Offset 0x070C - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.
 - UINT8 [PcieRpLtrConfigLock](#) [24]
Offset 0x0724 - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.
 - UINT8 [PcieEqPh3LaneParamCm](#) [24]
Offset 0x073C - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.
 - UINT8 [PcieEqPh3LaneParamCp](#) [24]
Offset 0x0754 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.
 - UINT8 [PcieSwEqCoeffListCm](#) [5]
Offset 0x076C - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.
 - UINT8 [PcieSwEqCoeffListCp](#) [5]
Offset 0x0771 - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.
 - UINT8 [PcieDisableRootPortClockGating](#)
Offset 0x0776 - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.
 - UINT8 [PcieEnablePeerMemoryWrite](#)
Offset 0x0777 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.
 - UINT8 [PcieComplianceTestMode](#)
Offset 0x0778 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.
 - UINT8 [PcieRpFunctionSwap](#)
Offset 0x0779 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.
 - UINT8 [SaPcieGen3ProgramStaticEq](#)
Offset 0x077A - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program Gen3 EQ Phase1 Static Presets.
 - UINT8 [SaPcieGen4ProgramStaticEq](#)
Offset 0x077B - Enable/Disable GEN4 Static EQ Phase1 programming Program Gen4 EQ Phase1 Static Presets.
 - UINT8 [PchPmPmeB0S5Dis](#)
Offset 0x077C - 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 [PcieRplmrEnabled](#)
Offset 0x077D - PCIE IMR Enables Isolated Memory Region for PCIe.
 - UINT8 [PcieRplmrSelection](#)
Offset 0x077E - PCIE IMR port number Selects PCIE root port number for IMR feature.
 - UINT8 [PchPmWolEnableOverride](#)
Offset 0x077F - 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 0x0780 - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.
 - UINT8 [PchPmWoWlanEnable](#)
Offset 0x0781 - 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 0x0782 - 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 0x0783 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.
 - UINT8 [PchPmDeepSxPol](#)
Offset 0x0784 - PCH Pm Deep Sx Pol Deep Sx Policy.
-

- UINT8 [PchPmSlpS3MinAssert](#)
Offset 0x0785 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.
 - UINT8 [PchPmSlpS4MinAssert](#)
Offset 0x0786 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.
 - UINT8 [PchPmSlpSusMinAssert](#)
Offset 0x0787 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.
 - UINT8 [PchPmSlpAMinAssert](#)
Offset 0x0788 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.
 - UINT8 [SlpS0Override](#)
*Offset 0x0789 - SLP_S0# Override Enabled will toggle SLP_S0# assertion
Disabled will enable SLP_S0# assertion when debug is enabled.*
 - UINT8 [SlpS0DisQForDebug](#)
Offset 0x078A - S0ix Override Settings 'No Change' will keep PMC BWG settings.
 - UINT8 [PchEnableDbcObs](#)
*Offset 0x078B - USB Overcurrent Override for Dbc This option overrides USB Over Current enablement state that
USB OC will be disabled after enabling this option.*
 - UINT8 [PchPmSlpStrchSusUp](#)
Offset 0x078C - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.
 - UINT8 [PchPmSlpLanLowDc](#)
Offset 0x078D - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.
 - UINT8 [PchPmPwrBtnOverridePeriod](#)
Offset 0x078E - PCH Pm Pwr Btn Override Period PCH power button override period.
 - UINT8 [PchPmDisableDsxAcPresentPulldown](#)
*Offset 0x078F - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRESENT
in deep SX and during G3 exit.*
 - UINT8 [PchPmDisableNativePowerButton](#)
Offset 0x0790 - PCH Pm Disable Native Power Button Power button native mode disable.
 - UINT8 [PchPmSlpS0Enable](#)
Offset 0x0791 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.
 - UINT8 [PchPmMeWakeSts](#)
*Offset 0x0792 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS)
register.*
 - UINT8 [PchPmWolOvrWkSts](#)
*Offset 0x0793 - PCH Pm WOL_OVR_WK_STS Clear the WOL_OVR_WK_STS bit in the Power and Reset Status
(PRSTS) register.*
 - UINT8 [PchPmPwrCycDur](#)
Offset 0x0794 - PCH Pm Reset Power Cycle Duration Could be customized in the unit of second.
 - UINT8 [PchPmPciePIISsc](#)
Offset 0x0795 - PCH Pm Pcie PII Ssc Specifies the Pcie PII Spread Spectrum Percentage.
 - UINT8 [SataPwrOptEnable](#)
Offset 0x0796 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.
 - UINT8 [EsataSpeedLimit](#)
*Offset 0x0797 - PCH Sata eSATA Speed Limit When enabled, BIOS will configure the PxSCTL.SPD to 2 to limit the
eSATA port speed.*
 - UINT8 [SataSpeedLimit](#)
*Offset 0x0798 - PCH Sata Speed Limit Indicates the maximum speed the SATA controller can support 0h: Pch↔
SataSpeedDefault.*
 - UINT8 [SataPortsHotPlug](#) [8]
Offset 0x0799 - Enable SATA Port HotPlug Enable SATA Port HotPlug.
 - UINT8 [SataPortsInterlockSw](#) [8]
Offset 0x07A1 - Enable SATA Port Interlock Sw Enable SATA Port Interlock Sw.
 - UINT8 [SataPortsExternal](#) [8]
-

- Offset 0x07A9 - Enable SATA Port External Enable SATA Port External.*

 - UINT8 [SataPortsSpinUp](#) [8]
 - Offset 0x07B1 - Enable SATA Port SpinUp Enable the COMRESET initialization Sequence to the device.*
 - UINT8 [SataPortsSolidStateDrive](#) [8]
 - Offset 0x07B9 - Enable SATA Port Solid State Drive 0: HDD; 1: SSD.*
 - UINT8 [SataPortsEnableDitoConfig](#) [8]
 - Offset 0x07C1 - Enable SATA Port Enable Dito Config Enable DEVSLP Idle Timeout settings (DmVal, DitoVal).*
 - UINT8 [SataPortsDmVal](#) [8]
 - Offset 0x07C9 - Enable SATA Port DmVal DITO multiplier.*
 - UINT8 [UnusedUpdSpace21](#) [1]
 - Offset 0x07D1.*
 - UINT16 [SataPortsDitoVal](#) [8]
 - Offset 0x07D2 - Enable SATA Port DmVal DEVSLP Idle Timeout (DITO), Default is 625.*
 - UINT8 [SataPortsZpOdd](#) [8]
 - Offset 0x07E2 - Enable SATA Port ZpOdd Support zero power ODD.*
 - UINT8 [SataRstRaidDeviceld](#)
 - Offset 0x07EA - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.*
 - UINT8 [SataRstRaid0](#)
 - Offset 0x07EB - PCH Sata Rst Raid0 RAID0.*
 - UINT8 [SataRstRaid1](#)
 - Offset 0x07EC - PCH Sata Rst Raid1 RAID1.*
 - UINT8 [SataRstRaid10](#)
 - Offset 0x07ED - PCH Sata Rst Raid10 RAID10.*
 - UINT8 [SataRstRaid5](#)
 - Offset 0x07EE - PCH Sata Rst Raid5 RAID5.*
 - UINT8 [SataRstIrrt](#)
 - Offset 0x07EF - PCH Sata Rst Irrt Intel Rapid Recovery Technology.*
 - UINT8 [SataRstOromUiBanner](#)
 - Offset 0x07F0 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.*
 - UINT8 [SataRstOromUiDelay](#)
 - Offset 0x07F1 - PCH Sata Rst Orom Ui Delay 00b: 2 secs; 01b: 4 secs; 10b: 6 secs; 11: 8 secs (see: PCH_SATA↔_OROM_DELAY).*
 - UINT8 [SataRstHddUnlock](#)
 - Offset 0x07F2 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.*
 - UINT8 [SataRstLedLocate](#)
 - Offset 0x07F3 - 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 0x07F4 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.*
 - UINT8 [SataRstSmartStorage](#)
 - Offset 0x07F5 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.*
 - UINT8 [SataRstPcieEnable](#) [3]
 - Offset 0x07F6 - PCH Sata Rst Pcie Storage Remap enable Enable Intel RST for PCIe Storage remapping.*
 - UINT8 [SataRstPcieStoragePort](#) [3]
 - Offset 0x07F9 - PCH Sata Rst Pcie Storage Port Intel RST for PCIe Storage remapping - PCIe Port Selection (1-based, 0 = autodetect).*
 - UINT8 [SataRstPcieDeviceResetDelay](#) [3]
 - Offset 0x07FC - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.*
 - UINT8 [UfsEnable](#) [2]
 - Offset 0x07FF - UFS enable/disable PCIe Storage Device Reset Delay in milliseconds.*
 - UINT8 [PchScsEmmcUseDiiValuesFromPolicy](#)
-

- Offset 0x0801 - Use HS400 DLL values from policy Set if FSP should use HS400 DLL values from policy \$EN_DIS.*

 - UINT8 [PchScsEmmcHs400RxDataDllValue](#)
 - Offset 0x0802 - HS400 Rx data path DLL value Set to the desired value of Rx data path delay.*
 - UINT8 [PchScsEmmcHs400TxDataDllValue](#)
 - Offset 0x0803 - HS400 Tx data path DLL value Set to the desired value of the Tx data path delay.*
 - UINT8 [SdCardPowerEnableActiveHigh](#)
 - Offset 0x0804 - SdCard power enable polarity Choose SD_PWREN# polarity 0: Active low, 1: Active high.*
 - UINT8 [PchStartFramePulse](#)
 - Offset 0x0805 - Start Frame Pulse Width Start Frame Pulse Width, 0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: PchSfpw8Clk.*
 - UINT8 [lehMode](#)
 - Offset 0x0806 - IEH Mode Integrated Error Handler Mode, 0: Bypass, 1: Enable 0: Bypass, 1:Enable.*
 - UINT8 [UnusedUpdSpace22](#)
 - Offset 0x0807.*
 - UINT16 [PchT0Level](#)
 - Offset 0x0808 - Thermal Throttling Customized T0Level Value Customized T0Level value.*
 - UINT16 [PchT1Level](#)
 - Offset 0x080A - Thermal Throttling Customized T1Level Value Customized T1Level value.*
 - UINT16 [PchT2Level](#)
 - Offset 0x080C - Thermal Throttling Customized T2Level Value Customized T2Level value.*
 - UINT8 [PchTTEnable](#)
 - Offset 0x080E - Enable The Thermal Throttle Enable the thermal throttle function.*
 - UINT8 [PchTTState13Enable](#)
 - Offset 0x080F - 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 0x0810 - Thermal Throttle Lock Thermal Throttle Lock.*
 - UINT8 [TTSuggestedSetting](#)
 - Offset 0x0811 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.*
 - UINT8 [TTCrossThrottling](#)
 - Offset 0x0812 - Enable PCH Cross Throttling Enable/Disable PCH Cross Throttling \$EN_DIS.*
 - UINT8 [PchDmiTsawEn](#)
 - Offset 0x0813 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.*
 - UINT8 [DmiSuggestedSetting](#)
 - Offset 0x0814 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.*
 - UINT8 [DmiTS0TW](#)
 - Offset 0x0815 - Thermal Sensor 0 Target Width Thermal Sensor 0 Target Width.*
 - UINT8 [DmiTS1TW](#)
 - Offset 0x0816 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.*
 - UINT8 [DmiTS2TW](#)
 - Offset 0x0817 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.*
 - UINT8 [DmiTS3TW](#)
 - Offset 0x0818 - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.*
 - UINT8 [SataP0T1M](#)
 - Offset 0x0819 - Port 0 T1 Multiplier Port 0 T1 Multiplier.*
 - UINT8 [SataP0T2M](#)
 - Offset 0x081A - Port 0 T2 Multiplier Port 0 T2 Multiplier.*
 - UINT8 [SataP0T3M](#)
 - Offset 0x081B - Port 0 T3 Multiplier Port 0 T3 Multiplier.*
 - UINT8 [SataP0TDisp](#)
 - Offset 0x081C - Port 0 Tdispatch Port 0 Tdispatch.*
-

- UINT8 [SataP1T1M](#)
Offset 0x081D - Port 1 T1 Multiplier Port 1 T1 Multiplier.
 - UINT8 [SataP1T2M](#)
Offset 0x081E - Port 1 T2 Multiplier Port 1 T2 Multiplier.
 - UINT8 [SataP1T3M](#)
Offset 0x081F - Port 1 T3 Multiplier Port 1 T3 Multiplier.
 - UINT8 [SataP1TDisp](#)
Offset 0x0820 - Port 1 Tdispatch Port 1 Tdispatch.
 - UINT8 [SataP0Tinact](#)
Offset 0x0821 - Port 0 Tinactive Port 0 Tinactive.
 - UINT8 [SataP0TDispFinit](#)
Offset 0x0822 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.
 - UINT8 [SataP1Tinact](#)
Offset 0x0823 - Port 1 Tinactive Port 1 Tinactive.
 - UINT8 [SataP1TDispFinit](#)
Offset 0x0824 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.
 - UINT8 [SataThermalSuggestedSetting](#)
Offset 0x0825 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.
 - UINT8 [PchMemoryThrottlingEnable](#)
Offset 0x0826 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
 - UINT8 [PchMemoryPmsyncEnable](#) [2]
Offset 0x0827 - Memory Thermal Throttling Enable Memory Thermal Throttling.
 - UINT8 [PchMemoryC0TransmitEnable](#) [2]
Offset 0x0829 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
 - UINT8 [PchMemoryPinSelection](#) [2]
Offset 0x082B - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.
 - UINT8 [UnusedUpdSpace23](#)
Offset 0x082D.
 - UINT16 [PchTemperatureHotLevel](#)
Offset 0x082E - Thermal Device Temperature Decides the temperature.
 - UINT8 [PchEnableComplianceMode](#)
Offset 0x0830 - Enable xHCI Compliance Mode Compliance Mode can be enabled for testing through this option but this is disabled by default.
 - UINT8 [Usb2OverCurrentPin](#) [16]
Offset 0x0831 - USB2 Port Over Current Pin Describe the specific over current pin number of USB 2.0 Port N.
 - UINT8 [Usb3OverCurrentPin](#) [10]
Offset 0x0841 - USB3 Port Over Current Pin Describe the specific over current pin number of USB 3.0 Port N.
 - UINT8 [Enable8254ClockGating](#)
Offset 0x084B - Enable 8254 Static Clock Gating Set 8254CGE=1 is required for SLP_S0 support.
 - UINT8 [SataRstOptaneMemory](#)
Offset 0x084C - PCH Sata Rst Optane Memory Optane Memory \$EN_DIS.
 - UINT8 [SataRstCpuAttachedStorage](#)
Offset 0x084D - PCH Sata Rst CPU Attached Storage CPU Attached Storage \$EN_DIS.
 - UINT8 [UnusedUpdSpace24](#) [2]
Offset 0x084E.
 - UINT32 [PchPcieDeviceOverrideTablePtr](#)
Offset 0x0850 - Pch PCIE device override table pointer The PCIE device table is being used to override PCIE device ASPM settings.
 - UINT8 [EnableTcoTimer](#)
Offset 0x0854 - Enable TCO timer.
 - UINT8 [EnableTimedGPIO](#)
-

- Offset 0x0855 - Enable Timed GPIO 0.*
 - UINT8 [EnableTimedGPIO1](#)
 - Offset 0x0856 - Enable Timed GPIO 1.*
 - UINT8 [UnusedUpdSpace25](#) [1]
 - Offset 0x0857.*
 - UINT64 [BgpdtHash](#) [4]
 - Offset 0x0858 - BgpdtHash[4] BgpdtHash values.*
 - UINT32 [BiosGuardAttr](#)
 - Offset 0x0878 - BiosGuardAttr BiosGuardAttr default values.*
 - UINT8 [UnusedUpdSpace26](#) [4]
 - Offset 0x087C.*
 - UINT64 [BiosGuardModulePtr](#)
 - Offset 0x0880 - BiosGuardModulePtr BiosGuardModulePtr default values.*
 - UINT64 [SendEcCmd](#)
 - Offset 0x0888 - SendEcCmd SendEcCmd function pointer.*
 - UINT8 [EcCmdProvisionEav](#)
 - Offset 0x0890 - EcCmdProvisionEav Ephemeral Authorization Value default values.*
 - UINT8 [EcCmdLock](#)
 - Offset 0x0891 - EcCmdLock EcCmdLock default values.*
 - UINT8 [UnusedUpdSpace27](#) [6]
 - Offset 0x0892.*
 - UINT64 [SgxEpoch0](#)
 - Offset 0x0898 - SgxEpoch0 SgxEpoch0 default values.*
 - UINT64 [SgxEpoch1](#)
 - Offset 0x08A0 - SgxEpoch1 SgxEpoch1 default values.*
 - UINT8 [SgxSinitNvsData](#)
 - Offset 0x08A8 - SgxSinitNvsData SgxSinitNvsData default values.*
 - UINT8 [SgxLCP](#)
 - Offset 0x08A9 - SgxLCP SgxLCP default values.*
 - UINT8 [UnusedUpdSpace28](#) [6]
 - Offset 0x08AA.*
 - UINT64 [SgxLEPubKeyHash0](#)
 - Offset 0x08B0 - EpcLength EpcLength default values.*
 - UINT64 [SgxLEPubKeyHash1](#)
 - Offset 0x08B8 - EpcLength EpcLength default values.*
 - UINT64 [SgxLEPubKeyHash2](#)
 - Offset 0x08C0 - EpcLength EpcLength default values.*
 - UINT64 [SgxLEPubKeyHash3](#)
 - Offset 0x08C8 - EpcLength EpcLength default values.*
 - UINT8 [SiCsmFlag](#)
 - Offset 0x08D0 - Si Config CSM Flag.*
 - UINT8 [UnusedUpdSpace29](#) [3]
 - Offset 0x08D1.*
 - UINT32 [SiSsidTablePtr](#)
 - Offset 0x08D4.*
 - UINT16 [SiNumberOfSsidTableEntry](#)
 - Offset 0x08D8.*
 - UINT8 [SataRstInterrupt](#)
 - Offset 0x08DA - SATA RST Interrupt Mode Allowes to choose which interrupts will be implemented by SATA controller in RAID mode.*
 - UINT8 [MeUnconfigOnRtcClear](#)
-

- Offset 0x08DB - ME Unconfig on RTC clear 0: Disable ME Unconfig On Rtc Clear.*

 - UINT8 [PsOnEnable](#)

Offset 0x08DC - Enable PS_ON.
- UINT8 [PmcCpuC10GatePinEnable](#)

Offset 0x08DD - Pmc Cpu C10 Gate Pin Enable Enable/Disable platform support for CPU_C10_GATE# pin to control gating of CPU VccIO and VccSTG rails instead of SLP_S0# pin.
- UINT8 [PchDmiAspmCtrl](#)

Offset 0x08DE - Pch Dmi Aspm Ctrl ASPM configuration on the PCH side of the DMI/OPI Link.
- UINT8 [PmcOsIdleEnable](#)

Offset 0x08DF - OS IDLE Mode Enable Enable/Disable OS Idle Mode (PCH-N only) \$EN_DIS.
- UINT8 [PchS0ixAutoDemotion](#)

Offset 0x08E0 - S0ix Auto-Demotion Enable/Disable the Low Power Mode Auto-Demotion Host Control feature.
- UINT8 [PmcGrTscEnable](#)

Offset 0x08E1 - Global Reset TSC Enable Enable/Disable PMC Global Reset Three Strike Counter feature.
- UINT8 [PchPmLatchEventsC10Exit](#)

Offset 0x08E2 - Latch Events C10 Exit When this bit is set to 1, SLP_S0# entry events in SLP_S0_DEBUG_REGx registers are captured on C10 exit (instead of C10 entry which is default) \$EN_DIS.
- UINT8 [SaPcieEqPh3LaneParamCm](#) [32]

Offset 0x08E3 - PCIE Eq Ph3 Lane Param Cm SA_PCIE_EQ_LANE_PARAM.
- UINT8 [SaPcieEqPh3LaneParamCp](#) [32]

Offset 0x0903 - PCIE Eq Ph3 Lane Param Cp SA_PCIE_EQ_LANE_PARAM.
- UINT8 [SaPcieHwEqGen3CoeffListCm](#) [5]

Offset 0x0923 - PCIE Hw Eq Gen3 CoeffList Cm SA_PCIE_EQ_PARAM.
- UINT8 [SaPcieHwEqGen3CoeffListCp](#) [5]

Offset 0x0928 - PCIE Hw Eq Gen3 CoeffList Cp SA_PCIE_EQ_PARAM.
- UINT8 [SaPcieHwEqGen4CoeffListCm](#) [5]

Offset 0x092D - PCIE Hw Eq Gen4 CoeffList Cm SA_PCIE_EQ_PARAM.
- UINT8 [SaPcieHwEqGen4CoeffListCp](#) [5]

Offset 0x0932 - PCIE Hw Eq Gen4 CoeffList Cp SA_PCIE_EQ_PARAM.
- UINT8 [SaPcieGen3RootPortPreset](#) [20]

Offset 0x0937 - Gen3 Root port preset values per lane Used for programming Pcie Gen3 preset values per lane.
- UINT8 [SaPcieGen4RootPortPreset](#) [20]

Offset 0x094B - Pcie Gen4 Root port preset values per lane Used for programming Pcie Gen4 preset values per lane.
- UINT8 [SaPcieGen3EndPointPreset](#) [20]

Offset 0x095F - Pcie Gen3 End port preset values per lane Used for programming Pcie Gen3 preset values per lane.
- UINT8 [SaPcieGen4EndPointPreset](#) [20]

Offset 0x0973 - Pcie Gen4 End port preset values per lane Used for programming Pcie Gen4 preset values per lane.
- UINT8 [SaPcieGen3EndPointHint](#) [20]

Offset 0x0987 - Pcie Gen3 End port Hint values per lane Used for programming Pcie Gen3 Hint values per lane.
- UINT8 [SaPcieGen4EndPointHint](#) [20]

Offset 0x099B - Pcie Gen4 End port Hint values per lane Used for programming Pcie Gen4 Hint values per lane.
- UINT8 [SaPcieDisableRootPortClockGating](#)

Offset 0x09AF - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.
- UINT8 [SaPcieDisableRootPortPowerGating](#)

Offset 0x09B0 - PCIE Disable RootPort Power Gating Describes whether the PCI Express Power Gating for each root port is enabled by platform modules.
- UINT8 [SaPcieComplianceTestMode](#)

Offset 0x09B1 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.
- UINT8 [SaPcieEnablePeerMemoryWrite](#)

Offset 0x09B2 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

- UINT8 [SaPcieRpFunctionSwap](#)
Offset 0x09B3 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.
- UINT32 [SaPcieDeviceOverrideTablePtr](#)
Offset 0x09B4 - Pch PCIE device override table pointer The PCIE device table is being used to override PCIE device ASPM settings.
- UINT8 [SaPcieRpHotPlug](#) [4]
Offset 0x09B8 - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.
- UINT8 [SaPcieRpPmSci](#) [4]
Offset 0x09BC - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.
- UINT8 [SaPcieRpTransmitterHalfSwing](#) [4]
Offset 0x09C0 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.
- UINT8 [SaPcieRpAcsEnabled](#) [4]
Offset 0x09C4 - PCIE RP Access Control Services Extended Capability Enable/Disable PCIE RP Access Control Services Extended Capability.
- UINT8 [SaPcieRpAdvancedErrorReporting](#) [4]
Offset 0x09C8 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.
- UINT8 [SaPcieRpUnsupportedRequestReport](#) [4]
Offset 0x09CC - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.
- UINT8 [SaPcieRpFatalErrorReport](#) [4]
Offset 0x09D0 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.
- UINT8 [SaPcieRpNoFatalErrorReport](#) [4]
Offset 0x09D4 - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.
- UINT8 [SaPcieRpCorrectableErrorReport](#) [4]
Offset 0x09D8 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.
- UINT8 [SaPcieRpSystemErrorOnFatalError](#) [4]
Offset 0x09DC - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.
- UINT8 [SaPcieRpSystemErrorOnNonFatalError](#) [4]
Offset 0x09E0 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.
- UINT8 [SaPcieRpSystemErrorOnCorrectableError](#) [4]
Offset 0x09E4 - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.
- UINT8 [SaPcieRpMaxPayload](#) [4]
Offset 0x09E8 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH_PCIE_MAX_PAYLOAD.
- UINT8 [SaPcieRpDpcEnabled](#) [4]
Offset 0x09EC - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.
- UINT8 [SaPcieRpDpcExtensionsEnabled](#) [4]
Offset 0x09F0 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.
- UINT8 [SaPcieRpSlotImplemented](#) [4]
Offset 0x09F4 - PCH PCIE root port connection type 0: built-in device, 1:slot.
- UINT8 [SaPcieRpPcieSpeed](#) [4]
Offset 0x09F8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.
- UINT8 [SaPcieRpGen3EqPh3Method](#) [4]
Offset 0x09FC - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see SA_PCIE_EQ_METADATA).
- UINT8 [SaPcieRpGen4EqPh3Method](#) [4]
Offset 0x0A00 - PCIE RP Gen4 Equalization Phase Method PCIe Gen4 Eq Ph3 Method (see SA_PCIE_EQ_METADATA).

- UINT8 [SaPcieRpGen3EqPh3Enable](#) [4]
Offset 0x0A04 - Phase3 RP Gen3 EQ enable Phase3 Gen3 EQ enable.
- UINT8 [SaPcieRpGen4EqPh3Enable](#) [4]
Offset 0x0A08 - Phase3 RP Gen4 EQ enable Phase3 Gen4 EQ enable.
- UINT8 [SaPcieRpGen3EqPh23Enable](#) [4]
Offset 0x0A0C - Phase2-3 RP Gen3 EQ enable Phase2-3 Gen3 EQ enable.
- UINT8 [SaPcieRpGen4EqPh23Enable](#) [4]
Offset 0x0A10 - Phase2-3 RP Gen4 EQ enable Phase2-3 Gen4 EQ enable.
- UINT8 [SaPcieRpPhysicalSlotNumber](#) [4]
Offset 0x0A14 - PCIE RP Physical Slot Number Indicates the slot number for the root port.
- UINT8 [SaPcieRpAspm](#) [4]
Offset 0x0A18 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).
- UINT8 [SaPcieRpL1Substates](#) [4]
Offset 0x0A1C - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: SA_PCIE_L1SUBSTATES_CONTROL).
- UINT8 [SaPcieRpLtrEnable](#) [4]
Offset 0x0A20 - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.
- UINT8 [SaPcieRpLtrConfigLock](#) [4]
Offset 0x0A24 - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.
- UINT8 [SaPcieRpPtmEnabled](#) [4]
Offset 0x0A28 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.
- UINT16 [SaPcieRpDetectTimeoutMs](#) [4]
Offset 0x0A2C - PCIE RP Detect Timeout Ms The number of milliseconds within 0~65535 in reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
- UINT8 [SaPcieRpVcEnabled](#) [4]
Offset 0x0A34 - VC for PCIE RP Mask Enable/disable Virtual Channel for PCIE Root Ports.
- UINT8 [UnusedUpdSpace30](#) [4]
Offset 0x0A38.
- UINT8 [ReservedFspUpd](#) [4]
Offset 0x0A3C.

10.10.1 Detailed Description

Fsp S Configuration.

Definition at line 86 of file FspUpd.h.

10.10.2 Member Data Documentation

10.10.2.1 AcLoadline

UINT16 FSP_S_CONFIG::AcLoadline [5]

Offset 0x0404 - 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 1453 of file FspUpd.h.

10.10.2.2 AcousticNoiseMitigation

UINT8 FSP_S_CONFIG::AcousticNoiseMitigation

Offset 0x03F5 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.

0: Disabled; 1: Enabled \$EN_DIS

Definition at line 1413 of file FspUpd.h.

10.10.2.3 AmtEnabled

UINT8 FSP_S_CONFIG::AmtEnabled

Offset 0x02A1 - AMT Switch Enable/Disable.

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

Definition at line 935 of file FspUpd.h.

10.10.2.4 AmtKvmEnabled

UINT8 FSP_S_CONFIG::AmtKvmEnabled

Offset 0x02AD - KVM Switch Enable/Disable.

0: Disable, 1: enable, KVM enable/disable state by Mebx \$EN_DIS

Definition at line 994 of file FspUpd.h.

10.10.2.5 AmtSolEnabled

UINT8 FSP_S_CONFIG::AmtSolEnabled

Offset 0x02A6 - SOL Switch Enable/Disable.

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

Definition at line 966 of file FspUpd.h.

10.10.2.6 AsfEnabled

UINT8 FSP_S_CONFIG::AsfEnabled

Offset 0x02A3 - ASF Switch Enable/Disable.

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

Definition at line 947 of file FspUpd.h.

10.10.2.7 CnviBtAudioOffload

UINT8 FSP_S_CONFIG::CnviBtAudioOffload

Offset 0x0280 - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.

0: DISABLE, 1: ENABLE \$EN_DIS

Definition at line 816 of file FspsUpd.h.

10.10.2.8 CnviBtCore

UINT8 FSP_S_CONFIG::CnviBtCore

Offset 0x027F - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.

0: DISABLE, 1: ENABLE \$EN_DIS

Definition at line 810 of file FspsUpd.h.

10.10.2.9 CnviClkreqPinMux

UINT32 FSP_S_CONFIG::CnviClkreqPinMux

Offset 0x0288 - CNVi CLKREQ pin muxing Select CNVi CLKREQ pin depending on board routing.

TGP-LP: GPP_A9 = 0x3942E609(default) or GPP_F5 = 0x394BE605. TGP-H: 0. TGP-K: 0. Refer to GPIO_*_MUXING_CNVI_MODEM_CLKREQ_* in GpioPins*.h.

Definition at line 834 of file FspsUpd.h.

10.10.2.10 CnviMode

UINT8 FSP_S_CONFIG::CnviMode

Offset 0x027E - CNVi Configuration This option allows for automatic detection of Connectivity Solution.

[Auto Detection] assumes that CNVi will be enabled when available, [Disable] allows for disabling CNVi. 0:Disable, 1:Auto

Definition at line 804 of file FspsUpd.h.

10.10.2.11 CnviRfResetPinMux

UINT32 FSP_S_CONFIG::CnviRfResetPinMux

Offset 0x0284 - CNVi RF_RESET pin muxing Select CNVi RF_RESET# pin depending on board routing.

TGP-LP: GPP_A8 = 0x2942E408(default) or GPP_F4 = 0x194BE404. TGP-H: 0. TGP-K: 0. Refer to GPIO_*_MUXING_CNVI_RF_RESET_* in GpioPins*.h.

Definition at line 827 of file FspsUpd.h.

10.10.2.12 DcLoadline

UINT16 FSP_S_CONFIG::DcLoadline[5]

Offset 0x040E - 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 1459 of file FspUpd.h.

10.10.2.13 DevIntConfigPtr

UINT32 FSP_S_CONFIG::DevIntConfigPtr

Offset 0x0074 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.

The address of the table of PCH_DEVICE_INTERRUPT_CONFIG.

Definition at line 219 of file FspUpd.h.

10.10.2.14 DmiSuggestedSetting

UINT8 FSP_S_CONFIG::DmiSuggestedSetting

Offset 0x0814 - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.

\$EN_DIS

Definition at line 2463 of file FspUpd.h.

10.10.2.15 DmiTS0TW

UINT8 FSP_S_CONFIG::DmiTS0TW

Offset 0x0815 - Thermal Sensor 0 Target Width Thermal Sensor 0 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2469 of file FspUpd.h.

10.10.2.16 DmiTS1TW

UINT8 FSP_S_CONFIG::DmiTS1TW

Offset 0x0816 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2475 of file FspUpd.h.

10.10.2.17 DmiTS2TW

UINT8 FSP_S_CONFIG::DmiTS2TW

Offset 0x0817 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2481 of file FspUpd.h.

10.10.2.18 DmiTS3TW

UINT8 FSP_S_CONFIG::DmiTS3TW

Offset 0x0818 - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.

0:x1, 1:x2, 2:x4, 3:x8, 4:x16

Definition at line 2487 of file FspUpd.h.

10.10.2.19 EcCmdLock

UINT8 FSP_S_CONFIG::EcCmdLock

Offset 0x0891 - EcCmdLock EcCmdLock default values.

Locks Ephemeral Authorization Value sent previously

Definition at line 2698 of file FspUpd.h.

10.10.2.20 EcCmdProvisionEav

UINT8 FSP_S_CONFIG::EcCmdProvisionEav

Offset 0x0890 - EcCmdProvisionEav Ephemeral Authorization Value default values.

Provisions an ephemeral shared secret to the EC

Definition at line 2693 of file FspUpd.h.

10.10.2.21 Enable8254ClockGating

UINT8 FSP_S_CONFIG::Enable8254ClockGating

Offset 0x084B - Enable 8254 Static Clock Gating Set 8254CGE=1 is required for SLP_S0 support.

However, set 8254CGE=1 in POST time might fail to boot legacy OS using 8254 timer. Make sure it is disabled to support legacy OS using 8254 timer. Also enable this while S0ix is enabled. \$EN_DIS

Definition at line 2610 of file FspUpd.h.

10.10.2.22 EnableMinVoltageOverride

UINT8 FSP_S_CONFIG::EnableMinVoltageOverride

Offset 0x045D - Enable or Disable Minimum Voltage Override Enable or disable Minimum Voltage overrides ; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 1573 of file FspUpd.h.

10.10.2.23 EnableTcoTimer

UINT8 FSP_S_CONFIG::EnableTcoTimer

Offset 0x0854 - 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 2642 of file FspUpd.h.

10.10.2.24 EnableTimedGPIO0

```
UINT8 FSP_S_CONFIG::EnableTimedGPIO0
```

Offset 0x0855 - Enable Timed GPIO 0.

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 2650 of file FspUpd.h.

10.10.2.25 EnableTimedGPIO1

```
UINT8 FSP_S_CONFIG::EnableTimedGPIO1
```

Offset 0x0856 - Enable Timed GPIO 1.

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 2658 of file FspUpd.h.

10.10.2.26 EsataSpeedLimit

```
UINT8 FSP_S_CONFIG::EsataSpeedLimit
```

Offset 0x0797 - 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 2220 of file FspUpd.h.

10.10.2.27 FastPkgCRampDisableFivr

```
UINT8 FSP_S_CONFIG::FastPkgCRampDisableFivr
```

Offset 0x0453 - Disable Fast Slew Rate for Deep Package C States for VR FIVR domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True \$EN_DIS

Definition at line 1544 of file FspUpd.h.

10.10.2.28 FastPkgCRampDisableGt

UINT8 FSP_S_CONFIG::FastPkgCRampDisableGt

Offset 0x044A - 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 1491 of file FspUpd.h.

10.10.2.29 FastPkgCRampDisableIa

UINT8 FSP_S_CONFIG::FastPkgCRampDisableIa

Offset 0x03F6 - 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 1420 of file FspUpd.h.

10.10.2.30 FastPkgCRampDisableSa

UINT8 FSP_S_CONFIG::FastPkgCRampDisableSa

Offset 0x044B - 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 1498 of file FspUpd.h.

10.10.2.31 FivrRfiFrequency

UINT16 FSP_S_CONFIG::FivrRfiFrequency

Offset 0x0450 - FIVR RFI Frequency PCODE MMIO Mailbox: Set the desired RFI frequency, in increments of 100KHz.

0: Auto. Range varies based on XTAL clock: 0-1918 (Up to 191.8MHz) for 24MHz clock; 0-1535 (Up to 153.5MHz) for 19MHz clock.

Definition at line 1531 of file FspUpd.h.

10.10.2.32 FivrSpreadSpectrum

UINT8 FSP_S_CONFIG::FivrSpreadSpectrum

Offset 0x0452 - FIVR RFI Spread Spectrum PCODE MMIO Mailbox: FIVR RFI Spread Spectrum, in 0.1% increments.

0: 0%; Range: 0.0% to 10.0% (0-100).

Definition at line 1537 of file FspUpd.h.

10.10.2.33 ForcMebxSyncUp

UINT8 FSP_S_CONFIG::ForcMebxSyncUp

Offset 0x02AE - KVM Switch Enable/Disable.

0: Disable, 1: enable, KVM enable/disable state by Mebx \$EN_DIS

Definition at line 1000 of file FspUpd.h.

10.10.2.34 FwProgress

UINT8 FSP_S_CONFIG::FwProgress

Offset 0x02A5 - PET Progress Enable/Disable.

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

Definition at line 960 of file FspUpd.h.

10.10.2.35 GpioIrqRoute

UINT8 FSP_S_CONFIG::GpioIrqRoute

Offset 0x0081 - Select GPIO IRQ Route GPIO IRQ Select.

The valid value is 14 or 15.

Definition at line 237 of file FspUpd.h.

10.10.2.36 Heci3Enabled

UINT8 FSP_S_CONFIG::Heci3Enabled

Offset 0x029A - 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 892 of file FspUpd.h.

10.10.2.37 IccMax

UINT16 FSP_S_CONFIG::IccMax[5]

Offset 0x0436 - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.

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

Definition at line 1479 of file FspUpd.h.

10.10.2.38 ImonOffset

UINT8 FSP_S_CONFIG::ImonOffset[5]

Offset 0x03DA - 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 1371 of file FspUpd.h.

10.10.2.39 ImonSlope

UINT8 FSP_S_CONFIG::ImonSlope[5]

Offset 0x03D5 - 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 1365 of file FspUpd.h.

10.10.2.40 IomTypeCPortPadCfg

UINT32 FSP_S_CONFIG::IomTypeCPortPadCfg[12]

Offset 0x036C - TypeC port GPIO setting GPIO Ping number for Type C Aux Orientation setting, use the GpioPad that is defined in GpioPinsXXXH.h and GpioPinsXXXLp.h as argument.

(XXX is platform name, Ex: Ehl = ElkhartLake)

Definition at line 1201 of file FspUpd.h.

10.10.2.41 ITbtConnectTopologyTimeoutInMs

UINT16 FSP_S_CONFIG::ITbtConnectTopologyTimeoutInMs

Offset 0x03C6 - ITbtConnectTopology Timeout value ITbtConnectTopologyTimeout value.

Specified increment values in milliseconds. Range is 0-10000. 100 = 100 ms.

Definition at line 1329 of file FspUpd.h.

10.10.2.42 ITbtForcePowerOnTimeoutInMs

UINT16 FSP_S_CONFIG::ITbtForcePowerOnTimeoutInMs

Offset 0x03C4 - ITBTForcePowerOn Timeout value ITBTForcePowerOn value.

Specified increment values in milliseconds. Range is 0-1000. 100 = 100 ms.

Definition at line 1323 of file FspUpd.h.

10.10.2.43 ManageabilityMode

UINT8 FSP_S_CONFIG::ManageabilityMode

Offset 0x02A4 - Manageability Mode set by Mebx Enable/Disable.

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

Definition at line 953 of file FspUpd.h.

10.10.2.44 MeUnconfigOnRtcClear

UINT8 FSP_S_CONFIG::MeUnconfigOnRtcClear

Offset 0x08DB - ME Unconfig on RTC clear 0: Disable ME Unconfig On Rtc Clear.

1: Enable ME Unconfig On Rtc Clear. 2: Cmos is clear, status unkonwn. 3: Reserved 0: Disable ME Unconfig On Rtc Clear, 1: Enable ME Unconfig On Rtc Clear, 2: Cmos is clear, 3: Reserved

Definition at line 2778 of file FspUpd.h.

10.10.2.45 MinVoltageC8

UINT16 FSP_S_CONFIG::MinVoltageC8

Offset 0x0460 - Min Voltage for C8 PCODE MMIO Mailbox: Minimum voltage for C8.

Valid if EnableMinVoltageOverride =

1. Range 0 to 1999mV. **0: 0mV**

Definition at line 1585 of file FspUpd.h.

10.10.2.46 MinVoltageRuntime

UINT16 FSP_S_CONFIG::MinVoltageRuntime

Offset 0x045E - Min Voltage for Runtime PCODE MMIO Mailbox: Minimum voltage for runtime.

Valid if EnableMinVoltageOverride = 1. Range 0 to 1999mV. **0: 0mV**

Definition at line 1579 of file FspUpd.h.

10.10.2.47 NumOfDevIntConfig

UINT8 FSP_S_CONFIG::NumOfDevIntConfig

Offset 0x0078 - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.

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

Definition at line 225 of file FspUpd.h.

10.10.2.48 PchCrid

UINT8 FSP_S_CONFIG::PchCrid

Offset 0x0517 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.

\$EN_DIS

Definition at line 1810 of file FspUpd.h.

10.10.2.49 PchDmiAspmCtrl

UINT8 FSP_S_CONFIG::PchDmiAspmCtrl

Offset 0x08DE - Pch Dmi Aspm Ctrl ASPM configuration on the PCH side of the DMI/OPI Link.

Default is **PchPcieAspmAutoConfig** 0:Disabled, 1:L0s, 2:L1, 3:L0sL1, 4:Auto

Definition at line 2799 of file FspUpd.h.

10.10.2.50 PchDmiTsawEn

UINT8 FSP_S_CONFIG::PchDmiTsawEn

Offset 0x0813 - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.

\$EN_DIS

Definition at line 2457 of file FspUpd.h.

10.10.2.51 PchEnableComplianceMode

UINT8 FSP_S_CONFIG::PchEnableComplianceMode

Offset 0x0830 - Enable xHCI Compliance Mode Compliance Mode can be enabled for testing through this option but this is disabled by default.

\$EN_DIS

Definition at line 2592 of file FspUpd.h.

10.10.2.52 PchEnableDbcObs

UINT8 FSP_S_CONFIG::PchEnableDbcObs

Offset 0x078B - USB Overcurrent Override for DbC This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option.

Enable when DbC is used to avoid signaling conflicts. \$EN_DIS

Definition at line 2149 of file FspUpd.h.

10.10.2.53 PchEspHostC10ReportEnable

UINT8 FSP_S_CONFIG::PchEspHostC10ReportEnable

Offset 0x028C - Enable Host C10 reporting through eSPI Enable/disable Host C10 reporting to Slave via eSPI Virtual Wire.

\$EN_DIS

Definition at line 840 of file FspUpd.h.

10.10.2.54 PchFivrDynPm

UINT8 FSP_S_CONFIG::PchFivrDynPm

Offset 0x0271 - FIVR Dynamic Power Management Enable/Disable FIVR Dynamic Power Management.

\$EN_DIS

Definition at line 766 of file FspsUpd.h.

10.10.2.55 PchFivrExtVnnRailSxEnabledStates

UINT8 FSP_S_CONFIG::PchFivrExtVnnRailSxEnabledStates

Offset 0x0263 - Mask to enable the usage of external Vnn VR rail in Sx states Use only if Ext Vnn Rail config is different in Sx.

Enable External Vnn Rail in Sx: BIT0-1:Reserved, BIT2:S3, BIT3:S4, BIT5:S5

Definition at line 711 of file FspsUpd.h.

10.10.2.56 PchFivrExtVnnRailSxIccMax

UINT8 FSP_S_CONFIG::PchFivrExtVnnRailSxIccMax

Offset 0x0266 - External Vnn Icc Max Value that will be used in Sx states Use only if Ext Vnn Rail config is different in Sx.

Granularity of this setting is 1mA and maximal possible value is 200mA

Definition at line 723 of file FspsUpd.h.

10.10.2.57 PchFivrExtVnnRailSxVoltage

UINT16 FSP_S_CONFIG::PchFivrExtVnnRailSxVoltage

Offset 0x0264 - External Vnn Voltage Value that will be used in Sx states Use only if Ext Vnn Rail config is different in Sx.

Value is given in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...)

Definition at line 717 of file FspsUpd.h.

10.10.2.58 PchFivrVccinAuxLowToHighCurModeVolTranTime

UINT8 FSP_S_CONFIG::PchFivrVccinAuxLowToHighCurModeVolTranTime

Offset 0x0267 - Transition time in microseconds from Low Current Mode Voltage to High Current Mode Voltage This field has 1us resolution.

When value is 0 PCH will not transition VCCIN_AUX to low current mode voltage.

Definition at line 729 of file FspsUpd.h.

10.10.2.59 PchFivrVccinAuxOffToHighCurModeVolTranTime

UINT16 FSP_S_CONFIG::PchFivrVccinAuxOffToHighCurModeVolTranTime

Offset 0x026A - Transition time in microseconds from Off (0V) to High Current Mode Voltage This field has 1us resolution.

When value is 0 Transition to 0V is disabled.

Definition at line 746 of file FspsUpd.h.

10.10.2.60 PchFivrVccinAuxRetToHighCurModeVolTranTime

UINT8 FSP_S_CONFIG::PchFivrVccinAuxRetToHighCurModeVolTranTime

Offset 0x0268 - Transition time in microseconds from Retention Mode Voltage to High Current Mode Voltage This field has 1us resolution.

When value is 0 PCH will not transition VCCIN_AUX to retention mode voltage.

Definition at line 735 of file FspsUpd.h.

10.10.2.61 PchFivrVccinAuxRetToLowCurModeVolTranTime

UINT8 FSP_S_CONFIG::PchFivrVccinAuxRetToLowCurModeVolTranTime

Offset 0x0269 - Transition time in microseconds from Retention Mode Voltage to Low Current Mode Voltage This field has 1us resolution.

When value is 0 PCH will not transition VCCIN_AUX to retention mode voltage.

Definition at line 741 of file FspsUpd.h.

10.10.2.62 PchHdaAudioLinkDmic0ClkAPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic0ClkAPinMux

Offset 0x0278 - DMIC0 ClkA Pin Muxing Determines DMIC0 ClkA Pin muxing.

See GPIO_*_MUXING_DMIC0_CLKA_*

Definition at line 791 of file FspsUpd.h.

10.10.2.63 PchHdaAudioLinkDmic0ClkBPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic0ClkBPinMux

Offset 0x0294 - DMIC0 ClkB Pin Muxing Determines DMIC0 ClkA Pin muxing.

See GPIO_*_MUXING_DMIC0_CLKB_*

Definition at line 875 of file FspsUpd.h.

10.10.2.64 PchHdaAudioLinkDmic0DataPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic0DataPinMux

Offset 0x03A8 - DMIC0 Data Pin Muxing Determines DMIC0 Data Pin muxing.

See GPIO_*_MUXING_DMIC0_DATA_*

Definition at line 1221 of file FspUpd.h.

10.10.2.65 PchHdaAudioLinkDmic0Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkDmic0Enable

Offset 0x0237 - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.

Muxed with SNDW4. \$EN_DIS

Definition at line 554 of file FspUpd.h.

10.10.2.66 PchHdaAudioLinkDmic1ClkAPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic1ClkAPinMux

Offset 0x0494 - DMIC1 ClkA Pin Muxing Determines DMIC1 ClkA RstA Pin muxing.

See GPIO_*_MUXING_DMIC1_CLKA_*

Definition at line 1679 of file FspUpd.h.

10.10.2.67 PchHdaAudioLinkDmic1ClkBPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic1ClkBPinMux

Offset 0x0498 - DMIC1 Data Pin Muxing Determines DMIC1 Data Pin muxing.

See GPIO_*_MUXING_DMIC1_CLKB_*

Definition at line 1684 of file FspUpd.h.

10.10.2.68 PchHdaAudioLinkDmic1DataPinMux

UINT32 FSP_S_CONFIG::PchHdaAudioLinkDmic1DataPinMux

Offset 0x049C - DMIC1 Data Pin Muxing Determines DMIC0 Data Pin muxing.

See GPIO_*_MUXING_DMIC1_DATA_*

Definition at line 1689 of file FspUpd.h.

10.10.2.69 PchHdaAudioLinkDmic1Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkDmic1Enable

Offset 0x0238 - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.

Muxed with SNDW3. \$EN_DIS

Definition at line 560 of file FspsUpd.h.

10.10.2.70 PchHdaAudioLinkHdaEnable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkHdaEnable

Offset 0x0236 - Enable HD Audio Link Enable/disable HD Audio Link.

Muxed with SSP0/SSP1/SNDW1. \$EN_DIS

Definition at line 548 of file FspsUpd.h.

10.10.2.71 PchHdaAudioLinkSndw1Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw1Enable

Offset 0x023F - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.

Muxed with HDA. \$EN_DIS

Definition at line 602 of file FspsUpd.h.

10.10.2.72 PchHdaAudioLinkSndw2Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw2Enable

Offset 0x0240 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.

Muxed with SSP1. \$EN_DIS

Definition at line 608 of file FspsUpd.h.

10.10.2.73 PchHdaAudioLinkSndw3Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw3Enable

Offset 0x0241 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.

Muxed with DMIC1. \$EN_DIS

Definition at line 614 of file FspsUpd.h.

10.10.2.74 PchHdaAudioLinkSndw4Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSndw4Enable

Offset 0x0242 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.

Muxed with DMIC0. \$EN_DIS

Definition at line 620 of file FspsUpd.h.

10.10.2.75 PchHdaAudioLinkSsp0Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp0Enable

Offset 0x0239 - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.

Muxed with HDA. \$EN_DIS

Definition at line 566 of file FspsUpd.h.

10.10.2.76 PchHdaAudioLinkSsp1Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp1Enable

Offset 0x023A - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.

Muxed with HDA/SNDW2. \$EN_DIS

Definition at line 572 of file FspsUpd.h.

10.10.2.77 PchHdaAudioLinkSsp2Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp2Enable

Offset 0x023B - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.

\$EN_DIS

Definition at line 578 of file FspsUpd.h.

10.10.2.78 PchHdaAudioLinkSsp3Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp3Enable

Offset 0x023C - Enable HD Audio SSP3 Link Enable/disable HD Audio SSP3/I2S link.

\$EN_DIS

Definition at line 584 of file FspsUpd.h.

10.10.2.79 PchHdaAudioLinkSsp4Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp4Enable

Offset 0x023D - Enable HD Audio SSP4 Link Enable/disable HD Audio SSP4/I2S link.

\$EN_DIS

Definition at line 590 of file FspsUpd.h.

10.10.2.80 PchHdaAudioLinkSsp5Enable

UINT8 FSP_S_CONFIG::PchHdaAudioLinkSsp5Enable

Offset 0x023E - Enable HD Audio SSP5 Link Enable/disable HD Audio SSP5/I2S link.

\$EN_DIS

Definition at line 596 of file FspsUpd.h.

10.10.2.81 PchHdaDspEnable

UINT8 FSP_S_CONFIG::PchHdaDspEnable

Offset 0x0035 - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

\$EN_DIS

Definition at line 124 of file FspsUpd.h.

10.10.2.82 PchHdaDspUaaCompliance

UINT8 FSP_S_CONFIG::PchHdaDspUaaCompliance

Offset 0x048F - 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 1659 of file FspsUpd.h.

10.10.2.83 PchHdaIDispCodecDisconnect

UINT8 FSP_S_CONFIG::PchHdaIDispCodecDisconnect

Offset 0x0490 - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.

\$EN_DIS

Definition at line 1665 of file FspsUpd.h.

10.10.2.84 PchHdaIDispLinkFrequency

UINT8 FSP_S_CONFIG::PchHdaIDispLinkFrequency

Offset 0x048D - iDisp-Link Frequency iDisp-Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 4: 96MHz, 3: 48MHz.

4: 96MHz, 3: 48MHz

Definition at line 1646 of file FspsUpd.h.

10.10.2.85 PchHdaLinkFrequency

UINT8 FSP_S_CONFIG::PchHdaLinkFrequency

Offset 0x048C - HD Audio Link Frequency HDA Link Freq (PCH_HDAUDIO_LINK_FREQUENCY enum): 0: 6MHz, 1: 12MHz, 2: 24MHz.

0: 6MHz, 1: 12MHz, 2: 24MHz

Definition at line 1640 of file FspUpd.h.

10.10.2.86 PchHdaPme

UINT8 FSP_S_CONFIG::PchHdaPme

Offset 0x048A - Enable Pme Enable Azalia wake-on-ring.

\$EN_DIS

Definition at line 1628 of file FspUpd.h.

10.10.2.87 PchHdaVcType

UINT8 FSP_S_CONFIG::PchHdaVcType

Offset 0x048B - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.

0: VC0, 1: VC1

Definition at line 1634 of file FspUpd.h.

10.10.2.88 PchHotEnable

UINT8 FSP_S_CONFIG::PchHotEnable

Offset 0x029B - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.

0: disable, 1: enable \$EN_DIS

Definition at line 898 of file FspUpd.h.

10.10.2.89 PchIoApicEntry24_119

UINT8 FSP_S_CONFIG::PchIoApicEntry24_119

Offset 0x04A0 - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 1695 of file FspUpd.h.

10.10.2.90 PchIoApicId

UINT8 FSP_S_CONFIG::PchIoApicId

Offset 0x04A1 - PCH Io Apic ID This member determines IOAPIC ID.

Default is 0x02.

Definition at line 1700 of file FspUpd.h.

10.10.2.91 PchIshGpEnable

UINT8 FSP_S_CONFIG::PchIshGpEnable[8]

Offset 0x04A8 - Enable PCH ISH GP pins assigned Set if ISH GP native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1720 of file FspUpd.h.

10.10.2.92 PchIshI2cEnable

UINT8 FSP_S_CONFIG::PchIshI2cEnable[3]

Offset 0x04A5 - Enable PCH ISH I2C pins assigned Set if ISH I2C native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1715 of file FspUpd.h.

10.10.2.93 PchIshPdtUnlock

UINT8 FSP_S_CONFIG::PchIshPdtUnlock

Offset 0x04B0 - PCH ISH PDT Unlock Msg 0: False; 1: True.

\$EN_DIS

Definition at line 1726 of file FspUpd.h.

10.10.2.94 PchIshSpiCs0Enable

UINT8 FSP_S_CONFIG::PchIshSpiCs0Enable[1]

Offset 0x0491 - Enable PCH ISH SPI Cs0 pins assigned Set if ISH SPI Cs0 pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1670 of file FspUpd.h.

10.10.2.95 PchIshSpiEnable

UINT8 FSP_S_CONFIG::PchIshSpiEnable[1]

Offset 0x04A2 - Enable PCH ISH SPI pins assigned Set if ISH SPI native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1705 of file FspUpd.h.

10.10.2.96 PchIshUartEnable

UINT8 FSP_S_CONFIG::PchIshUartEnable[2]

Offset 0x04A3 - Enable PCH ISH UART pins assigned Set if ISH UART native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1710 of file FspUpd.h.

10.10.2.97 PchLanEnable

UINT8 FSP_S_CONFIG::PchLanEnable

Offset 0x0234 - Enable LAN Enable/disable LAN controller.

\$EN_DIS

Definition at line 536 of file FspUpd.h.

10.10.2.98 PchLanLtrEnable

UINT8 FSP_S_CONFIG::PchLanLtrEnable

Offset 0x0515 - Enable PCH Lan LTR capability of PCH internal LAN 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 1797 of file FspUpd.h.

10.10.2.99 PchLockDownBiosLock

UINT8 FSP_S_CONFIG::PchLockDownBiosLock

Offset 0x0516 - 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 1804 of file FspUpd.h.

10.10.2.100 PchMemoryThrottlingEnable

UINT8 FSP_S_CONFIG::PchMemoryThrottlingEnable

Offset 0x0826 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.

\$EN_DIS

Definition at line 2561 of file FspUpd.h.

10.10.2.101 PchOseAdcEnable

UINT8 FSP_S_CONFIG::PchOseAdcEnable

Offset 0x04D2 - Enable PCH OSE ADC pins assigned Set if OSE ADC native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1771 of file FspUpd.h.

10.10.2.102 PchOseCanEnable

UINT8 FSP_S_CONFIG::PchOseCanEnable[2]

Offset 0x04D3 - Enable PCH OSE CAN pins assigned Set if OSE CAN native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1776 of file FspUpd.h.

10.10.2.103 PchOseHsuartEnable

UINT8 FSP_S_CONFIG::PchOseHsuartEnable[4]

Offset 0x04BA - Enable PCH OSE HSUART pins assigned Set if OSE HSUART native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1746 of file FspUpd.h.

10.10.2.104 PchOseI2cEnable

UINT8 FSP_S_CONFIG::PchOseI2cEnable[8]

Offset 0x04C2 - Enable PCH OSE I2C pins assigned Set if OSE I2C native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1756 of file FspUpd.h.

10.10.2.105 PchOseI2sEnable

UINT8 FSP_S_CONFIG::PchOseI2sEnable[2]

Offset 0x04B1 - Enable PCH OSE I2S pins assigned Set if OSE I2S native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1731 of file FspUpd.h.

10.10.2.106 PchOsePwmEnable

UINT8 FSP_S_CONFIG::PchOsePwmEnable

Offset 0x04B3 - Enable PCH OSE PWM pins assigned Set if OSE PWM native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1736 of file FspUpd.h.

10.10.2.107 PchOseQepEnable

UINT8 FSP_S_CONFIG::PchOseQepEnable[4]

Offset 0x04BE - Enable PCH OSE QEP pins assigned Set if OSE QEP native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1751 of file FspUpd.h.

10.10.2.108 PchOseSpiCs0Enable

```
UINT8 FSP_S_CONFIG::PchOseSpiCs0Enable[4]
```

Offset 0x04CE - Enable PCH OSE SPI CS0 pins assigned Set if OSE SPI CS0 pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1766 of file FspUpd.h.

10.10.2.109 PchOseSpiEnable

```
UINT8 FSP_S_CONFIG::PchOseSpiEnable[4]
```

Offset 0x04CA - Enable PCH OSE SPI pins assigned Set if OSE SPI native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1761 of file FspUpd.h.

10.10.2.110 PchOseTimedGpioEnable

```
UINT8 FSP_S_CONFIG::PchOseTimedGpioEnable[2]
```

Offset 0x04D5 - Enable PCH OSE Timed GPIO pins assigned Set if OSE Timed GPIO native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1781 of file FspUpd.h.

10.10.2.111 PchOseTimedGpioPinAllocation

```
UINT8 FSP_S_CONFIG::PchOseTimedGpioPinAllocation[2]
```

Offset 0x04D7 - Enable PCH OSE Timed GPIO 20 pins allocation Allocate 20 pins for PCH OSE Timed GPIO.

0: Top 20 pins; 1: Mid 20 pins; 2: Lower 20 pins.

Definition at line 1786 of file FspUpd.h.

10.10.2.112 PchOseTimedGpioPinEnable

```
UINT8 FSP_S_CONFIG::PchOseTimedGpioPinEnable[60]
```

Offset 0x04D9 - Enable PCH OSE Timed GPIO Pin to OSE TGPIO native function Set TGPIO pin to OSE TGPIO native function.

0: Disable; 1: Enable.

Definition at line 1791 of file FspUpd.h.

10.10.2.113 PchOseUartEnable

UINT8 FSP_S_CONFIG::PchOseUartEnable[6]

Offset 0x04B4 - Enable PCH OSE UART pins assigned Set if OSE UART native pins are to be enabled by BIOS.

0: Disable; 1: Enable.

Definition at line 1741 of file FspUpd.h.

10.10.2.114 PchPcieDeviceOverrideTablePtr

UINT32 FSP_S_CONFIG::PchPcieDeviceOverrideTablePtr

Offset 0x0850 - Pch PCIe device override table pointer The PCIe device table is being used to override PCIe device ASPM settings.

This is a pointer points to a 32bit address. And it's only used in PostMem phase. Please refer to PCH_PCIE_DEVICE_OVERRIDE structure for the table. Last entry VendorId must be 0.

Definition at line 2634 of file FspUpd.h.

10.10.2.115 PchPmDeepSxPol

UINT8 FSP_S_CONFIG::PchPmDeepSxPol

Offset 0x0784 - PCH Pm Deep Sx Pol Deep Sx Policy.

\$EN_DIS

Definition at line 2107 of file FspUpd.h.

10.10.2.116 PchPmDisableDsxAcPresentPulldown

UINT8 FSP_S_CONFIG::PchPmDisableDsxAcPresentPulldown

Offset 0x078F - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC_PRESENT in deep SX and during G3 exit.

\$EN_DIS

Definition at line 2172 of file FspUpd.h.

10.10.2.117 PchPmDisableNativePowerButton

UINT8 FSP_S_CONFIG::PchPmDisableNativePowerButton

Offset 0x0790 - PCH Pm Disable Native Power Button Power button native mode disable.

\$EN_DIS

Definition at line 2178 of file FspUpd.h.

10.10.2.118 PchPmLanWakeFromDeepSx

UINT8 FSP_S_CONFIG::PchPmLanWakeFromDeepSx

Offset 0x0783 - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.

\$EN_DIS

Definition at line 2101 of file FspUpd.h.

10.10.2.119 PchPmMeWakeSts

UINT8 FSP_S_CONFIG::PchPmMeWakeSts

Offset 0x0792 - PCH Pm ME_WAKE_STS Clear the ME_WAKE_STS bit in the Power and Reset Status (PRSTS) register.

\$EN_DIS

Definition at line 2190 of file FspUpd.h.

10.10.2.120 PchPmPciePllSsc

UINT8 FSP_S_CONFIG::PchPmPciePllSsc

Offset 0x0795 - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.

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

Definition at line 2208 of file FspUpd.h.

10.10.2.121 PchPmPcieWakeFromDeepSx

UINT8 FSP_S_CONFIG::PchPmPcieWakeFromDeepSx

Offset 0x0780 - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.

\$EN_DIS

Definition at line 2082 of file FspUpd.h.

10.10.2.122 PchPmPmeB0S5Dis

UINT8 FSP_S_CONFIG::PchPmPmeB0S5Dis

Offset 0x077C - 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 2059 of file FspUpd.h.

10.10.2.123 PchPmPwrBtnOverridePeriod

UINT8 FSP_S_CONFIG::PchPmPwrBtnOverridePeriod

Offset 0x078E - 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 2166 of file FspUpd.h.

10.10.2.124 PchPmPwrCycDur

UINT8 FSP_S_CONFIG::PchPmPwrCycDur

Offset 0x0794 - 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 2202 of file FspUpd.h.

10.10.2.125 PchPmSlpAMinAssert

UINT8 FSP_S_CONFIG::PchPmSlpAMinAssert

Offset 0x0788 - PCH Pm Slp A Min Assert SLP_A Minimum Assertion Width Policy.

Default is PchSlpA2s.

Definition at line 2127 of file FspUpd.h.

10.10.2.126 PchPmSlpLanLowDc

UINT8 FSP_S_CONFIG::PchPmSlpLanLowDc

Offset 0x078D - PCH Pm Slp Lan Low Dc Enable/Disable SLP_LAN# Low on DC Power.

\$EN_DIS

Definition at line 2161 of file FspUpd.h.

10.10.2.127 PchPmSlpS0Enable

UINT8 FSP_S_CONFIG::PchPmSlpS0Enable

Offset 0x0791 - PCH Pm Slp S0 Enable Indicates whether SLP_S0# is to be asserted when PCH reaches idle state.

\$EN_DIS

Definition at line 2184 of file FspUpd.h.

10.10.2.128 PchPmSlpS0Vm070VSupport

UINT8 FSP_S_CONFIG::PchPmSlpS0Vm070VSupport

Offset 0x029F - SLP_S0 VM 0.70V Support SLP_S0 Voltage Margining 0.70V Support Policy.

0: disable, 1: enable \$EN_DIS

Definition at line 923 of file FspUpd.h.

10.10.2.129 PchPmSlpS0Vm075VSupport

UINT8 FSP_S_CONFIG::PchPmSlpS0Vm075VSupport

Offset 0x02A0 - SLP_S0 VM 0.75V Support SLP_S0 Voltage Margining 0.75V Support Policy.

0: disable, 1: enable \$EN_DIS

Definition at line 929 of file FspsUpd.h.

10.10.2.130 PchPmSlpS0VmRuntimeControl

UINT8 FSP_S_CONFIG::PchPmSlpS0VmRuntimeControl

Offset 0x029E - SLP_S0 VM Dynamic Control SLP_S0 Voltage Margining Runtime Control Policy.

0: disable, 1: enable \$EN_DIS

Definition at line 917 of file FspsUpd.h.

10.10.2.131 PchPmSlpS3MinAssert

UINT8 FSP_S_CONFIG::PchPmSlpS3MinAssert

Offset 0x0785 - PCH Pm Slp S3 Min Assert SLP_S3 Minimum Assertion Width Policy.

Default is PchSlpS350ms.

Definition at line 2112 of file FspsUpd.h.

10.10.2.132 PchPmSlpS4MinAssert

UINT8 FSP_S_CONFIG::PchPmSlpS4MinAssert

Offset 0x0786 - PCH Pm Slp S4 Min Assert SLP_S4 Minimum Assertion Width Policy.

Default is PchSlpS44s.

Definition at line 2117 of file FspsUpd.h.

10.10.2.133 PchPmSlpStrchSusUp

UINT8 FSP_S_CONFIG::PchPmSlpStrchSusUp

Offset 0x078C - PCH Pm Slp Strch Sus Up Enable SLP_X Stretching After SUS Well Power Up.

\$EN_DIS

Definition at line 2155 of file FspsUpd.h.

10.10.2.134 PchPmSlpSusMinAssert

UINT8 FSP_S_CONFIG::PchPmSlpSusMinAssert

Offset 0x0787 - PCH Pm Slp Sus Min Assert SLP_SUS Minimum Assertion Width Policy.

Default is PchSlpSus4s.

Definition at line 2122 of file FspUpd.h.

10.10.2.135 PchPmVrAlert

UINT8 FSP_S_CONFIG::PchPmVrAlert

Offset 0x029D - VRAAlert# Pin When VRAAlert# feature pin is enabled and its state is '0', the PMC requests throttling to a T3 Tstate to the PCH throttling unit.

. 0: disable, 1: enable \$EN_DIS

Definition at line 911 of file FspUpd.h.

10.10.2.136 PchPmWolEnableOverride

UINT8 FSP_S_CONFIG::PchPmWolEnableOverride

Offset 0x077F - 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 2076 of file FspUpd.h.

10.10.2.137 PchPmWolOvrWkSts

UINT8 FSP_S_CONFIG::PchPmWolOvrWkSts

Offset 0x0793 - 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 2196 of file FspUpd.h.

10.10.2.138 PchPmWoWlanDeepSxEnable

UINT8 FSP_S_CONFIG::PchPmWoWlanDeepSxEnable

Offset 0x0782 - 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 2095 of file FspUpd.h.

10.10.2.139 PchPmWoWlanEnable

UINT8 FSP_S_CONFIG::PchPmWoWlanEnable

Offset 0x0781 - 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 2088 of file FspUpd.h.

10.10.2.140 PchPwrOptEnable

UINT8 FSP_S_CONFIG::PchPwrOptEnable

Offset 0x046A - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.

\$EN_DIS

Definition at line 1597 of file FspUpd.h.

10.10.2.141 PchS0ixAutoDemotion

UINT8 FSP_S_CONFIG::PchS0ixAutoDemotion

Offset 0x08E0 - S0ix Auto-Demotion Enable/Disable the Low Power Mode Auto-Demotion Host Control feature.

\$EN_DIS

Definition at line 2811 of file FspUpd.h.

10.10.2.142 PchSerialIoI2cPadsTermination

UINT8 FSP_S_CONFIG::PchSerialIoI2cPadsTermination[8]

Offset 0x01C4 - PCH SerialIo I2C Pads Termination 0x0: Hardware default, 0x1: None, 0x13: 1kOhm weak pull-up, 0x15: 5kOhm weak pull-up, 0x19: 20kOhm weak pull-up - Enable/disable SerialIo I2C0,I2C1,...

pads termination respectively. One byte for each controller, byte0 for I2C0, byte1 for I2C1, and so on. 0x1:None, 0x13:1kOhm WPU, 0x15:5kOhm WPU, 0x19:20kOhm WPU

Definition at line 482 of file FspUpd.h.

10.10.2.143 PchSerialIoI2cSclPinMux

UINT32 FSP_S_CONFIG::PchSerialIoI2cSclPinMux[8]

Offset 0x01A4 - Serial IO I2C SCL Pin Muxing Select SerialIo I2c Scl pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_I2Cx_SCL* for possible values.

Definition at line 474 of file FspUpd.h.

10.10.2.144 PchSerialIoI2cSdaPinMux

UINT32 FSP_S_CONFIG::PchSerialIoI2cSdaPinMux[8]

Offset 0x0184 - Serial IO I2C SDA Pin Muxing Select SerialIo I2c Sda pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_I2Cx_SDA* for possible values.

Definition at line 468 of file FspUpd.h.

10.10.2.145 PchStartFramePulse

UINT8 FSP_S_CONFIG::PchStartFramePulse

Offset 0x0805 - Start Frame Pulse Width Start Frame Pulse Width, 0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: PchSfpw8Clk.

0: PchSfpw4Clk, 1: PchSfpw6Clk, 2: PchSfpw8Clk

Definition at line 2395 of file FspUpd.h.

10.10.2.146 PchTsnEnable

UINT8 FSP_S_CONFIG::PchTsnEnable

Offset 0x0235 - Enable PCH TSN Enable/disable TSN on the PCH.

\$EN_DIS

Definition at line 542 of file FspUpd.h.

10.10.2.147 PchTTEnable

UINT8 FSP_S_CONFIG::PchTTEnable

Offset 0x080E - Enable The Thermal Throttle Enable the thermal throttle function.

\$EN_DIS

Definition at line 2426 of file FspUpd.h.

10.10.2.148 PchTTLock

UINT8 FSP_S_CONFIG::PchTTLock

Offset 0x0810 - Thermal Throttle Lock Thermal Throttle Lock.

\$EN_DIS

Definition at line 2439 of file FspUpd.h.

10.10.2.149 PchTTState13Enable

UINT8 FSP_S_CONFIG::PchTTState13Enable

Offset 0x080F - 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 2433 of file FspUpd.h.

10.10.2.150 PcieComplianceTestMode

UINT8 FSP_S_CONFIG::PcieComplianceTestMode

Offset 0x0778 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

\$EN_DIS

Definition at line 2032 of file FspUpd.h.

10.10.2.151 PcieDisableRootPortClockGating

UINT8 FSP_S_CONFIG::PcieDisableRootPortClockGating

Offset 0x0776 - 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 2020 of file FspUpd.h.

10.10.2.152 PcieEnablePeerMemoryWrite

UINT8 FSP_S_CONFIG::PcieEnablePeerMemoryWrite

Offset 0x0777 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

\$EN_DIS

Definition at line 2026 of file FspUpd.h.

10.10.2.153 PcieEqPh3LaneParamCm

UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCm[24]

Offset 0x073C - PCIE Eq Ph3 Lane Param Cm PCH_PCIE_EQ_LANE_PARAM.

Coefficient C-1.

Definition at line 1998 of file FspUpd.h.

10.10.2.154 PcieEqPh3LaneParamCp

UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCp[24]

Offset 0x0754 - PCIE Eq Ph3 Lane Param Cp PCH_PCIE_EQ_LANE_PARAM.

Coefficient C+1.

Definition at line 2003 of file FspUpd.h.

10.10.2.155 PcieRpAspm

UINT8 FSP_S_CONFIG::PcieRpAspm[24]

Offset 0x06DC - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 1977 of file FspsUpd.h.

10.10.2.156 PcieRpCompletionTimeout

UINT8 FSP_S_CONFIG::PcieRpCompletionTimeout[24]

Offset 0x06C4 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_TIMEOUT).

Default is PchPcieCompletionTO_Default.

Definition at line 1971 of file FspsUpd.h.

10.10.2.157 PcieRpDpcExtensionsMask

UINT32 FSP_S_CONFIG::PcieRpDpcExtensionsMask

Offset 0x024C - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 642 of file FspsUpd.h.

10.10.2.158 PcieRpDpcMask

UINT32 FSP_S_CONFIG::PcieRpDpcMask

Offset 0x0248 - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 636 of file FspsUpd.h.

10.10.2.159 PcieRpFunctionSwap

UINT8 FSP_S_CONFIG::PcieRpFunctionSwap

Offset 0x0779 - 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 2039 of file FspsUpd.h.

10.10.2.160 PcieRpGen3EqPh3Method

UINT8 FSP_S_CONFIG::PcieRpGen3EqPh3Method[24]

Offset 0x0694 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_METHOD).

0: DEPRECATED, hardware equalization; 1: hardware equalization; 4: Fixed Coefficients.

Definition at line 1961 of file FspUpd.h.

10.10.2.161 PcieRpImrEnabled

```
UINT8 FSP_S_CONFIG::PcieRpImrEnabled
```

Offset 0x077D - PCIE IMR Enables Isolated Memory Region for PCIe.

\$EN_DIS

Definition at line 2065 of file FspUpd.h.

10.10.2.162 PcieRpL1Substates

```
UINT8 FSP_S_CONFIG::PcieRpL1Substates[24]
```

Offset 0x06F4 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUBSTATES_CONTROL).

Default is PchPcieL1SubstatesL1_1_2.

Definition at line 1983 of file FspUpd.h.

10.10.2.163 PcieRpPcieSpeed

```
UINT8 FSP_S_CONFIG::PcieRpPcieSpeed[24]
```

Offset 0x067C - 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 1955 of file FspUpd.h.

10.10.2.164 PcieRpPhysicalSlotNumber

```
UINT8 FSP_S_CONFIG::PcieRpPhysicalSlotNumber[24]
```

Offset 0x06AC - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 1966 of file FspUpd.h.

10.10.2.165 PcieRpPtmMask

```
UINT32 FSP_S_CONFIG::PcieRpPtmMask
```

Offset 0x0244 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 630 of file FspUpd.h.

10.10.2.166 PcieSwEqCoeffListCm

UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCm[5]

Offset 0x076C - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.

Coefficient C-1.

Definition at line 2008 of file FspUpd.h.

10.10.2.167 PcieSwEqCoeffListCp

UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCp[5]

Offset 0x0771 - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

Coefficient C+1.

Definition at line 2013 of file FspUpd.h.

10.10.2.168 PmcCpuC10GatePinEnable

UINT8 FSP_S_CONFIG::PmcCpuC10GatePinEnable

Offset 0x08DD - Pmc Cpu C10 Gate Pin Enable Enable/Disable platform support for CPU_C10_GATE# pin to control gating of CPU VccIO and VccSTG rails instead of SLP_S0# pin.

\$EN_DIS

Definition at line 2793 of file FspUpd.h.

10.10.2.169 PmcDbgMsgEn

UINT8 FSP_S_CONFIG::PmcDbgMsgEn

Offset 0x0270 - PMC Debug Message Enable When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug messages to trace hub.

Noted: When Enabled, may not enter S0ix \$EN_DIS

Definition at line 760 of file FspUpd.h.

10.10.2.170 PmcGrTscEnable

UINT8 FSP_S_CONFIG::PmcGrTscEnable

Offset 0x08E1 - Global Reset TSC Enable Enable/Disable PMC Global Reset Three Strike Counter feature.

If enabled, PMC will keep the platform in S5 after the third consecutive type 7 global reset occurs during boot flow \$EN_DIS

Definition at line 2819 of file FspUpd.h.

10.10.2.171 PmcModPhySusPgEnable

UINT8 FSP_S_CONFIG::PmcModPhySusPgEnable

Offset 0x0348 - ModPHY SUS Power Domain Dynamic Gating Enable/Disable ModPHY SUS Power Domain Dynamic Gating.

Setting not supported on PCH-H. 0: disable, 1: enable \$EN_DIS

Definition at line 1045 of file FspUpd.h.

10.10.2.172 PmcPowerButtonDebounce

UINT32 FSP_S_CONFIG::PmcPowerButtonDebounce

Offset 0x0254 - Power button debounce configuration Debounce time for PWRBTN in microseconds.

For values not supported by HW, they will be rounded down to closest supported on. 0: disable, 250-1024000us: supported range

Definition at line 659 of file FspUpd.h.

10.10.2.173 PmcV1p05IsExtFetControlEn

UINT8 FSP_S_CONFIG::PmcV1p05IsExtFetControlEn

Offset 0x034A - V1p05-IS supply external FET control Enable/Disable control using EXT_PWR_GATE2# pin of external FET to power gate v1p05-IS supply.

0: disable, 1: enable \$EN_DIS

Definition at line 1059 of file FspUpd.h.

10.10.2.174 PmcV1p05PhyExtFetControlEn

UINT8 FSP_S_CONFIG::PmcV1p05PhyExtFetControlEn

Offset 0x0349 - V1p05-PHY supply external FET control Enable/Disable control using EXT_PWR_GATE# pin of external FET to power gate v1p05-PHY supply.

0: disable, 1: enable \$EN_DIS

Definition at line 1052 of file FspUpd.h.

10.10.2.175 PortUsb20Enable

UINT8 FSP_S_CONFIG::PortUsb20Enable[16]

Offset 0x0057 - 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 198 of file FspUpd.h.

10.10.2.176 PortUsb30Enable

UINT8 FSP_S_CONFIG::PortUsb30Enable[10]

Offset 0x0067 - 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 204 of file FspUpd.h.

10.10.2.177 PpinSupport

UINT8 FSP_S_CONFIG::PpinSupport

Offset 0x045C - PpinSupport to view Protected Processor Inventory Number Enable or Disable or Auto (Based on End of Manufacturing flag.

Disabled if this flag is set) for PPIN Support 0: Disable, 1: Enable, 2: Auto

Definition at line 1567 of file FspUpd.h.

10.10.2.178 Psi1Threshold

UINT16 FSP_S_CONFIG::Psi1Threshold[5]

Offset 0x0418 - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cutoff in 1/4 Amp increments.

Range is 0-128A.

Definition at line 1464 of file FspUpd.h.

10.10.2.179 Psi2Threshold

UINT16 FSP_S_CONFIG::Psi2Threshold[5]

Offset 0x0422 - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cutoff in 1/4 Amp increments.

Range is 0-128A.

Definition at line 1469 of file FspUpd.h.

10.10.2.180 Psi3Enable

UINT8 FSP_S_CONFIG::Psi3Enable[5]

Offset 0x03CB - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; **1: Enable.**

For all VR Indexes

Definition at line 1353 of file FspUpd.h.

10.10.2.181 Psi3Threshold

UINT16 FSP_S_CONFIG::Psi3Threshold[5]

Offset 0x042C - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cutoff in 1/4 Amp increments.

Range is 0-128A.

Definition at line 1474 of file FspUpd.h.

10.10.2.182 PsOnEnable

UINT8 FSP_S_CONFIG::PsOnEnable

Offset 0x08DC - Enable PS_ON.

PS_ON is a new C10 state from the CPU on desktop SKUs that enables a lower power target that will be required by the California Energy Commission (CEC). When FALSE, PS_ON is to be disabled. \$EN_DIS

Definition at line 2786 of file FspUpd.h.

10.10.2.183 PsysOffset

UINT8 FSP_S_CONFIG::PsysOffset

Offset 0x03F4 - 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 1407 of file FspUpd.h.

10.10.2.184 PsysSlope

UINT8 FSP_S_CONFIG::PsysSlope

Offset 0x03F3 - 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 1401 of file FspUpd.h.

10.10.2.185 PxRcConfig

UINT8 FSP_S_CONFIG::PxRcConfig[8]

Offset 0x0079 - 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 232 of file FspUpd.h.

10.10.2.186 RemoteAssistance

UINT8 FSP_S_CONFIG::RemoteAssistance

Offset 0x02AC - Remote Assistance Trigger Availabilty Enable/Disable.

0: Disable, 1: enable, Remote Assistance enable/disable state by Mebx \$EN_DIS

Definition at line 988 of file FspUpd.h.

10.10.2.187 RtcBiosInterfaceLock

UINT8 FSP_S_CONFIG::RtcBiosInterfaceLock

Offset 0x0518 - RTC BIOS Interface Lock Enable RTC BIOS interface lock.

When set, prevents RTC TS (BUC.TS) from being changed. \$EN_DIS

Definition at line 1816 of file FspUpd.h.

10.10.2.188 RtcMemoryLock

UINT8 FSP_S_CONFIG::RtcMemoryLock

Offset 0x0519 - RTC Cmos Memory Lock Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.

\$EN_DIS

Definition at line 1823 of file FspUpd.h.

10.10.2.189 SaPcieComplianceTestMode

UINT8 FSP_S_CONFIG::SaPcieComplianceTestMode

Offset 0x09B1 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

\$EN_DIS

Definition at line 2910 of file FspUpd.h.

10.10.2.190 SaPcieDeviceOverrideTablePtr

UINT32 FSP_S_CONFIG::SaPcieDeviceOverrideTablePtr

Offset 0x09B4 - 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 SA_PCIE_DEVICE_OVERRIDE structure for the table. Last entry VendorId must be 0.

Definition at line 2930 of file FspUpd.h.

10.10.2.191 SaPcieDisableRootPortClockGating

UINT8 FSP_S_CONFIG::SaPcieDisableRootPortClockGating

Offset 0x09AF - 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 2897 of file FspUpd.h.

10.10.2.192 SaPcieDisableRootPortPowerGating

UINT8 FSP_S_CONFIG::SaPcieDisableRootPortPowerGating

Offset 0x09B0 - PCIE Disable RootPort Power Gating Describes whether the PCI Express Power Gating for each root port is enabled by platform modules.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 2904 of file FspUpd.h.

10.10.2.193 SaPcieEnablePeerMemoryWrite

UINT8 FSP_S_CONFIG::SaPcieEnablePeerMemoryWrite

Offset 0x09B2 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

\$EN_DIS

Definition at line 2916 of file FspUpd.h.

10.10.2.194 SaPcieEqPh3LaneParamCm

UINT8 FSP_S_CONFIG::SaPcieEqPh3LaneParamCm[32]

Offset 0x08E3 - PCIE Eq Ph3 Lane Param Cm SA_PCIE_EQ_LANE_PARAM.

Coefficient C-1.

Definition at line 2831 of file FspUpd.h.

10.10.2.195 SaPcieEqPh3LaneParamCp

UINT8 FSP_S_CONFIG::SaPcieEqPh3LaneParamCp[32]

Offset 0x0903 - PCIE Eq Ph3 Lane Param Cp SA_PCIE_EQ_LANE_PARAM.

Coefficient C+1.

Definition at line 2836 of file FspUpd.h.

10.10.2.196 SaPcieGen3EndPointHint

UINT8 FSP_S_CONFIG::SaPcieGen3EndPointHint [20]

Offset 0x0987 - Pcie Gen3 End port Hint values per lane Used for programming Pcie Gen3 Hint values per lane.

Range: 0-6, 2 is default for each lane

Definition at line 2885 of file FspUpd.h.

10.10.2.197 SaPcieGen3EndPointPreset

UINT8 FSP_S_CONFIG::SaPcieGen3EndPointPreset [20]

Offset 0x095F - Pcie Gen3 End port preset values per lane Used for programming Pcie Gen3 preset values per lane.

Range: 0-9, 7 is default for each lane

Definition at line 2874 of file FspUpd.h.

10.10.2.198 SaPcieGen3ProgramStaticEq

UINT8 FSP_S_CONFIG::SaPcieGen3ProgramStaticEq

Offset 0x077A - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program 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 2046 of file FspUpd.h.

10.10.2.199 SaPcieGen3RootPortPreset

UINT8 FSP_S_CONFIG::SaPcieGen3RootPortPreset [20]

Offset 0x0937 - Gen3 Root port preset values per lane Used for programming Pcie Gen3 preset values per lane.

Range: 0-9, 8 is default for each lane

Definition at line 2862 of file FspUpd.h.

10.10.2.200 SaPcieGen4EndPointHint

UINT8 FSP_S_CONFIG::SaPcieGen4EndPointHint [20]

Offset 0x099B - Pcie Gen4 End port Hint values per lane Used for programming Pcie Gen4 Hint values per lane.

Range: 0-6, 2 is default for each lane

Definition at line 2890 of file FspUpd.h.

10.10.2.201 SaPcieGen4EndPointPreset

UINT8 FSP_S_CONFIG::SaPcieGen4EndPointPreset [20]

Offset 0x0973 - Pcie Gen4 End port preset values per lane Used for programming Pcie Gen4 preset values per lane.

Range: 0-9, 7 is default for each lane

Definition at line 2880 of file FspUpd.h.

10.10.2.202 SaPcieGen4ProgramStaticEq

UINT8 FSP_S_CONFIG::SaPcieGen4ProgramStaticEq

Offset 0x077B - Enable/Disable GEN4 Static EQ Phase1 programming Program Gen4 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 2053 of file FspUpd.h.

10.10.2.203 SaPcieGen4RootPortPreset

UINT8 FSP_S_CONFIG::SaPcieGen4RootPortPreset [20]

Offset 0x094B - Pcie Gen4 Root port preset values per lane Used for programming Pcie Gen4 preset values per lane.

Range: 0-9, 8 is default for each lane

Definition at line 2868 of file FspUpd.h.

10.10.2.204 SaPcieHwEqGen3CoeffListCm

UINT8 FSP_S_CONFIG::SaPcieHwEqGen3CoeffListCm [5]

Offset 0x0923 - PCIE Hw Eq Gen3 CoeffList Cm SA_PCIE_EQ_PARAM.

Coefficient C-1.

Definition at line 2841 of file FspUpd.h.

10.10.2.205 SaPcieHwEqGen3CoeffListCp

UINT8 FSP_S_CONFIG::SaPcieHwEqGen3CoeffListCp [5]

Offset 0x0928 - PCIE Hw Eq Gen3 CoeffList Cp SA_PCIE_EQ_PARAM.

Coefficient C+1.

Definition at line 2846 of file FspUpd.h.

10.10.2.206 SaPcieHwEqGen4CoeffListCm

UINT8 FSP_S_CONFIG::SaPcieHwEqGen4CoeffListCm[5]

Offset 0x092D - PCIE Hw Eq Gen4 CoeffList Cm SA_PCIE_EQ_PARAM.

Coefficient C-1.

Definition at line 2851 of file FspUpd.h.

10.10.2.207 SaPcieHwEqGen4CoeffListCp

UINT8 FSP_S_CONFIG::SaPcieHwEqGen4CoeffListCp[5]

Offset 0x0932 - PCIE Hw Eq Gen4 CoeffList Cp SA_PCIE_EQ_PARAM.

Coefficient C+1.

Definition at line 2856 of file FspUpd.h.

10.10.2.208 SaPcieRpAspm

UINT8 FSP_S_CONFIG::SaPcieRpAspm[4]

Offset 0x0A18 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH_PCIE_ASPM_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 3069 of file FspUpd.h.

10.10.2.209 SaPcieRpDpcEnabled

UINT8 FSP_S_CONFIG::SaPcieRpDpcEnabled[4]

Offset 0x09EC - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 3001 of file FspUpd.h.

10.10.2.210 SaPcieRpDpcExtensionsEnabled

UINT8 FSP_S_CONFIG::SaPcieRpDpcExtensionsEnabled[4]

Offset 0x09F0 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 3007 of file FspUpd.h.

10.10.2.211 SaPcieRpFunctionSwap

UINT8 FSP_S_CONFIG::SaPcieRpFunctionSwap

Offset 0x09B3 - 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 2923 of file FspUpd.h.

10.10.2.212 SaPcieRpGen3EqPh23Enable

UINT8 FSP_S_CONFIG::SaPcieRpGen3EqPh23Enable[4]

Offset 0x0A0C - Phase2-3 RP Gen3 EQ enable Phase2-3 Gen3 EQ enable.

Disabled(0x0): Disable Phase2-3, Enabled(0x1): Enable Phase2-3, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 3051 of file FspUpd.h.

10.10.2.213 SaPcieRpGen3EqPh3Enable

UINT8 FSP_S_CONFIG::SaPcieRpGen3EqPh3Enable[4]

Offset 0x0A04 - Phase3 RP Gen3 EQ enable Phase3 Gen3 EQ enable.

Disabled(0x0): Disable phase 3, Enabled(0x1): Enable phase 3, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 3037 of file FspUpd.h.

10.10.2.214 SaPcieRpGen3EqPh3Method

UINT8 FSP_S_CONFIG::SaPcieRpGen3EqPh3Method[4]

Offset 0x09FC - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see SA_PCIE_EQ_METHOD).

0: DEPRECATED, hardware equalization; 1: hardware equalization; 4: Fixed Coefficients.

Definition at line 3024 of file FspUpd.h.

10.10.2.215 SaPcieRpGen4EqPh23Enable

UINT8 FSP_S_CONFIG::SaPcieRpGen4EqPh23Enable[4]

Offset 0x0A10 - Phase2-3 RP Gen4 EQ enable Phase2-3 Gen4 EQ enable.

Disabled(0x0): Disable Phase2-3, Enabled(0x1): Enable Phase2-3, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 3058 of file FspUpd.h.

10.10.2.216 SaPcieRpGen4EqPh3Enable

UINT8 FSP_S_CONFIG::SaPcieRpGen4EqPh3Enable[4]

Offset 0x0A08 - Phase3 RP Gen4 EQ enable Phase3 Gen4 EQ enable.

Disabled(0x0): Disable phase 3, Enabled(0x1): Enable phase 3, Auto(0x2)(Default): Use the current default method
0:Disable, 1:Enable, 2:Auto

Definition at line 3044 of file FspsUpd.h.

10.10.2.217 SaPcieRpGen4EqPh3Method

```
UINT8 FSP_S_CONFIG::SaPcieRpGen4EqPh3Method[4]
```

Offset 0x0A00 - PCIE RP Gen4 Equalization Phase Method PCIe Gen4 Eq Ph3 Method (see SA_PCIE_EQ_METHODOD).

0: DEPRECATED, hardware equalization; 1: hardware equalization; 4: Fixed Coeficients.

Definition at line 3030 of file FspsUpd.h.

10.10.2.218 SaPcieRpL1Substates

```
UINT8 FSP_S_CONFIG::SaPcieRpL1Substates[4]
```

Offset 0x0A1C - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: SA_PCIE_L1SUBSTATES_CONTROL).

Default is SaPcieL1SubstatesL1_1_2.

Definition at line 3075 of file FspsUpd.h.

10.10.2.219 SaPcieRpPcieSpeed

```
UINT8 FSP_S_CONFIG::SaPcieRpPcieSpeed[4]
```

Offset 0x09F8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.

0: Auto; 1: Gen1; 2: Gen2; 3: Gen3; 4: Gen4 (see: SA_PCIE_SPEED).

Definition at line 3018 of file FspsUpd.h.

10.10.2.220 SaPcieRpPhysicalSlotNumber

```
UINT8 FSP_S_CONFIG::SaPcieRpPhysicalSlotNumber[4]
```

Offset 0x0A14 - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 3063 of file FspsUpd.h.

10.10.2.221 SaPcieRpPtmEnabled

```
UINT8 FSP_S_CONFIG::SaPcieRpPtmEnabled[4]
```

Offset 0x0A28 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 3091 of file FspUpd.h.

10.10.2.222 SaPcieRpVcEnabled

UINT8 FSP_S_CONFIG::SaPcieRpVcEnabled[4]

Offset 0x0A34 - VC for PCIE RP Mask Enable/disable Virtual Channel for PCIE Root Ports.

0: disable, 1: enable. One bit for each port, bit0 for port1, bit1 for port2, and so on.

Definition at line 3104 of file FspUpd.h.

10.10.2.223 SataEnable

UINT8 FSP_S_CONFIG::SataEnable

Offset 0x008D - Enable SATA Enable/disable SATA controller.

\$EN_DIS

Definition at line 278 of file FspUpd.h.

10.10.2.224 SataLedEnable

UINT8 FSP_S_CONFIG::SataLedEnable

Offset 0x029C - SATA LED SATA LED indicating SATA controller activity.

0: disable, 1: enable \$EN_DIS

Definition at line 904 of file FspUpd.h.

10.10.2.225 SataMode

UINT8 FSP_S_CONFIG::SataMode

Offset 0x008E - SATA Mode Select SATA controller working mode.

0:AHCI, 1:RAID

Definition at line 284 of file FspUpd.h.

10.10.2.226 SataP0TDispFinit

UINT8 FSP_S_CONFIG::SataP0TDispFinit

Offset 0x0822 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.

\$EN_DIS

Definition at line 2538 of file FspUpd.h.

10.10.2.227 SataP1TDispFinit

UINT8 FSP_S_CONFIG::SataP1TDispFinit

Offset 0x0824 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.

\$EN_DIS

Definition at line 2549 of file FspUpd.h.

10.10.2.228 SataPortsDevSlp

UINT8 FSP_S_CONFIG::SataPortsDevSlp[8]

Offset 0x004F - 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 192 of file FspUpd.h.

10.10.2.229 SataPortsDmVal

UINT8 FSP_S_CONFIG::SataPortsDmVal[8]

Offset 0x07C9 - Enable SATA Port DmVal DITO multiplier.

Default is 15.

Definition at line 2260 of file FspUpd.h.

10.10.2.230 SataPortsEnable

UINT8 FSP_S_CONFIG::SataPortsEnable[8]

Offset 0x0047 - Enable SATA ports Enable/disable SATA ports.

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

Definition at line 186 of file FspUpd.h.

10.10.2.231 SataPwrOptEnable

UINT8 FSP_S_CONFIG::SataPwrOptEnable

Offset 0x0796 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.

\$EN_DIS

Definition at line 2214 of file FspUpd.h.

10.10.2.232 SataRstHddUnlock

UINT8 FSP_S_CONFIG::SataRstHddUnlock

Offset 0x07F2 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.

\$EN_DIS

Definition at line 2327 of file FspUpd.h.

10.10.2.233 SataRstInterrupt

UINT8 FSP_S_CONFIG::SataRstInterrupt

Offset 0x08DA - SATA RST Interrupt Mode Allows to choose which interrupts will be implemented by SATA controller in RAID mode.

0:Msix, 1:Msi, 2:Legacy

Definition at line 2770 of file FspUpd.h.

10.10.2.234 SataRstIrrt

UINT8 FSP_S_CONFIG::SataRstIrrt

Offset 0x07EF - PCH Sata Rst Irrt Intel Rapid Recovery Technology.

\$EN_DIS

Definition at line 2310 of file FspUpd.h.

10.10.2.235 SataRstIrrtOnly

UINT8 FSP_S_CONFIG::SataRstIrrtOnly

Offset 0x07F4 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.

\$EN_DIS

Definition at line 2340 of file FspUpd.h.

10.10.2.236 SataRstLedLocate

UINT8 FSP_S_CONFIG::SataRstLedLocate

Offset 0x07F3 - 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 2334 of file FspUpd.h.

10.10.2.237 SataRstOromUiBanner

UINT8 FSP_S_CONFIG::SataRstOromUiBanner

Offset 0x07F0 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.

\$EN_DIS

Definition at line 2316 of file FspUpd.h.

10.10.2.238 SataRstPcieDeviceResetDelay

UINT8 FSP_S_CONFIG::SataRstPcieDeviceResetDelay[3]

Offset 0x07FC - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.

Default value is 100ms

Definition at line 2361 of file FspUpd.h.

10.10.2.239 SataRstRaid0

UINT8 FSP_S_CONFIG::SataRstRaid0

Offset 0x07EB - PCH Sata Rst Raid0 RAID0.

\$EN_DIS

Definition at line 2286 of file FspUpd.h.

10.10.2.240 SataRstRaid1

UINT8 FSP_S_CONFIG::SataRstRaid1

Offset 0x07EC - PCH Sata Rst Raid1 RAID1.

\$EN_DIS

Definition at line 2292 of file FspUpd.h.

10.10.2.241 SataRstRaid10

UINT8 FSP_S_CONFIG::SataRstRaid10

Offset 0x07ED - PCH Sata Rst Raid10 RAID10.

\$EN_DIS

Definition at line 2298 of file FspUpd.h.

10.10.2.242 SataRstRaid5

UINT8 FSP_S_CONFIG::SataRstRaid5

Offset 0x07EE - PCH Sata Rst Raid5 RAID5.

\$EN_DIS

Definition at line 2304 of file FspUpd.h.

10.10.2.243 SataRstRaidDeviceId

UINT8 FSP_S_CONFIG::SataRstRaidDeviceId

Offset 0x07EA - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.

\$EN_DIS

Definition at line 2280 of file FspUpd.h.

10.10.2.244 SataRstSmartStorage

UINT8 FSP_S_CONFIG::SataRstSmartStorage

Offset 0x07F5 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.

\$EN_DIS

Definition at line 2346 of file FspUpd.h.

10.10.2.245 SataSalpSupport

UINT8 FSP_S_CONFIG::SataSalpSupport

Offset 0x0045 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.

\$EN_DIS

Definition at line 174 of file FspUpd.h.

10.10.2.246 SataThermalSuggestedSetting

UINT8 FSP_S_CONFIG::SataThermalSuggestedSetting

Offset 0x0825 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.

\$EN_DIS

Definition at line 2555 of file FspUpd.h.

10.10.2.247 ScIirqSelect

UINT8 FSP_S_CONFIG::SciIirqSelect

Offset 0x0082 - Select ScIirqSelect SCI IRQ Select.

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

Definition at line 242 of file FspUpd.h.

10.10.2.248 ScsEmmcEnabled

UINT8 FSP_S_CONFIG::ScsEmmcEnabled

Offset 0x0036 - Enable eMMC Controller Enable/disable eMMC Controller.

\$EN_DIS

Definition at line 130 of file FspUpd.h.

10.10.2.249 ScsEmmcHs400Enabled

```
UINT8 FSP_S_CONFIG::ScsEmmcHs400Enabled
```

Offset 0x0037 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.

\$EN_DIS

Definition at line 136 of file FspUpd.h.

10.10.2.250 ScsSdCardEnabled

```
UINT8 FSP_S_CONFIG::ScsSdCardEnabled
```

Offset 0x0038 - Enable SdCard Controller Enable/disable SD Card Controller.

\$EN_DIS

Definition at line 142 of file FspUpd.h.

10.10.2.251 SendEcCmd

```
UINT64 FSP_S_CONFIG::SendEcCmd
```

Offset 0x0888 - SendEcCmd SendEcCmd function pointer.

```
typedef EFI_STATUS (EFI_API *PLATFORM_SEND_EC_COMMAND) (IN EC_COMMAND_TYPE  
EcCmdType, IN UINT8 EcCmd, IN UINT8 SendData, IN OUT UINT8 *ReceiveData);
```

Definition at line 2688 of file FspUpd.h.

10.10.2.252 SendVrMbxCmd

```
UINT8 FSP_S_CONFIG::SendVrMbxCmd
```

Offset 0x044C - 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 1506 of file FspUpd.h.

10.10.2.253 SerialIoDebugUartNumber

```
UINT8 FSP_S_CONFIG::SerialIoDebugUartNumber
```

Offset 0x0178 - UART Number For Debug Purpose UART number for debug purpose.

0:UART0, 1:UART1, 2:UART2, 3:UART3, 4:UART4, 5:UART5, 6:UART6. Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:UART0, 1:UART1, 2:UART2, 3:UART3, 4:UART4, 5:UART5, 6:UART6

Definition at line 452 of file FspUpd.h.

10.10.2.254 SerialIoI2cMode

```
UINT8 FSP_S_CONFIG::SerialIoI2cMode[8]
```

Offset 0x0179 - I2Cn Device Mode Selects I2c operation mode.

N represents controller index: I2c0, I2c1, ... Available modes: 0:SerialIoI2cDisabled, 1:SerialIoI2cPci, 2:SerialIoI2cHidden

Definition at line 458 of file FspUpd.h.

10.10.2.255 SerialIoSpi0CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi0CsEnable[2]
```

Offset 0x00A4 - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 337 of file FspUpd.h.

10.10.2.256 SerialIoSpi0CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi0CsPolarity[2]
```

Offset 0x0096 - SPI0 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 296 of file FspUpd.h.

10.10.2.257 SerialIoSpi1CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsEnable[2]
```

Offset 0x00A6 - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 342 of file FspUpd.h.

10.10.2.258 SerialIoSpi1CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsPolarity[2]
```

Offset 0x0098 - SPI1 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 302 of file FspsUpd.h.

10.10.2.259 SerialIoSpi2CsEnable

UINT8 FSP_S_CONFIG::SerialIoSpi2CsEnable[2]

Offset 0x00A8 - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 347 of file FspsUpd.h.

10.10.2.260 SerialIoSpi2CsPolarity

UINT8 FSP_S_CONFIG::SerialIoSpi2CsPolarity[2]

Offset 0x009A - SPI2 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 308 of file FspsUpd.h.

10.10.2.261 SerialIoSpi3CsEnable

UINT8 FSP_S_CONFIG::SerialIoSpi3CsEnable[2]

Offset 0x00AA - SPI3 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 352 of file FspsUpd.h.

10.10.2.262 SerialIoSpi3CsPolarity

UINT8 FSP_S_CONFIG::SerialIoSpi3CsPolarity[2]

Offset 0x009C - SPI3 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 314 of file FspsUpd.h.

10.10.2.263 SerialIoSpi4CsEnable

UINT8 FSP_S_CONFIG::SerialIoSpi4CsEnable[2]

Offset 0x00AC - SPI4 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 357 of file FspsUpd.h.

10.10.2.264 SerialIoSpi4CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi4CsPolarity[2]
```

Offset 0x009E - SPI4 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 320 of file FspsUpd.h.

10.10.2.265 SerialIoSpi5CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi5CsEnable[2]
```

Offset 0x00AE - SPI5 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 362 of file FspsUpd.h.

10.10.2.266 SerialIoSpi5CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi5CsPolarity[2]
```

Offset 0x00A0 - SPI5 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 326 of file FspsUpd.h.

10.10.2.267 SerialIoSpi6CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi6CsEnable[2]
```

Offset 0x00B0 - SPI6 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 367 of file FspsUpd.h.

10.10.2.268 SerialIoSpi6CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi6CsPolarity[2]
```

Offset 0x00A2 - SPI6 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 332 of file FspsUpd.h.

10.10.2.269 SerialIoSpiDefaultCsOutput

```
UINT8 FSP_S_CONFIG::SerialIoSpiDefaultCsOutput[7]
```

Offset 0x00B2 - SPIn Default Chip Select Output Sets Default CS as Output.

N represents controller index: SPI0, SPI1, ... Available options: 0:CS0, 1:CS1

Definition at line 373 of file FspsUpd.h.

10.10.2.270 SerialIoSpiMode

UINT8 FSP_S_CONFIG::SerialIoSpiMode[7]

Offset 0x008F - SPIn Device Mode Selects SPI operation mode.

N represents controller index: SPI0, SPI1, ... Available modes: 0:SerialIoSpiDisabled, 1:SerialIoSpiPci, 2:SerialIoSpiHidden

Definition at line 290 of file FspsUpd.h.

10.10.2.271 SerialIoUartCtsPinMuxPolicy

UINT32 FSP_S_CONFIG::SerialIoUartCtsPinMuxPolicy[7]

Offset 0x0124 - SerialIoUartCtsPinMuxPolicy Select SerialIo Uart Cts pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_CTS* for possible values.

Definition at line 432 of file FspsUpd.h.

10.10.2.272 SerialIoUartDataBits

UINT8 FSP_S_CONFIG::SerialIoUartDataBits[7]

Offset 0x00E3 - Default DataBits for each Serial IO UART Set default word length.

0: Default, 5,6,7,8

Definition at line 395 of file FspsUpd.h.

10.10.2.273 SerialIoUartDmaEnable

UINT8 FSP_S_CONFIG::SerialIoUartDmaEnable[7]

Offset 0x00F8 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.

0: Disabled, 1: Enabled

Definition at line 411 of file FspsUpd.h.

10.10.2.274 SerialIoUartMode

UINT8 FSP_S_CONFIG::SerialIoUartMode[7]

Offset 0x00B9 - UARTn Device Mode Selects Uart operation mode.

N represents controller index: Uart0, Uart1, ... Available modes: 0:SerialIoUartDisabled, 1:SerialIoUartPci, 2:SerialIoUartHidden, 3:SerialIoUartCom, 4:SerialIoUartSkipInit

Definition at line 380 of file FspsUpd.h.

10.10.2.275 SerialIoUartParity

UINT8 FSP_S_CONFIG::SerialIoUartParity[7]

Offset 0x00DC - Default ParityType for each Serial IO UART Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 390 of file FspUpd.h.

10.10.2.276 SerialIoUartPowerGating

UINT8 FSP_S_CONFIG::SerialIoUartPowerGating[7]

Offset 0x00F1 - Power Gating mode for each Serial IO UART that works in COM mode Set Power Gating.

0: Disabled, 1: Enabled, 2: Auto

Definition at line 406 of file FspUpd.h.

10.10.2.277 SerialIoUartRtsPinMuxPolicy

UINT32 FSP_S_CONFIG::SerialIoUartRtsPinMuxPolicy[7]

Offset 0x0108 - SerialIoUartRtsPinMuxPolicy Select SerialIo Uart Rts pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_RTS* for possible values.

Definition at line 426 of file FspUpd.h.

10.10.2.278 SerialIoUartRxPinMuxPolicy

UINT32 FSP_S_CONFIG::SerialIoUartRxPinMuxPolicy[7]

Offset 0x0140 - SerialIoUartRxPinMuxPolicy Select SerialIo Uart Rx pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_RX* for possible values.

Definition at line 438 of file FspUpd.h.

10.10.2.279 SerialIoUartStopBits

UINT8 FSP_S_CONFIG::SerialIoUartStopBits[7]

Offset 0x00EA - Default StopBits for each Serial IO UART Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 401 of file FspUpd.h.

10.10.2.280 SerialIoUartTxPinMuxPolicy

UINT32 FSP_S_CONFIG::SerialIoUartTxPinMuxPolicy[7]

Offset 0x015C - SerialIoUartTxPinMuxPolicy Select SerialIoUart Tx pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_TX* for possible values.

Definition at line 444 of file FspsUpd.h.

10.10.2.281 ShowSpiController

UINT8 FSP_S_CONFIG::ShowSpiController

Offset 0x0039 - Show SPI controller Enable/disable to show SPI controller.

\$EN_DIS

Definition at line 148 of file FspsUpd.h.

10.10.2.282 SiCsmFlag

UINT8 FSP_S_CONFIG::SiCsmFlag

Offset 0x08D0 - Si Config CSM Flag.

Platform specific common policies that used by several silicon components. CSM status flag. \$EN_DIS

Definition at line 2752 of file FspsUpd.h.

10.10.2.283 SkipMpInit

UINT8 FSP_S_CONFIG::SkipMpInit

Offset 0x044F - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SilicionInit API.

0: Initialize; **1: Skip \$EN_DIS**

Definition at line 1524 of file FspsUpd.h.

10.10.2.284 SlowSlewRateForFivr

UINT8 FSP_S_CONFIG::SlowSlewRateForFivr

Offset 0x0454 - Slew Rate configuration for Deep Package C States for VR FIVR domain Slew Rate configuration for Deep Package C States for VR FIVR domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 1551 of file FspsUpd.h.

10.10.2.285 SlowSlewRateForGt

UINT8 FSP_S_CONFIG::SlowSlewRateForGt

Offset 0x03F8 - 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 1434 of file FspUpd.h.

10.10.2.286 SlowSlewRateForIa

UINT8 FSP_S_CONFIG::SlowSlewRateForIa

Offset 0x03F7 - 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 1427 of file FspUpd.h.

10.10.2.287 SlowSlewRateForSa

UINT8 FSP_S_CONFIG::SlowSlewRateForSa

Offset 0x03F9 - 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 1441 of file FspUpd.h.

10.10.2.288 SlpS0DisQForDebug

UINT8 FSP_S_CONFIG::SlpS0DisQForDebug

Offset 0x078A - S0ix Override Settings 'No Change' will keep PMC BWG settings.

Or select the desired debug probe type for S0ix Override settings.

Reminder: DCI OOB (aka BSSB) uses CCA probe. 0:No Change, 1:DCI OOB, 2:USB2 DbC

Definition at line 2142 of file FspUpd.h.

10.10.2.289 SlpS0Override

UINT8 FSP_S_CONFIG::SlpS0Override

Offset 0x0789 - SLP_S0# Override Enabled will toggle SLP_S0# assertion Disabled will enable SLP_S0# assertion when debug is enabled.

0:Disabled, 1:Enabled

Definition at line 2134 of file FspUpd.h.

10.10.2.290 TcolrqSelect

UINT8 FSP_S_CONFIG::TcoIrqSelect

Offset 0x0083 - Select TcolrqSelect TCO IRQ Select.

The valid value is 9, 10, 11, 20, 21, 22, 23.

Definition at line 247 of file FspUpd.h.

10.10.2.291 TcssAuxOri

UINT16 FSP_S_CONFIG::TcssAuxOri

Offset 0x03B8 - TCSS Aux Orientation Override Enable Bits 0, 2, ...

10 control override enables, bits 1, 3, ... 11 control overrides

Definition at line 1295 of file FspUpd.h.

10.10.2.292 TcssHslOri

UINT16 FSP_S_CONFIG::TcssHslOri

Offset 0x03BA - TCSS HSL Orientation Override Enable Bits 0, 2, ...

10 control override enables, bits 1, 3, ... 11 control overrides

Definition at line 1300 of file FspUpd.h.

10.10.2.293 TdcPowerLimit

UINT16 FSP_S_CONFIG::TdcPowerLimit[5]

Offset 0x03FA - 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 1447 of file FspUpd.h.

10.10.2.294 TdcTimeWindow

UINT8 FSP_S_CONFIG::TdcTimeWindow[5]

Offset 0x03E9 - 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 1389 of file FspUpd.h.

10.10.2.295 ThcPort0InterruptPinMuxing

UINT32 FSP_S_CONFIG::ThcPort0InterruptPinMuxing

Offset 0x0670 - THC Port 0 Interrupt Pin Mux Set THC Port 0 Pin Muxing Value if signal can be enabled on multiple pads.

Refer to GPIO_*_MUXING_THC_SPIx_INTB_* for possible values.

Definition at line 1921 of file FspUpd.h.

10.10.2.296 ThcPort1InterruptPinMuxing

UINT32 FSP_S_CONFIG::ThcPort1InterruptPinMuxing

Offset 0x0678 - THC Port 1 Interrupt Pin Mux Set THC Port 1 Pin Muxing Value if signal can be enabled on multiple pads.

Refer to GPIO*_MUXING_THC_SPI*_INTB_* for possible values.

Definition at line 1949 of file FspUpd.h.

10.10.2.297 TTSuggestedSetting

UINT8 FSP_S_CONFIG::TTSuggestedSetting

Offset 0x0811 - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.

\$EN_DIS

Definition at line 2445 of file FspUpd.h.

10.10.2.298 TurboMode

UINT8 FSP_S_CONFIG::TurboMode

Offset 0x0044 - Turbo Mode Enable/Disable Turbo mode.

0: disable, 1: enable \$EN_DIS

Definition at line 168 of file FspUpd.h.

10.10.2.299 TxtEnable

UINT8 FSP_S_CONFIG::TxtEnable

Offset 0x044E - Enable or Disable TXT Enable or Disable TXT; 0: Disable; **1: Enable.**

\$EN_DIS

Definition at line 1517 of file FspUpd.h.

10.10.2.300 UfsEnable

UINT8 FSP_S_CONFIG::UfsEnable[2]

Offset 0x07FF - UFS enable/disable PCIe Storage Device Reset Delay in milliseconds.

Default value is 100ms \$EN_DIS

Definition at line 2367 of file FspUpd.h.

10.10.2.301 Usb2PhyPehalfbit

UINT8 FSP_S_CONFIG::Usb2PhyPehalfbit[16]

Offset 0x01FC - 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 506 of file FspsUpd.h.

10.10.2.302 Usb2PhyPetxiset

UINT8 FSP_S_CONFIG::Usb2PhyPetxiset[16]

Offset 0x01CC - 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 488 of file FspsUpd.h.

10.10.2.303 Usb2PhyPredeemp

UINT8 FSP_S_CONFIG::Usb2PhyPredeemp[16]

Offset 0x01EC - 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 500 of file FspsUpd.h.

10.10.2.304 Usb2PhyTxiset

UINT8 FSP_S_CONFIG::Usb2PhyTxiset[16]

Offset 0x01DC - 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 494 of file FspsUpd.h.

10.10.2.305 Usb3HsioTxDeEmph

UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmph[10]

Offset 0x0216 - 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 518 of file FspsUpd.h.

10.10.2.306 Usb3HsioTxDeEmphEnable

UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmphEnable[10]

Offset 0x020C - 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 array can be between 0-1. One byte for each port.

Definition at line 512 of file FspsUpd.h.

10.10.2.307 Usb3HsioTxDownscaleAmp

UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmp[10]

Offset 0x022A - 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 530 of file FspsUpd.h.

10.10.2.308 Usb3HsioTxDownscaleAmpEnable

UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmpEnable[10]

Offset 0x0220 - 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 array can be between 0-1.

One byte for each port.

Definition at line 524 of file FspsUpd.h.

10.10.2.309 UsbPdoProgramming

UINT8 FSP_S_CONFIG::UsbPdoProgramming

Offset 0x0250 - USB PDO Programming Enable/disable PDO programming for USB in PEI phase.

Disabling will allow for programming during later phase. 1: enable, 0: disable \$EN_DIS

Definition at line 649 of file FspsUpd.h.

10.10.2.310 UsbTcPortEn

UINT8 FSP_S_CONFIG::UsbTcPortEn

Offset 0x03BD - TCSS USB Port Enable Bits 0, 1, ...

max Type C port control enables

Definition at line 1311 of file FspsUpd.h.

10.10.2.311 VmdEnable

UINT8 FSP_S_CONFIG::VmdEnable

Offset 0x03AC - Enable VMD controller Enable/disable to VMD controller.

\$EN_DIS

Definition at line 1227 of file FspUpd.h.

10.10.2.312 VmdPortA

UINT8 FSP_S_CONFIG::VmdPortA

Offset 0x03AD - Enable VMD portA Support Enable/disable to VMD portA Support.

\$EN_DIS

Definition at line 1233 of file FspUpd.h.

10.10.2.313 VmdPortB

UINT8 FSP_S_CONFIG::VmdPortB

Offset 0x03AE - Enable VMD portB Support Enable/disable to VMD portB Support.

\$EN_DIS

Definition at line 1239 of file FspUpd.h.

10.10.2.314 VmdPortC

UINT8 FSP_S_CONFIG::VmdPortC

Offset 0x03AF - Enable VMD portC Support Enable/disable to VMD portC Support.

\$EN_DIS

Definition at line 1245 of file FspUpd.h.

10.10.2.315 VmdPortD

UINT8 FSP_S_CONFIG::VmdPortD

Offset 0x03B0 - Enable VMD portD Support Enable/disable to VMD portD Support.

\$EN_DIS

Definition at line 1251 of file FspUpd.h.

10.10.2.316 VrVoltageLimit

UINT16 FSP_S_CONFIG::VrVoltageLimit[5]

Offset 0x0440 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.

Range is 0-7999mV.

Definition at line 1484 of file FspUpd.h.

10.10.2.317 WatchDog

UINT8 FSP_S_CONFIG::WatchDog

Offset 0x02A2 - WatchDog Timer Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable WatchDog timer. \$EN_DIS

Definition at line 941 of file FspUpd.h.

10.10.2.318 WatchDogTimerBios

UINT16 FSP_S_CONFIG::WatchDogTimerBios

Offset 0x02AA - BIOS Timer 16 bits Value, Set BIOS watchdog timer.

\$EN_DIS

Definition at line 982 of file FspUpd.h.

10.10.2.319 WatchDogTimerOs

UINT16 FSP_S_CONFIG::WatchDogTimerOs

Offset 0x02A8 - OS Timer 16 bits Value, Set OS watchdog timer.

\$EN_DIS

Definition at line 976 of file FspUpd.h.

10.10.2.320 XdciEnable

UINT8 FSP_S_CONFIG::XdciEnable

Offset 0x0071 - Enable xDCI controller Enable/disable to xDCI controller.

\$EN_DIS

Definition at line 210 of file FspUpd.h.

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

- [FspUpd.h](#)

10.11 FSP_S_TEST_CONFIG Struct Reference

Fsp S Test Configuration.

```
#include <FspUpd.h>
```

Public Attributes

- [UINT32 Signature](#)
Offset 0x0A40.
- [UINT8 SkipPamLock](#)
Offset 0x0A44 - Skip PAM regsiter 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 0x0A45 - 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 RenderStandby](#)
Offset 0x0A46 - Enable/Disable IGFX RenderStandby Enable(Default): Enable IGFX RenderStandby, Disable: Disable IGFX RenderStandby \$EN_DIS.
- [UINT8 PmSupport](#)
Offset 0x0A47 - Enable/Disable IGFX PmSupport Enable(Default): Enable IGFX PmSupport, Disable: Disable IGFX PmSupport \$EN_DIS.
- [UINT8 CdynmaxClampEnable](#)
Offset 0x0A48 - Enable/Disable CdynmaxClamp Enable: Enable CdynmaxClamp, Disable(Default): Disable CdynmaxClamp \$EN_DIS.
- [UINT8 VtdDisable](#)
Offset 0x0A49 - Disable VT-d 0=Enable/FALSE(VT-d enabled), 1=Disable/TRUE (VT-d disabled) \$EN_DIS.
- [UINT8 GtFreqMax](#)
Offset 0x0A4A - GT Frequency Limit 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz.
- [UINT8 DisableTurboGt](#)
Offset 0x0A4B - Disable Turbo GT 0=Disable: GT frequency is not limited, 1=Enable: Disables Turbo GT frequency \$EN_DIS.
- [UINT8 SkipCdClockInit](#)
Offset 0x0A4C - Enable/Disable CdClock Init Enable: Skip Full CD clock initializaton, Disable(Default): Initialize the full CD clock if not initialized by Gfx PEIM \$EN_DIS.
- [UINT8 SaPostMemTestRsvd](#) [12]
Offset 0x0A4D - SaPostMemTestRsvd Reserved for SA Post-Mem Test \$EN_DIS.
- [UINT8 EnableRsr](#)
Offset 0x0A59 - RSR feature Enable or Disable RSR feature; 0: Disable; **1: Enable** \$EN_DIS.
- [UINT8 OneCoreRatioLimit](#)
Offset 0x0A5A - 1-Core Ratio Limit 1-Core Ratio Limit: For XE part: LFM to 255, For overclocking part: LFM to Fused 1-Core Ratio Limit + OC Bins.This 1-Core Ratio Limit Must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit.
- [UINT8 TwoCoreRatioLimit](#)
Offset 0x0A5B - 2-Core Ratio Limit 2-Core Ratio Limit: For XE part: LFM to 255, For overclocking part: LFM to Fused 2-Core Ratio Limit + OC Bins.This 2-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83.
- [UINT8 ThreeCoreRatioLimit](#)
Offset 0x0A5C - 3-Core Ratio Limit 3-Core Ratio Limit: For XE part: LFM to 255, For overclocking part: LFM to Fused 3-Core Ratio Limit + OC Bins.This 3-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83.
- [UINT8 FourCoreRatioLimit](#)
Offset 0x0A5D - 4-Core Ratio Limit 4-Core Ratio Limit: For XE part: LFM to 255, For overclocking part: LFM to Fused 4-Core Ratio Limit + OC Bins.This 4-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83.

- UINT8 [Hwp](#)
Offset 0x0A5E - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.
 - UINT8 [HdcControl](#)
Offset 0x0A5F - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.
 - UINT8 [PowerLimit1Time](#)
Offset 0x0A60 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.
 - UINT8 [PowerLimit2](#)
Offset 0x0A61 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.
 - UINT8 [TurboPowerLimitLock](#)
*Offset 0x0A62 - Turbo settings Lock Lock all Turbo settings Enable/Disable; **0: Disable** , **1: Enable** \$EN_DIS.*
 - UINT8 [PowerLimit3Time](#)
Offset 0x0A63 - Package PL3 time window Package PL3 time window range for this policy from 0 to 64ms.
 - UINT8 [PowerLimit3DutyCycle](#)
Offset 0x0A64 - Package PL3 Duty Cycle Package PL3 Duty Cycle; Valid Range is 0 to 100.
 - UINT8 [PowerLimit3Lock](#)
*Offset 0x0A65 - Package PL3 Lock Package PL3 Lock Enable/Disable; **0: Disable** ; **1: Enable** \$EN_DIS.*
 - UINT8 [PowerLimit4Lock](#)
*Offset 0x0A66 - Package PL4 Lock Package PL4 Lock Enable/Disable; **0: Disable** ; **1: Enable** \$EN_DIS.*
 - UINT8 [TccActivationOffset](#)
Offset 0x0A67 - TCC Activation Offset TCC Activation Offset.
 - UINT8 [TccOffsetClamp](#)
*Offset 0x0A68 - 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 0x0A69 - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; **1: Enabled**.*
 - UINT8 [NumberOfEntries](#)
Offset 0x0A6A - 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 0x0A6B - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDp level 1.
 - UINT8 [Custom1TurboActivationRatio](#)
Offset 0x0A6C - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.
 - UINT8 [Custom1ConfigTdpControl](#)
Offset 0x0A6D - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
 - UINT8 [Custom2PowerLimit1Time](#)
Offset 0x0A6E - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDp level 2.
 - UINT8 [Custom2TurboActivationRatio](#)
Offset 0x0A6F - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.
 - UINT8 [Custom2ConfigTdpControl](#)
Offset 0x0A70 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
 - UINT8 [Custom3PowerLimit1Time](#)
Offset 0x0A71 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDp level 3.
 - UINT8 [Custom3TurboActivationRatio](#)
Offset 0x0A72 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.
 - UINT8 [Custom3ConfigTdpControl](#)
Offset 0x0A73 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.
 - UINT8 [ConfigTdpLock](#)
-

- Offset 0x0A74 - ConfigTdp mode settings Lock Lock the ConfigTdp mode settings from runtime changes; **0: Disable**; 1: Enable \$EN_DIS.
- UINT8 [ConfigTdpBios](#)

Offset 0x0A75 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.
 - UINT8 [PsysPowerLimit1](#)

Offset 0x0A76 - PL1 Enable value PL1 Enable value to limit average platform power.
 - UINT8 [PsysPowerLimit1Time](#)

Offset 0x0A77 - 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 0x0A78 - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.
 - UINT8 [MlcStreamerPrefetcher](#)

Offset 0x0A79 - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0: Disable; **1: Enable**.
 - UINT8 [MlcSpatialPrefetcher](#)

Offset 0x0A7A - Enable or Disable MLC Spatial Prefetcher Enable or Disable MLC Spatial Prefetcher; 0: Disable; **1: Enable** \$EN_DIS.
 - UINT8 [MonitorMwaitEnable](#)

Offset 0x0A7B - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable**.
 - UINT8 [MachineCheckEnable](#)

Offset 0x0A7C - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.
 - UINT8 [DebugInterfaceEnable](#)

Offset 0x0A7D - CPU Run Control Enable, Disable or Do not configure CPU Run Control; 0: Disable; 1: Enable ; **2: No Change** 0:Disabled, 1:Enabled, 2:No Change.
 - UINT8 [DebugInterfaceLockEnable](#)

Offset 0x0A7E - CPU Run Control Lock Lock or Unlock CPU Run Control; 0: Disable; **1: Enable**.
 - UINT8 [AplIdleManner](#)

Offset 0x0A7F - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.
 - UINT8 [ProcessorTraceOutputScheme](#)

Offset 0x0A80 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.
 - UINT8 [ProcessorTraceEnable](#)

Offset 0x0A81 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.
 - UINT8 [UnusedUpdSpace31](#) [6]

Offset 0x0A82.
 - UINT64 [ProcessorTraceMemBase](#)

Offset 0x0A88 - Base of memory region allocated for Processor Trace Base address of memory region allocated for Processor Trace.
 - UINT32 [ProcessorTraceMemLength](#)

Offset 0x0A90 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.
 - UINT8 [VoltageOptimization](#)

Offset 0x0A94 - Enable or Disable Voltage Optimization feature Enable or Disable Voltage Optimization feature 0: Disable; **1: Enable** \$EN_DIS.
 - UINT8 [Eist](#)

Offset 0x0A95 - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.
 - UINT8 [EnergyEfficientPState](#)

Offset 0x0A96 - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.
-

- UUINT8 [EnergyEfficientTurbo](#)
Offset 0x0A97 - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.
 - UUINT8 [TStates](#)
Offset 0x0A98 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.
 - UUINT8 [BiProcHot](#)
Offset 0x0A99 - Enable or Disable Bi-Directional PROCHOT# Enable or Disable Bi-Directional PROCHOT#; 0: Disable; 1: **Enable** \$EN_DIS.
 - UUINT8 [DisableProcHotOut](#)
Offset 0x0A9A - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; 1: **Enable**.
 - UUINT8 [ProcHotResponse](#)
Offset 0x0A9B - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.
 - UUINT8 [DisableVrThermalAlert](#)
Offset 0x0A9C - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.
 - UUINT8 [AutoThermalReporting](#)
Offset 0x0A9D - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; 1: **Enable**.
 - UUINT8 [ThermalMonitor](#)
Offset 0x0A9E - Enable or Disable Thermal Monitor Enable or Disable Thermal Monitor; 0: Disable; 1: **Enable** \$EN_DIS.
 - UUINT8 [Cx](#)
Offset 0x0A9F - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).
 - UUINT8 [PmgCstCfgCtrlLock](#)
Offset 0x0AA0 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; 1: **Enable**.
 - UUINT8 [C1e](#)
Offset 0x0AA1 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.
 - UUINT8 [PkgCStateDemotion](#)
Offset 0x0AA2 - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.
 - UUINT8 [PkgCStateUnDemotion](#)
Offset 0x0AA3 - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.
 - UUINT8 [CStatePreWake](#)
Offset 0x0AA4 - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.
 - UUINT8 [TimedMwait](#)
Offset 0x0AA5 - Enable or Disable TimedMwait Support.
 - UUINT8 [CstCfgCtrlIoMwaitRedirection](#)
Offset 0x0AA6 - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.
 - UUINT8 [PkgCStateLimit](#)
Offset 0x0AA7 - Set the Max Pkg Cstate Set the Max Pkg Cstate.
 - UUINT8 [CstateLatencyControl0TimeUnit](#)
Offset 0x0AA8 - 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.
 - UUINT8 [CstateLatencyControl1TimeUnit](#)
Offset 0x0AA9 - 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.
 - UUINT8 [CstateLatencyControl2TimeUnit](#)
Offset 0x0AAA - 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.
 - UUINT8 [CstateLatencyControl3TimeUnit](#)
Offset 0x0AAB - 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 0x0AAC - TimeUnit for C-State Latency Control4 Time - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.
 - UINT8 [CstateLatencyControl5TimeUnit](#)
Offset 0x0AAD - 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 [PpmlrmSetting](#)
Offset 0x0AAE - Interrupt Redirection Mode Select Interrupt Redirection Mode Select.0: Fixed priority; 1: Round robin;2: Hash vector;7: No change.
 - UINT8 [ProcHotLock](#)
Offset 0x0AAF - Lock prochot configuration Lock prochot configuration Enable/Disable; **0: Disable**; 1: Enable \$EN←_DIS.
 - UINT8 [ConfigTdpLevel](#)
Offset 0x0AB0 - Configuration for boot TDP selection Configuration for boot TDP selection; **0: TDP Nominal**; 1: TDP Down; 2: TDP Up;0xFF : Deactivate.
 - UINT8 [MaxRatio](#)
Offset 0x0AB1 - Max P-State Ratio Max P-State Ratio, Valid Range 0 to 0x7F.
 - UINT8 [StateRatio](#) [40]
Offset 0x0AB2 - P-state ratios for custom P-state table P-state ratios for custom P-state table.
 - UINT8 [StateRatioMax16](#) [16]
Offset 0x0ADA - P-state ratios for max 16 version of custom P-state table P-state ratios for max 16 version of custom P-state table.
 - UINT16 [PsysPmax](#)
Offset 0x0AEA - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.
 - UINT8 [Reserved0](#) [2]
Offset 0x0AEC.
 - UINT16 [CstateLatencyControl1Irtl](#)
Offset 0x0AEE - Interrupt Response Time Limit of C-State LatencyControl1 Interrupt Response Time Limit of C-State LatencyControl1.Range of value 0 to 0x3FF.
 - UINT16 [CstateLatencyControl2Irtl](#)
Offset 0x0AF0 - Interrupt Response Time Limit of C-State LatencyControl2 Interrupt Response Time Limit of C-State LatencyControl2.Range of value 0 to 0x3FF.
 - UINT16 [CstateLatencyControl3Irtl](#)
Offset 0x0AF2 - Interrupt Response Time Limit of C-State LatencyControl3 Interrupt Response Time Limit of C-State LatencyControl3.Range of value 0 to 0x3FF.
 - UINT16 [CstateLatencyControl4Irtl](#)
Offset 0x0AF4 - Interrupt Response Time Limit of C-State LatencyControl4 Interrupt Response Time Limit of C-State LatencyControl4.Range of value 0 to 0x3FF.
 - UINT16 [CstateLatencyControl5Irtl](#)
Offset 0x0AF6 - Interrupt Response Time Limit of C-State LatencyControl5 Interrupt Response Time Limit of C-State LatencyControl5.Range of value 0 to 0x3FF.
 - UINT32 [PowerLimit1](#)
Offset 0x0AF8 - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.
 - UINT32 [PowerLimit2Power](#)
Offset 0x0AFC - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.
 - UINT32 [PowerLimit3](#)
Offset 0x0B00 - Package PL3 power limit Package PL3 power limit.
 - UINT32 [PowerLimit4](#)
Offset 0x0B04 - Package PL4 power limit Package PL4 power limit.
 - UINT32 [TccOffsetTimeWindowForRatl](#)
Offset 0x0B08 - Tcc Offset Time Window for RATL Package PL4 power limit.
 - UINT32 [Custom1PowerLimit1](#)
-

- Offset 0x0B0C - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.
- UINT32 [Custom1PowerLimit2](#)
Offset 0x0B10 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.
 - UINT32 [Custom2PowerLimit1](#)
Offset 0x0B14 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.
 - UINT32 [Custom2PowerLimit2](#)
Offset 0x0B18 - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.
 - UINT32 [Custom3PowerLimit1](#)
Offset 0x0B1C - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.
 - UINT32 [Custom3PowerLimit2](#)
Offset 0x0B20 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.
 - UINT32 [PsysPowerLimit1Power](#)
Offset 0x0B24 - Platform PL1 power Platform PL1 power.
 - UINT32 [PsysPowerLimit2Power](#)
Offset 0x0B28 - Platform PL2 power Platform PL2 power.
 - UINT8 [RaceToHalt](#)
Offset 0x0B2C - Race To Halt Enable/Disable Race To Halt feature.
 - UINT8 [ThreeStrikeCounterDisable](#)
Offset 0x0B2D - 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 [HwpiInterruptControl](#)
Offset 0x0B2E - Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT; **0: Disable**; 1: Enable.
 - UINT8 [FiveCoreRatioLimit](#)
Offset 0x0B2F - 5-Core Ratio Limit 5-Core Ratio Limit: For XE part: LFM to 255, For overlocking part: LFM to Fused 5-Core Ratio Limit + OC Bins.This 5-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83 0x0:0xFF.
 - UINT8 [SixCoreRatioLimit](#)
Offset 0x0B30 - 6-Core Ratio Limit 6-Core Ratio Limit: For XE part: LFM to 255, For overlocking part: LFM to Fused 6-Core Ratio Limit + OC Bins.This 6-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83 0x0:0xFF.
 - UINT8 [SevenCoreRatioLimit](#)
Offset 0x0B31 - 7-Core Ratio Limit 7-Core Ratio Limit: For XE part: LFM to 255, For overlocking part: LFM to Fused 7-Core Ratio Limit + OC Bins.This 7-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83 0x0:0xFF.
 - UINT8 [EightCoreRatioLimit](#)
Offset 0x0B32 - 8-Core Ratio Limit 8-Core Ratio Limit: For XE part: LFM to 255, For overlocking part: LFM to Fused 8-Core Ratio Limit + OC Bins.This 8-Core Ratio Limit Must be Less than or equal to 1-Core Ratio Limit.Range is 0 to 83 0x0:0xFF.
 - UINT8 [Enablelbtm](#)
Offset 0x0B33 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.
 - UINT8 [EnablelbtmDriver](#)
Offset 0x0B34 - Intel Turbo Boost Max Technology 3.0 Driver Intel Turbo Boost Max Technology 3.0 Driver **0: Disabled**; 1: Enabled \$EN_DIS.
 - UINT8 [C1StateAutoDemotion](#)
Offset 0x0B35 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.
 - UINT8 [C1StateUnDemotion](#)
Offset 0x0B36 - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.

- UINT8 [MinRingRatioLimit](#)
Offset 0x0B37 - Minimum Ring ratio limit override Minimum Ring ratio limit override.
 - UINT8 [MaxRingRatioLimit](#)
Offset 0x0B38 - Maximum Ring ratio limit override Maximum Ring ratio limit override.
 - UINT8 [EnablePerCorePState](#)
Offset 0x0B39 - Enable or Disable Per Core P State OS control Enable or Disable Per Core P State OS control.
 - UINT8 [EnableHwpAutoPerCorePstate](#)
Offset 0x0B3A - Enable or Disable HwP Autonomous Per Core P State OS control Enable or Disable HwP Autonomous Per Core P State OS control.
 - UINT8 [EnableHwpAutoEppGrouping](#)
Offset 0x0B3B - Enable or Disable HwP Autonomous EPP Grouping Enable or Disable HwP Autonomous EPP Grouping.
 - UINT8 [EnableEpbPeciOverride](#)
Offset 0x0B3C - Enable or Disable EPB override over PECl Enable or Disable EPB override over PECl.
 - UINT8 [EnableFastMsrHwpReq](#)
Offset 0x0B3D - Enable or Disable Fast MSR for IA32_HWP_REQUEST Enable or Disable Fast MSR for IA32_HWP_REQUEST.
 - UINT8 [CoreCStateLimit](#)
Offset 0x0B3E - Set the Max Cstate Set the Max Cstate.
 - UINT8 [ReservedCpuPostMemTest](#) [17]
Offset 0x0B3F - ReservedCpuPostMemTest Reserved for CPU Post-Mem Test \$EN_DIS.
 - UINT8 [SgxSinitDataFromTpm](#)
Offset 0x0B50 - SgxSinitDataFromTpm SgxSinitDataFromTpm default values.
 - UINT8 [EndOfPostMessage](#)
Offset 0x0B51 - End of Post message Test, Send End of Post message.
 - UINT8 [DisableD0I3SettingForHeci](#)
Offset 0x0B52 - D0I3 Setting for HECI Disable Test, 0: disable, 1: enable, Setting this option disables setting D0I3 bit for all HECI devices \$EN_DIS.
 - UINT8 [UnusedUpdSpace32](#)
Offset 0x0B53.
 - UINT16 [PchHdaResetWaitTimer](#)
Offset 0x0B54 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.
 - UINT8 [PchLockDownGlobalSmi](#)
Offset 0x0B56 - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.
 - UINT8 [PchLockDownBiosInterface](#)
Offset 0x0B57 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.
 - UINT8 [PchUnlockGpioPads](#)
Offset 0x0B58 - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.
 - UINT8 [PchSbAccessUnlock](#)
Offset 0x0B59 - PCH Unlock SideBand access The SideBand PortID mask for certain end point (e.g.
 - UINT16 [PcieRpLtrMaxSnoopLatency](#) [24]
Offset 0x0B5A - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.
 - UINT16 [PcieRpLtrMaxNoSnoopLatency](#) [24]
Offset 0x0B8A - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.
 - UINT8 [PcieRpSnoopLatencyOverrideMode](#) [24]
Offset 0x0BBA - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.
 - UINT8 [PcieRpSnoopLatencyOverrideMultiplier](#) [24]
Offset 0x0BD2 - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.
 - UINT16 [PcieRpSnoopLatencyOverrideValue](#) [24]
-

- Offset 0x0BEA - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.*
- UINT8 [PcieRpNonSnoopLatencyOverrideMode](#) [24]

Offset 0x0C1A - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.
 - UINT8 [PcieRpNonSnoopLatencyOverrideMultiplier](#) [24]

Offset 0x0C32 - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.
 - UINT16 [PcieRpNonSnoopLatencyOverrideValue](#) [24]

Offset 0x0C4A - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.
 - UINT8 [PcieRpSlotPowerLimitScale](#) [24]

Offset 0x0C7A - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.
 - UINT16 [PcieRpSlotPowerLimitValue](#) [24]

Offset 0x0C92 - PCIE RP Slot Power Limit Value Specifies upper limit on power supplied by slot.
 - UINT8 [PcieRpUptp](#) [24]

Offset 0x0CC2 - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.
 - UINT8 [PcieRpDptp](#) [24]

Offset 0x0CDA - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.
 - UINT8 [PcieEnablePort8xhDecode](#)

Offset 0x0CF2 - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.
 - UINT8 [PchPciePort8xhDecodePortIndex](#)

Offset 0x0CF3 - PCIE Port8xh Decode Port Index The Index of PCIe Port that is selected for Port8xh Decode (0 Based).
 - UINT8 [PchPmDisableEnergyReport](#)

Offset 0x0CF4 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.
 - UINT8 [SataTestMode](#)

Offset 0x0CF5 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.
 - UINT8 [PchXhciOcLock](#)

Offset 0x0CF6 - PCH USB OverCurrent mapping lock enable If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.
 - UINT8 [PmLpmS0ixSubStateEnableMask](#)

Offset 0x0CF7 - Low Power Mode Enable/Disable config mask Configure if respective S0i2/3 sub-states are to be supported.
 - UINT8 [SkipPostBootSai](#)

Offset 0x0CF8 - Skip POSTBOOT SAI This skip the Post Boot Sai programming.
 - UINT8 [MctpBroadcastCycle](#)

*Offset 0x0CF9 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.*
 - UINT16 [SaPcieRpLtrMaxSnoopLatency](#) [4]

Offset 0x0CFA - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.
 - UINT16 [SaPcieRpLtrMaxNoSnoopLatency](#) [4]

Offset 0x0D02 - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.
 - UINT8 [SaPcieRpSnoopLatencyOverrideMode](#) [4]

Offset 0x0D0A - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.
 - UINT8 [SaPcieRpSnoopLatencyOverrideMultiplier](#) [4]

Offset 0x0D0E - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.
 - UINT16 [SaPcieRpSnoopLatencyOverrideValue](#) [4]

Offset 0x0D12 - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.
-

- UINT8 [SaPcieRpNonSnoopLatencyOverrideMode](#) [4]
Offset 0x0D1A - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.
- UINT8 [SaPcieRpNonSnoopLatencyOverrideMultiplier](#) [4]
Offset 0x0D1E - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.
- UINT16 [SaPcieRpNonSnoopLatencyOverrideValue](#) [4]
Offset 0x0D22 - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.
- UINT8 [SaPcieRpGen3Uptp](#) [4]
Offset 0x0D2A - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.
- UINT8 [SaPcieRpGen3Dptp](#) [4]
Offset 0x0D2E - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.
- UINT8 [SaPcieRpGen4Uptp](#) [4]
Offset 0x0D32 - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.
- UINT8 [SaPcieRpGen4Dptp](#) [4]
Offset 0x0D36 - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.
- UINT8 [UnusedUpdSpace33](#) [2]
Offset 0x0D3A.
- UINT8 [ReservedFspstestUpd](#) [12]
Offset 0x0D3C.

10.11.1 Detailed Description

Fsp S Test Configuration.

Definition at line 3117 of file FspUpd.h.

10.11.2 Member Data Documentation

10.11.2.1 ApIdleManner

UINT8 FSP_S_TEST_CONFIG::ApIdleManner

Offset 0x0A7F - 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 3427 of file FspUpd.h.

10.11.2.2 AutoThermalReporting

UINT8 FSP_S_TEST_CONFIG::AutoThermalReporting

Offset 0x0A9D - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; 1: **Enable**.

\$EN_DIS

Definition at line 3517 of file FspUpd.h.

10.11.2.3 C1e

UINT8 FSP_S_TEST_CONFIG::C1e

Offset 0x0AA1 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

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

Definition at line 3541 of file FspUpd.h.

10.11.2.4 C1StateAutoDemotion

UINT8 FSP_S_TEST_CONFIG::C1StateAutoDemotion

Offset 0x0B35 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.

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

Definition at line 3836 of file FspUpd.h.

10.11.2.5 C1StateUnDemotion

UINT8 FSP_S_TEST_CONFIG::C1StateUnDemotion

Offset 0x0B36 - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.

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

Definition at line 3842 of file FspUpd.h.

10.11.2.6 ConfigTdpBios

UINT8 FSP_S_TEST_CONFIG::ConfigTdpBios

Offset 0x0A75 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; 0: **Disable**; 1: **Enable**.

\$EN_DIS

Definition at line 3365 of file FspUpd.h.

10.11.2.7 CoreCStateLimit

UINT8 FSP_S_TEST_CONFIG::CoreCStateLimit

Offset 0x0B3E - Set the Max Cstate Set the Max Cstate.

Default set to Auto which limits the Max Cstate to deep C-state. Valid values 1 - C3 , 2 - C3 , 3 - C6, 5 - Auto

Definition at line 3891 of file FspUpd.h.

10.11.2.8 CStatePreWake

UINT8 FSP_S_TEST_CONFIG::CStatePreWake

Offset 0x0AA4 - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

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

Definition at line 3559 of file FspUpd.h.

10.11.2.9 CstCfgCtrlIoMwaitRedirection

UINT8 FSP_S_TEST_CONFIG::CstCfgCtrlIoMwaitRedirection

Offset 0x0AA6 - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable;**
1: Enable.

\$EN_DIS

Definition at line 3571 of file FspUpd.h.

10.11.2.10 Custom1ConfigTdpControl

UINT8 FSP_S_TEST_CONFIG::Custom1ConfigTdpControl

Offset 0x0A6D - 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 3323 of file FspUpd.h.

10.11.2.11 Custom1PowerLimit1

UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit1

Offset 0x0B0C - 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 3723 of file FspUpd.h.

10.11.2.12 Custom1PowerLimit1Time

UINT8 FSP_S_TEST_CONFIG::Custom1PowerLimit1Time

Offset 0x0A6B - 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 3313 of file FspUpd.h.

10.11.2.13 Custom1PowerLimit2

UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit2

Offset 0x0B10 - 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 3729 of file FspUpd.h.

10.11.2.14 Custom1TurboActivationRatio

UINT8 FSP_S_TEST_CONFIG::Custom1TurboActivationRatio

Offset 0x0A6C - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

Valid Range 0 to 255

Definition at line 3318 of file FspUpd.h.

10.11.2.15 Custom2ConfigTdpControl

UINT8 FSP_S_TEST_CONFIG::Custom2ConfigTdpControl

Offset 0x0A70 - 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 3338 of file FspUpd.h.

10.11.2.16 Custom2PowerLimit1

UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit1

Offset 0x0B14 - 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 3735 of file FspUpd.h.

10.11.2.17 Custom2PowerLimit1Time

UINT8 FSP_S_TEST_CONFIG::Custom2PowerLimit1Time

Offset 0x0A6E - 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 3328 of file FspUpd.h.

10.11.2.18 Custom2PowerLimit2

UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit2

Offset 0x0B18 - 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 3741 of file FspUpd.h.

10.11.2.19 Custom2TurboActivationRatio

UINT8 FSP_S_TEST_CONFIG::Custom2TurboActivationRatio

Offset 0x0A6F - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

Valid Range 0 to 255

Definition at line 3333 of file FspUpd.h.

10.11.2.20 Custom3ConfigTdpControl

UINT8 FSP_S_TEST_CONFIG::Custom3ConfigTdpControl

Offset 0x0A73 - 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 3353 of file FspUpd.h.

10.11.2.21 Custom3PowerLimit1

UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit1

Offset 0x0B1C - 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 3747 of file FspUpd.h.

10.11.2.22 Custom3PowerLimit1Time

UINT8 FSP_S_TEST_CONFIG::Custom3PowerLimit1Time

Offset 0x0A71 - 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 3343 of file FspUpd.h.

10.11.2.23 Custom3PowerLimit2

UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit2

Offset 0x0B20 - 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 3753 of file FspUpd.h.

10.11.2.24 Custom3TurboActivationRatio

UINT8 FSP_S_TEST_CONFIG::Custom3TurboActivationRatio

Offset 0x0A72 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

Valid Range 0 to 255

Definition at line 3348 of file FspUpd.h.

10.11.2.25 Cx

UINT8 FSP_S_TEST_CONFIG::Cx

Offset 0x0A9F - 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 3529 of file FspUpd.h.

10.11.2.26 DebugInterfaceLockEnable

UINT8 FSP_S_TEST_CONFIG::DebugInterfaceLockEnable

Offset 0x0A7E - CPU Run Control Lock Lock or Unlock CPU Run Control; 0: Disable; 1: **Enable**.

\$EN_DIS

Definition at line 3421 of file FspUpd.h.

10.11.2.27 DisableProcHotOut

UINT8 FSP_S_TEST_CONFIG::DisableProcHotOut

Offset 0x0A9A - 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 3499 of file FspUpd.h.

10.11.2.28 DisableVrThermalAlert

UINT8 FSP_S_TEST_CONFIG::DisableVrThermalAlert

Offset 0x0A9C - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; 0: **Disable**; 1: Enable.

\$EN_DIS

Definition at line 3511 of file FspUpd.h.

10.11.2.29 Eist

UINT8 FSP_S_TEST_CONFIG::Eist

Offset 0x0A95 - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

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

Definition at line 3467 of file FspsUpd.h.

10.11.2.30 EnableEpbPeciOverride

UINT8 FSP_S_TEST_CONFIG::EnableEpbPeciOverride

Offset 0x0B3C - Enable or Disable EPB override over PECl Enable or Disable EPB override over PECl.

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

Definition at line 3879 of file FspsUpd.h.

10.11.2.31 EnableFastMsrHwpReq

UINT8 FSP_S_TEST_CONFIG::EnableFastMsrHwpReq

Offset 0x0B3D - Enable or Disable Fast MSR for IA32_HWP_REQUEST Enable or Disable Fast MSR for IA32_HWP_REQUEST.

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

Definition at line 3885 of file FspsUpd.h.

10.11.2.32 EnableHwpAutoEppGrouping

UINT8 FSP_S_TEST_CONFIG::EnableHwpAutoEppGrouping

Offset 0x0B3B - Enable or Disable HwP Autonomous EPP Grouping Enable or Disable HwP Autonomous EPP Grouping.

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

Definition at line 3873 of file FspsUpd.h.

10.11.2.33 EnableHwpAutoPerCorePstate

UINT8 FSP_S_TEST_CONFIG::EnableHwpAutoPerCorePstate

Offset 0x0B3A - Enable or Disable HwP Autonomous Per Core P State OS control Enable or Disable HwP Autonomous Per Core P State OS control.

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

Definition at line 3867 of file FspsUpd.h.

10.11.2.34 EnableItbm

UINT8 FSP_S_TEST_CONFIG::EnableItbm

Offset 0x0B33 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.

0: Disabled; **1: Enabled** \$EN_DIS

Definition at line 3824 of file FspUpd.h.

10.11.2.35 EnablePerCorePState

UINT8 FSP_S_TEST_CONFIG::EnablePerCorePState

Offset 0x0B39 - Enable or Disable Per Core P State OS control Enable or Disable Per Core P State OS control.

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

Definition at line 3860 of file FspUpd.h.

10.11.2.36 EndOfPostMessage

UINT8 FSP_S_TEST_CONFIG::EndOfPostMessage

Offset 0x0B51 - 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 DXE 0:Disable, 1:Send in PEI, 2:Send in DXE, 3:Reserved

Definition at line 3909 of file FspUpd.h.

10.11.2.37 EnergyEfficientPState

UINT8 FSP_S_TEST_CONFIG::EnergyEfficientPState

Offset 0x0A96 - 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 3474 of file FspUpd.h.

10.11.2.38 EnergyEfficientTurbo

UINT8 FSP_S_TEST_CONFIG::EnergyEfficientTurbo

Offset 0x0A97 - 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 3481 of file FspUpd.h.

10.11.2.39 HdcControl

UINT8 FSP_S_TEST_CONFIG::HdcControl

Offset 0x0A5F - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

0: Disabled; **1: Enabled** 2-3:Reserved \$EN_DIS

Definition at line 3239 of file FspUpd.h.

10.11.2.40 Hwp

UINT8 FSP_S_TEST_CONFIG::Hwp

Offset 0x0A5E - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

0: Disable; **1: Enable**; 2-3:Reserved \$EN_DIS

Definition at line 3233 of file FspUpd.h.

10.11.2.41 HwpInterruptControl

UINT8 FSP_S_TEST_CONFIG::HwpInterruptControl

Offset 0x0B2E - Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT Set HW P-State Interrupts Enabled for for MISC_PWR_MGMT; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 3786 of file FspUpd.h.

10.11.2.42 MachineCheckEnable

UINT8 FSP_S_TEST_CONFIG::MachineCheckEnable

Offset 0x0A7C - 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 3408 of file FspUpd.h.

10.11.2.43 MaxRingRatioLimit

UINT8 FSP_S_TEST_CONFIG::MaxRingRatioLimit

Offset 0x0B38 - Maximum Ring ratio limit override Maximum Ring ratio limit override.

0: Hardware defaults. Range: 0 - Max turbo ratio limit

Definition at line 3854 of file FspUpd.h.

10.11.2.44 MctpBroadcastCycle

UINT8 FSP_S_TEST_CONFIG::MctpBroadcastCycle

Offset 0x0CF9 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 4060 of file FspUpd.h.

10.11.2.45 MinRingRatioLimit

UINT8 FSP_S_TEST_CONFIG::MinRingRatioLimit

Offset 0x0B37 - Minimum Ring ratio limit override Minimum Ring ratio limit override.

0: Hardware defaults. Range: 0 - Max turbo ratio limit

Definition at line 3848 of file FspUpd.h.

10.11.2.46 MlcStreamerPrefetcher

UINT8 FSP_S_TEST_CONFIG::MlcStreamerPrefetcher

Offset 0x0A79 - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0: Disable; **1: Enable.**

\$EN_DIS

Definition at line 3390 of file FspUpd.h.

10.11.2.47 MonitorMwaitEnable

UINT8 FSP_S_TEST_CONFIG::MonitorMwaitEnable

Offset 0x0A7B - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable.**

\$EN_DIS

Definition at line 3402 of file FspUpd.h.

10.11.2.48 NumberOfEntries

UINT8 FSP_S_TEST_CONFIG::NumberOfEntries

Offset 0x0A6A - 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 3308 of file FspUpd.h.

10.11.2.49 OneCoreRatioLimit

UINT8 FSP_S_TEST_CONFIG::OneCoreRatioLimit

Offset 0x0A5A - 1-Core Ratio Limit 1-Core Ratio Limit: For XE part: LFM to 255, For overclocking part: LFM to Fused 1-Core Ratio Limit + OC Bins.This 1-Core Ratio Limit Must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit.

Range is 0 to 83

Definition at line 3205 of file FspUpd.h.

10.11.2.50 PchHdaResetWaitTimer

UINT16 FSP_S_TEST_CONFIG::PchHdaResetWaitTimer

Offset 0x0B54 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.

Default is 600.

Definition at line 3925 of file FspUpd.h.

10.11.2.51 PchLockDownBiosInterface

UINT8 FSP_S_TEST_CONFIG::PchLockDownBiosInterface

Offset 0x0B57 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

\$EN_DIS

Definition at line 3937 of file FspUpd.h.

10.11.2.52 PchLockDownGlobalSmi

UINT8 FSP_S_TEST_CONFIG::PchLockDownGlobalSmi

Offset 0x0B56 - Enable LOCKDOWN SMI Enable SMI_LOCK bit to prevent writes to the Global SMI Enable bit.

\$EN_DIS

Definition at line 3931 of file FspUpd.h.

10.11.2.53 PchPmDisableEnergyReport

UINT8 FSP_S_TEST_CONFIG::PchPmDisableEnergyReport

Offset 0x0CF4 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.

\$EN_DIS

Definition at line 4028 of file FspUpd.h.

10.11.2.54 PchSbAccessUnlock

UINT8 FSP_S_TEST_CONFIG::PchSbAccessUnlock

Offset 0x0B59 - PCH Unlock SideBand access The SideBand PortID mask for certain end point (e.g.

PSFx) will be locked before 3rd party code execution. 0: Lock SideBand access; 1: Unlock SideBand access.

\$EN_DIS

Definition at line 3950 of file FspUpd.h.

10.11.2.55 PchUnlockGpioPads

UINT8 FSP_S_TEST_CONFIG::PchUnlockGpioPads

Offset 0x0B58 - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.

\$EN_DIS

Definition at line 3943 of file FspUpd.h.

10.11.2.56 PchXhciOcLock

UINT8 FSP_S_TEST_CONFIG::PchXhciOcLock

Offset 0x0CF6 - PCH USB OverCurrent mapping lock enable If this policy option is enabled then BIOS will program OCCFDONE bit in xHCI meaning that OC mapping data will be consumed by xHCI and OC mapping registers will be locked.

\$EN_DIS

Definition at line 4041 of file FspUpd.h.

10.11.2.57 PcieEnablePort8xhDecode

UINT8 FSP_S_TEST_CONFIG::PcieEnablePort8xhDecode

Offset 0x0CF2 - 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 4017 of file FspUpd.h.

10.11.2.58 PcieRpDptp

UINT8 FSP_S_TEST_CONFIG::PcieRpDptp[24]

Offset 0x0CDA - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 4010 of file FspUpd.h.

10.11.2.59 PcieRpSlotPowerLimitScale

UINT8 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitScale[24]

Offset 0x0C7A - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

Leave as 0 to set to default.

Definition at line 3995 of file FspUpd.h.

10.11.2.60 PcieRpSlotPowerLimitValue

UINT16 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitValue[24]

Offset 0x0C92 - PCIE RP Slot Power Limit Value Specifies upper limit on power supplied by slot.

Leave as 0 to set to default.

Definition at line 4000 of file FspUpd.h.

10.11.2.61 PcieRpUtp

UINT8 FSP_S_TEST_CONFIG::PcieRpUtp[24]

Offset 0x0CC2 - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 4005 of file FspUpd.h.

10.11.2.62 PkgCStateDemotion

UINT8 FSP_S_TEST_CONFIG::PkgCStateDemotion

Offset 0x0AA2 - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.

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

Definition at line 3547 of file FspUpd.h.

10.11.2.63 PkgCStateLimit

UINT8 FSP_S_TEST_CONFIG::PkgCStateLimit

Offset 0x0AA7 - 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 3578 of file FspUpd.h.

10.11.2.64 PkgCStateUnDemotion

UINT8 FSP_S_TEST_CONFIG::PkgCStateUnDemotion

Offset 0x0AA3 - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.

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

Definition at line 3553 of file FspUpd.h.

10.11.2.65 PmcLpmS0ixSubStateEnableMask

UINT8 FSP_S_TEST_CONFIG::PmcLpmS0ixSubStateEnableMask

Offset 0x0CF7 - Low Power Mode Enable/Disable config mask Configure if respective S0i2/3 sub-states are to be supported.

Each bit corresponds to one sub-state (LPMx - BITx): LPM0-s0i2.0, LPM1-s0i2.1, LPM2-s0i2.2, LPM3-s0i3.0, LPM4-s0i3.1, LPM5-s0i3.2, LPM6-s0i3.3, LPM7-s0i3.4.

Definition at line 4048 of file FspUpd.h.

10.11.2.66 PmgCstCfgCtrlLock

UINT8 FSP_S_TEST_CONFIG::PmgCstCfgCtrlLock

Offset 0x0AA0 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; **1: Enable.**
\$EN_DIS

Definition at line 3535 of file FspUpd.h.

10.11.2.67 PowerLimit1

UINT32 FSP_S_TEST_CONFIG::PowerLimit1

Offset 0x0AF8 - 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 3693 of file FspUpd.h.

10.11.2.68 PowerLimit1Time

UINT8 FSP_S_TEST_CONFIG::PowerLimit1Time

Offset 0x0A60 - 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 3245 of file FspUpd.h.

10.11.2.69 PowerLimit2

UINT8 FSP_S_TEST_CONFIG::PowerLimit2

Offset 0x0A61 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

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

Definition at line 3251 of file FspUpd.h.

10.11.2.70 PowerLimit2Power

UINT32 FSP_S_TEST_CONFIG::PowerLimit2Power

Offset 0x0AFC - 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 3699 of file FspUpd.h.

10.11.2.71 PowerLimit3

UINT32 FSP_S_TEST_CONFIG::PowerLimit3

Offset 0x0B00 - 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 3705 of file FspUpd.h.

10.11.2.72 PowerLimit4

UINT32 FSP_S_TEST_CONFIG::PowerLimit4

Offset 0x0B04 - 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 3711 of file FspUpd.h.

10.11.2.73 ProcessorTraceEnable

UINT8 FSP_S_TEST_CONFIG::ProcessorTraceEnable

Offset 0x0A81 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 3439 of file FspUpd.h.

10.11.2.74 ProcessorTraceMemBase

UINT64 FSP_S_TEST_CONFIG::ProcessorTraceMemBase

Offset 0x0A88 - Base of memory region allocated for Processor Trace Base address of memory region allocated for Processor Trace.

Processor Trace requires 2^N alignment and size in bytes per thread, from 4KB to 128MB. **0: Disable**

Definition at line 3449 of file FspUpd.h.

10.11.2.75 ProcessorTraceMemLength

UINT32 FSP_S_TEST_CONFIG::ProcessorTraceMemLength

Offset 0x0A90 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.

Processor Trace requires 2^N alignment and size in bytes per thread, from 4KB to 128MB. **0: Disable**

Definition at line 3455 of file FspUpd.h.

10.11.2.76 ProcessorTraceOutputScheme

UINT8 FSP_S_TEST_CONFIG::ProcessorTraceOutputScheme

Offset 0x0A80 - 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 3433 of file FspUpd.h.

10.11.2.77 ProcHotResponse

UINT8 FSP_S_TEST_CONFIG::ProcHotResponse

Offset 0x0A9B - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 3505 of file FspUpd.h.

10.11.2.78 PsysPmax

UINT16 FSP_S_TEST_CONFIG::PsysPmax

Offset 0x0AEA - 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 3658 of file FspUpd.h.

10.11.2.79 PsysPowerLimit1

UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit1

Offset 0x0A76 - PL1 Enable value PL1 Enable value to limit average platform power.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 3371 of file FspUpd.h.

10.11.2.80 PsysPowerLimit1Power

UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit1Power

Offset 0x0B24 - 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 3759 of file FspUpd.h.

10.11.2.81 PsysPowerLimit2

UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit2

Offset 0x0A78 - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 3384 of file FspsUpd.h.

10.11.2.82 PsysPowerLimit2Power

UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit2Power

Offset 0x0B28 - 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 3765 of file FspsUpd.h.

10.11.2.83 RaceToHalt

UINT8 FSP_S_TEST_CONFIG::RaceToHalt

Offset 0x0B2C - 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 3773 of file FspsUpd.h.

10.11.2.84 SaPcieRpGen3Dptp

UINT8 FSP_S_TEST_CONFIG::SaPcieRpGen3Dptp[4]

Offset 0x0D2E - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 4110 of file FspsUpd.h.

10.11.2.85 SaPcieRpGen3Uptp

UINT8 FSP_S_TEST_CONFIG::SaPcieRpGen3Uptp[4]

Offset 0x0D2A - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 4105 of file FspsUpd.h.

10.11.2.86 SaPcieRpGen4Dptp

UINT8 FSP_S_TEST_CONFIG::SaPcieRpGen4Dptp[4]

Offset 0x0D36 - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 4120 of file FspsUpd.h.

10.11.2.87 SaPcieRpGen4Uptp

UINT8 FSP_S_TEST_CONFIG::SaPcieRpGen4Uptp[4]

Offset 0x0D32 - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 4115 of file FspUpd.h.

10.11.2.88 SataTestMode

UINT8 FSP_S_TEST_CONFIG::SataTestMode

Offset 0x0CF5 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

\$EN_DIS

Definition at line 4034 of file FspUpd.h.

10.11.2.89 SkipPostBootSai

UINT8 FSP_S_TEST_CONFIG::SkipPostBootSai

Offset 0x0CF8 - Skip POSTBOOT SAI This skip the Post Boot Sai programming.

0: Set Post Boot Sai; 1: Skip Post Boot Sai. \$EN_DIS

Definition at line 4054 of file FspUpd.h.

10.11.2.90 StateRatio

UINT8 FSP_S_TEST_CONFIG::StateRatio[40]

Offset 0x0AB2 - P-state ratios for custom P-state table P-state ratios for custom P-state table.

NumberOfEntries has valid range between 0 to 40. For no. of P-States supported(NumberOfEntries) , StateRatio[NumberOfEntries] are configurable. Valid Range of each entry is 0 to 0x7F

Definition at line 3643 of file FspUpd.h.

10.11.2.91 StateRatioMax16

UINT8 FSP_S_TEST_CONFIG::StateRatioMax16[16]

Offset 0x0ADA - P-state ratios for max 16 version of custom P-state table P-state ratios for max 16 version of custom P-state table.

This table is used for OS versions limited to a max of 16 P-States. If the first entry of this table is 0, or if Number of Entries is 16 or less, then this table will be ignored, and up to the top 16 values of the StateRatio table will be used instead. Valid Range of each entry is 0 to 0x7F

Definition at line 3652 of file FspUpd.h.

10.11.2.92 TccActivationOffset

UINT8 FSP_S_TEST_CONFIG::TccActivationOffset

Offset 0x0A67 - 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 3287 of file FspUpd.h.

10.11.2.93 TccOffsetClamp

UINT8 FSP_S_TEST_CONFIG::TccOffsetClamp

Offset 0x0A68 - 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 3295 of file FspUpd.h.

10.11.2.94 TccOffsetLock

UINT8 FSP_S_TEST_CONFIG::TccOffsetLock

Offset 0x0A69 - 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 3302 of file FspUpd.h.

10.11.2.95 TccOffsetTimeWindowForRatl

UINT32 FSP_S_TEST_CONFIG::TccOffsetTimeWindowForRatl

Offset 0x0B08 - 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 3717 of file FspUpd.h.

10.11.2.96 ThreeStrikeCounterDisable

UINT8 FSP_S_TEST_CONFIG::ThreeStrikeCounterDisable

Offset 0x0B2D - 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 3780 of file FspUpd.h.

10.11.2.97 TimedMwait

```
UINT8 FSP_S_TEST_CONFIG::TimedMwait
```

Offset 0x0AA5 - Enable or Disable TimedMwait Support.

Enable or Disable TimedMwait Support. **0: Disable**; 1: Enable \$EN_DIS

Definition at line 3565 of file FspUpd.h.

10.11.2.98 TStates

```
UINT8 FSP_S_TEST_CONFIG::TStates
```

Offset 0x0A98 - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.

\$EN_DIS

Definition at line 3487 of file FspUpd.h.

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

- [FspUpd.h](#)

10.12 FSP_T_CONFIG Struct Reference

Fsp T Configuration.

```
#include <FsptUpd.h>
```

Public Attributes

- [UINT8 PcdSerialloUartDebugEnabled](#)
Offset 0x0040 - PcdSerialloUartDebugEnabled Enable Seriallo Uart debug library with/without initializing Seriallo Uart device in FSP.
- [UINT8 PcdSerialloUartNumber](#)
Offset 0x0041 - PcdSerialloUartNumber Select Seriallo Uart Controller for debug.
- [UINT8 PcdSerialloUartMode](#)
Offset 0x0042 - PcdSerialloUartMode - FSPT Select Seriallo Uart Controller mode 0:SerialloUartDisabled, 1:SerialloUartPci, 2:SerialloUartHidden, 3:SerialloUartCom, 4:SerialloUartSkipInit.
- [UINT8 UnusedUpdSpace0](#)
Offset 0x0043.
- [UINT32 PcdSerialloUartBaudRate](#)
Offset 0x0044 - PcdSerialloUartBaudRate - FSPT Set default BaudRate Supported from 0 - default to 6000000.
- [UINT64 PcdPciExpressBaseAddress](#)
Offset 0x0048 - Pci Express Base Address Base address to be programmed for Pci Express.
- [UINT32 PcdPciExpressRegionLength](#)
Offset 0x0050 - Pci Express Region Length Region Length to be programmed for Pci Express.
- [UINT8 PcdSerialloUartParity](#)
Offset 0x0054 - PcdSerialloUartParity - FSPT Set default Parity.
- [UINT8 PcdSerialloUartDataBits](#)
Offset 0x0055 - PcdSerialloUartDataBits - FSPT Set default word length.
- [UINT8 PcdSerialloUartStopBits](#)
Offset 0x0056 - PcdSerialloUartStopBits - FSPT Set default stop bits.
- [UINT8 PcdSerialloUartAutoFlow](#)

- Offset 0x0057 - PcdSerialIoUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.*

 - UINT32 [PcdSerialIoUartRxPinMux](#)

Offset 0x0058 - PcdSerialIoUartRxPinMux - FSPT Select RX pin muxing for SerialIo UART used for debug.
 - UINT32 [PcdSerialIoUartTxPinMux](#)

Offset 0x005C - PcdSerialIoUartTxPinMux - FSPT Select TX pin muxing for SerialIo UART used for debug.
 - UINT32 [PcdSerialIoUartRtsPinMux](#)

Offset 0x0060 - PcdSerialIoUartRtsPinMux - FSPT Select SerialIo Uart used for debug Rts pin muxing.
 - UINT32 [PcdSerialIoUartCtsPinMux](#)

Offset 0x0064 - PcdSerialIoUartCtsPinMux - FSPT Select SerialIo Uart used for debug Cts pin muxing.
 - UINT8 [UnusedUpdSpace1](#) [7]

Offset 0x0068.
 - UINT8 [ReservedFsptUpd1](#) [25]

Offset 0x006F.

10.12.1 Detailed Description

Fsp T Configuration.

Definition at line 68 of file FsptUpd.h.

10.12.2 Member Data Documentation

10.12.2.1 PcdSerialIoUartAutoFlow

UINT8 FSP_T_CONFIG::PcdSerialIoUartAutoFlow

Offset 0x0057 - PcdSerialIoUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.

0: Disable, 1:Enable

Definition at line 130 of file FsptUpd.h.

10.12.2.2 PcdSerialIoUartCtsPinMux

UINT32 FSP_T_CONFIG::PcdSerialIoUartCtsPinMux

Offset 0x0064 - PcdSerialIoUartCtsPinMux - FSPT Select SerialIo Uart used for debug Cts pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_CTS* for possible values.

Definition at line 152 of file FsptUpd.h.

10.12.2.3 PcdSerialIoUartDataBits

UINT8 FSP_T_CONFIG::PcdSerialIoUartDataBits

Offset 0x0055 - PcdSerialIoUartDataBits - FSPT Set default word length.

0: Default, 5,6,7,8

Definition at line 118 of file FsptUpd.h.

10.12.2.4 PcdSerialIoUartDebugEnabled

UINT8 FSP_T_CONFIG::PcdSerialIoUartDebugEnabled

Offset 0x0040 - PcdSerialIoUartDebugEnabled Enable SerialIo Uart debug library with/without initializing SerialIo Uart device in FSP.

0:Disable, 1:Enable and Initialize, 2:Enable without Initializing

Definition at line 74 of file FsptUpd.h.

10.12.2.5 PcdSerialIoUartNumber

UINT8 FSP_T_CONFIG::PcdSerialIoUartNumber

Offset 0x0041 - PcdSerialIoUartNumber Select SerialIo Uart Controller for debug.

Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 81 of file FsptUpd.h.

10.12.2.6 PcdSerialIoUartParity

UINT8 FSP_T_CONFIG::PcdSerialIoUartParity

Offset 0x0054 - PcdSerialIoUartParity - FSPT Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 113 of file FsptUpd.h.

10.12.2.7 PcdSerialIoUartRtsPinMux

UINT32 FSP_T_CONFIG::PcdSerialIoUartRtsPinMux

Offset 0x0060 - PcdSerialIoUartRtsPinMux - FSPT Select SerialIo Uart used for debug Rts pin muxing.

Refer to GPIO_*_MUXING_SERIALIO_UARTx_RTS* for possible values.

Definition at line 146 of file FsptUpd.h.

10.12.2.8 PcdSerialIoUartStopBits

UINT8 FSP_T_CONFIG::PcdSerialIoUartStopBits

Offset 0x0056 - PcdSerialIoUartStopBits - FSPT Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 124 of file FsptUpd.h.

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

- [FsptUpd.h](#)

10.13 FSP_T_TEST_CONFIG Struct Reference

Fsp T Test Configuration.

```
#include <FsptUpd.h>
```

Public Attributes

- [UINT32 Signature](#)
Offset 0x0088.
- [UINT8 ReservedFsptTestUpd \[28\]](#)
Offset 0x008C.

10.13.1 Detailed Description

Fsp T Test Configuration.

Definition at line 165 of file FsptUpd.h.

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

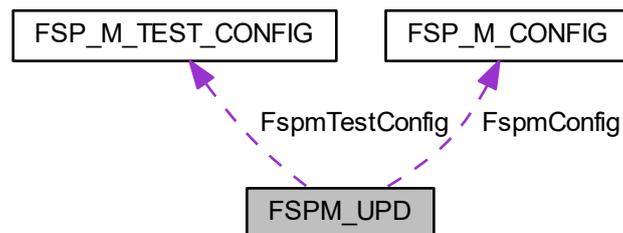
- [FsptUpd.h](#)

10.14 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 0x0540.
- [UINT8 UnusedUpdSpace16](#) [6]
Offset 0x06E8.
- [UINT16 UpdTerminator](#)
Offset 0x06EE.

10.14.1 Detailed Description

Fsp M UPD Configuration.

Definition at line 2481 of file FspmUpd.h.

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

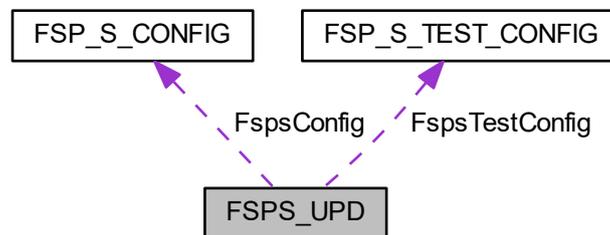
- [FspmUpd.h](#)

10.15 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 0x0A40.
- [UINT8 UnusedUpdSpace36](#) [6]
Offset 0x0EE0.
- [UINT16 UpdTerminator](#)
Offset 0x0EE6.

10.15.1 Detailed Description

Fsp S UPD Configuration.

Definition at line 4133 of file FspUpd.h.

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

- [FspUpd.h](#)

10.16 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.

10.16.1 Detailed Description

Fsp T Core UPD.

Definition at line 43 of file FsptUpd.h.

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

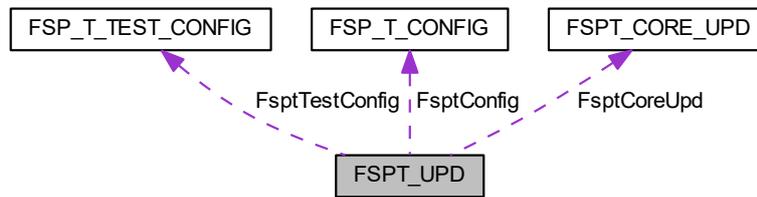
- [FsptUpd.h](#)

10.17 FSPT_UPD Struct Reference

Fsp T UPD Configuration.

```
#include <FsptUpd.h>
```

Collaboration diagram for FSPT_UPD:



Public Attributes

- FSP_UPD_HEADER [FspUpdHeader](#)
Offset 0x0000.
- FSPT_CORE_UPD [FsptCoreUpd](#)
Offset 0x0020.
- FSP_T_CONFIG [FsptConfig](#)
Offset 0x0040.
- FSP_T_TEST_CONFIG [FsptTestConfig](#)
Offset 0x0088.
- UINT8 [UnusedUpdSpace2](#) [6]
Offset 0x00B8.
- UINT16 [UpdTerminator](#)
Offset 0x00BE.

10.17.1 Detailed Description

Fsp T UPD Configuration.

Definition at line 178 of file [FsptUpd.h](#).

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

- [FsptUpd.h](#)

10.18 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.

10.18.1 Detailed Description

GPIO configuration structure used for pin programming.

Structure contains fields that can be used to configure pad.

Definition at line 66 of file GpioConfig.h.

10.18.2 Member Data Documentation

10.18.2.1 Direction

```
UINT32 GPIO_CONFIG::Direction
```

GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.

Refer to definition of GPIO_DIRECTION for supported settings.

Definition at line 87 of file GpioConfig.h.

10.18.2.2 ElectricalConfig

UINT32 GPIO_CONFIG::ElectricalConfig

GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.

Refer to definition of GPIO_ELECTRICAL_CONFIG for supported settings.

Definition at line 113 of file GpioConfig.h.

10.18.2.3 HostSoftPadOwn

UINT32 GPIO_CONFIG::HostSoftPadOwn

Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.

Refer to definition of GPIO_HOSTSW_OWN.

Definition at line 81 of file GpioConfig.h.

10.18.2.4 InterruptConfig

UINT32 GPIO_CONFIG::InterruptConfig

GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).

This setting is applicable only if GPIO is in GpioMode with input enabled. Refer to definition of GPIO_INT_CONFIG for supported settings.

Definition at line 101 of file GpioConfig.h.

10.18.2.5 LockConfig

UINT32 GPIO_CONFIG::LockConfig

GPIO Lock Configuration This setting controls pads lock.

Refer to definition of GPIO_LOCK_CONFIG for supported settings.

Definition at line 119 of file GpioConfig.h.

10.18.2.6 OutputState

UINT32 GPIO_CONFIG::OutputState

Output State Set Pad output value.

Refer to definition of GPIO_OUTPUT_STATE for supported settings. This setting takes place when output is enabled.

Definition at line 94 of file GpioConfig.h.

10.18.2.7 PadMode

UINT32 GPIO_CONFIG::PadMode

Pad Mode Pad can be set as GPIO or one of its native functions.

When in native mode setting Direction (except Inversion), OutputState, InterruptConfig, Host Software Pad Ownership and OutputStateLock are unnecessary. Refer to definition of GPIO_PAD_MODE. Refer to EDS for each native mode according to the pad.

Definition at line 75 of file GpioConfig.h.

10.18.2.8 PowerConfig

UINT32 GPIO_CONFIG::PowerConfig

GPIO Power Configuration.

This setting controls Pad Reset Configuration. Refer to definition of GPIO_RESET_CONFIG for supported settings.

Definition at line 107 of file GpioConfig.h.

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

- [GpioConfig.h](#)

10.19 HOB_USAGE_DATA_HOB Struct Reference

Hob Usage Data Hob.

```
#include <HobUsageDataHob.h>
```

10.19.1 Detailed Description

Hob Usage Data Hob.

Revision 1:

- Initial version.

Definition at line 49 of file HobUsageDataHob.h.

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

- [HobUsageDataHob.h](#)

10.20 MEMORY_PLATFORM_DATA Struct Reference

Memory Platform Data Hob.

```
#include <MemInfoHob.h>
```

10.20.1 Detailed Description

Memory Platform Data Hob.

Revision 1:

- Initial version. **Revision 2:**
- Added TsegBase, PrmrrSize, PrmrrBase, Gttbase, MmioSize, PciEBaseAddress fields

Definition at line 257 of file MemInfoHob.h.

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

- [MemInfoHob.h](#)

10.21 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

- UUINT8 [Device](#)
Device number.
- UUINT8 [Function](#)
Device function.
- UUINT8 [IntX](#)
Interrupt pin: INTA-INTD (see SI_PCH_INT_PIN)
- UUINT8 [Irq](#)
IRQ to be set for device.

10.21.1 Detailed Description

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

Definition at line 74 of file FspsUpd.h.

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

- [FspsUpd.h](#)

10.22 SMBIOS_CACHE_INFO Struct Reference

SMBIOS Cache Info HOB Structure.

```
#include <SmbiosCacheInfoHob.h>
```

Public Attributes

- UUINT16 [NumberOfCacheLevels](#)
Based on Number of Cache Types L1/L2/L3.
- UUINT8 [SocketDesignationStrIndex](#)
String Index in the string Buffer. Example "L1-CACHE".
- UUINT16 [CacheConfiguration](#)
Format defined in SMBIOS Spec v3.1 Section7.8 Table36.

- UIN16 [MaxCacheSize](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.1.
- UIN16 [InstalledSize](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.1.
- UIN16 [SupportedSramType](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.2.
- UIN16 [CurrentSramType](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.2.
- UIN8 [CacheSpeed](#)
Cache Speed in nanoseconds. 0 if speed is unknown.
- UIN8 [ErrorCorrectionType](#)
ENUM Format defined in SMBIOS Spec v3.1 Section 7.8.3.
- UIN8 [SystemCacheType](#)
ENUM Format defined in SMBIOS Spec v3.1 Section 7.8.4.
- UIN8 [Associativity](#)
ENUM Format defined in SMBIOS Spec v3.1 Section 7.8.5.
- UIN32 [MaximumCacheSize2](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.1.
- UIN32 [InstalledSize2](#)
Format defined in SMBIOS Spec v3.1 Section 7.8.1.

10.22.1 Detailed Description

SMBIOS Cache Info HOB Structure.

Definition at line 30 of file SmbiosCacheInfoHob.h.

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

- [SmbiosCacheInfoHob.h](#)

10.23 SMBIOS_PROCESSOR_INFO Struct Reference

SMBIOS Processor Info HOB Structure.

```
#include <SmbiosProcessorInfoHob.h>
```

Public Attributes

- UIN8 [ProcessorType](#)
ENUM defined in SMBIOS Spec v3.1 Section 7.5.1.
- UIN16 [ProcessorFamily](#)
This info is used for both ProcessorFamily and ProcessorFamily2 fields See ENUM defined in SMBIOS Spec v3.1 Section 7.5.2.
- UIN8 [ProcessorManufacturerStrIndex](#)
Index of the String in the String Buffer.
- UIN64 [ProcessorId](#)
ENUM defined in SMBIOS Spec v3.1 Section 7.5.3.
- UIN8 [ProcessorVersionStrIndex](#)
Index of the String in the String Buffer.
- UIN8 [Voltage](#)
Format defined in SMBIOS Spec v3.1 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 v3.1 Table 21.
- UINT8 [ProcessorUpgrade](#)
ENUM defined in SMBIOS Spec v3.1 Section 7.5.5.
- UINT16 [CoreCount](#)
This info is used for both CoreCount & CoreCount2 fields See detailed description in SMBIOS Spec v3.1 Section 7.5.6.
- UINT16 [EnabledCoreCount](#)
This info is used for both CoreEnabled & CoreEnabled2 fields See detailed description in SMBIOS Spec v3.1 Section 7.5.7.
- UINT16 [ThreadCount](#)
This info is used for both ThreadCount & ThreadCount2 fields See detailed description in SMBIOS Spec v3.1 Section 7.5.8.
- UINT16 [ProcessorCharacteristics](#)
Format defined in SMBIOS Spec v3.1 Section 7.5.9.

10.23.1 Detailed Description

SMBIOS Processor Info HOB Structure.

Definition at line 29 of file SmbiosProcessorInfoHob.h.

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

- [SmbiosProcessorInfoHob.h](#)

10.24 SMBIOS_STRUCTURE Struct Reference

The Smbios structure header.

```
#include <FirmwareVersionInfoHob.h>
```

10.24.1 Detailed Description

The Smbios structure header.

Definition at line 48 of file FirmwareVersionInfoHob.h.

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

- [FirmwareVersionInfoHob.h](#)
-

Chapter 11

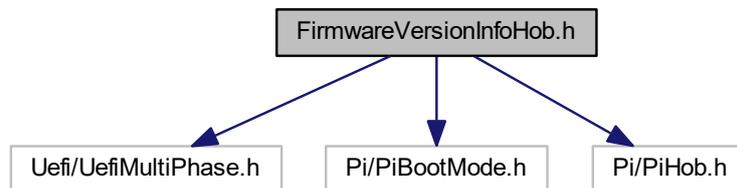
File Documentation

11.1 FirmwareVersionInfoHob.h File Reference

Header file for Firmware Version Information.

```
#include <Uefi/UefiMultiPhase.h>
#include <Pi/PiBootMode.h>
#include <Pi/PiHob.h>
```

Include dependency graph for FirmwareVersionInfoHob.h:



Classes

- struct [FIRMWARE_VERSION](#)
Firmware Version Structure.
- struct [FIRMWARE_VERSION_INFO](#)
Firmware Version Information Structure.
- struct [SMBIOS_STRUCTURE](#)
The Smbios structure header.
- struct [FIRMWARE_VERSION_INFO_HOB](#)
Firmware Version Information HOB Structure.

11.1.1 Detailed Description

Header file for Firmware Version Information.

Copyright

Copyright (c) 2015 - 2018, 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.

11.2 FspFixedPcds.h File Reference

This file lists all FixedAtBuild PCDs referenced in FSP integration guide.

Macros

- #define [PcdFspAreaBaseAddress](#) 0xFFEF3000
FspAreaBaseAddress.
- #define [PcdFspImageldString](#) \$EHLFSP\$
FspImageldString.
- #define [PcdSiliconInitVersionMajor](#) 0x08
SiliconInitVersionMajor.
- #define [PcdSiliconInitVersionMinor](#) 0x07
SiliconInitVersionMinor.
- #define [PcdSiliconInitVersionRevision](#) 0x01
SiliconInitVersionRevision.
- #define [PcdSiliconInitVersionBuild](#) 0x10
SiliconInitVersionBuild.
- #define [PcdGlobalDataPointerAddress](#) 0xFED00148
GlobalDataPointerAddress.
- #define [PcdTemporaryRamBase](#) 0xFE000000
TemporaryRamBase.
- #define [PcdTemporaryRamSize](#) 0x00080000
TemporaryRamSize.
- #define [PcdFspReservedBufferSize](#) 0x100
FspReservedBufferSize.

11.2.1 Detailed Description

This file lists all FixedAtBuild PCDs referenced in FSP integration guide.

Those value may vary in different FSP revision to meet different requirements.

11.3 FspInfoHob.h File Reference

Header file for FSP Information HOB.

11.3.1 Detailed Description

Header file for FSP Information HOB.

Copyright

INTEL CONFIDENTIAL Copyright 2017 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.

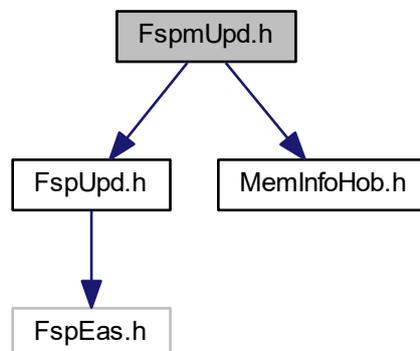
This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

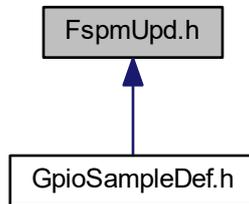
11.4 FspmUpd.h File Reference

Copyright (c) 2018, Intel Corporation.

```
#include <FspUpd.h>
#include <MemInfoHob.h>
Include dependency graph for FspmUpd.h:
```



This graph shows which files directly or indirectly include this file:



Classes

- struct [CHIPSET_INIT_INFO](#)
The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.
- struct [FSP_M_CONFIG](#)
Fsp M Configuration.
- struct [FSP_M_TEST_CONFIG](#)
Fsp M Test Configuration.
- struct [FSPM_UPD](#)
Fsp M UPD Configuration.

11.4.1 Detailed Description

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 SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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.

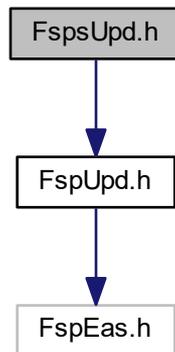
This file is automatically generated. Please do NOT modify !!!

11.5 FspUpd.h File Reference

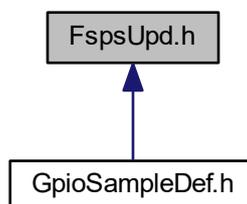
Copyright (c) 2018, Intel Corporation.

```
#include <FspUpd.h>
```

Include dependency graph for FspUpd.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.

11.5.1 Detailed Description

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 SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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 !!!

11.5.2 Enumeration Type Documentation

11.5.2.1 SI_PCH_INT_PIN

enum [SI_PCH_INT_PIN](#)

Refer to the definition of PCH_INT_PIN.

Enumerator

SiPchNoInt	No Interrupt Pin.
------------	-------------------

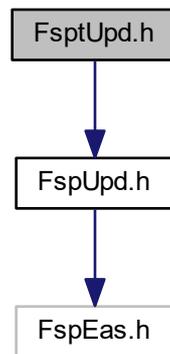
Definition at line 64 of file FspUpd.h.

11.6 FsptUpd.h File Reference

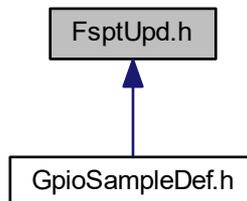
Copyright (c) 2018, Intel Corporation.

```
#include <FsptUpd.h>
```

Include dependency graph for FsptUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

- struct [FSPT_CORE_UPD](#)
Fsp T Core UPD.
 - struct [FSP_T_CONFIG](#)
Fsp T Configuration.
 - struct [FSP_T_TEST_CONFIG](#)
Fsp T Test Configuration.
 - struct [FSPT_UPD](#)
Fsp T UPD Configuration.
-

11.6.1 Detailed Description

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 SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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.

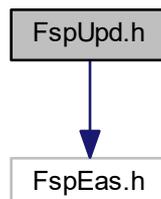
This file is automatically generated. Please do NOT modify !!!

11.7 FspUpd.h File Reference

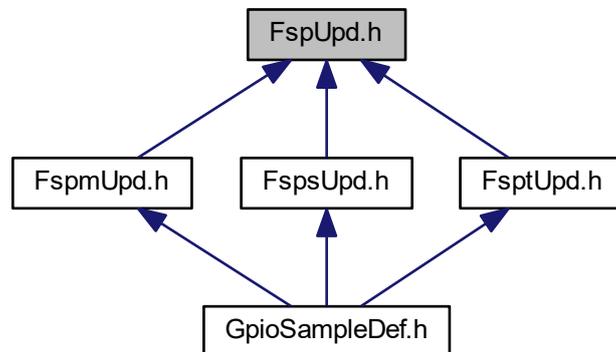
Copyright (c) 2018, Intel Corporation.

```
#include <FspEas.h>
```

Include dependency graph for FspUpd.h:



This graph shows which files directly or indirectly include this file:



11.7.1 Detailed Description

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 SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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 !!!

11.8 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:

11.8.1 Detailed Description

Header file for GpioConfig structure used by GPIO library.

Copyright

INTEL CONFIDENTIAL Copyright 2014 - 2017 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:

11.8.2 Enumeration Type Documentation

11.8.2.1 GPIO_DIRECTION

enum [GPIO_DIRECTION](#)

GPIO Direction.

Enumerator

GpioDirDefault	Leave pad direction setting unmodified.
GpioDirInOut	Set pad for both output and input.
GpioDirInInvOut	Set pad for both output and input with inversion.
GpioDirIn	Set pad for input only.
GpioDirInInv	Set pad for input with inversion.
GpioDirOut	Set pad for output only.
GpioDirNone	Disable both output and input.

Definition at line 195 of file GpioConfig.h.

11.8.2.2 GPIO_ELECTRICAL_CONFIG

enum [GPIO_ELECTRICAL_CONFIG](#)

GPIO Electrical Configuration Set GPIO termination and Pad Tolerance (applicable only for some pads) Field from GpioTermNone to GpioTermNative can be OR'ed with GpioTolerance1v8.

Enumerator

GpioTermDefault	Leave termination setting unmodified.
GpioTermNone	none
GpioTermWpd5K	5kOhm weak pull-down
GpioTermWpd20K	20kOhm weak pull-down
GpioTermWpu1K	1kOhm weak pull-up
GpioTermWpu2K	2kOhm weak pull-up
GpioTermWpu5K	5kOhm weak pull-up
GpioTermWpu20K	20kOhm weak pull-up
GpioTermWpu1K2K	1kOhm & 2kOhm weak pull-up
GpioTermNative	Native function controls pads termination This setting is applicable only to some native modes. Please check EDS to determine which native functionality can control pads termination
GpioNoTolerance1v8	Disable 1.8V pad tolerance.
GpioTolerance1v8	Enable 1.8V pad tolerance.

Definition at line 324 of file GpioConfig.h.

11.8.2.3 GPIO_HARDWARE_DEFAULT

enum [GPIO_HARDWARE_DEFAULT](#)

Enumerator

GpioHardwareDefault	Leave setting unmodified.
---------------------	---------------------------

Definition at line 146 of file GpioConfig.h.

11.8.2.4 GPIO_HOSTSW_OWN

enum [GPIO_HOSTSW_OWN](#)

Host Software Pad Ownership modes This setting affects GPIO interrupt status registers.

Depending on chosen ownership some GPIO Interrupt status register get updated and other masked. Please refer to EDS for HOSTSW_OWN register description.

Enumerator

GpioHostOwnDefault	Leave ownership value unmodified.
GpioHostOwnAcpi	Set HOST ownership to ACPI. Use this setting if pad is not going to be used by GPIO OS driver. If GPIO is configured to generate SCI/SMI/NMI then this setting must be used for interrupts to work
GpioHostOwnGpio	Set HOST ownership to GPIO Driver mode. Use this setting only if GPIO pad should be controlled by GPIO OS Driver. GPIO OS Driver will be able to control the pad if appropriate entry in ACPI exists (refer to ACPI specification for Gpiolo and GpioInt descriptors)

Definition at line 174 of file GpioConfig.h.

11.8.2.5 GPIO_INT_CONFIG

enum [GPIO_INT_CONFIG](#)

GPIO interrupt configuration This setting is applicable only if pad is in GPIO mode and has input enabled.

GPIO_INT_CONFIG allows to choose which interrupt is generated (IOxAPIC/SCI/SMI/NMI) and how it is triggered (edge or level). Refer to PADCFG_DW0 register description in EDS for details on this settings. Field from 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 235 of file GpioConfig.h.

11.8.2.6 GPIO_LOCK_CONFIG

enum [GPIO_LOCK_CONFIG](#)

GPIO LockConfiguration Set GPIO configuration lock and output state lock.

GpioLockPadConfig and GpioLockOutputState can be OR'ed. Lock settings reset is in Powergood domain. Care must be taken when using this setting as fields it locks may be reset by a different signal and can be controllable by what is in GPIO_RESET_CONFIG (PADCFG_DW0.PadRstCfg). GPIO library provides functions which allow to unlock a GPIO pad.

Enumerator

GpioLockDefault	Leave lock setting unmodified.
GpioPadConfigLock	Lock Pad Configuration.
GpioOutputStateLock	Lock GPIO pad output value.

Definition at line 357 of file GpioConfig.h.

11.8.2.7 GPIO_OTHER_CONFIG

enum [GPIO_OTHER_CONFIG](#)

Other GPIO Configuration `GPIO_OTHER_CONFIG` is used for less often settings and for future extensions Supported settings:

- RX raw override to '1' - allows to override input value to '1' This setting is applicable only if in input mode (both in GPIO and native usage). The override takes place at the internal pad state directly from buffer and before the `RXINV`.

Enumerator

<code>GpioRxRaw1Default</code>	Use default input override value.
<code>GpioRxRaw1Dis</code>	Don't override input.
<code>GpioRxRaw1En</code>	Override input to '1'.

Definition at line 374 of file `GpioConfig.h`.

11.8.2.8 GPIO_OUTPUT_STATE

enum [GPIO_OUTPUT_STATE](#)

GPIO Output State This field is relevant only if output is enabled.

Enumerator

<code>GpioOutDefault</code>	Leave output value unmodified.
<code>GpioOutLow</code>	Set output to low.
<code>GpioOutHigh</code>	Set output to high.

Definition at line 209 of file `GpioConfig.h`.

11.8.2.9 GPIO_PAD_MODE

enum [GPIO_PAD_MODE](#)

GPIO Pad Mode Refer to GPIO documentation on native functions available for certain pad.

If GPIO is set to one of NativeX modes then following settings are not applicable and can be skipped:

- Interrupt related settings
- Host Software Ownership
- Output/Input enabling/disabling
- Output lock

Definition at line 160 of file `GpioConfig.h`.

11.8.2.10 GPIO_RESET_CONFIG

enum `GPIO_RESET_CONFIG`

GPIO Power Configuration `GPIO_RESET_CONFIG` allows to set GPIO Reset type (`PADCFG_DW0.PadRstCfg`) which will be used to reset certain GPIO settings.

Refer to EDS for settings that are controllable by `PadRstCfg`.

Enumerator

<code>GpioResetDefault</code>	Leave value of pad reset unmodified.
<code>GpioResetPwrGood</code>	Deprecated settings. Maintained only for compatibility. GPP: <code>RSMRST</code> ; GPD: <code>DSW_PWROK</code> ; (<code>PadRstCfg = 00b = "Powergood"</code>)
<code>GpioResetDeep</code>	Deep GPIO Reset (<code>PadRstCfg = 01b = "Deep GPIO Reset"</code>)
<code>GpioResetNormal</code>	GPIO Reset (<code>PadRstCfg = 10b = "GPIO Reset"</code>)
<code>GpioResetResume</code>	GPP: Reserved; GPD: <code>RSMRST</code> ; (<code>PadRstCfg = 11b = "Resume Reset"</code>)
<code>GpioResumeReset</code>	New GPIO reset configuration options. Resume Reset (<code>RSMRST</code>) GPP: <code>PadRstCfg = 00b = "Powergood"</code> GPD: <code>PadRstCfg = 11b = "Resume Reset"</code> Pad setting will reset on: <ul style="list-style-type: none"> • DeepSx transition • G3 Pad settings will not reset on: • S3/S4/S5 transition • Warm/Cold/Global reset
<code>GpioHostDeepReset</code>	Host Deep Reset <code>PadRstCfg = 01b = "Deep GPIO Reset"</code> Pad settings will reset on: <ul style="list-style-type: none"> • Warm/Cold/Global reset • DeepSx transition • G3 Pad settings will not reset on: • S3/S4/S5 transition
<code>GpioPlatformReset</code>	Platform Reset (<code>PLTRST</code>) <code>PadRstCfg = 10b = "GPIO Reset"</code> Pad settings will reset on: <ul style="list-style-type: none"> • S3/S4/S5 transition • Warm/Cold/Global reset • DeepSx transition • G3
<code>GpioDswReset</code>	Deep Sleep Well Reset (<code>DSW_PWROK</code>) GPP: not applicable GPD: <code>PadRstCfg = 00b = "Powergood"</code> Pad settings will reset on: <ul style="list-style-type: none"> • G3 Pad settings will not reset on: • S3/S4/S5 transition • Warm/Cold/Global reset • DeepSx transition

Definition at line 257 of file `GpioConfig.h`.

11.9 GpioSampleDef.h File Reference

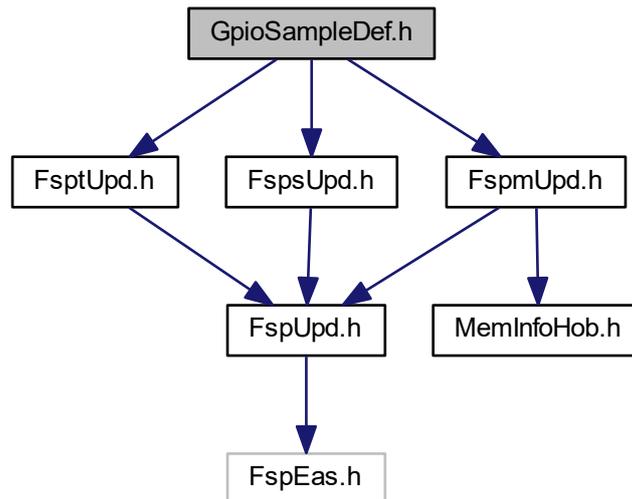
Copyright (c) 2015 - 2017, Intel Corporation.

```
#include <FsptUpd.h>
```

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

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

Include dependency graph for GpioSampleDef.h:



11.9.1 Detailed Description

Copyright (c) 2015 - 2017, 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 SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) 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 !!!

11.10 HobUsageDataHob.h File Reference

Definitions for Hob Usage data HOB.

Classes

- struct [HOB_USAGE_DATA_HOB](#)

Hob Usage Data Hob.

11.10.1 Detailed Description

Definitions for Hob Usage data HOB.

Copyright

INTEL CONFIDENTIAL Copyright 2017 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.

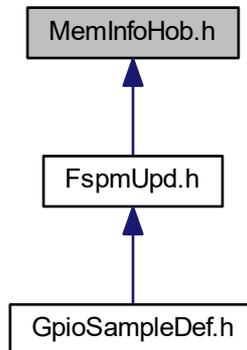
This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

11.11 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 MrInterface.h.

Enumerations

- enum [MRC_BOOT_MODE](#)

11.11.1 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:

11.11.2 Enumeration Type Documentation

11.11.2.1 MRC_BOOT_MODE

```
enum MRC_BOOT_MODE
```

Enumerator

bmCold	Cold boot.
bmWarm	Warm boot.
bmS3	S3 resume.
bmFast	Fast boot.
MrcBootModeMax	MRC_BOOT_MODE enumeration maximum value.
MrcBootModeDelim	This value ensures the enum size is consistent on both sides of the PPI.

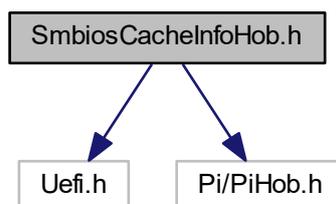
Definition at line 131 of file MemInfoHob.h.

11.12 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.

11.12.1 Detailed Description

Header file for SMBIOS Cache Info HOB.

Copyright

Copyright (c) 2015 - 2018, 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.

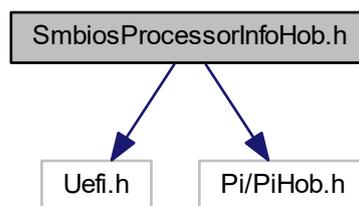
System Management BIOS (SMBIOS) Reference Specification v3.1.0 dated 2016-Nov-16 (DSP0134) http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.1.0.pdf

11.13 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.

11.13.1 Detailed Description

Header file for SMBIOS Processor Info HOB.

Copyright

Copyright (c) 2015 - 2018, 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 that 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.

System Management BIOS (SMBIOS) Reference Specification v3.1.0 dated 2016-Nov-16 (DSP0134) http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.1.0.pdf

Index

- AUDIO_AZALIA_VERB_TABLE, [31](#)
- AZALIA_HEADER, [32](#)
- AcLoadline
 - FSP_S_CONFIG, [112](#)
- AcousticNoiseMitigation
 - FSP_S_CONFIG, [112](#)
- ActiveCoreCount
 - FSP_M_CONFIG, [53](#)
- AmtEnabled
 - FSP_S_CONFIG, [113](#)
- AmtKvmEnabled
 - FSP_S_CONFIG, [113](#)
- AmtSolEnabled
 - FSP_S_CONFIG, [113](#)
- ApIdleManner
 - FSP_S_TEST_CONFIG, [182](#)
- ApStartupBase
 - FSP_M_CONFIG, [53](#)
- ApertureSize
 - FSP_M_CONFIG, [53](#)
- AsfEnabled
 - FSP_S_CONFIG, [113](#)
- AutoThermalReporting
 - FSP_S_TEST_CONFIG, [182](#)
- Avx2RatioOffset
 - FSP_M_CONFIG, [53](#)
- Avx3RatioOffset
 - FSP_M_CONFIG, [54](#)

- BclkAdaptiveVoltage
 - FSP_M_CONFIG, [54](#)
- BclkRfiFreq
 - FSP_M_CONFIG, [54](#)
- BdatEnable
 - FSP_M_TEST_CONFIG, [85](#)
- BdatTestType
 - FSP_M_TEST_CONFIG, [85](#)
- BiosAcmBase
 - FSP_M_CONFIG, [54](#)
- BiosAcmSize
 - FSP_M_CONFIG, [54](#)
- BiosGuard
 - FSP_M_CONFIG, [55](#)
- BiosSize
 - FSP_M_TEST_CONFIG, [85](#)
- BistOnReset
 - FSP_M_CONFIG, [55](#)
- BootFrequency
 - FSP_M_CONFIG, [55](#)
- BypassPhySyncReset
 - FSP_M_TEST_CONFIG, [85](#)

- C1StateAutoDemotion
 - FSP_S_TEST_CONFIG, [183](#)
- C1StateUnDemotion
 - FSP_S_TEST_CONFIG, [183](#)
- C1e
 - FSP_S_TEST_CONFIG, [182](#)
- CHIPSET_INIT_INFO, [32](#)
- CStatePreWake
 - FSP_S_TEST_CONFIG, [183](#)
- ChHashEnable
 - FSP_M_CONFIG, [55](#)
- ChHashInterleaveBit
 - FSP_M_CONFIG, [55](#)
- ChHashMask
 - FSP_M_CONFIG, [56](#)
- ChipsetInitMessage
 - FSP_M_TEST_CONFIG, [85](#)
- CkeRankMapping
 - FSP_M_CONFIG, [56](#)
- CleanMemory
 - FSP_M_CONFIG, [56](#)
- CmdRanksTerminated
 - FSP_M_CONFIG, [56](#)
- CnviBtAudioOffload
 - FSP_S_CONFIG, [113](#)
- CnviBtCore
 - FSP_S_CONFIG, [114](#)
- CnviClkreqPinMux
 - FSP_S_CONFIG, [114](#)
- CnviMode
 - FSP_S_CONFIG, [114](#)
- CnviRfResetPinMux
 - FSP_S_CONFIG, [114](#)
- ConfigTdpBios
 - FSP_S_TEST_CONFIG, [183](#)
- CoreCStateLimit
 - FSP_S_TEST_CONFIG, [183](#)
- CoreMaxOcRatio
 - FSP_M_CONFIG, [56](#)
- CorePllVoltageOffset
 - FSP_M_CONFIG, [56](#)
- CoreVoltageAdaptive
 - FSP_M_CONFIG, [57](#)
- CoreVoltageMode
 - FSP_M_CONFIG, [57](#)
- CoreVoltageOverride
 - FSP_M_CONFIG, [57](#)
- Count

- FIRMWARE_VERSION_INFO_HOB, [35](#)
- CpuRatio
 - FSP_M_CONFIG, [57](#)
- CpuRatioOverride
 - FSP_M_CONFIG, [57](#)
- CpuTraceHubMemReg0Size
 - FSP_M_CONFIG, [58](#)
- CpuTraceHubMemReg1Size
 - FSP_M_CONFIG, [58](#)
- CpuTraceHubMode
 - FSP_M_CONFIG, [58](#)
- CridEnable
 - FSP_M_CONFIG, [58](#)
- CstCfgCtrlIoMwaitRedirection
 - FSP_S_TEST_CONFIG, [184](#)
- Custom1ConfigTdpControl
 - FSP_S_TEST_CONFIG, [184](#)
- Custom1PowerLimit1
 - FSP_S_TEST_CONFIG, [184](#)
- Custom1PowerLimit1Time
 - FSP_S_TEST_CONFIG, [184](#)
- Custom1PowerLimit2
 - FSP_S_TEST_CONFIG, [184](#)
- Custom1TurboActivationRatio
 - FSP_S_TEST_CONFIG, [185](#)
- Custom2ConfigTdpControl
 - FSP_S_TEST_CONFIG, [185](#)
- Custom2PowerLimit1
 - FSP_S_TEST_CONFIG, [185](#)
- Custom2PowerLimit1Time
 - FSP_S_TEST_CONFIG, [185](#)
- Custom2PowerLimit2
 - FSP_S_TEST_CONFIG, [185](#)
- Custom2TurboActivationRatio
 - FSP_S_TEST_CONFIG, [186](#)
- Custom3ConfigTdpControl
 - FSP_S_TEST_CONFIG, [186](#)
- Custom3PowerLimit1
 - FSP_S_TEST_CONFIG, [186](#)
- Custom3PowerLimit1Time
 - FSP_S_TEST_CONFIG, [186](#)
- Custom3PowerLimit2
 - FSP_S_TEST_CONFIG, [186](#)
- Custom3TurboActivationRatio
 - FSP_S_TEST_CONFIG, [186](#)
- Cx
 - FSP_S_TEST_CONFIG, [187](#)
- DIMM_INFO, [33](#)
- DcLoadline
 - FSP_S_CONFIG, [114](#)
- DciUsb3TypecUfpDbg
 - FSP_M_CONFIG, [58](#)
- DdrFreqLimit
 - FSP_M_CONFIG, [59](#)
- DdrSpeedControl
 - FSP_M_CONFIG, [59](#)
- DebugInterfaceLockEnable
 - FSP_S_TEST_CONFIG, [187](#)
- DevIntConfigPtr
 - FSP_S_CONFIG, [115](#)
- Direction
 - GPIO_CONFIG, [208](#)
- DisableDimmChannel0
 - FSP_M_CONFIG, [59](#)
- DisableDimmChannel1
 - FSP_M_CONFIG, [59](#)
- DisableMessageCheck
 - FSP_M_TEST_CONFIG, [86](#)
- DisableProcHotOut
 - FSP_S_TEST_CONFIG, [187](#)
- DisableVrThermalAlert
 - FSP_S_TEST_CONFIG, [187](#)
- DmiDeEmphasis
 - FSP_M_CONFIG, [59](#)
- DmiGen3EndPointHint
 - FSP_M_CONFIG, [60](#)
- DmiGen3EndPointPreset
 - FSP_M_CONFIG, [60](#)
- DmiGen3EqPh2Enable
 - FSP_M_TEST_CONFIG, [86](#)
- DmiGen3EqPh3Method
 - FSP_M_TEST_CONFIG, [86](#)
- DmiGen3ProgramStaticEq
 - FSP_M_CONFIG, [60](#)
- DmiGen3RootPortPreset
 - FSP_M_CONFIG, [60](#)
- DmiSuggestedSetting
 - FSP_S_CONFIG, [115](#)
- DmiTS0TW
 - FSP_S_CONFIG, [115](#)
- DmiTS1TW
 - FSP_S_CONFIG, [115](#)
- DmiTS2TW
 - FSP_S_CONFIG, [115](#)
- DmiTS3TW
 - FSP_S_CONFIG, [115](#)
- EcCmdLock
 - FSP_S_CONFIG, [116](#)
- EcCmdProvisionEav
 - FSP_S_CONFIG, [116](#)
- Eist
 - FSP_S_TEST_CONFIG, [187](#)
- ElectricalConfig
 - GPIO_CONFIG, [208](#)
- EnCmdRate
 - FSP_M_CONFIG, [61](#)
- Enable8254ClockGating
 - FSP_S_CONFIG, [116](#)
- EnableC6Dram
 - FSP_M_CONFIG, [60](#)
- EnableEpbPeciOverride
 - FSP_S_TEST_CONFIG, [188](#)
- EnableFastMsrHwpReq
 - FSP_S_TEST_CONFIG, [188](#)
- EnableHwpAutoEppGrouping
 - FSP_S_TEST_CONFIG, [188](#)

- EnableHwpAutoPerCorePstate
 - FSP_S_TEST_CONFIG, 188
- EnableIbtm
 - FSP_S_TEST_CONFIG, 188
- EnableMinVoltageOverride
 - FSP_S_CONFIG, 116
- EnablePerCorePState
 - FSP_S_TEST_CONFIG, 189
- EnableSgx
 - FSP_M_CONFIG, 61
- EnableTcoTimer
 - FSP_S_CONFIG, 116
- EnableTimedGPIO0
 - FSP_S_CONFIG, 117
- EnableTimedGPIO1
 - FSP_S_CONFIG, 117
- EndOfPostMessage
 - FSP_S_TEST_CONFIG, 189
- EnergyEfficientPState
 - FSP_S_TEST_CONFIG, 189
- EnergyEfficientTurbo
 - FSP_S_TEST_CONFIG, 189
- EpgEnable
 - FSP_M_CONFIG, 61
- EsataSpeedLimit
 - FSP_S_CONFIG, 117
- FCLKFrequency
 - FSP_M_CONFIG, 61
- FIRMWARE_VERSION_INFO_HOB, 34
 - Count, 35
- FIRMWARE_VERSION_INFO, 34
- FIRMWARE_VERSION, 33
- FSP_M_CONFIG, 35
 - ActiveCoreCount, 53
 - ApStartupBase, 53
 - ApertureSize, 53
 - Avx2RatioOffset, 53
 - Avx3RatioOffset, 54
 - BclkAdaptiveVoltage, 54
 - BclkRfiFreq, 54
 - BiosAcmBase, 54
 - BiosAcmSize, 54
 - BiosGuard, 55
 - BistOnReset, 55
 - BootFrequency, 55
 - ChHashEnable, 55
 - ChHashInterleaveBit, 55
 - ChHashMask, 56
 - CkeRankMapping, 56
 - CleanMemory, 56
 - CmdRanksTerminated, 56
 - CoreMaxOcRatio, 56
 - CorePIIVoltageOffset, 56
 - CoreVoltageAdaptive, 57
 - CoreVoltageMode, 57
 - CoreVoltageOverride, 57
 - CpuRatio, 57
 - CpuRatioOverride, 57
 - CpuTraceHubMemReg0Size, 58
 - CpuTraceHubMemReg1Size, 58
 - CpuTraceHubMode, 58
 - CridEnable, 58
 - DciUsb3TypecUfpDbg, 58
 - DdrFreqLimit, 59
 - DdrSpeedControl, 59
 - DisableDimmChannel0, 59
 - DisableDimmChannel1, 59
 - DmiDeEmphasis, 59
 - DmiGen3EndPointHint, 60
 - DmiGen3EndPointPreset, 60
 - DmiGen3ProgramStaticEq, 60
 - DmiGen3RootPortPreset, 60
 - EnCmdRate, 61
 - EnableC6Dram, 60
 - EnableSgx, 61
 - EpgEnable, 61
 - FCLKFrequency, 61
 - FivrEfficiency, 61
 - FivrFaults, 62
 - ForceOltmOrRefresh2x, 62
 - FreqSaGvLow, 62
 - FreqSaGvMid, 62
 - GmAdr, 62
 - GtPIIVoltageOffset, 63
 - GtPsmiSupport, 63
 - GttMmAdr, 63
 - HobBufferSize, 63
 - HotThresholdCh0Dimm0, 63
 - HotThresholdCh0Dimm1, 64
 - HotThresholdCh1Dimm0, 64
 - HotThresholdCh1Dimm1, 64
 - Idd3n, 64
 - Idd3p, 64
 - IgdDvmt50PreAlloc, 64
 - ImguClkOutEn, 65
 - ImrRpSelection, 65
 - InitPcieAspmAfterOprom, 65
 - InternalGfx, 65
 - IsvtloPort, 65
 - JtagC10PowerGateDisable, 66
 - McPIIVoltageOffset, 66
 - MmioSize, 66
 - OcLock, 66
 - PcdDebugInterfaceFlags, 66
 - PcdIlsaSerialUartBase, 67
 - PcdSerialDebugBaudRate, 67
 - PcdSerialDebugLevel, 67
 - PcdSerialUartNumber, 67
 - PchLpcEnhancePort8xhDecoding, 67
 - PchNumRsvdSmbusAddresses, 68
 - PchPort80Route, 68
 - PchSmbAlertEnable, 68
 - PchTraceHubMemReg0Size, 68
 - PchTraceHubMemReg1Size, 68
 - PchTraceHubMode, 69
 - PcieImrSize, 69

- PcieMultipleSegmentEnabled, 69
- PcieRpEnableMask, 69
- PlatformDebugConsent, 69
- PrmrrSize, 70
- ProbelessTrace, 70
- PwdwnIdleCounter, 70
- RMTLoopCount, 73
- RMT, 72
- RankInterleave, 70
- Ratio, 70
- RealtimeMemoryTiming, 71
- RefClk, 71
- RhSolution, 71
- RingDownBin, 71
- RingMaxOcRatio, 71
- RingPllVoltageOffset, 71
- RingVoltageAdaptive, 72
- RingVoltageMode, 72
- RingVoltageOffset, 72
- RingVoltageOverride, 72
- RmtPerTask, 73
- SaGv, 73
- SaPcieRpEnableMask, 73
- SaPcieRpLinkDownGpios, 74
- SaPllVoltageOffset, 74
- SafeMode, 73
- ScramblerSupport, 74
- SinitMemorySize, 74
- SmbusArpEnable, 74
- SmbusEnable, 74
- SpdAddressTable, 75
- SpdProfileSelected, 75
- tRTP, 78
- TcssDma0En, 75
- TcssDma1En, 75
- TcssDma2En, 75
- TcssItbtPcie0En, 76
- TcssItbtPcie1En, 76
- TcssItbtPcie2En, 76
- TcssItbtPcie3En, 76
- TcssItbtPcie4En, 76
- TcssItbtPcie5En, 76
- TcssXdciEn, 77
- TcssXhciEn, 77
- TgaSize, 77
- ThrtCkeMinTmr, 77
- TjMaxOffset, 77
- TmeEnable, 78
- TrainTrace, 78
- TsegSize, 78
- TsodAlarmwindowLockBit, 78
- TsodCriticalEventOnly, 79
- TsodCriticaltripLockBit, 79
- TsodEventMode, 79
- TsodEventOutputControl, 79
- TsodEventPolarity, 79
- TsodManualEnable, 80
- TsodShutdownMode, 80
- TsodTcritMax, 80
- Txt, 80
- TxtDprMemoryBase, 80
- TxtDprMemorySize, 81
- TxtHeapMemorySize, 81
- TxtImplemented, 81
- TxtLcpPdBase, 81
- TxtLcpPdSize, 81
- UserBudgetEnable, 81
- UserThresholdEnable, 82
- VddVoltage, 82
- VmxEnable, 82
- WarmThresholdCh0Dimm0, 82
- WarmThresholdCh0Dimm1, 82
- WarmThresholdCh1Dimm0, 83
- WarmThresholdCh1Dimm1, 83
- FSP_M_TEST_CONFIG, 83
 - BdatEnable, 85
 - BdatTestType, 85
 - BiosSize, 85
 - BypassPhySyncReset, 85
 - ChipsetInitMessage, 85
 - DisableMessageCheck, 86
 - DmiGen3EqPh2Enable, 86
 - DmiGen3EqPh3Method, 86
 - HeciCommunication2, 86
 - KtDeviceEnable, 86
 - LockPTMregs, 87
 - PanelPowerEnable, 87
 - ScanExtGfxForLegacyOpRom, 87
 - SkipMbpHob, 87
 - SmbusDynamicPowerGating, 87
 - SmbusSpdWriteDisable, 88
 - TotalFlashSize, 88
 - TxtAcheckRequest, 88
 - WdtDisableAndLock, 88
- FSP_S_CONFIG, 88
 - AcLoadline, 112
 - AcousticNoiseMitigation, 112
 - AmtEnabled, 113
 - AmtKvmEnabled, 113
 - AmtSolEnabled, 113
 - AsfEnabled, 113
 - CnviBtAudioOffload, 113
 - CnviBtCore, 114
 - CnviClkreqPinMux, 114
 - CnviMode, 114
 - CnviRfResetPinMux, 114
 - DcLoadline, 114
 - DevIntConfigPtr, 115
 - DmiSuggestedSetting, 115
 - DmiTS0TW, 115
 - DmiTS1TW, 115
 - DmiTS2TW, 115
 - DmiTS3TW, 115
 - EcCmdLock, 116
 - EcCmdProvisionEav, 116
 - Enable8254ClockGating, 116

- EnableMinVoltageOverride, 116
- EnableTcoTimer, 116
- EnableTimedGPIO0, 117
- EnableTimedGPIO1, 117
- EsataSpeedLimit, 117
- FastPkgCRampDisableFivr, 117
- FastPkgCRampDisableGt, 117
- FastPkgCRampDisableIa, 118
- FastPkgCRampDisableSa, 118
- FivrRfiFrequency, 118
- FivrSpreadSpectrum, 118
- ForcMebxSyncUp, 118
- FwProgress, 119
- GpioIrqRoute, 119
- Heci3Enabled, 119
- ITbtConnectTopologyTimeoutInMs, 120
- ITbtForcePowerOnTimeoutInMs, 120
- IccMax, 119
- ImonOffset, 119
- ImonSlope, 120
- IomTypeCPortPadCfg, 120
- ManageabilityMode, 120
- MeUnconfigOnRtcClear, 121
- MinVoltageC8, 121
- MinVoltageRuntime, 121
- NumOfDevIntConfig, 121
- PchCrid, 121
- PchDmiAspmCtrl, 121
- PchDmiTsaWen, 122
- PchEnableComplianceMode, 122
- PchEnableDbcObs, 122
- PchEspHostC10ReportEnable, 122
- PchFivrDynPm, 122
- PchFivrExtVnnRailSxEnabledStates, 123
- PchFivrExtVnnRailSxIccMax, 123
- PchFivrExtVnnRailSxVoltage, 123
- PchFivrVccinAuxLowToHighCurModeVolTranTime, 123
- PchFivrVccinAuxOffToHighCurModeVolTranTime, 123
- PchFivrVccinAuxRetToHighCurModeVolTranTime, 124
- PchFivrVccinAuxRetToLowCurModeVolTranTime, 124
- PchHdaAudioLinkDmic0ClkAPinMux, 124
- PchHdaAudioLinkDmic0ClkBPinMux, 124
- PchHdaAudioLinkDmic0DataPinMux, 124
- PchHdaAudioLinkDmic0Enable, 125
- PchHdaAudioLinkDmic1ClkAPinMux, 125
- PchHdaAudioLinkDmic1ClkBPinMux, 125
- PchHdaAudioLinkDmic1DataPinMux, 125
- PchHdaAudioLinkDmic1Enable, 125
- PchHdaAudioLinkHdaEnable, 126
- PchHdaAudioLinkSndw1Enable, 126
- PchHdaAudioLinkSndw2Enable, 126
- PchHdaAudioLinkSndw3Enable, 126
- PchHdaAudioLinkSndw4Enable, 126
- PchHdaAudioLinkSsp0Enable, 126
- PchHdaAudioLinkSsp1Enable, 127
- PchHdaAudioLinkSsp2Enable, 127
- PchHdaAudioLinkSsp3Enable, 127
- PchHdaAudioLinkSsp4Enable, 127
- PchHdaAudioLinkSsp5Enable, 127
- PchHdaDspEnable, 128
- PchHdaDspUaaCompliance, 128
- PchHdaDispCodecDisconnect, 128
- PchHdaDispLinkFrequency, 128
- PchHdaLinkFrequency, 128
- PchHdaPme, 129
- PchHdaVcType, 129
- PchHotEnable, 129
- PchIoApicEntry24_119, 129
- PchIoApicId, 129
- PchIshGpEnable, 129
- PchIshI2cEnable, 130
- PchIshPdtUnlock, 130
- PchIshSpiCs0Enable, 130
- PchIshSpiEnable, 130
- PchIshUartEnable, 130
- PchLanEnable, 131
- PchLanLtrEnable, 131
- PchLockDownBiosLock, 131
- PchMemoryThrottlingEnable, 131
- PchOseAdcEnable, 131
- PchOseCanEnable, 131
- PchOseHsuartEnable, 132
- PchOseI2cEnable, 132
- PchOseI2sEnable, 132
- PchOsePwmEnable, 132
- PchOseQepEnable, 132
- PchOseSpiCs0Enable, 133
- PchOseSpiEnable, 133
- PchOseTimedGpioEnable, 133
- PchOseTimedGpioPinAllocation, 133
- PchOseTimedGpioPinEnable, 133
- PchOseUartEnable, 134
- PchPcieDeviceOverrideTablePtr, 134
- PchPmDeepSxPol, 134
- PchPmDisableDsxAcPresentPulldown, 134
- PchPmDisableNativePowerButton, 134
- PchPmLanWakeFromDeepSx, 134
- PchPmMeWakeSts, 135
- PchPmPciePIISsc, 135
- PchPmPcieWakeFromDeepSx, 135
- PchPmPmeB0S5Dis, 135
- PchPmPwrBtnOverridePeriod, 135
- PchPmPwrCycDur, 136
- PchPmSlpAMinAssert, 136
- PchPmSlpLanLowDc, 136
- PchPmSlpS0Enable, 136
- PchPmSlpS0Vm070VSupport, 136
- PchPmSlpS0Vm075VSupport, 136
- PchPmSlpS0VmRuntimeControl, 137
- PchPmSlpS3MinAssert, 137
- PchPmSlpS4MinAssert, 137
- PchPmSlpStrchSusUp, 137

- PchPmSlpSusMinAssert, 137
- PchPmVrAlert, 138
- PchPmWoWlanDeepSxEnable, 138
- PchPmWoWlanEnable, 138
- PchPmWolEnableOverride, 138
- PchPmWolOvrWkSts, 138
- PchPwrOptEnable, 139
- PchS0ixAutoDemotion, 139
- PchSerialIol2cPadsTermination, 139
- PchSerialIol2cScIpinMux, 139
- PchSerialIol2cSdaPinMux, 139
- PchStartFramePulse, 140
- PchTTEnable, 140
- PchTTLock, 140
- PchTTState13Enable, 140
- PchTsnEnable, 140
- PcieComplianceTestMode, 140
- PcieDisableRootPortClockGating, 141
- PcieEnablePeerMemoryWrite, 141
- PcieEqPh3LaneParamCm, 141
- PcieEqPh3LaneParamCp, 141
- PcieRpAspm, 141
- PcieRpCompletionTimeout, 142
- PcieRpDpcExtensionsMask, 142
- PcieRpDpcMask, 142
- PcieRpFunctionSwap, 142
- PcieRpGen3EqPh3Method, 142
- PcieRpImrEnabled, 143
- PcieRpL1Substates, 143
- PcieRpPcieSpeed, 143
- PcieRpPhysicalSlotNumber, 143
- PcieRpPtmMask, 143
- PcieSwEqCoeffListCm, 144
- PcieSwEqCoeffListCp, 144
- PmcCpuC10GatePinEnable, 144
- PmcDbgMsgEn, 144
- PmcGrTscEnable, 144
- PmcModPhySusPgEnable, 144
- PmcPowerButtonDebounce, 145
- PmcV1p05IsExtFetControlEn, 145
- PmcV1p05PhyExtFetControlEn, 145
- PortUsb20Enable, 145
- PortUsb30Enable, 145
- PpinSupport, 146
- PsOnEnable, 147
- Psi1Threshold, 146
- Psi2Threshold, 146
- Psi3Enable, 146
- Psi3Threshold, 146
- PsysOffset, 147
- PsysSlope, 147
- PxRcConfig, 147
- RemoteAssistance, 147
- RtcBiosInterfaceLock, 148
- RtcMemoryLock, 148
- SaPcieComplianceTestMode, 148
- SaPcieDeviceOverrideTablePtr, 148
- SaPcieDisableRootPortClockGating, 148
- SaPcieDisableRootPortPowerGating, 149
- SaPcieEnablePeerMemoryWrite, 149
- SaPcieEqPh3LaneParamCm, 149
- SaPcieEqPh3LaneParamCp, 149
- SaPcieGen3EndPointHint, 149
- SaPcieGen3EndPointPreset, 150
- SaPcieGen3ProgramStaticEq, 150
- SaPcieGen3RootPortPreset, 150
- SaPcieGen4EndPointHint, 150
- SaPcieGen4EndPointPreset, 150
- SaPcieGen4ProgramStaticEq, 151
- SaPcieGen4RootPortPreset, 151
- SaPcieHwEqGen3CoeffListCm, 151
- SaPcieHwEqGen3CoeffListCp, 151
- SaPcieHwEqGen4CoeffListCm, 151
- SaPcieHwEqGen4CoeffListCp, 152
- SaPcieRpAspm, 152
- SaPcieRpDpcEnabled, 152
- SaPcieRpDpcExtensionsEnabled, 152
- SaPcieRpFunctionSwap, 152
- SaPcieRpGen3EqPh23Enable, 153
- SaPcieRpGen3EqPh3Enable, 153
- SaPcieRpGen3EqPh3Method, 153
- SaPcieRpGen4EqPh23Enable, 153
- SaPcieRpGen4EqPh3Enable, 153
- SaPcieRpGen4EqPh3Method, 154
- SaPcieRpL1Substates, 154
- SaPcieRpPcieSpeed, 154
- SaPcieRpPhysicalSlotNumber, 154
- SaPcieRpPtmEnabled, 154
- SaPcieRpVcEnabled, 155
- SataEnable, 155
- SataLedEnable, 155
- SataMode, 155
- SataP0TDispFinit, 155
- SataP1TDispFinit, 155
- SataPortsDevSlp, 156
- SataPortsDmVal, 156
- SataPortsEnable, 156
- SataPwrOptEnable, 156
- SataRstHddUnlock, 156
- SataRstInterrupt, 157
- SataRstLrrt, 157
- SataRstLrrtOnly, 157
- SataRstLedLocate, 157
- SataRstOromUiBanner, 157
- SataRstPcieDeviceResetDelay, 158
- SataRstRaid0, 158
- SataRstRaid1, 158
- SataRstRaid10, 158
- SataRstRaid5, 158
- SataRstRaidDeviceId, 158
- SataRstSmartStorage, 159
- SataSalpSupport, 159
- SataThermalSuggestedSetting, 159
- ScIirqSelect, 159
- ScsEmmcEnabled, 159
- ScsEmmcHs400Enabled, 160

- ScsSdCardEnabled, 160
- SendEcCmd, 160
- SendVrMbxCmd, 160
- SerialloDebugUartNumber, 160
- SerialloI2cMode, 161
- SerialloSpi0CsEnable, 161
- SerialloSpi0CsPolarity, 161
- SerialloSpi1CsEnable, 161
- SerialloSpi1CsPolarity, 161
- SerialloSpi2CsEnable, 162
- SerialloSpi2CsPolarity, 162
- SerialloSpi3CsEnable, 162
- SerialloSpi3CsPolarity, 162
- SerialloSpi4CsEnable, 162
- SerialloSpi4CsPolarity, 162
- SerialloSpi5CsEnable, 163
- SerialloSpi5CsPolarity, 163
- SerialloSpi6CsEnable, 163
- SerialloSpi6CsPolarity, 163
- SerialloSpiDefaultCsOutput, 163
- SerialloSpiMode, 164
- SerialloUartCtsPinMuxPolicy, 164
- SerialloUartDataBits, 164
- SerialloUartDmaEnable, 164
- SerialloUartMode, 164
- SerialloUartParity, 165
- SerialloUartPowerGating, 165
- SerialloUartRtsPinMuxPolicy, 165
- SerialloUartRxPinMuxPolicy, 165
- SerialloUartStopBits, 165
- SerialloUartTxPinMuxPolicy, 165
- ShowSpiController, 166
- SiCsmFlag, 166
- SkipMplnit, 166
- SlowSlewRateForFivr, 166
- SlowSlewRateForGt, 166
- SlowSlewRateForIa, 167
- SlowSlewRateForSa, 167
- SlpS0DisQForDebug, 167
- SlpS0Override, 167
- TTSuggestedSetting, 169
- TcolrqSelect, 167
- TcssAuxOri, 168
- TcssHslOri, 168
- TdcPowerLimit, 168
- TdcTimeWindow, 168
- ThcPort0InterruptPinMuxing, 168
- ThcPort1InterruptPinMuxing, 169
- TurboMode, 169
- TxtEnable, 169
- UfsEnable, 169
- Usb2PhyPehalfbit, 169
- Usb2PhyPetxiset, 170
- Usb2PhyPredeemp, 170
- Usb2PhyTxiset, 170
- Usb3HsioTxDeEmph, 170
- Usb3HsioTxDeEmphEnable, 170
- Usb3HsioTxDownscaleAmp, 171
- Usb3HsioTxDownscaleAmpEnable, 171
- UsbPdoProgramming, 171
- UsbTcPortEn, 171
- VmdEnable, 171
- VmdPortA, 172
- VmdPortB, 172
- VmdPortC, 172
- VmdPortD, 172
- VrVoltageLimit, 172
- WatchDog, 173
- WatchDogTimerBios, 173
- WatchDogTimerOs, 173
- XdciEnable, 173
- FSP_S_TEST_CONFIG, 173
 - AplIdleManner, 182
 - AutoThermalReporting, 182
 - C1StateAutoDemotion, 183
 - C1StateUnDemotion, 183
 - C1e, 182
 - CStatePreWake, 183
 - ConfigTdpBios, 183
 - CoreCStateLimit, 183
 - CstCfgCtrlMwaitRedirection, 184
 - Custom1ConfigTdpControl, 184
 - Custom1PowerLimit1, 184
 - Custom1PowerLimit1Time, 184
 - Custom1PowerLimit2, 184
 - Custom1TurboActivationRatio, 185
 - Custom2ConfigTdpControl, 185
 - Custom2PowerLimit1, 185
 - Custom2PowerLimit1Time, 185
 - Custom2PowerLimit2, 185
 - Custom2TurboActivationRatio, 186
 - Custom3ConfigTdpControl, 186
 - Custom3PowerLimit1, 186
 - Custom3PowerLimit1Time, 186
 - Custom3PowerLimit2, 186
 - Custom3TurboActivationRatio, 186
 - Cx, 187
 - DebugInterfaceLockEnable, 187
 - DisableProcHotOut, 187
 - DisableVrThermalAlert, 187
 - Eist, 187
 - EnableEpbPeciOverride, 188
 - EnableFastMsrHwpReq, 188
 - EnableHwpAutoEppGrouping, 188
 - EnableHwpAutoPerCorePstate, 188
 - EnableIltbm, 188
 - EnablePerCorePState, 189
 - EndOfPostMessage, 189
 - EnergyEfficientPState, 189
 - EnergyEfficientTurbo, 189
 - HdcControl, 189
 - Hwp, 190
 - HwpInterruptControl, 190
 - MachineCheckEnable, 190
 - MaxRingRatioLimit, 190
 - MctpBroadcastCycle, 190

- MinRingRatioLimit, [190](#)
- MlcStreamerPrefetcher, [191](#)
- MonitorMwaitEnable, [191](#)
- NumberOfEntries, [191](#)
- OneCoreRatioLimit, [191](#)
- PchHdaResetWaitTimer, [191](#)
- PchLockDownBiosInterface, [192](#)
- PchLockDownGlobalSmi, [192](#)
- PchPmDisableEnergyReport, [192](#)
- PchSbAccessUnlock, [192](#)
- PchUnlockGpioPads, [192](#)
- PchXhciOclLock, [193](#)
- PcieEnablePort8xhDecode, [193](#)
- PcieRpDptp, [193](#)
- PcieRpSlotPowerLimitScale, [193](#)
- PcieRpSlotPowerLimitValue, [193](#)
- PcieRpUptp, [194](#)
- PkgCStateDemotion, [194](#)
- PkgCStateLimit, [194](#)
- PkgCStateUnDemotion, [194](#)
- PmcLpmS0ixSubStateEnableMask, [194](#)
- PmgCstCfgCtrlLock, [195](#)
- PowerLimit1, [195](#)
- PowerLimit1Time, [195](#)
- PowerLimit2, [195](#)
- PowerLimit2Power, [195](#)
- PowerLimit3, [195](#)
- PowerLimit4, [196](#)
- ProcHotResponse, [197](#)
- ProcessorTraceEnable, [196](#)
- ProcessorTraceMemBase, [196](#)
- ProcessorTraceMemLength, [196](#)
- ProcessorTraceOutputScheme, [196](#)
- PsysPmax, [197](#)
- PsysPowerLimit1, [197](#)
- PsysPowerLimit1Power, [197](#)
- PsysPowerLimit2, [197](#)
- PsysPowerLimit2Power, [198](#)
- RaceToHalt, [198](#)
- SaPcieRpGen3Dptp, [198](#)
- SaPcieRpGen3Uptp, [198](#)
- SaPcieRpGen4Dptp, [198](#)
- SaPcieRpGen4Uptp, [199](#)
- SataTestMode, [199](#)
- SkipPostBootSai, [199](#)
- StateRatio, [199](#)
- StateRatioMax16, [199](#)
- TStates, [201](#)
- TccActivationOffset, [199](#)
- TccOffsetClamp, [200](#)
- TccOffsetLock, [200](#)
- TccOffsetTimeWindowForRatl, [200](#)
- ThreeStrikeCounterDisable, [200](#)
- TimedMwait, [200](#)
- FSP_T_CONFIG, [201](#)
 - PcdSerialloUartAutoFlow, [202](#)
 - PcdSerialloUartCtsPinMux, [202](#)
 - PcdSerialloUartDataBits, [202](#)
 - PcdSerialloUartDebugEnable, [202](#)
 - PcdSerialloUartNumber, [203](#)
 - PcdSerialloUartParity, [203](#)
 - PcdSerialloUartRtsPinMux, [203](#)
 - PcdSerialloUartStopBits, [203](#)
- FSP_T_TEST_CONFIG, [204](#)
- FSPM_UPD, [204](#)
- FSPS_UPD, [205](#)
- FSPT_CORE_UPD, [206](#)
- FSPT_UPD, [206](#)
- FastPkgCRampDisableFivr
 - FSP_S_CONFIG, [117](#)
- FastPkgCRampDisableGt
 - FSP_S_CONFIG, [117](#)
- FastPkgCRampDisableIa
 - FSP_S_CONFIG, [118](#)
- FastPkgCRampDisableSa
 - FSP_S_CONFIG, [118](#)
- FirmwareVersionInfoHob.h, [215](#)
- FivrEfficiency
 - FSP_M_CONFIG, [61](#)
- FivrFaults
 - FSP_M_CONFIG, [62](#)
- FivrRfiFrequency
 - FSP_S_CONFIG, [118](#)
- FivrSpreadSpectrum
 - FSP_S_CONFIG, [118](#)
- ForcMebxSyncUp
 - FSP_S_CONFIG, [118](#)
- ForceOltmOrRefresh2x
 - FSP_M_CONFIG, [62](#)
- FreqSaGvLow
 - FSP_M_CONFIG, [62](#)
- FreqSaGvMid
 - FSP_M_CONFIG, [62](#)
- FspFixedPcds.h, [216](#)
- FspInfoHob.h, [216](#)
- FspUpd.h, [222](#)
- FspmUpd.h, [217](#)
- FspsUpd.h, [219](#)
 - SI_PCH_INT_PIN, [220](#)
- FsptUpd.h, [221](#)
- FwProgress
 - FSP_S_CONFIG, [119](#)
- GPIO_CONFIG, [207](#)
 - Direction, [208](#)
 - ElectricalConfig, [208](#)
 - HostSoftPadOwn, [209](#)
 - InterruptConfig, [209](#)
 - LockConfig, [209](#)
 - OutputState, [209](#)
 - PadMode, [209](#)
 - PowerConfig, [210](#)
- GPIO_DIRECTION
 - GpioConfig.h, [225](#)
- GPIO_ELECTRICAL_CONFIG
 - GpioConfig.h, [225](#)
- GPIO_HARDWARE_DEFAULT

- GpioConfig.h, [226](#)
- GPIO_HOSTSW_OWN
 - GpioConfig.h, [226](#)
- GPIO_INT_CONFIG
 - GpioConfig.h, [227](#)
- GPIO_LOCK_CONFIG
 - GpioConfig.h, [227](#)
- GPIO_OTHER_CONFIG
 - GpioConfig.h, [228](#)
- GPIO_OUTPUT_STATE
 - GpioConfig.h, [228](#)
- GPIO_PAD_MODE
 - GpioConfig.h, [228](#)
- GPIO_RESET_CONFIG
 - GpioConfig.h, [228](#)
- GmAdr
 - FSP_M_CONFIG, [62](#)
- GpioConfig.h, [223](#)
 - GPIO_DIRECTION, [225](#)
 - GPIO_ELECTRICAL_CONFIG, [225](#)
 - GPIO_HARDWARE_DEFAULT, [226](#)
 - GPIO_HOSTSW_OWN, [226](#)
 - GPIO_INT_CONFIG, [227](#)
 - GPIO_LOCK_CONFIG, [227](#)
 - GPIO_OTHER_CONFIG, [228](#)
 - GPIO_OUTPUT_STATE, [228](#)
 - GPIO_PAD_MODE, [228](#)
 - GPIO_RESET_CONFIG, [228](#)
- GpioIrqRoute
 - FSP_S_CONFIG, [119](#)
- GpioSampleDef.h, [230](#)
- GtPllVoltageOffset
 - FSP_M_CONFIG, [63](#)
- GtPsmiSupport
 - FSP_M_CONFIG, [63](#)
- GttMmAdr
 - FSP_M_CONFIG, [63](#)
- HOB_USAGE_DATA_HOB, [210](#)
- HdcControl
 - FSP_S_TEST_CONFIG, [189](#)
- Heci3Enabled
 - FSP_S_CONFIG, [119](#)
- HeciCommunication2
 - FSP_M_TEST_CONFIG, [86](#)
- HobBufferSize
 - FSP_M_CONFIG, [63](#)
- HobUsageDataHob.h, [231](#)
- HostSoftPadOwn
 - GPIO_CONFIG, [209](#)
- HotThresholdCh0Dimm0
 - FSP_M_CONFIG, [63](#)
- HotThresholdCh0Dimm1
 - FSP_M_CONFIG, [64](#)
- HotThresholdCh1Dimm0
 - FSP_M_CONFIG, [64](#)
- HotThresholdCh1Dimm1
 - FSP_M_CONFIG, [64](#)
- Hwp
 - FSP_S_TEST_CONFIG, [190](#)
- HwplInterruptControl
 - FSP_S_TEST_CONFIG, [190](#)
- ITbtConnectTopologyTimeoutInMs
 - FSP_S_CONFIG, [120](#)
- ITbtForcePowerOnTimeoutInMs
 - FSP_S_CONFIG, [120](#)
- IccMax
 - FSP_S_CONFIG, [119](#)
- Idd3n
 - FSP_M_CONFIG, [64](#)
- Idd3p
 - FSP_M_CONFIG, [64](#)
- IgdDvmt50PreAlloc
 - FSP_M_CONFIG, [64](#)
- ImguClkOutEn
 - FSP_M_CONFIG, [65](#)
- ImonOffset
 - FSP_S_CONFIG, [119](#)
- ImonSlope
 - FSP_S_CONFIG, [120](#)
- ImrRpSelection
 - FSP_M_CONFIG, [65](#)
- InitPcieAspmAfterOprom
 - FSP_M_CONFIG, [65](#)
- InternalGfx
 - FSP_M_CONFIG, [65](#)
- InterruptConfig
 - GPIO_CONFIG, [209](#)
- IomTypeCPortPadCfg
 - FSP_S_CONFIG, [120](#)
- IsvtIoPort
 - FSP_M_CONFIG, [65](#)
- JtagC10PowerGateDisable
 - FSP_M_CONFIG, [66](#)
- KtDeviceEnable
 - FSP_M_TEST_CONFIG, [86](#)
- LockConfig
 - GPIO_CONFIG, [209](#)
- LockPTMregs
 - FSP_M_TEST_CONFIG, [87](#)
- MEMORY_PLATFORM_DATA, [210](#)
- MRC_BOOT_MODE
 - MemInfoHob.h, [233](#)
- MachineCheckEnable
 - FSP_S_TEST_CONFIG, [190](#)
- ManageabilityMode
 - FSP_S_CONFIG, [120](#)
- MaxRingRatioLimit
 - FSP_S_TEST_CONFIG, [190](#)
- McPllVoltageOffset
 - FSP_M_CONFIG, [66](#)
- MctpBroadcastCycle
 - FSP_S_TEST_CONFIG, [190](#)

- MeUnconfigOnRtcClear
 - FSP_S_CONFIG, 121
- MemInfoHob.h, 231
 - MRC_BOOT_MODE, 233
- MinRingRatioLimit
 - FSP_S_TEST_CONFIG, 190
- MinVoltageC8
 - FSP_S_CONFIG, 121
- MinVoltageRuntime
 - FSP_S_CONFIG, 121
- MlcStreamerPrefetcher
 - FSP_S_TEST_CONFIG, 191
- MmioSize
 - FSP_M_CONFIG, 66
- MonitorMwaitEnable
 - FSP_S_TEST_CONFIG, 191
- NumOfDevIntConfig
 - FSP_S_CONFIG, 121
- NumberOfEntries
 - FSP_S_TEST_CONFIG, 191
- OcLock
 - FSP_M_CONFIG, 66
- OneCoreRatioLimit
 - FSP_S_TEST_CONFIG, 191
- OutputState
 - GPIO_CONFIG, 209
- PadMode
 - GPIO_CONFIG, 209
- PanelPowerEnable
 - FSP_M_TEST_CONFIG, 87
- PcdDebugInterfaceFlags
 - FSP_M_CONFIG, 66
- PcdIlsaSerialUartBase
 - FSP_M_CONFIG, 67
- PcdSerialDebugBaudRate
 - FSP_M_CONFIG, 67
- PcdSerialDebugLevel
 - FSP_M_CONFIG, 67
- PcdSerialIoUartAutoFlow
 - FSP_T_CONFIG, 202
- PcdSerialIoUartCtsPinMux
 - FSP_T_CONFIG, 202
- PcdSerialIoUartDataBits
 - FSP_T_CONFIG, 202
- PcdSerialIoUartDebugEnabled
 - FSP_T_CONFIG, 202
- PcdSerialIoUartNumber
 - FSP_M_CONFIG, 67
 - FSP_T_CONFIG, 203
- PcdSerialIoUartParity
 - FSP_T_CONFIG, 203
- PcdSerialIoUartRtsPinMux
 - FSP_T_CONFIG, 203
- PcdSerialIoUartStopBits
 - FSP_T_CONFIG, 203
- PchCrid
 - FSP_S_CONFIG, 121
- PchDmiAspmCtrl
 - FSP_S_CONFIG, 121
- PchDmiTsawEn
 - FSP_S_CONFIG, 122
- PchEnableComplianceMode
 - FSP_S_CONFIG, 122
- PchEnableDbcObs
 - FSP_S_CONFIG, 122
- PchEspHostC10ReportEnable
 - FSP_S_CONFIG, 122
- PchFivrDynPm
 - FSP_S_CONFIG, 122
- PchFivrExtVnnRailSxEnabledStates
 - FSP_S_CONFIG, 123
- PchFivrExtVnnRailSxIccMax
 - FSP_S_CONFIG, 123
- PchFivrExtVnnRailSxVoltage
 - FSP_S_CONFIG, 123
- PchFivrVccinAuxLowToHighCurModeVolTranTime
 - FSP_S_CONFIG, 123
- PchFivrVccinAuxOffToHighCurModeVolTranTime
 - FSP_S_CONFIG, 123
- PchFivrVccinAuxRetToHighCurModeVolTranTime
 - FSP_S_CONFIG, 124
- PchFivrVccinAuxRetToLowCurModeVolTranTime
 - FSP_S_CONFIG, 124
- PchHdaAudioLinkDmic0ClkAPinMux
 - FSP_S_CONFIG, 124
- PchHdaAudioLinkDmic0ClkBPinMux
 - FSP_S_CONFIG, 124
- PchHdaAudioLinkDmic0DataPinMux
 - FSP_S_CONFIG, 124
- PchHdaAudioLinkDmic0Enable
 - FSP_S_CONFIG, 125
- PchHdaAudioLinkDmic1ClkAPinMux
 - FSP_S_CONFIG, 125
- PchHdaAudioLinkDmic1ClkBPinMux
 - FSP_S_CONFIG, 125
- PchHdaAudioLinkDmic1DataPinMux
 - FSP_S_CONFIG, 125
- PchHdaAudioLinkDmic1Enable
 - FSP_S_CONFIG, 125
- PchHdaAudioLinkHdaEnable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSndw1Enable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSndw2Enable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSndw3Enable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSndw4Enable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSsp0Enable
 - FSP_S_CONFIG, 126
- PchHdaAudioLinkSsp1Enable
 - FSP_S_CONFIG, 127
- PchHdaAudioLinkSsp2Enable

- FSP_S_CONFIG, 127
- PchHdaAudioLinkSsp3Enable
 - FSP_S_CONFIG, 127
- PchHdaAudioLinkSsp4Enable
 - FSP_S_CONFIG, 127
- PchHdaAudioLinkSsp5Enable
 - FSP_S_CONFIG, 127
- PchHdaDspEnable
 - FSP_S_CONFIG, 128
- PchHdaDspUaaCompliance
 - FSP_S_CONFIG, 128
- PchHdaDispCodecDisconnect
 - FSP_S_CONFIG, 128
- PchHdaDispLinkFrequency
 - FSP_S_CONFIG, 128
- PchHdaLinkFrequency
 - FSP_S_CONFIG, 128
- PchHdaPme
 - FSP_S_CONFIG, 129
- PchHdaResetWaitTimer
 - FSP_S_TEST_CONFIG, 191
- PchHdaVcType
 - FSP_S_CONFIG, 129
- PchHotEnable
 - FSP_S_CONFIG, 129
- PchIoApicEntry24_119
 - FSP_S_CONFIG, 129
- PchIoApicId
 - FSP_S_CONFIG, 129
- PchIshGpEnable
 - FSP_S_CONFIG, 129
- PchIshI2cEnable
 - FSP_S_CONFIG, 130
- PchIshPdtUnlock
 - FSP_S_CONFIG, 130
- PchIshSpiCs0Enable
 - FSP_S_CONFIG, 130
- PchIshSpiEnable
 - FSP_S_CONFIG, 130
- PchIshUartEnable
 - FSP_S_CONFIG, 130
- PchLanEnable
 - FSP_S_CONFIG, 131
- PchLanLtrEnable
 - FSP_S_CONFIG, 131
- PchLockDownBiosInterface
 - FSP_S_TEST_CONFIG, 192
- PchLockDownBiosLock
 - FSP_S_CONFIG, 131
- PchLockDownGlobalSmi
 - FSP_S_TEST_CONFIG, 192
- PchLpcEnhancePort8xhDecoding
 - FSP_M_CONFIG, 67
- PchMemoryThrottlingEnable
 - FSP_S_CONFIG, 131
- PchNumRsvdSmbusAddresses
 - FSP_M_CONFIG, 68
- PchOseAdcEnable
 - FSP_S_CONFIG, 131
- PchOseCanEnable
 - FSP_S_CONFIG, 131
- PchOseHsuartEnable
 - FSP_S_CONFIG, 132
- PchOseI2cEnable
 - FSP_S_CONFIG, 132
- PchOseI2sEnable
 - FSP_S_CONFIG, 132
- PchOsePwmEnable
 - FSP_S_CONFIG, 132
- PchOseQepEnable
 - FSP_S_CONFIG, 132
- PchOseSpiCs0Enable
 - FSP_S_CONFIG, 133
- PchOseSpiEnable
 - FSP_S_CONFIG, 133
- PchOseTimedGpioEnable
 - FSP_S_CONFIG, 133
- PchOseTimedGpioPinAllocation
 - FSP_S_CONFIG, 133
- PchOseTimedGpioPinEnable
 - FSP_S_CONFIG, 133
- PchOseUartEnable
 - FSP_S_CONFIG, 134
- PchPcieDeviceOverrideTablePtr
 - FSP_S_CONFIG, 134
- PchPmDeepSxPol
 - FSP_S_CONFIG, 134
- PchPmDisableDsxAcPresentPulldown
 - FSP_S_CONFIG, 134
- PchPmDisableEnergyReport
 - FSP_S_TEST_CONFIG, 192
- PchPmDisableNativePowerButton
 - FSP_S_CONFIG, 134
- PchPmLanWakeFromDeepSx
 - FSP_S_CONFIG, 134
- PchPmMeWakeSts
 - FSP_S_CONFIG, 135
- PchPmPciePIISsc
 - FSP_S_CONFIG, 135
- PchPmPcieWakeFromDeepSx
 - FSP_S_CONFIG, 135
- PchPmPmeB0S5Dis
 - FSP_S_CONFIG, 135
- PchPmPwrBtnOverridePeriod
 - FSP_S_CONFIG, 135
- PchPmPwrCycDur
 - FSP_S_CONFIG, 136
- PchPmSlpAMinAssert
 - FSP_S_CONFIG, 136
- PchPmSlpLanLowDc
 - FSP_S_CONFIG, 136
- PchPmSlpS0Enable
 - FSP_S_CONFIG, 136
- PchPmSlpS0Vm070VSupport
 - FSP_S_CONFIG, 136
- PchPmSlpS0Vm075VSupport

- FSP_S_CONFIG, 136
- PchPmSlpS0VmRuntimeControl
 - FSP_S_CONFIG, 137
- PchPmSlpS3MinAssert
 - FSP_S_CONFIG, 137
- PchPmSlpS4MinAssert
 - FSP_S_CONFIG, 137
- PchPmSlpStrchSusUp
 - FSP_S_CONFIG, 137
- PchPmSlpSusMinAssert
 - FSP_S_CONFIG, 137
- PchPmVrAlert
 - FSP_S_CONFIG, 138
- PchPmWoWlanDeepSxEnable
 - FSP_S_CONFIG, 138
- PchPmWoWlanEnable
 - FSP_S_CONFIG, 138
- PchPmWolEnableOverride
 - FSP_S_CONFIG, 138
- PchPmWolOvrWkSts
 - FSP_S_CONFIG, 138
- PchPort80Route
 - FSP_M_CONFIG, 68
- PchPwrOptEnable
 - FSP_S_CONFIG, 139
- PchS0ixAutoDemotion
 - FSP_S_CONFIG, 139
- PchSbAccessUnlock
 - FSP_S_TEST_CONFIG, 192
- PchSerialIoI2cPadsTermination
 - FSP_S_CONFIG, 139
- PchSerialIoI2cSclPinMux
 - FSP_S_CONFIG, 139
- PchSerialIoI2cSdaPinMux
 - FSP_S_CONFIG, 139
- PchSmbAlertEnable
 - FSP_M_CONFIG, 68
- PchStartFramePulse
 - FSP_S_CONFIG, 140
- PchTTEnable
 - FSP_S_CONFIG, 140
- PchTTLock
 - FSP_S_CONFIG, 140
- PchTTState13Enable
 - FSP_S_CONFIG, 140
- PchTraceHubMemReg0Size
 - FSP_M_CONFIG, 68
- PchTraceHubMemReg1Size
 - FSP_M_CONFIG, 68
- PchTraceHubMode
 - FSP_M_CONFIG, 69
- PchTsnEnable
 - FSP_S_CONFIG, 140
- PchUnlockGpioPads
 - FSP_S_TEST_CONFIG, 192
- PchXhciOcLock
 - FSP_S_TEST_CONFIG, 193
- PcieComplianceTestMode
 - FSP_S_CONFIG, 140
- PcieDisableRootPortClockGating
 - FSP_S_CONFIG, 141
- PcieEnablePeerMemoryWrite
 - FSP_S_CONFIG, 141
- PcieEnablePort8xhDecode
 - FSP_S_TEST_CONFIG, 193
- PcieEqPh3LaneParamCm
 - FSP_S_CONFIG, 141
- PcieEqPh3LaneParamCp
 - FSP_S_CONFIG, 141
- PcieImrSize
 - FSP_M_CONFIG, 69
- PcieMultipleSegmentEnabled
 - FSP_M_CONFIG, 69
- PcieRpAspm
 - FSP_S_CONFIG, 141
- PcieRpCompletionTimeout
 - FSP_S_CONFIG, 142
- PcieRpDpcExtensionsMask
 - FSP_S_CONFIG, 142
- PcieRpDpcMask
 - FSP_S_CONFIG, 142
- PcieRpDptp
 - FSP_S_TEST_CONFIG, 193
- PcieRpEnableMask
 - FSP_M_CONFIG, 69
- PcieRpFunctionSwap
 - FSP_S_CONFIG, 142
- PcieRpGen3EqPh3Method
 - FSP_S_CONFIG, 142
- PcieRpImrEnabled
 - FSP_S_CONFIG, 143
- PcieRpL1Substates
 - FSP_S_CONFIG, 143
- PcieRpPcieSpeed
 - FSP_S_CONFIG, 143
- PcieRpPhysicalSlotNumber
 - FSP_S_CONFIG, 143
- PcieRpPtmMask
 - FSP_S_CONFIG, 143
- PcieRpSlotPowerLimitScale
 - FSP_S_TEST_CONFIG, 193
- PcieRpSlotPowerLimitValue
 - FSP_S_TEST_CONFIG, 193
- PcieRpUptp
 - FSP_S_TEST_CONFIG, 194
- PcieSwEqCoeffListCm
 - FSP_S_CONFIG, 144
- PcieSwEqCoeffListCp
 - FSP_S_CONFIG, 144
- PkgCStateDemotion
 - FSP_S_TEST_CONFIG, 194
- PkgCStateLimit
 - FSP_S_TEST_CONFIG, 194
- PkgCStateUnDemotion
 - FSP_S_TEST_CONFIG, 194
- PlatformDebugConsent

- FSP_M_CONFIG, 69
- PmcCpuC10GatePinEnable
 - FSP_S_CONFIG, 144
- PmcDbgMsgEn
 - FSP_S_CONFIG, 144
- PmcGrTscEnable
 - FSP_S_CONFIG, 144
- PmcLpmS0ixSubStateEnableMask
 - FSP_S_TEST_CONFIG, 194
- PmcModPhySusPgEnable
 - FSP_S_CONFIG, 144
- PmcPowerButtonDebounce
 - FSP_S_CONFIG, 145
- PmcV1p05IsExtFetControlEn
 - FSP_S_CONFIG, 145
- PmcV1p05PhyExtFetControlEn
 - FSP_S_CONFIG, 145
- PmgCstCfgCtrlLock
 - FSP_S_TEST_CONFIG, 195
- PortUsb20Enable
 - FSP_S_CONFIG, 145
- PortUsb30Enable
 - FSP_S_CONFIG, 145
- PowerConfig
 - GPIO_CONFIG, 210
- PowerLimit1
 - FSP_S_TEST_CONFIG, 195
- PowerLimit1Time
 - FSP_S_TEST_CONFIG, 195
- PowerLimit2
 - FSP_S_TEST_CONFIG, 195
- PowerLimit2Power
 - FSP_S_TEST_CONFIG, 195
- PowerLimit3
 - FSP_S_TEST_CONFIG, 195
- PowerLimit4
 - FSP_S_TEST_CONFIG, 196
- PpinSupport
 - FSP_S_CONFIG, 146
- PmrrSize
 - FSP_M_CONFIG, 70
- ProbelessTrace
 - FSP_M_CONFIG, 70
- ProcHotResponse
 - FSP_S_TEST_CONFIG, 197
- ProcessorTraceEnable
 - FSP_S_TEST_CONFIG, 196
- ProcessorTraceMemBase
 - FSP_S_TEST_CONFIG, 196
- ProcessorTraceMemLength
 - FSP_S_TEST_CONFIG, 196
- ProcessorTraceOutputScheme
 - FSP_S_TEST_CONFIG, 196
- PsOnEnable
 - FSP_S_CONFIG, 147
- Psi1Threshold
 - FSP_S_CONFIG, 146
- Psi2Threshold
 - FSP_S_CONFIG, 146
- Psi3Enable
 - FSP_S_CONFIG, 146
- Psi3Threshold
 - FSP_S_CONFIG, 146
- PsysOffset
 - FSP_S_CONFIG, 147
- PsysPmax
 - FSP_S_TEST_CONFIG, 197
- PsysPowerLimit1
 - FSP_S_TEST_CONFIG, 197
- PsysPowerLimit1Power
 - FSP_S_TEST_CONFIG, 197
- PsysPowerLimit2
 - FSP_S_TEST_CONFIG, 197
- PsysPowerLimit2Power
 - FSP_S_TEST_CONFIG, 198
- PsysSlope
 - FSP_S_CONFIG, 147
- PwdnIdleCounter
 - FSP_M_CONFIG, 70
- PxRcConfig
 - FSP_S_CONFIG, 147
- RMTLoopCount
 - FSP_M_CONFIG, 73
- RMT
 - FSP_M_CONFIG, 72
- RaceToHalt
 - FSP_S_TEST_CONFIG, 198
- RankInterleave
 - FSP_M_CONFIG, 70
- Ratio
 - FSP_M_CONFIG, 70
- RealtimeMemoryTiming
 - FSP_M_CONFIG, 71
- RefClk
 - FSP_M_CONFIG, 71
- RemoteAssistance
 - FSP_S_CONFIG, 147
- RhSolution
 - FSP_M_CONFIG, 71
- RingDownBin
 - FSP_M_CONFIG, 71
- RingMaxOcRatio
 - FSP_M_CONFIG, 71
- RingPIIVoltageOffset
 - FSP_M_CONFIG, 71
- RingVoltageAdaptive
 - FSP_M_CONFIG, 72
- RingVoltageMode
 - FSP_M_CONFIG, 72
- RingVoltageOffset
 - FSP_M_CONFIG, 72
- RingVoltageOverride
 - FSP_M_CONFIG, 72
- RmtPerTask
 - FSP_M_CONFIG, 73
- RtcBiosInterfaceLock

- FSP_S_CONFIG, 148
- RtcMemoryLock
 - FSP_S_CONFIG, 148
- SI_PCH_DEVICE_INTERRUPT_CONFIG, 211
- SI_PCH_INT_PIN
 - FspUpd.h, 220
- SMBIOS_CACHE_INFO, 211
- SMBIOS_PROCESSOR_INFO, 212
- SMBIOS_STRUCTURE, 213
- SaGv
 - FSP_M_CONFIG, 73
- SaPcieComplianceTestMode
 - FSP_S_CONFIG, 148
- SaPcieDeviceOverrideTablePtr
 - FSP_S_CONFIG, 148
- SaPcieDisableRootPortClockGating
 - FSP_S_CONFIG, 148
- SaPcieDisableRootPortPowerGating
 - FSP_S_CONFIG, 149
- SaPcieEnablePeerMemoryWrite
 - FSP_S_CONFIG, 149
- SaPcieEqPh3LaneParamCm
 - FSP_S_CONFIG, 149
- SaPcieEqPh3LaneParamCp
 - FSP_S_CONFIG, 149
- SaPcieGen3EndPointHint
 - FSP_S_CONFIG, 149
- SaPcieGen3EndPointPreset
 - FSP_S_CONFIG, 150
- SaPcieGen3ProgramStaticEq
 - FSP_S_CONFIG, 150
- SaPcieGen3RootPortPreset
 - FSP_S_CONFIG, 150
- SaPcieGen4EndPointHint
 - FSP_S_CONFIG, 150
- SaPcieGen4EndPointPreset
 - FSP_S_CONFIG, 150
- SaPcieGen4ProgramStaticEq
 - FSP_S_CONFIG, 151
- SaPcieGen4RootPortPreset
 - FSP_S_CONFIG, 151
- SaPcieHwEqGen3CoeffListCm
 - FSP_S_CONFIG, 151
- SaPcieHwEqGen3CoeffListCp
 - FSP_S_CONFIG, 151
- SaPcieHwEqGen4CoeffListCm
 - FSP_S_CONFIG, 151
- SaPcieHwEqGen4CoeffListCp
 - FSP_S_CONFIG, 152
- SaPcieRpAspm
 - FSP_S_CONFIG, 152
- SaPcieRpDpcEnabled
 - FSP_S_CONFIG, 152
- SaPcieRpDpcExtensionsEnabled
 - FSP_S_CONFIG, 152
- SaPcieRpEnableMask
 - FSP_M_CONFIG, 73
- SaPcieRpFunctionSwap
 - FSP_S_CONFIG, 152
- SaPcieRpGen3Dptp
 - FSP_S_TEST_CONFIG, 198
- SaPcieRpGen3EqPh23Enable
 - FSP_S_CONFIG, 153
- SaPcieRpGen3EqPh3Enable
 - FSP_S_CONFIG, 153
- SaPcieRpGen3EqPh3Method
 - FSP_S_CONFIG, 153
- SaPcieRpGen3Uptp
 - FSP_S_TEST_CONFIG, 198
- SaPcieRpGen4Dptp
 - FSP_S_TEST_CONFIG, 198
- SaPcieRpGen4EqPh23Enable
 - FSP_S_CONFIG, 153
- SaPcieRpGen4EqPh3Enable
 - FSP_S_CONFIG, 153
- SaPcieRpGen4EqPh3Method
 - FSP_S_CONFIG, 154
- SaPcieRpGen4Uptp
 - FSP_S_TEST_CONFIG, 199
- SaPcieRpL1Substates
 - FSP_S_CONFIG, 154
- SaPcieRpLinkDownGpios
 - FSP_M_CONFIG, 74
- SaPcieRpPcieSpeed
 - FSP_S_CONFIG, 154
- SaPcieRpPhysicalSlotNumber
 - FSP_S_CONFIG, 154
- SaPcieRpPtmEnabled
 - FSP_S_CONFIG, 154
- SaPcieRpVcEnabled
 - FSP_S_CONFIG, 155
- SaPllVoltageOffset
 - FSP_M_CONFIG, 74
- SafeMode
 - FSP_M_CONFIG, 73
- SataEnable
 - FSP_S_CONFIG, 155
- SataLedEnable
 - FSP_S_CONFIG, 155
- SataMode
 - FSP_S_CONFIG, 155
- SataP0TDispFinit
 - FSP_S_CONFIG, 155
- SataP1TDispFinit
 - FSP_S_CONFIG, 155
- SataPortsDevSlp
 - FSP_S_CONFIG, 156
- SataPortsDmVal
 - FSP_S_CONFIG, 156
- SataPortsEnable
 - FSP_S_CONFIG, 156
- SataPwrOptEnable
 - FSP_S_CONFIG, 156
- SataRstHddUnlock
 - FSP_S_CONFIG, 156
- SataRstInterrupt

- FSP_S_CONFIG, 157
- SataRstIrrt
 - FSP_S_CONFIG, 157
- SataRstIrrtOnly
 - FSP_S_CONFIG, 157
- SataRstLedLocate
 - FSP_S_CONFIG, 157
- SataRstOromUiBanner
 - FSP_S_CONFIG, 157
- SataRstPcieDeviceResetDelay
 - FSP_S_CONFIG, 158
- SataRstRaid0
 - FSP_S_CONFIG, 158
- SataRstRaid1
 - FSP_S_CONFIG, 158
- SataRstRaid10
 - FSP_S_CONFIG, 158
- SataRstRaid5
 - FSP_S_CONFIG, 158
- SataRstRaidDeviceId
 - FSP_S_CONFIG, 158
- SataRstSmartStorage
 - FSP_S_CONFIG, 159
- SataSalpSupport
 - FSP_S_CONFIG, 159
- SataTestMode
 - FSP_S_TEST_CONFIG, 199
- SataThermalSuggestedSetting
 - FSP_S_CONFIG, 159
- ScanExtGfxForLegacyOpRom
 - FSP_M_TEST_CONFIG, 87
- ScilrqSelect
 - FSP_S_CONFIG, 159
- ScramblerSupport
 - FSP_M_CONFIG, 74
- ScsEmmcEnabled
 - FSP_S_CONFIG, 159
- ScsEmmcHs400Enabled
 - FSP_S_CONFIG, 160
- ScsSdCardEnabled
 - FSP_S_CONFIG, 160
- SendEcCmd
 - FSP_S_CONFIG, 160
- SendVrMbxCmd
 - FSP_S_CONFIG, 160
- SerialloDebugUartNumber
 - FSP_S_CONFIG, 160
- SerialloI2cMode
 - FSP_S_CONFIG, 161
- SerialloSpi0CsEnable
 - FSP_S_CONFIG, 161
- SerialloSpi0CsPolarity
 - FSP_S_CONFIG, 161
- SerialloSpi1CsEnable
 - FSP_S_CONFIG, 161
- SerialloSpi1CsPolarity
 - FSP_S_CONFIG, 161
- SerialloSpi2CsEnable
 - FSP_S_CONFIG, 162
- SerialloSpi2CsPolarity
 - FSP_S_CONFIG, 162
- SerialloSpi3CsEnable
 - FSP_S_CONFIG, 162
- SerialloSpi3CsPolarity
 - FSP_S_CONFIG, 162
- SerialloSpi4CsEnable
 - FSP_S_CONFIG, 162
- SerialloSpi4CsPolarity
 - FSP_S_CONFIG, 162
- SerialloSpi5CsEnable
 - FSP_S_CONFIG, 163
- SerialloSpi5CsPolarity
 - FSP_S_CONFIG, 163
- SerialloSpi6CsEnable
 - FSP_S_CONFIG, 163
- SerialloSpi6CsPolarity
 - FSP_S_CONFIG, 163
- SerialloSpiDefaultCsOutput
 - FSP_S_CONFIG, 163
- SerialloSpiMode
 - FSP_S_CONFIG, 164
- SerialloUartCtsPinMuxPolicy
 - FSP_S_CONFIG, 164
- SerialloUartDataBits
 - FSP_S_CONFIG, 164
- SerialloUartDmaEnable
 - FSP_S_CONFIG, 164
- SerialloUartMode
 - FSP_S_CONFIG, 164
- SerialloUartParity
 - FSP_S_CONFIG, 165
- SerialloUartPowerGating
 - FSP_S_CONFIG, 165
- SerialloUartRtsPinMuxPolicy
 - FSP_S_CONFIG, 165
- SerialloUartRxPinMuxPolicy
 - FSP_S_CONFIG, 165
- SerialloUartStopBits
 - FSP_S_CONFIG, 165
- SerialloUartTxPinMuxPolicy
 - FSP_S_CONFIG, 165
- ShowSpiController
 - FSP_S_CONFIG, 166
- SiCsmFlag
 - FSP_S_CONFIG, 166
- SinitMemorySize
 - FSP_M_CONFIG, 74
- SkipMbpHob
 - FSP_M_TEST_CONFIG, 87
- SkipMpInit
 - FSP_S_CONFIG, 166
- SkipPostBootSai
 - FSP_S_TEST_CONFIG, 199
- SlowSlewRateForFivr
 - FSP_S_CONFIG, 166
- SlowSlewRateForGt

- FSP_S_CONFIG, 166
- SlowSlewRateForIa
 - FSP_S_CONFIG, 167
- SlowSlewRateForSa
 - FSP_S_CONFIG, 167
- SlpS0DisQForDebug
 - FSP_S_CONFIG, 167
- SlpS0Override
 - FSP_S_CONFIG, 167
- SmbiosCacheInfoHob.h, 233
- SmbiosProcessorInfoHob.h, 234
- SmbusArpEnable
 - FSP_M_CONFIG, 74
- SmbusDynamicPowerGating
 - FSP_M_TEST_CONFIG, 87
- SmbusEnable
 - FSP_M_CONFIG, 74
- SmbusSpdWriteDisable
 - FSP_M_TEST_CONFIG, 88
- SpdAddressTable
 - FSP_M_CONFIG, 75
- SpdProfileSelected
 - FSP_M_CONFIG, 75
- StateRatio
 - FSP_S_TEST_CONFIG, 199
- StateRatioMax16
 - FSP_S_TEST_CONFIG, 199
- tRTP
 - FSP_M_CONFIG, 78
- TStates
 - FSP_S_TEST_CONFIG, 201
- TTSuggestedSetting
 - FSP_S_CONFIG, 169
- TccActivationOffset
 - FSP_S_TEST_CONFIG, 199
- TccOffsetClamp
 - FSP_S_TEST_CONFIG, 200
- TccOffsetLock
 - FSP_S_TEST_CONFIG, 200
- TccOffsetTimeWindowForRatl
 - FSP_S_TEST_CONFIG, 200
- TcolrqSelect
 - FSP_S_CONFIG, 167
- TcssAuxOri
 - FSP_S_CONFIG, 168
- TcssDma0En
 - FSP_M_CONFIG, 75
- TcssDma1En
 - FSP_M_CONFIG, 75
- TcssDma2En
 - FSP_M_CONFIG, 75
- TcssHslOri
 - FSP_S_CONFIG, 168
- TcssltbtPcie0En
 - FSP_M_CONFIG, 76
- TcssltbtPcie1En
 - FSP_M_CONFIG, 76
- TcssltbtPcie2En
 - FSP_M_CONFIG, 76
- TcssltbtPcie3En
 - FSP_M_CONFIG, 76
- TcssltbtPcie4En
 - FSP_M_CONFIG, 76
- TcssltbtPcie5En
 - FSP_M_CONFIG, 76
- TcssXdcEn
 - FSP_M_CONFIG, 77
- TcssXhciEn
 - FSP_M_CONFIG, 77
- TdcPowerLimit
 - FSP_S_CONFIG, 168
- TdcTimeWindow
 - FSP_S_CONFIG, 168
- TgaSize
 - FSP_M_CONFIG, 77
- ThcPort0InterruptPinMuxing
 - FSP_S_CONFIG, 168
- ThcPort1InterruptPinMuxing
 - FSP_S_CONFIG, 169
- ThreeStrikeCounterDisable
 - FSP_S_TEST_CONFIG, 200
- ThrtCkeMinTmr
 - FSP_M_CONFIG, 77
- TimedMwait
 - FSP_S_TEST_CONFIG, 200
- TjMaxOffset
 - FSP_M_CONFIG, 77
- TmeEnable
 - FSP_M_CONFIG, 78
- TotalFlashSize
 - FSP_M_TEST_CONFIG, 88
- TrainTrace
 - FSP_M_CONFIG, 78
- TsegSize
 - FSP_M_CONFIG, 78
- TsodAlarmwindowLockBit
 - FSP_M_CONFIG, 78
- TsodCriticalEventOnly
 - FSP_M_CONFIG, 79
- TsodCriticaltripLockBit
 - FSP_M_CONFIG, 79
- TsodEventMode
 - FSP_M_CONFIG, 79
- TsodEventOutputControl
 - FSP_M_CONFIG, 79
- TsodEventPolarity
 - FSP_M_CONFIG, 79
- TsodManualEnable
 - FSP_M_CONFIG, 80
- TsodShutdownMode
 - FSP_M_CONFIG, 80
- TsodTcritMax
 - FSP_M_CONFIG, 80
- TurboMode
 - FSP_S_CONFIG, 169
- Txt

- FSP_M_CONFIG, 80
 - TxtAcheckRequest
 - FSP_M_TEST_CONFIG, 88
 - TxtDprMemoryBase
 - FSP_M_CONFIG, 80
 - TxtDprMemorySize
 - FSP_M_CONFIG, 81
 - TxtEnable
 - FSP_S_CONFIG, 169
 - TxtHeapMemorySize
 - FSP_M_CONFIG, 81
 - TxtImplemented
 - FSP_M_CONFIG, 81
 - TxtLcpPdBase
 - FSP_M_CONFIG, 81
 - TxtLcpPdSize
 - FSP_M_CONFIG, 81
 - UfsEnable
 - FSP_S_CONFIG, 169
 - Usb2PhyPehalfbit
 - FSP_S_CONFIG, 169
 - Usb2PhyPetxiset
 - FSP_S_CONFIG, 170
 - Usb2PhyPredeemp
 - FSP_S_CONFIG, 170
 - Usb2PhyTxiset
 - FSP_S_CONFIG, 170
 - Usb3HsioTxDeEmph
 - FSP_S_CONFIG, 170
 - Usb3HsioTxDeEmphEnable
 - FSP_S_CONFIG, 170
 - Usb3HsioTxDownscaleAmp
 - FSP_S_CONFIG, 171
 - Usb3HsioTxDownscaleAmpEnable
 - FSP_S_CONFIG, 171
 - UsbPdoProgramming
 - FSP_S_CONFIG, 171
 - UsbTcPortEn
 - FSP_S_CONFIG, 171
 - UserBudgetEnable
 - FSP_M_CONFIG, 81
 - UserThresholdEnable
 - FSP_M_CONFIG, 82
 - VddVoltage
 - FSP_M_CONFIG, 82
 - VmdEnable
 - FSP_S_CONFIG, 171
 - VmdPortA
 - FSP_S_CONFIG, 172
 - VmdPortB
 - FSP_S_CONFIG, 172
 - VmdPortC
 - FSP_S_CONFIG, 172
 - VmdPortD
 - FSP_S_CONFIG, 172
 - VmxEnable
 - FSP_M_CONFIG, 82
 - VrVoltageLimit
 - FSP_S_CONFIG, 172
 - WarmThresholdCh0Dimm0
 - FSP_M_CONFIG, 82
 - WarmThresholdCh0Dimm1
 - FSP_M_CONFIG, 82
 - WarmThresholdCh1Dimm0
 - FSP_M_CONFIG, 83
 - WarmThresholdCh1Dimm1
 - FSP_M_CONFIG, 83
 - WatchDog
 - FSP_S_CONFIG, 173
 - WatchDogTimerBios
 - FSP_S_CONFIG, 173
 - WatchDogTimerOs
 - FSP_S_CONFIG, 173
 - WdtDisableAndLock
 - FSP_M_TEST_CONFIG, 88
 - XdciEnable
 - FSP_S_CONFIG, 173
-