

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

Fri Sep 20 2019 01:12:27

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/](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 FSP DISPATCH MODE 27**
- 9 Todo List 29**
- 10 Class Index 31**
  - 10.1 Class List . . . . . 31
- 11 File Index 33**
  - 11.1 File List . . . . . 33
- 12 Class Documentation 35**
  - 12.1 AUDIO\_AZALIA\_VERB\_TABLE Struct Reference . . . . . 35
    - 12.1.1 Detailed Description . . . . . 35
  - 12.2 AZALIA\_HEADER Struct Reference . . . . . 36
    - 12.2.1 Detailed Description . . . . . 36
  - 12.3 CHIPSET\_INIT\_INFO Struct Reference . . . . . 36
    - 12.3.1 Detailed Description . . . . . 37
  - 12.4 FIRMWARE\_VERSION Struct Reference . . . . . 37
    - 12.4.1 Detailed Description . . . . . 37
  - 12.5 FIRMWARE\_VERSION\_INFO Struct Reference . . . . . 37
    - 12.5.1 Detailed Description . . . . . 38
  - 12.6 FIRMWARE\_VERSION\_INFO\_HOB Struct Reference . . . . . 38

---

12.6.1 Detailed Description . . . . .	38
12.6.2 Member Data Documentation . . . . .	38
12.6.2.1 Count . . . . .	39
12.7 FSP_M_CONFIG Struct Reference . . . . .	39
12.7.1 Detailed Description . . . . .	63
12.7.2 Member Data Documentation . . . . .	63
12.7.2.1 ActiveCoreCount . . . . .	63
12.7.2.2 ApertureSize . . . . .	63
12.7.2.3 ApStartupBase . . . . .	63
12.7.2.4 Avx2RatioOffset . . . . .	63
12.7.2.5 Avx2VoltageScaleFactor . . . . .	64
12.7.2.6 Avx3RatioOffset . . . . .	64
12.7.2.7 Avx512VoltageScaleFactor . . . . .	64
12.7.2.8 BclkAdaptiveVoltage . . . . .	64
12.7.2.9 BdatEnable . . . . .	64
12.7.2.10 BdatTestType . . . . .	65
12.7.2.11 BiosAcmBase . . . . .	65
12.7.2.12 BiosAcmSize . . . . .	65
12.7.2.13 BiosGuard . . . . .	65
12.7.2.14 BiosSize . . . . .	65
12.7.2.15 BistOnReset . . . . .	65
12.7.2.16 BootFrequency . . . . .	66
12.7.2.17 BypassPhySyncReset . . . . .	66
12.7.2.18 ChHashEnable . . . . .	66
12.7.2.19 ChHashInterleaveBit . . . . .	66
12.7.2.20 ChHashMask . . . . .	66
12.7.2.21 CkeRankMapping . . . . .	67
12.7.2.22 CleanMemory . . . . .	67
12.7.2.23 CmdRanksTerminated . . . . .	67
12.7.2.24 CoreHighVoltageMode . . . . .	67
12.7.2.25 CoreMaxOcRatio . . . . .	67
12.7.2.26 CorePIIVoltageOffset . . . . .	68
12.7.2.27 CoreVoltageAdaptive . . . . .	68
12.7.2.28 CoreVoltageMode . . . . .	68
12.7.2.29 CoreVoltageOverride . . . . .	68
12.7.2.30 CpuCrashLogEnable . . . . .	68
12.7.2.31 CpuRatio . . . . .	69
12.7.2.32 CpuTraceHubMemReg0Size . . . . .	69
12.7.2.33 CpuTraceHubMemReg1Size . . . . .	69
12.7.2.34 CpuTraceHubMode . . . . .	69

---

---

12.7.2.35 DciUsb3TypecUfpDbg . . . . .	69
12.7.2.36 Ddr4OneDpc . . . . .	70
12.7.2.37 DdrFreqLimit . . . . .	70
12.7.2.38 DdrSpeedControl . . . . .	70
12.7.2.39 DebugInterfaceLockEnable . . . . .	70
12.7.2.40 DisableDimmChannel0 . . . . .	70
12.7.2.41 DisableDimmChannel1 . . . . .	71
12.7.2.42 DisableMessageCheck . . . . .	71
12.7.2.43 DmiDeEmphasis . . . . .	71
12.7.2.44 DmiGen3EndPointHint . . . . .	71
12.7.2.45 DmiGen3EndPointPreset . . . . .	71
12.7.2.46 DmiGen3EqPh2Enable . . . . .	71
12.7.2.47 DmiGen3EqPh3Method . . . . .	72
12.7.2.48 DmiGen3ProgramStaticEq . . . . .	72
12.7.2.49 DmiGen3RootPortPreset . . . . .	72
12.7.2.50 EnableC6Dram . . . . .	72
12.7.2.51 EnableSgx . . . . .	73
12.7.2.52 EnCmdRate . . . . .	73
12.7.2.53 EpgEnable . . . . .	73
12.7.2.54 FClkFrequency . . . . .	73
12.7.2.55 FivrEfficiency . . . . .	73
12.7.2.56 FivrFaults . . . . .	73
12.7.2.57 FivrProtection . . . . .	74
12.7.2.58 FivrPs . . . . .	74
12.7.2.59 FivrTdc . . . . .	74
12.7.2.60 ForceOltmOrRefresh2x . . . . .	74
12.7.2.61 FreqSaGvLow . . . . .	74
12.7.2.62 FreqSaGvMid . . . . .	75
12.7.2.63 FullRangeMultiplierUnlockEn . . . . .	75
12.7.2.64 Gen3SwEqAlwaysAttempt . . . . .	75
12.7.2.65 Gen3SwEqEnableVocTest . . . . .	75
12.7.2.66 Gen3SwEqJitterDwellTime . . . . .	75
12.7.2.67 Gen3SwEqJitterErrorTarget . . . . .	76
12.7.2.68 Gen3SwEqNumberOfPresets . . . . .	76
12.7.2.69 Gen3SwEqVocDwellTime . . . . .	76
12.7.2.70 Gen3SwEqVocErrorTarget . . . . .	76
12.7.2.71 GmAdr . . . . .	77
12.7.2.72 GtPIIVoltageOffset . . . . .	77
12.7.2.73 GtPsmiSupport . . . . .	77
12.7.2.74 GttMmAdr . . . . .	77

---

---

12.7.2.75 HeciCommunication2 . . . . .	77
12.7.2.76 HobBufferSize . . . . .	78
12.7.2.77 HotThresholdCh0Dimm0 . . . . .	78
12.7.2.78 HotThresholdCh0Dimm1 . . . . .	78
12.7.2.79 HotThresholdCh1Dimm0 . . . . .	78
12.7.2.80 HotThresholdCh1Dimm1 . . . . .	78
12.7.2.81 Idd3n . . . . .	79
12.7.2.82 Idd3p . . . . .	79
12.7.2.83 IgdDvmt50PreAlloc . . . . .	79
12.7.2.84 ImgUclkOutEn . . . . .	79
12.7.2.85 ImrRpSelection . . . . .	79
12.7.2.86 InitPcieAspmAfterOprom . . . . .	79
12.7.2.87 InternalGfx . . . . .	80
12.7.2.88 lsvtloPort . . . . .	80
12.7.2.89 JtagC10PowerGateDisable . . . . .	80
12.7.2.90 KtDeviceEnable . . . . .	80
12.7.2.91 LockPTMregs . . . . .	80
12.7.2.92 MarginLimitCheck . . . . .	81
12.7.2.93 McPllVoltageOffset . . . . .	81
12.7.2.94 MemoryTrace . . . . .	81
12.7.2.95 MmioSize . . . . .	81
12.7.2.96 NonCoreHighVoltageMode . . . . .	81
12.7.2.97 OcLock . . . . .	82
12.7.2.98 PanelPowerEnable . . . . .	82
12.7.2.99 PcdDebugInterfaceFlags . . . . .	82
12.7.2.100PcdIlsaSerialUartBase . . . . .	82
12.7.2.101PcdSerialDebugBaudRate . . . . .	82
12.7.2.102PcdSerialDebugLevel . . . . .	82
12.7.2.103PchLpcEnhancePort8xhDecoding . . . . .	83
12.7.2.104PchNumRsvdSmbusAddresses . . . . .	83
12.7.2.105PchPort80Route . . . . .	83
12.7.2.106PchSmbAlertEnable . . . . .	83
12.7.2.107PchTraceHubMemReg0Size . . . . .	83
12.7.2.108PchTraceHubMemReg1Size . . . . .	84
12.7.2.109PchTraceHubMode . . . . .	84
12.7.2.110PcieImrSize . . . . .	84
12.7.2.111PcieMultipleSegmentEnabled . . . . .	84
12.7.2.112PcieRpEnableMask . . . . .	84
12.7.2.113Peg0Gen3EqPh2Enable . . . . .	85
12.7.2.114Peg0Gen3EqPh3Method . . . . .	85

---

---

12.7.2.115Peg1Gen3EqPh2Enable . . . . .	85
12.7.2.116Peg1Gen3EqPh3Method . . . . .	85
12.7.2.117Peg2Gen3EqPh2Enable . . . . .	86
12.7.2.118Peg2Gen3EqPh3Method . . . . .	86
12.7.2.119Peg3Gen3EqPh2Enable . . . . .	86
12.7.2.120Peg3Gen3EqPh3Method . . . . .	86
12.7.2.121PegDataPtr . . . . .	86
12.7.2.122PegDisableSpreadSpectrumClocking . . . . .	87
12.7.2.123PegGen3EndPointHint . . . . .	87
12.7.2.124PegGen3EndPointPreset . . . . .	87
12.7.2.125PegGen3ProgramStaticEq . . . . .	87
12.7.2.126PegGen3RootPortPreset . . . . .	87
12.7.2.127PegGenerateBdatMarginTable . . . . .	88
12.7.2.128PegImrEnable . . . . .	88
12.7.2.129PegImrRpSelection . . . . .	88
12.7.2.130PegRxCemLoopbackLane . . . . .	88
12.7.2.131PegRxCemNonProtocolAwareness . . . . .	88
12.7.2.132PerCoreRatioLimit . . . . .	89
12.7.2.133PlatformDebugConsent . . . . .	89
12.7.2.134PrmrrSize . . . . .	89
12.7.2.135ProbelessTrace . . . . .	89
12.7.2.136PvdRatioThreshold . . . . .	89
12.7.2.137PwdownIdleCounter . . . . .	90
12.7.2.138RankInterleave . . . . .	90
12.7.2.139Ratio . . . . .	90
12.7.2.140RealtimeMemoryTiming . . . . .	90
12.7.2.141RefClk . . . . .	90
12.7.2.142RetrainOnFastFail . . . . .	91
12.7.2.143RhSolution . . . . .	91
12.7.2.144RingDownBin . . . . .	91
12.7.2.145RingMaxOcRatio . . . . .	91
12.7.2.146RingPIIVoltageOffset . . . . .	91
12.7.2.147RingVoltageAdaptive . . . . .	91
12.7.2.148RingVoltageMode . . . . .	92
12.7.2.149RingVoltageOffset . . . . .	92
12.7.2.150RingVoltageOverride . . . . .	92
12.7.2.151RMT . . . . .	92
12.7.2.152RMTBIT . . . . .	92
12.7.2.153RMTLoopCount . . . . .	93
12.7.2.154RmtPerTask . . . . .	93

---

12.7.2.155SafeMode . . . . .	93
12.7.2.156SaGv . . . . .	93
12.7.2.157SaPcieRpEnableMask . . . . .	93
12.7.2.158SaPcieRpLinkDownGpios . . . . .	94
12.7.2.159SaPIIFreqOverride . . . . .	94
12.7.2.160SaPIIVoltageOffset . . . . .	94
12.7.2.161ScanExtGfxForLegacyOpRom . . . . .	94
12.7.2.162ScramblerSupport . . . . .	94
12.7.2.163SerialIoUartDebugAutoFlow . . . . .	95
12.7.2.164SerialIoUartDebugBaudRate . . . . .	95
12.7.2.165SerialIoUartDebugControllerNumber . . . . .	95
12.7.2.166SerialIoUartDebugDataBits . . . . .	95
12.7.2.167SerialIoUartDebugParity . . . . .	95
12.7.2.168SerialIoUartDebugStopBits . . . . .	95
12.7.2.169SinitMemorySize . . . . .	96
12.7.2.170SkipMbpHob . . . . .	96
12.7.2.171SkipMplnitPreMem . . . . .	96
12.7.2.172SmbusArpEnable . . . . .	96
12.7.2.173SmbusDynamicPowerGating . . . . .	96
12.7.2.174SmbusEnable . . . . .	97
12.7.2.175SmbusSpdWriteDisable . . . . .	97
12.7.2.176SpdAddressTable . . . . .	97
12.7.2.177SpdProfileSelected . . . . .	97
12.7.2.178TcssDma0En . . . . .	97
12.7.2.179TcssDma1En . . . . .	98
12.7.2.180TcssltbtPcie0En . . . . .	98
12.7.2.181TcssltbtPcie1En . . . . .	98
12.7.2.182TcssltbtPcie2En . . . . .	98
12.7.2.183TcssltbtPcie3En . . . . .	98
12.7.2.184TcssXhciEn . . . . .	98
12.7.2.185TcssXhciEn . . . . .	99
12.7.2.186TgaSize . . . . .	99
12.7.2.187ThrtCkeMinTmr . . . . .	99
12.7.2.188ThrtCkeMinTmrLpddr . . . . .	99
12.7.2.189TjMaxOffset . . . . .	99
12.7.2.190TmeEnable . . . . .	100
12.7.2.191TrainTrace . . . . .	100
12.7.2.192RTP . . . . .	100
12.7.2.193TschwFixup . . . . .	100
12.7.2.194TsegSize . . . . .	100

---

12.7.2.195T	sodAlarmwindowLockBit	100
12.7.2.196T	sodCriticalEventOnly	101
12.7.2.197T	sodCriticaltripLockBit	101
12.7.2.198T	sodEventMode	101
12.7.2.199T	sodEventOutputControl	101
12.7.2.200T	sodEventPolarity	101
12.7.2.201T	sodManualEnable	102
12.7.2.202T	sodShutdownMode	102
12.7.2.203T	sodTcritMax	102
12.7.2.204T	xt	102
12.7.2.205T	xtAcheckRequest	102
12.7.2.206T	xtDprMemoryBase	103
12.7.2.207T	xtDprMemorySize	103
12.7.2.208T	xtHeapMemorySize	103
12.7.2.209T	xtImplemented	103
12.7.2.210T	xtLcpPdBase	103
12.7.2.211T	xtLcpPdSize	104
12.7.2.212	UserBudgetEnable	104
12.7.2.213	UserThresholdEnable	104
12.7.2.214	vccInVoltageOverride	104
12.7.2.215	vccinVrMaxVoltage	104
12.7.2.216	VddVoltage	105
12.7.2.217	VmxEnable	105
12.7.2.218	WarmThresholdCh0Dimm0	105
12.7.2.219	WarmThresholdCh0Dimm1	105
12.7.2.220	WarmThresholdCh1Dimm0	105
12.7.2.221	WarmThresholdCh1Dimm1	105
12.7.2.222	WdtDisableAndLock	106
12.7.2.223	XhciPIIOVERRIDE	106
12.8	FSP_M_RESTRICTED_CONFIG Struct Reference	106
12.8.1	Detailed Description	112
12.8.2	Member Data Documentation	112
12.8.2.1	DisableResets	112
12.8.2.2	HeciCommunication	112
12.8.2.3	HeciCommunication3	113
12.8.2.4	LowMemChannel	113
12.8.2.5	MsegSize	113
12.8.2.6	PchTestDmiMeUmaRootSpaceCheck	113
12.8.2.7	PcuDdrVoltage	113
12.8.2.8	TestMenuDprLock	114

---

12.8.2.9	tRRDD	114
12.8.2.10	tRRDG	114
12.8.2.11	tRRDR	114
12.8.2.12	tRRSG	114
12.8.2.13	tRWDD	114
12.8.2.14	tRWDG	115
12.8.2.15	tRWDR	115
12.8.2.16	tRWSG	115
12.8.2.17	tWRDD	115
12.8.2.18	tWRDG	115
12.8.2.19	tWRDR	116
12.8.2.20	tWRSG	116
12.8.2.21	tWWDD	116
12.8.2.22	tWWDG	116
12.8.2.23	tWWDR	116
12.8.2.24	tWWSG	117
12.9	FSP_S_CONFIG Struct Reference	117
12.9.1	Detailed Description	145
12.9.2	Member Data Documentation	145
12.9.2.1	AcLoadline	145
12.9.2.2	AcousticNoiseMitigation	145
12.9.2.3	AmtEnabled	145
12.9.2.4	AmtKvmEnabled	146
12.9.2.5	AmtSolEnabled	146
12.9.2.6	ApldleManner	146
12.9.2.7	AsfEnabled	146
12.9.2.8	AutoThermalReporting	146
12.9.2.9	C1e	147
12.9.2.10	C1StateAutoDemotion	147
12.9.2.11	C1StateUnDemotion	147
12.9.2.12	CnviBtAudioOffload	147
12.9.2.13	CnviBtCore	147
12.9.2.14	CnviClkreqPinMux	147
12.9.2.15	CnviMode	148
12.9.2.16	CnviRfResetPinMux	148
12.9.2.17	ConfigTdpBios	148
12.9.2.18	CpuMpHob	148
12.9.2.19	CStatePreWake	148
12.9.2.20	CstCfgCtrlIoMwaitRedirection	149
12.9.2.21	Custom1PowerLimit1	149

---

12.9.2.22 Custom1PowerLimit1Time . . . . .	149
12.9.2.23 Custom1PowerLimit2 . . . . .	149
12.9.2.24 Custom1TurboActivationRatio . . . . .	149
12.9.2.25 Custom2PowerLimit1 . . . . .	150
12.9.2.26 Custom2PowerLimit1Time . . . . .	150
12.9.2.27 Custom2PowerLimit2 . . . . .	150
12.9.2.28 Custom2TurboActivationRatio . . . . .	150
12.9.2.29 Custom3PowerLimit1 . . . . .	150
12.9.2.30 Custom3PowerLimit1Time . . . . .	151
12.9.2.31 Custom3PowerLimit2 . . . . .	151
12.9.2.32 Custom3TurboActivationRatio . . . . .	151
12.9.2.33 Cx . . . . .	151
12.9.2.34 DcLoadline . . . . .	151
12.9.2.35 DevIntConfigPtr . . . . .	151
12.9.2.36 DisableProcHotOut . . . . .	152
12.9.2.37 DisableVrThermalAlert . . . . .	152
12.9.2.38 DmiSuggestedSetting . . . . .	152
12.9.2.39 DmiTS0TW . . . . .	152
12.9.2.40 DmiTS1TW . . . . .	152
12.9.2.41 DmiTS2TW . . . . .	153
12.9.2.42 DmiTS3TW . . . . .	153
12.9.2.43 EcCmdLock . . . . .	153
12.9.2.44 EcCmdProvisionEav . . . . .	153
12.9.2.45 Eist . . . . .	153
12.9.2.46 Enable8254ClockGating . . . . .	154
12.9.2.47 Enable8254ClockGatingOnS3 . . . . .	154
12.9.2.48 EnableEpbPeciOverride . . . . .	154
12.9.2.49 EnableFastMsrHwpReq . . . . .	154
12.9.2.50 EnableHwpAutoEppGrouping . . . . .	154
12.9.2.51 EnableHwpAutoPerCorePstate . . . . .	155
12.9.2.52 EnableIltbm . . . . .	155
12.9.2.53 EnableMinVoltageOverride . . . . .	155
12.9.2.54 EnablePerCorePState . . . . .	155
12.9.2.55 EnableTcoTimer . . . . .	155
12.9.2.56 EndOfPostMessage . . . . .	156
12.9.2.57 EnergyEfficientPState . . . . .	156
12.9.2.58 EnergyEfficientTurbo . . . . .	156
12.9.2.59 EsataSpeedLimit . . . . .	156
12.9.2.60 FastPkgCRampDisableFivr . . . . .	156
12.9.2.61 FivrRfiFrequency . . . . .	157

---

12.9.2.62 FivrSpreadSpectrum . . . . .	157
12.9.2.63 ForcMebxSyncUp . . . . .	157
12.9.2.64 FwProgress . . . . .	157
12.9.2.65 GpioIrqRoute . . . . .	157
12.9.2.66 HdcControl . . . . .	158
12.9.2.67 Heci3Enabled . . . . .	158
12.9.2.68 Hwp . . . . .	158
12.9.2.69 HwpInterruptControl . . . . .	158
12.9.2.70 lccMax . . . . .	158
12.9.2.71 lmonOffset . . . . .	158
12.9.2.72 lmonSlope . . . . .	159
12.9.2.73 lomTypeCPortPadCfg . . . . .	159
12.9.2.74 ITbtConnectTopologyTimeoutInMs . . . . .	159
12.9.2.75 ITbtForcePowerOnTimeoutInMs . . . . .	159
12.9.2.76 MachineCheckEnable . . . . .	159
12.9.2.77 ManageabilityMode . . . . .	160
12.9.2.78 MaxRingRatioLimit . . . . .	160
12.9.2.79 MctpBroadcastCycle . . . . .	160
12.9.2.80 MeUnconfigOnRtcClear . . . . .	160
12.9.2.81 MinRingRatioLimit . . . . .	160
12.9.2.82 MinVoltageC8 . . . . .	161
12.9.2.83 MinVoltageRuntime . . . . .	161
12.9.2.84 MlcStreamerPrefetcher . . . . .	161
12.9.2.85 MonitorMwaitEnable . . . . .	161
12.9.2.86 NumberOfEntries . . . . .	161
12.9.2.87 NumOfDevIntConfig . . . . .	162
12.9.2.88 OneCoreRatioLimit . . . . .	162
12.9.2.89 PchCrid . . . . .	162
12.9.2.90 PchDmiAspmCtrl . . . . .	162
12.9.2.91 PchDmiTsawEn . . . . .	162
12.9.2.92 PchEnableComplianceMode . . . . .	163
12.9.2.93 PchEnableDbcObs . . . . .	163
12.9.2.94 PchEspHostC10ReportEnable . . . . .	163
12.9.2.95 PchFivrDynPm . . . . .	163
12.9.2.96 PchFivrExtVnnRailSxEnabledStates . . . . .	163
12.9.2.97 PchFivrExtVnnRailSxlccMax . . . . .	164
12.9.2.98 PchFivrExtVnnRailSxVoltage . . . . .	164
12.9.2.99 PchFivrVccinAuxLowToHighCurModeVolTranTime . . . . .	164
12.9.2.100PchFivrVccinAuxOffToHighCurModeVolTranTime . . . . .	164
12.9.2.101PchFivrVccinAuxRetToHighCurModeVolTranTime . . . . .	164

---

12.9.2.102PchFivrVccinAuxRetToLowCurModeVolTranTime . . . . .	165
12.9.2.103PchHdaAudioLinkDmic0 . . . . .	165
12.9.2.104PchHdaAudioLinkDmic1 . . . . .	165
12.9.2.105PchHdaAudioLinkHda . . . . .	165
12.9.2.106PchHdaAudioLinkSndw1 . . . . .	165
12.9.2.107PchHdaAudioLinkSndw2 . . . . .	165
12.9.2.108PchHdaAudioLinkSndw3 . . . . .	166
12.9.2.109PchHdaAudioLinkSndw4 . . . . .	166
12.9.2.110PchHdaAudioLinkSsp0 . . . . .	166
12.9.2.111PchHdaAudioLinkSsp1 . . . . .	166
12.9.2.112PchHdaAudioLinkSsp2 . . . . .	166
12.9.2.113PchHdaAudioLinkSsp3 . . . . .	167
12.9.2.114PchHdaAudioLinkSsp4 . . . . .	167
12.9.2.115PchHdaAudioLinkSsp5 . . . . .	167
12.9.2.116PchHdaDspEnable . . . . .	167
12.9.2.117PchHdaDspUaaCompliance . . . . .	167
12.9.2.118PchHdaDispCodecDisconnect . . . . .	167
12.9.2.119PchHdaDispLinkFrequency . . . . .	168
12.9.2.120PchHdaLinkFrequency . . . . .	168
12.9.2.121PchHdaPme . . . . .	168
12.9.2.122PchHdaResetWaitTimer . . . . .	168
12.9.2.123PchHdaVcType . . . . .	168
12.9.2.124PchHotEnable . . . . .	169
12.9.2.125PchIoApicEntry24_119 . . . . .	169
12.9.2.126PchIoApicId . . . . .	169
12.9.2.127PchIshGp0GpioAssign . . . . .	169
12.9.2.128PchIshGp1GpioAssign . . . . .	169
12.9.2.129PchIshGp2GpioAssign . . . . .	170
12.9.2.130PchIshGp3GpioAssign . . . . .	170
12.9.2.131PchIshGp4GpioAssign . . . . .	170
12.9.2.132PchIshGp5GpioAssign . . . . .	170
12.9.2.133PchIshGp6GpioAssign . . . . .	170
12.9.2.134PchIshGp7GpioAssign . . . . .	170
12.9.2.135PchIshI2c0GpioAssign . . . . .	171
12.9.2.136PchIshI2c1GpioAssign . . . . .	171
12.9.2.137PchIshI2c2GpioAssign . . . . .	171
12.9.2.138PchIshPdtUnlock . . . . .	171
12.9.2.139PchIshSpiGpioAssign . . . . .	171
12.9.2.140PchIshUart0GpioAssign . . . . .	172
12.9.2.141PchIshUart1GpioAssign . . . . .	172

---

---

12.9.2.142PchLanEnable . . . . .	172
12.9.2.143PchLanLtrEnable . . . . .	172
12.9.2.144PchLockDownBiosInterface . . . . .	172
12.9.2.145PchLockDownBiosLock . . . . .	172
12.9.2.146PchLockDownGlobalSmi . . . . .	173
12.9.2.147PchLockDownRtcMemoryLock . . . . .	173
12.9.2.148PchMemoryThrottlingEnable . . . . .	173
12.9.2.149PchPmDeepSxPol . . . . .	173
12.9.2.150PchPmDisableDsxAcPresentPulldown . . . . .	173
12.9.2.151PchPmDisableEnergyReport . . . . .	174
12.9.2.152PchPmDisableNativePowerButton . . . . .	174
12.9.2.153PchPmLanWakeFromDeepSx . . . . .	174
12.9.2.154PchPmMeWakeSts . . . . .	174
12.9.2.155PchPmPciePllSsc . . . . .	174
12.9.2.156PchPmPcieWakeFromDeepSx . . . . .	175
12.9.2.157PchPmPmeB0S5Dis . . . . .	175
12.9.2.158PchPmPwrBtnOverridePeriod . . . . .	175
12.9.2.159PchPmPwrCycDur . . . . .	175
12.9.2.160PchPmS0i3Support . . . . .	175
12.9.2.161PchPmSlpAMinAssert . . . . .	175
12.9.2.162PchPmSlpLanLowDc . . . . .	176
12.9.2.163PchPmSlpS0Enable . . . . .	176
12.9.2.164PchPmSlpS3MinAssert . . . . .	176
12.9.2.165PchPmSlpS4MinAssert . . . . .	176
12.9.2.166PchPmSlpStrchSusUp . . . . .	176
12.9.2.167PchPmSlpSusMinAssert . . . . .	177
12.9.2.168PchPmVrAlert . . . . .	177
12.9.2.169PchPmWoIEnableOverride . . . . .	177
12.9.2.170PchPmWoIovrWkSts . . . . .	177
12.9.2.171PchPmWoWlanDeepSxEnable . . . . .	177
12.9.2.172PchPmWoWlanEnable . . . . .	178
12.9.2.173PchPwrOptEnable . . . . .	178
12.9.2.174PchSbAccessUnlock . . . . .	178
12.9.2.175PchScsEmmcHs400DIIIDataValid . . . . .	178
12.9.2.176PchSerialIoI2cPadsTermination . . . . .	178
12.9.2.177PchTTEnable . . . . .	179
12.9.2.178PchTTLock . . . . .	179
12.9.2.179PchTTState13Enable . . . . .	179
12.9.2.180PchUnlockGpioPads . . . . .	179
12.9.2.181PchXhciOcLock . . . . .	179

---

---

12.9.2.182PcieComplianceTestMode . . . . .	180
12.9.2.183PcieEnablePeerMemoryWrite . . . . .	180
12.9.2.184PcieEnablePort8xhDecode . . . . .	180
12.9.2.185PcieEqPh3LaneParamCm . . . . .	180
12.9.2.186PcieEqPh3LaneParamCp . . . . .	180
12.9.2.187PcieRpAspm . . . . .	181
12.9.2.188PcieRpCompletionTimeout . . . . .	181
12.9.2.189PcieRpDpcExtensionsMask . . . . .	181
12.9.2.190PcieRpDpcMask . . . . .	181
12.9.2.191PcieRpDptp . . . . .	181
12.9.2.192PcieRpFunctionSwap . . . . .	181
12.9.2.193PcieRpGen3EqPh3Method . . . . .	182
12.9.2.194PcieRpL1Substates . . . . .	182
12.9.2.195PcieRpPcieSpeed . . . . .	182
12.9.2.196PcieRpPhysicalSlotNumber . . . . .	182
12.9.2.197PcieRpPtmMask . . . . .	182
12.9.2.198PcieRpSlotPowerLimitScale . . . . .	183
12.9.2.199PcieRpSlotPowerLimitValue . . . . .	183
12.9.2.200PcieRpUptp . . . . .	183
12.9.2.201PcieSwEqCoeffListCm . . . . .	183
12.9.2.202PcieSwEqCoeffListCp . . . . .	183
12.9.2.203PkgCStateDemotion . . . . .	184
12.9.2.204PkgCStateLimit . . . . .	184
12.9.2.205PkgCStateUnDemotion . . . . .	184
12.9.2.206PmcCpuC10GatePinEnable . . . . .	184
12.9.2.207PmcCrashLogEnable . . . . .	184
12.9.2.208PmcDbgMsgEn . . . . .	184
12.9.2.209PmcModPhySusPgEnable . . . . .	185
12.9.2.210PmcPowerButtonDebounce . . . . .	185
12.9.2.211PmgCstCfgCtrlLock . . . . .	185
12.9.2.212PortUsb20Enable . . . . .	185
12.9.2.213PortUsb30Enable . . . . .	185
12.9.2.214PowerLimit1 . . . . .	186
12.9.2.215PowerLimit1Time . . . . .	186
12.9.2.216PowerLimit2 . . . . .	186
12.9.2.217PowerLimit2Power . . . . .	186
12.9.2.218PowerLimit3 . . . . .	186
12.9.2.219PowerLimit4 . . . . .	187
12.9.2.220PpinSupport . . . . .	187
12.9.2.221PreWake . . . . .	187

---

---

12.9.2.222	ProcessorTraceEnable	187
12.9.2.223	ProcessorTraceMemBase	187
12.9.2.224	ProcessorTraceMemLength	188
12.9.2.225	ProcessorTraceOutputScheme	188
12.9.2.226	ProcHotResponse	188
12.9.2.227	Psi1Threshold	188
12.9.2.228	Psi2Threshold	188
12.9.2.229	Psi3Enable	189
12.9.2.230	Psi3Threshold	189
12.9.2.231	PsOnEnable	189
12.9.2.232	PsysOffset	189
12.9.2.233	PsysPmax	189
12.9.2.234	PsysPowerLimit1	190
12.9.2.235	PsysPowerLimit1Power	190
12.9.2.236	PsysPowerLimit2	190
12.9.2.237	PsysPowerLimit2Power	190
12.9.2.238	PsysSlope	190
12.9.2.239	PxRcConfig	190
12.9.2.240	RaceToHalt	191
12.9.2.241	RemoteAssistance	191
12.9.2.242	SaPcieComplianceTestMode	191
12.9.2.243	SaPcieDeviceOverrideTablePtr	191
12.9.2.244	SaPcieDisableRootPortClockGating	191
12.9.2.245	SaPcieEnablePeerMemoryWrite	192
12.9.2.246	SaPcieEqPh3LaneParamCm	192
12.9.2.247	SaPcieEqPh3LaneParamCp	192
12.9.2.248	SaPcieRpAspm	192
12.9.2.249	SaPcieRpDpcExtensionsMask	192
12.9.2.250	SaPcieRpDpcMask	193
12.9.2.251	SaPcieRpDptp	193
12.9.2.252	SaPcieRpFunctionSwap	193
12.9.2.253	SaPcieRpGen3EqPh3Method	193
12.9.2.254	SaPcieRpL1Substates	193
12.9.2.255	SaPcieRpPcieSpeed	194
12.9.2.256	SaPcieRpPhysicalSlotNumber	194
12.9.2.257	SaPcieRpPtmMask	194
12.9.2.258	SaPcieRpUptp	194
12.9.2.259	SataEnable	194
12.9.2.260	SataLedEnable	194
12.9.2.261	SataMode	195

---

---

12.9.2.262SataP0TDispFinit . . . . .	195
12.9.2.263SataP1TDispFinit . . . . .	195
12.9.2.264SataPortsDevSlp . . . . .	195
12.9.2.265SataPortsDmVal . . . . .	195
12.9.2.266SataPortsEnable . . . . .	196
12.9.2.267SataPwrOptEnable . . . . .	196
12.9.2.268SataRstHddUnlock . . . . .	196
12.9.2.269SataRstInterrupt . . . . .	196
12.9.2.270SataRstIrrt . . . . .	196
12.9.2.271SataRstIrrtOnly . . . . .	196
12.9.2.272SataRstLedLocate . . . . .	197
12.9.2.273SataRstOromUiBanner . . . . .	197
12.9.2.274SataRstPcieDeviceResetDelay . . . . .	197
12.9.2.275SataRstRaid0 . . . . .	197
12.9.2.276SataRstRaid1 . . . . .	197
12.9.2.277SataRstRaid10 . . . . .	198
12.9.2.278SataRstRaid5 . . . . .	198
12.9.2.279SataRstRaidDeviceld . . . . .	198
12.9.2.280SataRstSmartStorage . . . . .	198
12.9.2.281SataSalpSupport . . . . .	198
12.9.2.282SataTestMode . . . . .	199
12.9.2.283SataThermalSuggestedSetting . . . . .	199
12.9.2.284ScilrqSelect . . . . .	199
12.9.2.285ScsEmmcEnabled . . . . .	199
12.9.2.286ScsEmmcHs400Enabled . . . . .	199
12.9.2.287ScsSdCardEnabled . . . . .	199
12.9.2.288SendEcCmd . . . . .	200
12.9.2.289SendVrMbxCmd . . . . .	200
12.9.2.290SerialIoDebugUartNumber . . . . .	200
12.9.2.291SerialIoI2cMode . . . . .	200
12.9.2.292SerialIoSpi0CsEnable . . . . .	200
12.9.2.293SerialIoSpi0CsPolarity . . . . .	201
12.9.2.294SerialIoSpi1CsEnable . . . . .	201
12.9.2.295SerialIoSpi1CsPolarity . . . . .	201
12.9.2.296SerialIoSpi2CsEnable . . . . .	201
12.9.2.297SerialIoSpi2CsPolarity . . . . .	201
12.9.2.298SerialIoSpiDefaultCsOutput . . . . .	202
12.9.2.299SerialIoSpiMode . . . . .	202
12.9.2.300SerialIoUartCtsPinMux . . . . .	202
12.9.2.301SerialIoUartDataBits . . . . .	202

---

---

12.9.2.302SerialIoUartDmaEnable . . . . .	202
12.9.2.303SerialIoUartMode . . . . .	202
12.9.2.304SerialIoUartParity . . . . .	203
12.9.2.305SerialIoUartPowerGating . . . . .	203
12.9.2.306SerialIoUartRtsPinMux . . . . .	203
12.9.2.307SerialIoUartRxPinMux . . . . .	203
12.9.2.308SerialIoUartStopBits . . . . .	203
12.9.2.309SerialIoUartTxPinMux . . . . .	204
12.9.2.310SiCsmFlag . . . . .	204
12.9.2.311SkipMplnit . . . . .	204
12.9.2.312SlowSlewRateForFivr . . . . .	204
12.9.2.313SlpS0DisQForDebug . . . . .	204
12.9.2.314SlpS0Override . . . . .	205
12.9.2.315StateRatio . . . . .	205
12.9.2.316StateRatioMax16 . . . . .	205
12.9.2.317TccActivationOffset . . . . .	205
12.9.2.318TccOffsetClamp . . . . .	205
12.9.2.319TccOffsetLock . . . . .	206
12.9.2.320TccOffsetTimeWindowForRatl . . . . .	206
12.9.2.321TcolrqSelect . . . . .	206
12.9.2.322TcssAuxOri . . . . .	206
12.9.2.323TcssHslOri . . . . .	206
12.9.2.324TcssLoopbackModeBitMap . . . . .	207
12.9.2.325TcssXhciEnableComplianceMode . . . . .	207
12.9.2.326TdcPowerLimit . . . . .	207
12.9.2.327TdcTimeWindow . . . . .	207
12.9.2.328ThreeStrikeCounterDisable . . . . .	207
12.9.2.329TimedMwait . . . . .	207
12.9.2.330TStates . . . . .	208
12.9.2.331TTsuggestedSetting . . . . .	208
12.9.2.332TurboMode . . . . .	208
12.9.2.333TxtEnable . . . . .	208
12.9.2.334UfsEnable . . . . .	208
12.9.2.335Usb2PhyPehalfbit . . . . .	209
12.9.2.336Usb2PhyPetxiset . . . . .	209
12.9.2.337Usb2PhyPredeemp . . . . .	209
12.9.2.338Usb2PhyTxiset . . . . .	209
12.9.2.339Usb3HsioTxDeEmph . . . . .	209
12.9.2.340Usb3HsioTxDeEmphEnable . . . . .	210
12.9.2.341Usb3HsioTxDownscaleAmp . . . . .	210

---

---

12.9.2.342Usb3HsioTxDownscaleAmpEnable . . . . .	210
12.9.2.343UsbPdoProgramming . . . . .	210
12.9.2.344UsbTcPortEn . . . . .	210
12.9.2.345VmdEnable . . . . .	211
12.9.2.346VmdPortA . . . . .	211
12.9.2.347VmdPortB . . . . .	211
12.9.2.348VmdPortC . . . . .	211
12.9.2.349VmdPortD . . . . .	211
12.9.2.350VrVoltageLimit . . . . .	211
12.9.2.351WatchDog . . . . .	212
12.9.2.352WatchDogTimerBios . . . . .	212
12.9.2.353WatchDogTimerOs . . . . .	212
12.9.2.354XhciEnable . . . . .	212
12.10FSP_S_RESTRICTED_CONFIG Struct Reference . . . . .	212
12.10.1 Detailed Description . . . . .	218
12.10.2 Member Data Documentation . . . . .	218
12.10.2.1 PchDmiTestClientObffEn . . . . .	218
12.10.2.2 PchDmiTestDmiSecureRegLock . . . . .	219
12.10.2.3 PchDmiTestExternalObffEn . . . . .	219
12.10.2.4 PchDmiTestInternalObffEn . . . . .	219
12.10.2.5 PchDmiTestMemCloseStateEn . . . . .	219
12.10.2.6 PchDmiTestOpiPllPowerGating . . . . .	219
12.10.2.7 PchDmiTestPchTcLockDown . . . . .	219
12.10.2.8 PchHdaTestConfigLockdown . . . . .	220
12.10.2.9 PchHdaTestLowFreqLinkClkSrc . . . . .	220
12.10.2.10PchHdaTestPowerClockGating . . . . .	220
12.10.2.11PchLanTestPchWOLFastSupport . . . . .	220
12.10.2.12PchLockDownTestSmiUnlock . . . . .	220
12.10.2.13PchPmTestPchClearPowerSts . . . . .	221
12.10.2.14PchTestClkGatingXhci . . . . .	221
12.10.2.15PchTestPhlcLock . . . . .	221
12.10.2.16PchTestTscLock . . . . .	221
12.10.2.17PchTestTselLock . . . . .	221
12.10.2.18PchTestUnlockUsbForSvNoa . . . . .	222
12.10.2.19SaPcieAllowL0sWithGen3 . . . . .	222
12.10.2.20SataTestRstPcieStorageDeviceInterface . . . . .	222
12.10.2.21SiSvPolicyEnable . . . . .	222
12.10.2.22TestCnviBtWirelessCharging . . . . .	222
12.10.2.23TestCnviLteCoex . . . . .	223
12.10.2.24TestCnviSharedXtalClocking . . . . .	223

---

12.10.2.25	TestCnviWifiLtrEn	223
12.10.2.26	TestPchPcieClockGating	223
12.10.2.27	TestPchPmErDebugMode	223
12.10.2.28	TestPchPmLatchEventsC10Exit	223
12.10.2.29	TestPcieRpSrlEnable	224
12.10.2.30	TestPmcDbgModeLock	224
12.10.2.31	TestPmcSlpsxStrPolLock	224
12.10.2.32	TestUsbXhciAccessControlLock	224
12.11	FSP_T_CONFIG Struct Reference	225
12.11.1	Detailed Description	225
12.11.2	Member Data Documentation	226
12.11.2.1	PcdSerialloUartAutoFlow	226
12.11.2.2	PcdSerialloUartCtsPinMux	226
12.11.2.3	PcdSerialloUartDataBits	226
12.11.2.4	PcdSerialloUartDebugEnable	226
12.11.2.5	PcdSerialloUartNumber	226
12.11.2.6	PcdSerialloUartParity	227
12.11.2.7	PcdSerialloUartRtsPinMux	227
12.11.2.8	PcdSerialloUartStopBits	227
12.12	FSP_T_RESTRICTED_CONFIG Struct Reference	227
12.12.1	Detailed Description	227
12.13	FSPM_UPD Struct Reference	228
12.13.1	Detailed Description	228
12.14	FSPS_UPD Struct Reference	228
12.14.1	Detailed Description	229
12.15	FSPT_CORE_UPD Struct Reference	229
12.15.1	Detailed Description	230
12.16	FSPT_UPD Struct Reference	230
12.16.1	Detailed Description	231
12.17	GPIO_CONFIG Struct Reference	231
12.17.1	Detailed Description	231
12.17.2	Member Data Documentation	231
12.17.2.1	Direction	232
12.17.2.2	ElectricalConfig	232
12.17.2.3	HostSoftPadOwn	232
12.17.2.4	InterruptConfig	232
12.17.2.5	LockConfig	232
12.17.2.6	OutputState	232
12.17.2.7	PadMode	233
12.17.2.8	PowerConfig	233

12.18	SI_PCH_DEVICE_INTERRUPT_CONFIG Struct Reference	233
12.18.1	Detailed Description	233
12.19	SMBIOS_STRUCTURE Struct Reference	234
12.19.1	Detailed Description	234
<b>13</b>	<b>File Documentation</b>	<b>235</b>
13.1	FirmwareVersionInfoHob.h File Reference	235
13.1.1	Detailed Description	235
13.2	FspFixedPcds.h File Reference	236
13.2.1	Detailed Description	236
13.3	FspInfoHob.h File Reference	236
13.3.1	Detailed Description	236
13.4	FspmUpd.h File Reference	237
13.4.1	Detailed Description	238
13.5	FspsUpd.h File Reference	238
13.5.1	Detailed Description	240
13.5.2	Enumeration Type Documentation	240
13.5.2.1	SI_PCH_INT_PIN	240
13.6	FsptUpd.h File Reference	241
13.6.1	Detailed Description	242
13.7	FspUpd.h File Reference	242
13.7.1	Detailed Description	243
13.8	GpioConfig.h File Reference	243
13.8.1	Detailed Description	245
13.8.2	Enumeration Type Documentation	245
13.8.2.1	GPIO_DIRECTION	245
13.8.2.2	GPIO_ELECTRICAL_CONFIG	245
13.8.2.3	GPIO_HARDWARE_DEFAULT	246
13.8.2.4	GPIO_HOSTSW_OWN	246
13.8.2.5	GPIO_INT_CONFIG	247
13.8.2.6	GPIO_LOCK_CONFIG	247
13.8.2.7	GPIO_OTHER_CONFIG	248
13.8.2.8	GPIO_OUTPUT_STATE	248
13.8.2.9	GPIO_PAD_MODE	248
13.8.2.10	GPIO_RESET_CONFIG	249
13.9	GpioSampleDef.h File Reference	250
13.9.1	Detailed Description	250
	<b>Index</b>	<b>251</b>



# 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 IceLake platforms with IceLake processor and IceLake 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](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

---

<b>Acronym</b>	<b>Definition</b>
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)**
    - IceLake\_FSP\_Integration\_Guide.pdf
    - IceLake\_FSP\_Integration\_Guide.chm
  - **Include**
    - [FsptUpd.h](#), [FspmUpd.h](#) and [FspsUpd.h](#) (FSP UPD structure and related definitions)
    - [GpioSampleDef.h](#) (Sample enum definitions for Gpio table)
  - \*FspBinPkg.dec (EDKII declaration file for package)
  - Fsp.bsf (BSF file for configuring the data using BCT tool)
  - Fsp.fd (FSP Binary)
-

## Chapter 3

# FSP INTEGRATION

### 3 FSP Integration

#### 3.1 Assumptions Used in this Document

The FSP for the IceLake 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 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 - 0x00040000	Write back
CodeCacheBase - CodeCacheLength	Write protect

#### 3.6.2 FspMemoryInit API

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

The **FspmUpdPtr** is pointer to **FSPM\_UPD** structure which is described in header file [FspmUpd.h](#).

Boot Loader must pass valid CAR region for FSP stack use through **FSPM\_UPD.FspmArchUpd.StackBase** and **FSPM\_UPD.FspmArchUpd.StackSize** UPDs.

The minimum FSP stack size required for this revision of FSP is 160KB, stack base is 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. If the boot loader wish to reconfigure the MTRRs differently, it can be overridden immediately after this API call.

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

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

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

### 3.6.4 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.

---

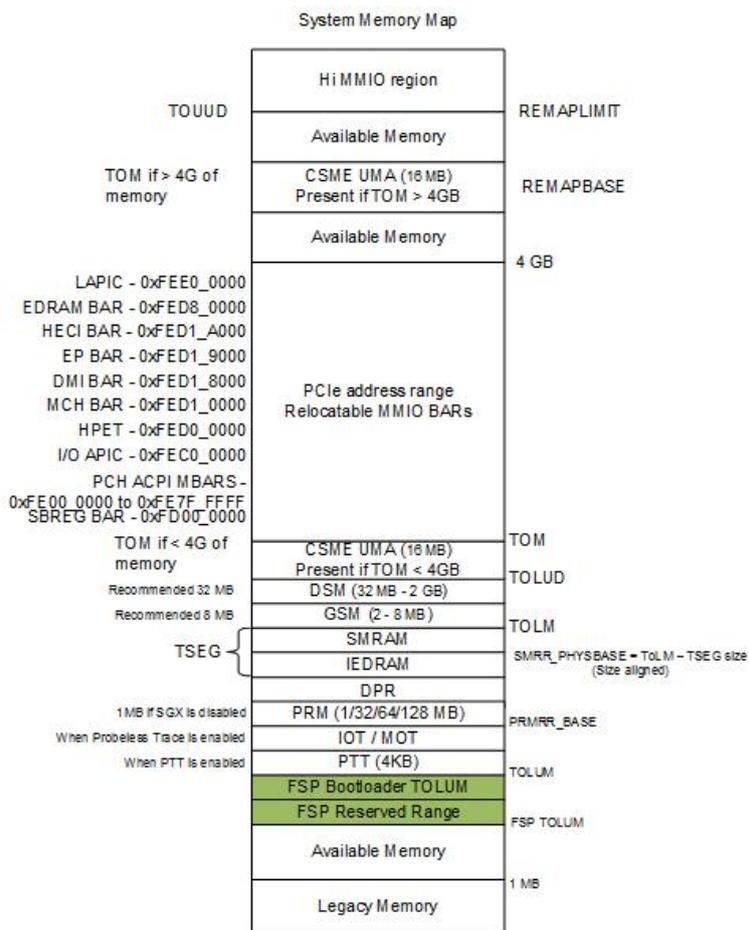


Figure 3.1: System Memory Map

/\*\*



# 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 for recommendation values:

UPD	Dependency	Description	Value
EnableSgx	IceLake 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
PchSataHsioTxGen1DownscaleAmp↔ Enable	Board design	Different board requires different value	tune
PchSataHsioTxGen1DownscaleAmp	Board design	Different board requires different value	tune
PchSataHsioTxGen2DownscaleAmp↔ Enable	Board design	Different board requires different value	tune
PchSataHsioTxGen2DownscaleAmp	Board design	Different board requires different value	tune
PchNumRsvdSmbusAddresses	Board design	Different board requires different value	tune
RsvdSmbusAddressTablePtr	Board design	Different board requires different value	tune
BiosSize	Board design	Different board requires different value	tune



# Chapter 6

## FSP OUTPUT

### 6 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 , Smbios↔CacheInfoHob.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 DDR4
    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
    ///< This info is used for both ProcessorFamily and ProcessorFamily2 fields
    ///< See ENUM defined in SMBIOS Spec v3.0 Section 7.5.2
    UINT16    ProcessorFamily;
    UINT8     ProcessorManufacturerStrIndex; ///< Index of the String in the String Buffer
    UINT64    ProcessorId;                ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.3
    UINT8     ProcessorVersionStrIndex;    ///< Index of the String in the String Buffer
    UINT8     Voltage;                     ///< Format defined in SMBIOS Spec v3.0 Section 7.5.4
    UINT16    ExternalClockInMHz;         ///< External Clock Frequency. Set to 0 if unknown.
    UINT16    CurrentSpeedInMHz;         ///< Snapshot of current processor speed during boot
    UINT8     Status;                     ///< Format defined in the SMBIOS Spec v3.0 Table 21
    UINT8     ProcessorUpgrade;           ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.5
    ///< This info is used for both CoreCount & CoreCount2 fields
    ///< See detailed description in SMBIOS Spec v3.0 Section 7.5.6
    UINT16    CoreCount;
    ///< This info is used for both CoreEnabled & CoreEnabled2 fields
    ///< See detailed description in SMBIOS Spec v3.0 Section 7.5.7
    UINT16    EnabledCoreCount;
    ///< This info is used for both ThreadCount & ThreadCount2 fields
    ///< See detailed description in SMBIOS Spec v3.0 Section 7.5.8
    UINT16    ThreadCount;
    UINT16    ProcessorCharacteristics;    ///< Format defined in SMBIOS Spec v3.0 Section 7.5.9
    ///< String Buffer - each string terminated by NULL "0x00"
    ///< String buffer terminated by double NULL "0x0000"
} SMBIOS_PROCESSOR_INFO;

#define SMBIOS_FIRMWARE_VERSION_INFO_HOB_GUID \
    { 0x947c974a, 0xc5aa, 0x48a2, {0xa4, 0x77, 0x1a, 0x4c, 0x9f, 0x52, 0xe7, 0x82} }

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

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

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

///
/// Firmware Version Information HOB Structure
///
typedef struct {
    EFI_HOB_GUID_TYPE    Header;          ///< Offset 0-23   The header of FVI HOB
    SMBIOS_STRUCTURE     SmbiosData;      ///< Offset 24-27   The SMBIOS
    header of FVI HOB
    UINT8     Count;                      ///< Offset 28     Number of FVI elements
    included.
}

///
/// FIRMWARE_VERSION_INFO structures followed by the null terminated string buffer
///
} FIRMWARE_VERSION_INFO_HOB;

```

### 6.3 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

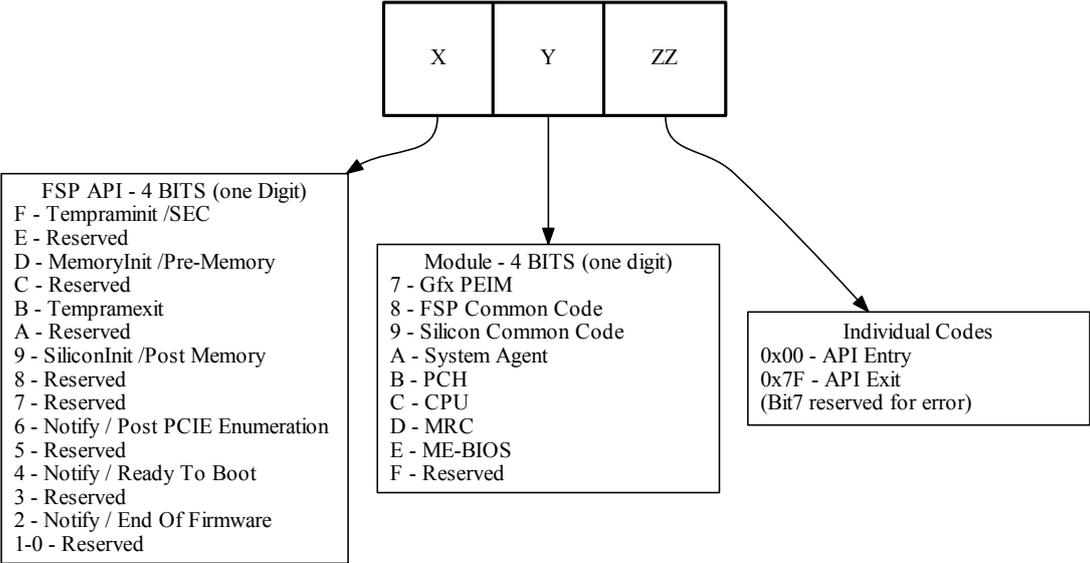
### 7 FSP PostCode

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

# FSP DISPATCH MODE

### 8 FSP Dispatch mode support

#### 8.1 Integration notes

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

Below are some integration notes:

1. Since FSP Binary can be integrated into anywhere in flash, boot loader has to report FSP FV to PEI and DXE dispatcher following standard way so those PEIMs and DXE drivers inside FSP Binary can be dispatched.
2. FSP binary package will include a DSC file which contains all DynamicEx PCDs consumed by FSP binary. Boot loader should incorporate the DSC and build those PCD into PCD database so same PCDs can be shared between boot loader and FSP.
3. In Dispatch mode, boot loader should not make FSP API calls. TempRamInit API is supported in both API mode and Dispatch mode, but rest of the APIs (MemoryInitApi, TempRamExitApi and SiliconInitApi) should not be invoked.
4. Dispatch mode FSP contains x64 DXE drivers for NotifyPhase callbacks. No thunkcall from 32bits to 64bits anymore and boot loader should remove S3EndOfPeiNotify and FspWrapperNotifyDxe as they are not used.
5. `EFI_PEI_CORE_FV_LOCATION_PPI` should be installed by boot loader SEC core and pointed to FSP-M FV location so the PeiCore inside FSP can be invoked. If this PPI was not installed or no PeiCore can be found by the pointer, the PeiCore from BFV will be invoked.
6. Some EDK2 overrides may be required for Dispatch mode support, please refer to override folders in reference code or the override EDK2 github repo for detail.



## Chapter 9

### Todo List

Member [FSP\\_S\\_RESTRICTED\\_CONFIG::PchPmTestPchClearPowerSts](#)  
ADD DESCRIPTION.



# Chapter 10

## Class Index

### 10.1 Class List

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

<a href="#">AUDIO_AZALIA_VERB_TABLE</a>	
Audio Azalia Verb Table structure . . . . .	35
<a href="#">AZALIA_HEADER</a>	
Azalia Header structure . . . . .	36
<a href="#">CHIPSET_INIT_INFO</a>	
The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC . . . . .	36
<a href="#">FIRMWARE_VERSION</a>	
Firmware Version Structure . . . . .	37
<a href="#">FIRMWARE_VERSION_INFO</a>	
Firmware Version Information Structure . . . . .	37
<a href="#">FIRMWARE_VERSION_INFO_HOB</a>	
Firmware Version Information HOB Structure . . . . .	38
<a href="#">FSP_M_CONFIG</a>	
Fsp M Configuration . . . . .	39
<a href="#">FSP_M_RESTRICTED_CONFIG</a>	
Fsp M Restricted Configuration . . . . .	106
<a href="#">FSP_S_CONFIG</a>	
Fsp S Configuration . . . . .	117
<a href="#">FSP_S_RESTRICTED_CONFIG</a>	
Fsp S Restricted Configuration . . . . .	212
<a href="#">FSP_T_CONFIG</a>	
Fsp T Configuration . . . . .	225
<a href="#">FSP_T_RESTRICTED_CONFIG</a>	
Fsp T Restricted Configuration . . . . .	227
<a href="#">FSPM_UPD</a>	
Fsp M UPD Configuration . . . . .	228
<a href="#">FSPS_UPD</a>	
Fsp S UPD Configuration . . . . .	228
<a href="#">FSPT_CORE_UPD</a>	
Fsp T Core UPD . . . . .	229
<a href="#">FSPT_UPD</a>	
Fsp T UPD Configuration . . . . .	230
<a href="#">GPIO_CONFIG</a>	
GPIO configuration structure used for pin programming . . . . .	231
<a href="#">SI_PCH_DEVICE_INTERRUPT_CONFIG</a>	
The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device . . . . .	233

**SMBIOS\_STRUCTURE**

The Smbios structure header . . . . . [234](#)

---

# Chapter 11

## File Index

### 11.1 File List

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

- [FirmwareVersionInfoHob.h](#)  
Header file for Firmware Version Information . . . . . 235
- [FspFixedPcds.h](#)  
This file lists all FixedAtBuild PCDs referenced in FSP integration guide . . . . . 236
- [FspInfoHob.h](#)  
Header file for FSP Information HOB . . . . . 236
- [FspmUpd.h](#)  
Copyright (c) 2019, Intel Corporation . . . . . 237
- [FspUpd.h](#)  
Copyright (c) 2018, Intel Corporation . . . . . 238
- [FspTUpd.h](#)  
Copyright (c) 2018, Intel Corporation . . . . . 241
- [FspUpd.h](#)  
Copyright (c) 2018, Intel Corporation . . . . . 242
- [GpioConfig.h](#)  
Header file for GpioConfig structure used by GPIO library . . . . . 243
- [GpioSampleDef.h](#)  
Sample enum definitions for GPIO table . . . . . 250



# Chapter 12

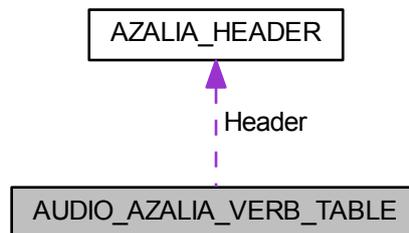
## Class Documentation

### 12.1 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.*

#### 12.1.1 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](#)

## 12.2 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.*

### 12.2.1 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](#)

## 12.3 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*
-

### 12.3.1 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](#)

## 12.4 FIRMWARE\_VERSION Struct Reference

Firmware Version Structure.

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

### 12.4.1 Detailed Description

Firmware Version Structure.

Definition at line 27 of file FirmwareVersionInfoHob.h.

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

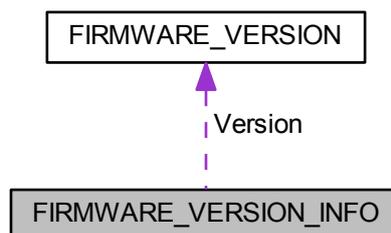
- [FirmwareVersionInfoHob.h](#)

## 12.5 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.*

### 12.5.1 Detailed Description

Firmware Version Information Structure.

Definition at line 37 of file FirmwareVersionInfoHob.h.

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

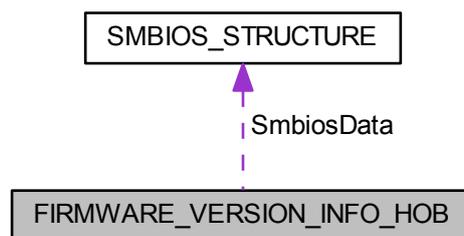
- [FirmwareVersionInfoHob.h](#)

## 12.6 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.*

### 12.6.1 Detailed Description

Firmware Version Information HOB Structure.

Definition at line 57 of file FirmwareVersionInfoHob.h.

### 12.6.2 Member Data Documentation

## 12.6.2.1 Count

```
UINT8 FIRMWARE_VERSION_INFO_HOB::Count
```

Offset 28 Number of FVI elements included.

Definition at line 60 of file FirmwareVersionInfoHob.h.

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

- [FirmwareVersionInfoHob.h](#)

## 12.7 FSP\_M\_CONFIG Struct Reference

Fsp M Configuration.

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

## Public Attributes

- [UINT32 MemorySpdPtr00](#)  
*Offset 0x0040 - Memory SPD Pointer Channel 0 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.*
- [UINT32 MemorySpdPtr01](#)  
*Offset 0x0044 - Memory SPD Pointer Channel 0 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.*
- [UINT32 MemorySpdPtr10](#)  
*Offset 0x0048 - Memory SPD Pointer Channel 1 Dimm 0 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.*
- [UINT32 MemorySpdPtr11](#)  
*Offset 0x004C - Memory SPD Pointer Channel 1 Dimm 1 Pointer to SPD data, will be used only when SpdAddress↔ Table SPD Address are marked as 00.*
- [UINT8 SpdAddressTable](#) [4]  
*Offset 0x0050 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.*
- [UINT16 MemorySpdDataLen](#)  
*Offset 0x0054 - SPD Data Length Length of SPD Data 0x100:256 Bytes, 0x200:512 Bytes.*
- [UINT8 DqByteMapCh0](#) [12]  
*Offset 0x0056 - Dq Byte Map CH0 Dq byte mapping between CPU and DRAM, Channel 0: board-dependent.*
- [UINT8 DqByteMapCh1](#) [12]  
*Offset 0x0062 - Dq Byte Map CH1 Dq byte mapping between CPU and DRAM, Channel 1: board-dependent.*
- [UINT8 DqsMapCpu2DramCh0](#) [8]  
*Offset 0x006E - Dqs Map CPU to DRAM CH 0 Set Dqs mapping relationship between CPU and DRAM, Channel 0: board-dependent.*
- [UINT8 DqsMapCpu2DramCh1](#) [8]  
*Offset 0x0076 - Dqs Map CPU to DRAM CH 1 Set Dqs mapping relationship between CPU and DRAM, Channel 1: board-dependent.*
- [UINT16 RcompResistor](#) [3]  
*Offset 0x007E - RcompResister settings Indicates RcompReister settings: Board-dependent.*
- [UINT16 RcompTarget](#) [5]  
*Offset 0x0084 - RcompTarget settings RcompTarget settings: board-dependent.*
- [UINT8 UnusedUpdSpace0](#) [2]  
*Offset 0x008E.*
- [UINT64 PlatformMemorySize](#)

- Offset 0x0090 - Platform Reserved Memory Size The minimum platform memory size required to pass control into DXE.*
- UINT8 [PcdSerialDebugLevel](#)  
*Offset 0x0098 - PcdSerialDebugLevel Serial Debug Message Level.*
  - UINT8 [CleanMemory](#)  
*Offset 0x0099 - Ask MRC to clear memory content Ask MRC to clear memory content 0: **Do not Clear Memory**; 1: Clear Memory.*
  - UINT8 [SmramMask](#)  
*Offset 0x009A - Smram Mask The SMM Regions AB-SEG and/or H-SEG reserved 0: Neither, 1:AB-SEG, 2:H-SEG, 3: Both.*
  - UINT8 [DqPinsInterleaved](#)  
*Offset 0x009B - Dqs Pins Interleaved Setting Indicates DqPinsInterleaved setting: board-dependent \$EN\_DIS.*
  - UINT8 [SaGv](#)  
*Offset 0x009C - SA GV System Agent dynamic frequency support and when enabled memory will be training at three different frequencies.*
  - UINT8 [UnusedUpdSpace1](#)  
*Offset 0x009D.*
  - UINT16 [DdrFreqLimit](#)  
*Offset 0x009E - DDR Frequency Limit Maximum Memory Frequency Selections in Mhz.*
  - UINT8 [DisableDimmChannel0](#)  
*Offset 0x00A0 - Channel A DIMM Control Channel A DIMM Control Support - Enable or Disable Dimms on Channel A.*
  - UINT8 [DisableDimmChannel1](#)  
*Offset 0x00A1 - Channel B DIMM Control Channel B DIMM Control Support - Enable or Disable Dimms on Channel B.*
  - UINT8 [MrcSafeConfig](#)  
*Offset 0x00A2 - MRC Safe Config Enables/Disable MRC Safe Config \$EN\_DIS.*
  - UINT8 [Lp4DqsOscEn](#)  
*Offset 0x00A3 - LPDDR4 Write DQ/DQS Retraining Enables/Disable LPDDR4 Write DQ/DQS Retraining \$EN\_DIS.*
  - UINT8 [TrainTrace](#)  
*Offset 0x00A4 - Training Trace This option enables the trained state tracing feature in MRC.*
  - UINT8 [RmtPerTask](#)  
*Offset 0x00A5 - Rank Margin Tool per Task This option enables the user to execute Rank Margin Tool per major training step in the MRC.*
  - UINT8 [LowSupplyEnData](#)  
*Offset 0x00A6 - LowSupplyEnData Enable: Enable Low Supply for LPDDR4 Data, Disable(Default) \$EN\_DIS.*
  - UINT8 [LowSupplyEnCcc](#)  
*Offset 0x00A7 - LowSupplyEnCcc Enable: Enable Low Supply for LPDDR4 Clock/Command/Control, Disable(Default) \$EN\_DIS.*
  - UINT8 [MemTestOnWarmBoot](#)  
*Offset 0x00A8 - Memory Test on Warm Boot Run Base Memory Test on Warm Boot 0:Disable, 1:Enable.*
  - UINT8 [UnusedUpdSpace2](#)  
*Offset 0x00A9.*
  - UINT16 [FreqSaGvLow](#)  
*Offset 0x00AA - Low Frequency SAGV Low Frequency Selections in Mhz.*
  - UINT16 [FreqSaGvMid](#)  
*Offset 0x00AC - Mid Frequency SAGV Mid Frequency Selections in Mhz.*
  - UINT8 [DdrSpeedControl](#)  
*Offset 0x00AE - DDR Speed Control DDR Frequency and Gear control for all SAGV points.*
  - UINT8 [SaGvLowGear2](#)  
*Offset 0x00AF - SA GV Low Gear Gear Selection for SAGV Low point 0:Gear1, 1:Gear2.*
  - UINT8 [SaGvMidGear2](#)
-

- Offset 0x00B0 - SA GV Mid Gear Gear Selection for SAGV Mid point 0:Gear1, 1:Gear2.*

    - UINT8 [SaGvHighGear2](#)
  - Offset 0x00B1 - SA GV High Gear Gear Selection for SAGV High point, or when SAGV is disabled 0:Gear1, 1:Gear2.*

    - UINT8 [ScramblerSupport](#)
  - Offset 0x00B2 - Scrambler Support This option enables data scrambling in memory.*

    - UINT8 [SafeMode](#)
  - Offset 0x00B3 - Safe Mode Support This option configures the various items in the IO and MC to be more conservative.*

    - UINT8 [Ddr4OneDpc](#)
  - Offset 0x00B4 - Ddr4OneDpc DDR4 1DPC performance feature for 2R DIMMs.*

    - UINT8 [ProbelessTrace](#)
  - Offset 0x00B5 - Probeless Trace Probeless Trace: 0=Disabled, 1=Enable.*

    - UINT8 [CaVrefConfig](#)
  - Offset 0x00B6 - VREF\_CA CA Vref routing: board-dependent 0:VREF\_CA goes to both CH\_A and CH\_B, 1: VREF\_CA to CH\_A and VREF\_DQ\_A to CH\_B, 2:VREF\_CA to CH\_A and VREF\_DQ\_B to CH\_B.*

    - UINT8 [SpdProfileSelected](#)
  - Offset 0x00B7 - SPD Profile Selected Select DIMM timing profile.*

    - UINT16 [VddVoltage](#)
  - Offset 0x00B8 - Memory Voltage Memory Voltage Override (Vddq).*

    - UINT8 [RefClk](#)
  - Offset 0x00BA - Memory Reference Clock 100MHz, 133MHz.*

    - UINT8 [Ratio](#)
  - Offset 0x00BB - Memory Ratio Automatic or the frequency will equal ratio times reference clock.*

    - UINT8 [tCL](#)
  - Offset 0x00BC - tCL CAS Latency, 0: AUTO, max: 31.*

    - UINT8 [tCWL](#)
  - Offset 0x00BD - tCWL Min CAS Write Latency Delay Time, 0: AUTO, max: 34.*

    - UINT16 [tFAW](#)
  - Offset 0x00BE - tFAW Min Four Activate Window Delay Time, 0: AUTO, max: 63.*

    - UINT16 [tRAS](#)
  - Offset 0x00C0 - tRAS RAS Active Time, 0: AUTO, max: 64.*

    - UINT8 [tRCDtRP](#)
  - Offset 0x00C2 - tRCD/tRP RAS to CAS delay time and Row Precharge delay time, 0: AUTO, max: 63.*

    - UINT8 [UnusedUpdSpace3](#)
  - Offset 0x00C3.*

    - UINT16 [tREFI](#)
  - Offset 0x00C4 - tREFI Refresh Interval, 0: AUTO, max: 65535.*

    - UINT16 [tRFC](#)
  - Offset 0x00C6 - tRFC Min Refresh Recovery Delay Time, 0: AUTO, max: 1023.*

    - UINT8 [tRRD](#)
  - Offset 0x00C8 - tRRD Min Row Active to Row Active Delay Time, 0: AUTO, max: 15.*

    - UINT8 [tRTP](#)
  - Offset 0x00C9 - tRTP Min Internal Read to Precharge Command Delay Time, 0: AUTO, max: 15.*

    - UINT8 [tWR](#)
  - Offset 0x00CA - tWR Min Write Recovery Time, 0: AUTO, legal values: 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 24, 30, 34, 40 0:Auto, 5:5, 6:6, 7:7, 8:8, 10:10, 12:12, 14:14, 16:16, 18:18, 20:20, 24:24, 30:30, 34:34, 40:40.*

    - UINT8 [tWTR](#)
  - Offset 0x00CB - tWTR Min Internal Write to Read Command Delay Time, 0: AUTO, max: 28.*

    - UINT8 [NModeSupport](#)
  - Offset 0x00CC - NMode System command rate, range 0-2, 0 means auto, 1 = 1N, 2 = 2N.*

    - UINT8 [DIIbWEn0](#)
  - Offset 0x00CD - DIIbWEn[0] DIIbWEn[0], for 1067 (0..7)*
-

- UINT8 [DIIbWEn1](#)  
*Offset 0x00CE - DIIbWEn[1] DIIbWEn[1], for 1333 (0..7)*
- UINT8 [DIIbWEn2](#)  
*Offset 0x00CF - DIIbWEn[2] DIIbWEn[2], for 1600 (0..7)*
- UINT8 [DIIbWEn3](#)  
*Offset 0x00D0 - DIIbWEn[3] DIIbWEn[3], for 1867 and up (0..7)*
- UINT8 [IsvtIoPort](#)  
*Offset 0x00D1 - ISVT IO Port Address ISVT IO Port Address.*
- UINT8 [HobBufferSize](#)  
*Offset 0x00D2 - HobBufferSize Size to set HOB Buffer.*
- UINT8 [ECT](#)  
*Offset 0x00D3 - Early Command Training Enables/Disable Early Command Training \$EN\_DIS.*
- UINT8 [SOT](#)  
*Offset 0x00D4 - SenseAmp Offset Training Enables/Disable SenseAmp Offset Training \$EN\_DIS.*
- UINT8 [ERDMPRTC2D](#)  
*Offset 0x00D5 - Early ReadMPR Timing Centering 2D Enables/Disable Early ReadMPR Timing Centering 2D \$EN\_DIS.*
- UINT8 [RDMPRT](#)  
*Offset 0x00D6 - Read MPR Training Enables/Disable Read MPR Training \$EN\_DIS.*
- UINT8 [RCVET](#)  
*Offset 0x00D7 - Receive Enable Training Enables/Disable Receive Enable Training \$EN\_DIS.*
- UINT8 [JWRL](#)  
*Offset 0x00D8 - Jedec Write Leveling Enables/Disable Jedec Write Leveling \$EN\_DIS.*
- UINT8 [EWRTC2D](#)  
*Offset 0x00D9 - Early Write Time Centering 2D Enables/Disable Early Write Time Centering 2D \$EN\_DIS.*
- UINT8 [ERDTC2D](#)  
*Offset 0x00DA - Early Read Time Centering 2D Enables/Disable Early Read Time Centering 2D \$EN\_DIS.*
- UINT8 [WRTC1D](#)  
*Offset 0x00DB - Write Timing Centering 1D Enables/Disable Write Timing Centering 1D \$EN\_DIS.*
- UINT8 [WRVC1D](#)  
*Offset 0x00DC - Write Voltage Centering 1D Enables/Disable Write Voltage Centering 1D \$EN\_DIS.*
- UINT8 [RDTC1D](#)  
*Offset 0x00DD - Read Timing Centering 1D Enables/Disable Read Timing Centering 1D \$EN\_DIS.*
- UINT8 [DIMMODTT](#)  
*Offset 0x00DE - Dimm ODT Training Enables/Disable Dimm ODT Training \$EN\_DIS.*
- UINT8 [DIMMFRONT](#)  
*Offset 0x00DF - DIMM RON Training Enables/Disable DIMM RON Training \$EN\_DIS.*
- UINT8 [WRSRT](#)  
*Offset 0x00E0 - Write Slew Rate Training Enables/Disable Write Slew Rate Training \$EN\_DIS.*
- UINT8 [RDODTT](#)  
*Offset 0x00E1 - Read ODT Training Enables/Disable Read ODT Training \$EN\_DIS.*
- UINT8 [RDEQT](#)  
*Offset 0x00E2 - Read Equalization Training Enables/Disable Read Equalization Training \$EN\_DIS.*
- UINT8 [RDAPT](#)  
*Offset 0x00E3 - Read Amplifier Training Enables/Disable Read Amplifier Training \$EN\_DIS.*
- UINT8 [WRTC2D](#)  
*Offset 0x00E4 - Write Timing Centering 2D Enables/Disable Write Timing Centering 2D \$EN\_DIS.*
- UINT8 [RDTC2D](#)  
*Offset 0x00E5 - Read Timing Centering 2D Enables/Disable Read Timing Centering 2D \$EN\_DIS.*
- UINT8 [WRVC2D](#)  
*Offset 0x00E6 - Write Voltage Centering 2D Enables/Disable Write Voltage Centering 2D \$EN\_DIS.*

- UINT8 [RDVC2D](#)  
*Offset 0x00E7 - Read Voltage Centering 2D Enables/Disable Read Voltage Centering 2D \$EN\_DIS.*
  - UINT8 [CMDVC](#)  
*Offset 0x00E8 - Command Voltage Centering Enables/Disable Command Voltage Centering \$EN\_DIS.*
  - UINT8 [LCT](#)  
*Offset 0x00E9 - Late Command Training Enables/Disable Late Command Training \$EN\_DIS.*
  - UINT8 [RTL](#)  
*Offset 0x00EA - Round Trip Latency Training Enables/Disable Round Trip Latency Training \$EN\_DIS.*
  - UINT8 [TAT](#)  
*Offset 0x00EB - Turn Around Timing Training Enables/Disable Turn Around Timing Training \$EN\_DIS.*
  - UINT8 [RCVENC1D](#)  
*Offset 0x00EC - Receive Enable Centering 1D Enables/Disable Receive Enable Centering 1D \$EN\_DIS.*
  - UINT8 [RMT](#)  
*Offset 0x00ED - Rank Margin Tool Enable/disable Rank Margin Tool.*
  - UINT8 [MarginLimitCheck](#)  
*Offset 0x00EE - Margin Limit Check Margin Limit Check.*
  - UINT8 [UnusedUpdSpace4](#)  
*Offset 0x00EF.*
  - UINT16 [MarginLimitL2](#)  
*Offset 0x00F0 - Margin Limit L2 % of L1 check for margin limit check.*
  - UINT8 [MEMTST](#)  
*Offset 0x00F2 - Memory Test Enables/Disable Memory Test \$EN\_DIS.*
  - UINT8 [ALIASCHK](#)  
*Offset 0x00F3 - DIMM SPD Alias Test Enables/Disable DIMM SPD Alias Test \$EN\_DIS.*
  - UINT8 [RMC](#)  
*Offset 0x00F4 - Retrain Margin Check Enables/Disable Retrain Margin Check \$EN\_DIS.*
  - UINT8 [WRDSUDT](#)  
*Offset 0x00F5 - Write Drive Strength Up/Dn independently Enables/Disable Write Drive Strength Up/Dn independently \$EN\_DIS.*
  - UINT8 [CMDSR](#)  
*Offset 0x00F6 - Command Slew Rate Training Enables/Disable Command Slew Rate Training \$EN\_DIS.*
  - UINT8 [CMDSEQ](#)  
*Offset 0x00F7 - Command Drive Strength and Equalization 2D Enables/Disable Command Drive Strength and Equalization 2D \$EN\_DIS.*
  - UINT8 [CMDNORM](#)  
*Offset 0x00F8 - Command Normalization Enables/Disable Command Normalization \$EN\_DIS.*
  - UINT8 [EWRDSEQ](#)  
*Offset 0x00F9 - Early DQ Write Drive Strength and Equalization Training Enables/Disable Early DQ Write Drive Strength and Equalization Training \$EN\_DIS.*
  - UINT8 [RDVC1D](#)  
*Offset 0x00FA - Read Voltage Centering Enables/Disable Read Voltage Centering \$EN\_DIS.*
  - UINT8 [TXTCO](#)  
*Offset 0x00FB - Write TCO Comp Training Enables/Disable Write TCO Comp Training \$EN\_DIS.*
  - UINT8 [CLKTCO](#)  
*Offset 0x00FC - Clock TCO Comp Training Enables/Disable Clock TCO Comp Training \$EN\_DIS.*
  - UINT8 [DIMMODTCA](#)  
*Offset 0x00FD - Dimm ODT CA Training Enables/Disable Dimm ODT CA Training \$EN\_DIS.*
  - UINT8 [TXTCODQS](#)  
*Offset 0x00FE - Write TCO Dqs Training Enables/Disable Write TCO Dqs Training \$EN\_DIS.*
  - UINT8 [DCC](#)  
*Offset 0x00FF - Duty Cycle Correction Enables/Disable Duty Cycle Correction \$EN\_DIS.*
-

- UINT8 [DQDFE](#)  
*Offset 0x0100 - DQ DFE Training Enable/Disable DQ DFE Training \$EN\_DIS.*
  - UINT8 [SOTC](#)  
*Offset 0x0101 - Sense Amplifier Correction Training Enable/Disable Sense Amplifier Correction Training \$EN\_DIS.*
  - UINT8 [EccSupport](#)  
*Offset 0x0102 - ECC Support Enables/Disable ECC Support \$EN\_DIS.*
  - UINT8 [RemapEnable](#)  
*Offset 0x0103 - Memory Remap Enables/Disable Memory Remap \$EN\_DIS.*
  - UINT8 [MrcTimeMeasure](#)  
*Offset 0x0104 - MRC Time Measure Enable/Disable MRC Time Measure \$EN\_DIS.*
  - UINT8 [MrcFastBoot](#)  
*Offset 0x0105 - MRC Fast Boot Enable/Disable MRC Fast flow \$EN\_DIS.*
  - UINT8 [MrcTrainOnWarm](#)  
*Offset 0x0106 - MRC Force Training on Warm Enables/Disable the MRC training on warm boot \$EN\_DIS.*
  - UINT8 [RankInterleave](#)  
*Offset 0x0107 - Rank Interleave support Enables/Disable Rank Interleave support.*
  - UINT8 [EnhancedInterleave](#)  
*Offset 0x0108 - Enhanced Interleave support Enables/Disable Enhanced Interleave support \$EN\_DIS.*
  - UINT8 [MemoryTrace](#)  
*Offset 0x0109 - Memory Trace Enable Memory Trace of Ch 0 to Ch 1 using Stacked Mode.*
  - UINT8 [ChHashEnable](#)  
*Offset 0x010A - Ch Hash Support Enable/Disable Channel Hash Support.*
  - UINT8 [EnableExtts](#)  
*Offset 0x010B - Extern Therm Status Enables/Disable Extern Therm Status \$EN\_DIS.*
  - UINT8 [EnableCltm](#)  
*Offset 0x010C - Closed Loop Therm Manage Enables/Disable Closed Loop Therm Manage \$EN\_DIS.*
  - UINT8 [EnableOltn](#)  
*Offset 0x010D - Open Loop Therm Manage Enables/Disable Open Loop Therm Manage \$EN\_DIS.*
  - UINT8 [EnablePwrDn](#)  
*Offset 0x010E - DDR PowerDown and idle counter Enables/Disable DDR PowerDown and idle counter \$EN\_DIS.*
  - UINT8 [EnablePwrDnLpddr](#)  
*Offset 0x010F - DDR PowerDown and idle counter - LPDDR Enables/Disable DDR PowerDown and idle counter(For LPDDR Only) \$EN\_DIS.*
  - UINT8 [UserPowerWeightsEn](#)  
*Offset 0x0110 - Use user provided power weights, scale factor, and channel power floor values Enables/Disable Use user provided power weights, scale factor, and channel power floor values \$EN\_DIS.*
  - UINT8 [RaplLim2Lock](#)  
*Offset 0x0111 - RAPL PL Lock Enables/Disable RAPL PL Lock \$EN\_DIS.*
  - UINT8 [RaplLim2Ena](#)  
*Offset 0x0112 - RAPL PL 2 enable Enables/Disable RAPL PL 2 enable \$EN\_DIS.*
  - UINT8 [RaplLim1Ena](#)  
*Offset 0x0113 - RAPL PL 1 enable Enables/Disable RAPL PL 1 enable \$EN\_DIS.*
  - UINT8 [SrefCfgEna](#)  
*Offset 0x0114 - SelfRefresh Enable Enables/Disable SelfRefresh Enable \$EN\_DIS.*
  - UINT8 [ThrtCkeMinDefeatLpddr](#)  
*Offset 0x0115 - Throttler CKEMin Defeature - LPDDR Enables/Disable Throttler CKEMin Defeature(For LPDDR Only) \$EN\_DIS.*
  - UINT8 [ThrtCkeMinDefeat](#)  
*Offset 0x0116 - Throttler CKEMin Defeature Enables/Disable Throttler CKEMin Defeature \$EN\_DIS.*
  - UINT8 [RhPrevention](#)  
*Offset 0x0117 - Enable RH Prevention Enables/Disable RH Prevention \$EN\_DIS.*
-

- UINT8 [ExitOnFailure](#)  
*Offset 0x0118 - Exit On Failure (MRC) Enables/Disable Exit On Failure (MRC) \$EN\_DIS.*
  - UINT8 [DdrThermalSensor](#)  
*Offset 0x0119 - LPDDR Thermal Sensor Enables/Disable LPDDR Thermal Sensor \$EN\_DIS.*
  - UINT8 [Ddr4DdpSharedClock](#)  
*Offset 0x011A - 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 0x011B - 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.*
  - UINT32 [BClkFrequency](#)  
*Offset 0x011C - Base reference clock value Base reference clock value, in Hertz(Default is 125Hz) 10000000:100Hz, 125000000:125Hz, 167000000:167Hz, 250000000:250Hz.*
  - UINT8 [ChHashInterleaveBit](#)  
*Offset 0x0120 - Ch Hash Interleaved Bit Select the BIT to be used for Channel Interleaved mode.*
  - UINT8 [UnusedUpdSpace5](#)  
*Offset 0x0121.*
  - UINT16 [ChHashMask](#)  
*Offset 0x0122 - Ch Hash Mask Set the BIT(s) to be included in the XOR function.*
  - UINT8 [ExtendedBankHashing](#)  
*Offset 0x0124 - Extended Bank Hashing Enable/Disable ExtendedBankHashing \$EN\_DIS.*
  - UINT8 [EnergyScaleFact](#)  
*Offset 0x0125 - Energy Scale Factor Energy Scale Factor, Default is 4.*
  - UINT16 [Idd3n](#)  
*Offset 0x0126 - EPG DIMM Idd3N Active standby current (Idd3N) in milliamps from datasheet.*
  - UINT16 [Idd3p](#)  
*Offset 0x0128 - EPG DIMM Idd3P Active power-down current (Idd3P) in milliamps from datasheet.*
  - UINT8 [RhActProbability](#)  
*Offset 0x012A - RH Activation Probability RH Activation Probability, Probability value is  $1/2^y$  (inputvalue)*
  - UINT8 [RaplLim2WindX](#)  
*Offset 0x012B - RAPL PL 2 WindowX Power PL 2 time window X value,  $(1/1024)*(1+(x/4))*2^y$  (0=Def)*
  - UINT8 [RaplLim2WindY](#)  
*Offset 0x012C - RAPL PL 2 WindowY Power PL 2 time window Y value,  $(1/1024)*(1+(x/4))*2^y$  (0=Def)*
  - UINT8 [RaplLim1WindX](#)  
*Offset 0x012D - RAPL PL 1 WindowX Power PL 1 time window X value,  $(1/1024)*(1+(x/4))*2^y$  (0=Def)*
  - UINT8 [RaplLim1WindY](#)  
*Offset 0x012E - RAPL PL 1 WindowY Power PL 1 time window Y value,  $(1/1024)*(1+(x/4))*2^y$  (0=Def)*
  - UINT8 [UnusedUpdSpace6](#)  
*Offset 0x012F.*
  - UINT16 [RaplLim2Pwr](#)  
*Offset 0x0130 - RAPL PL 2 Power range $[0;2^{14}-1]=[2047.875;0]$ in W, (224= Def)*
  - UINT16 [RaplLim1Pwr](#)  
*Offset 0x0132 - RAPL PL 1 Power range $[0;2^{14}-1]=[2047.875;0]$ in W, (224= Def)*
  - UINT8 [WarmThresholdCh0Dimm0](#)  
*Offset 0x0134 - Warm Threshold Ch0 Dimm0 range $[255;0]=[31.875;0]$  in W for OLTM,  $[127.5;0]$  in C for CLTM.*
  - UINT8 [WarmThresholdCh0Dimm1](#)  
*Offset 0x0135 - Warm Threshold Ch0 Dimm1 range $[255;0]=[31.875;0]$  in W for OLTM,  $[127.5;0]$  in C for CLTM.*
  - UINT8 [WarmThresholdCh1Dimm0](#)  
*Offset 0x0136 - Warm Threshold Ch1 Dimm0 range $[255;0]=[31.875;0]$  in W for OLTM,  $[127.5;0]$  in C for CLTM.*
  - UINT8 [WarmThresholdCh1Dimm1](#)  
*Offset 0x0137 - Warm Threshold Ch1 Dimm1 range $[255;0]=[31.875;0]$  in W for OLTM,  $[127.5;0]$  in C for CLTM.*
-

- UINT8 [HotThresholdCh0Dimm0](#)  
*Offset 0x0138 - Hot Threshold Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotThresholdCh0Dimm1](#)  
*Offset 0x0139 - Hot Threshold Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotThresholdCh1Dimm0](#)  
*Offset 0x013A - Hot Threshold Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotThresholdCh1Dimm1](#)  
*Offset 0x013B - Hot Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [WarmBudgetCh0Dimm0](#)  
*Offset 0x013C - Warm Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [WarmBudgetCh0Dimm1](#)  
*Offset 0x013D - Warm Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [WarmBudgetCh1Dimm0](#)  
*Offset 0x013E - Warm Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [WarmBudgetCh1Dimm1](#)  
*Offset 0x013F - Warm Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotBudgetCh0Dimm0](#)  
*Offset 0x0140 - Hot Budget Ch0 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotBudgetCh0Dimm1](#)  
*Offset 0x0141 - Hot Budget Ch0 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotBudgetCh1Dimm0](#)  
*Offset 0x0142 - Hot Budget Ch1 Dimm0 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [HotBudgetCh1Dimm1](#)  
*Offset 0x0143 - Hot Budget Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTM, [127.5;0] in C for CLTM.*
  - UINT8 [IdleEnergyCh0Dimm0](#)  
*Offset 0x0144 - Idle Energy Ch0Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)*
  - UINT8 [IdleEnergyCh0Dimm1](#)  
*Offset 0x0145 - Idle Energy Ch0Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)*
  - UINT8 [IdleEnergyCh1Dimm0](#)  
*Offset 0x0146 - Idle Energy Ch1Dimm0 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)*
  - UINT8 [IdleEnergyCh1Dimm1](#)  
*Offset 0x0147 - Idle Energy Ch1Dimm1 Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def)*
  - UINT8 [PdEnergyCh0Dimm0](#)  
*Offset 0x0148 - PowerDown Energy Ch0Dimm0 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)*
  - UINT8 [PdEnergyCh0Dimm1](#)  
*Offset 0x0149 - PowerDown Energy Ch0Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)*
  - UINT8 [PdEnergyCh1Dimm0](#)  
*Offset 0x014A - PowerDown Energy Ch1Dimm0 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)*
  - UINT8 [PdEnergyCh1Dimm1](#)  
*Offset 0x014B - PowerDown Energy Ch1Dimm1 PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(5= Def)*
  - UINT8 [ActEnergyCh0Dimm0](#)  
*Offset 0x014C - Activate Energy Ch0Dimm0 Activate Energy Contribution, range[255;0],(172= Def)*
  - UINT8 [ActEnergyCh0Dimm1](#)  
*Offset 0x014D - Activate Energy Ch0Dimm1 Activate Energy Contribution, range[255;0],(172= Def)*
  - UINT8 [ActEnergyCh1Dimm0](#)  
*Offset 0x014E - Activate Energy Ch1Dimm0 Activate Energy Contribution, range[255;0],(172= Def)*
  - UINT8 [ActEnergyCh1Dimm1](#)
-

- Offset 0x014F - Activate Energy Ch1Dimm1 Activate Energy Contribution, range[255;0],(172= Def)*

    - UINT8 [RdEnergyCh0Dimm0](#)
  - Offset 0x0150 - Read Energy Ch0Dimm0 Read Energy Contribution, range[255;0],(212= Def)*

    - UINT8 [RdEnergyCh0Dimm1](#)
  - Offset 0x0151 - Read Energy Ch0Dimm1 Read Energy Contribution, range[255;0],(212= Def)*

    - UINT8 [RdEnergyCh1Dimm0](#)
  - Offset 0x0152 - Read Energy Ch1Dimm0 Read Energy Contribution, range[255;0],(212= Def)*

    - UINT8 [RdEnergyCh1Dimm1](#)
  - Offset 0x0153 - Read Energy Ch1Dimm1 Read Energy Contribution, range[255;0],(212= Def)*

    - UINT8 [WrEnergyCh0Dimm0](#)
  - Offset 0x0154 - Write Energy Ch0Dimm0 Write Energy Contribution, range[255;0],(221= Def)*

    - UINT8 [WrEnergyCh0Dimm1](#)
  - Offset 0x0155 - Write Energy Ch0Dimm1 Write Energy Contribution, range[255;0],(221= Def)*

    - UINT8 [WrEnergyCh1Dimm0](#)
  - Offset 0x0156 - Write Energy Ch1Dimm0 Write Energy Contribution, range[255;0],(221= Def)*

    - UINT8 [WrEnergyCh1Dimm1](#)
  - Offset 0x0157 - Write Energy Ch1Dimm1 Write Energy Contribution, range[255;0],(221= Def)*

    - UINT8 [ThrtCkeMinTmr](#)
  - Offset 0x0158 - Throttler CKEMin Timer Timer value for CKEMin, range[255;0].*

    - UINT8 [CkeRankMapping](#)
  - Offset 0x0159 - Cke Rank Mapping Bits [7:4] - Channel 1, bits [3:0] - Channel 0.*

    - UINT8 [RaplPwrFICh0](#)
  - Offset 0x015A - Rapl Power Floor Ch0 Power budget ,range[255;0],(0= 5.3W Def)*

    - UINT8 [RaplPwrFICh1](#)
  - Offset 0x015B - Rapl Power Floor Ch1 Power budget ,range[255;0],(0= 5.3W Def)*

    - UINT8 [EnCmdRate](#)
  - Offset 0x015C - Command Rate Support CMD Rate and Limit Support Option.*

    - UINT8 [Refresh2X](#)
  - Offset 0x015D - 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 0x015E - Energy Performance Gain Enable/disable(default) Energy Performance Gain.*

    - UINT8 [RhSolution](#)
  - Offset 0x015F - Row Hammer Solution Type of method used to prevent Row Hammer.*

    - UINT8 [UserThresholdEnable](#)
  - Offset 0x0160 - User Manual Threshold Disabled: Predefined threshold will be used.*

    - UINT8 [UserBudgetEnable](#)
  - Offset 0x0161 - User Manual Budget Disabled: Configuration of memories will defined the Budget value.*

    - UINT8 [TsodTcritMax](#)
  - Offset 0x0162 - TcritMax Maximum Critical Temperature in Centigrade of the On-DIMM Thermal Sensor.*

    - UINT8 [TsodEventMode](#)
  - Offset 0x0163 - Event mode Disable:Comparator mode.*

    - UINT8 [TsodEventPolarity](#)
  - Offset 0x0164 - EVENT polarity Disable:Active LOW.*

    - UINT8 [TsodCriticalEventOnly](#)
  - Offset 0x0165 - Critical event only Disable:Trips on alarm or critical.*

    - UINT8 [TsodEventOutputControl](#)
  - Offset 0x0166 - Event output control Disable:Event output disable.*

    - UINT8 [TsodAlarmwindowLockBit](#)
  - Offset 0x0167 - Alarm window lock bit Disable:Alarm trips are not locked and can be changed.*

    - UINT8 [TsodCriticaltripLockBit](#)
-

- Offset 0x0168 - Critical trip lock bit Disable:Critical trip is not locked and can be changed.*

    - UINT8 [TsodShutdownMode](#)
  - Offset 0x0169 - Shutdown mode Disable:Temperature sensor enable.*

    - UINT8 [TsodThighMax](#)
  - Offset 0x016A - ThighMax Thigh = ThighMax (Default is 93)*

    - UINT8 [TsodManualEnable](#)
  - Offset 0x016B - User Manual Thigh and Tcrit Disabled(Default): Temperature will be given by the configuration of memories and 1x or 2xrefresh rate.*

    - UINT8 [ForceOltmOrRefresh2x](#)
  - Offset 0x016C - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.*

    - UINT8 [PwdownIdleCounter](#)
  - Offset 0x016D - Pwr Down Idle Timer The minimum value should = to the worst case Roundtrip delay + Burst\_Length.*

    - UINT8 [CmdRanksTerminated](#)
  - Offset 0x016E - Bitmask of ranks that have CA bus terminated Offset 225 LPDDR4: Bitmask of ranks that have CA bus terminated.*

    - UINT8 [RMTLoopCount](#)
  - Offset 0x016F - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.*

    - UINT8 [ThrtCkeMinTmrLpddr](#)
  - Offset 0x0170 - Throttler CKEMin Timer for LPDDR LPDDR Timer value for CKEMin, range[255;0].*

    - UINT8 [RetrainOnFastFail](#)
  - Offset 0x0171 - Retrain on Fast Fail Restart MRC in Cold mode if SW MemTest fails during Fast flow.*

    - UINT8 [RMTBIT](#)
  - Offset 0x0172 - Rank Margin Tool Per Bit Enable/disable Rank Margin Tool Per Bit.*

    - UINT8 [RDTOPT](#)
  - Offset 0x0173 - Read Timing Optimization Enables/Disable Read Timing Optimization \$EN\_DIS.*

    - UINT8 [MrcPreMemRsvd](#) [13]
  - Offset 0x0174.*

    - UINT8 [OcSupport](#)
  - Offset 0x0181 - Over clocking support Over clocking support; **0: Disable**; 1: Enable \$EN\_DIS.*

    - UINT8 [OcLock](#)
  - Offset 0x0182 - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.*

    - UINT8 [CoreMaxOcRatio](#)
  - Offset 0x0183 - 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 0x0184 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.*

    - UINT8 [RingMaxOcRatio](#)
  - Offset 0x0185 - Maximum clr turbo ratio override Maximum clr turbo ratio override allows to increase CPU clr frequency beyond the fused max turbo ratio limit.*

    - UINT8 [RingDownBin](#)
  - Offset 0x0186 - Ring Downbin Ring Downbin enable/disable.*

    - UINT8 [RingVoltageMode](#)
  - Offset 0x0187 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.*

    - UINT16 [RingVoltageOverride](#)
  - Offset 0x0188 - Ring voltage override The ring voltage override which is applied to the entire range of cpu ring frequencies.*

    - UINT16 [RingVoltageAdaptive](#)
  - Offset 0x018A - Ring Turbo voltage Adaptive Extra Turbo voltage applied to the cpu ring when the cpu is operating in turbo mode.*

    - UINT16 [RingVoltageOffset](#)
  - Offset 0x018C - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.*

    - UINT16 [CoreVoltageOverride](#)
-

- Offset 0x018E - core voltage override The core voltage override which is applied to the entire range of cpu core frequencies.*
- UINT16 [CoreVoltageAdaptive](#)  
*Offset 0x0190 - Core Turbo voltage Adaptive Extra Turbo voltage applied to the cpu core when the cpu is operating in turbo mode.*
  - UINT16 [CoreVoltageOffset](#)  
*Offset 0x0192 - Core Turbo voltage Offset The voltage offset applied to the core while operating in turbo mode. Valid Range 0 to 1000.*
  - UINT8 [CorePllVoltageOffset](#)  
*Offset 0x0194 - Core PLL voltage offset Core PLL voltage offset.*
  - UINT8 [GtPllVoltageOffset](#)  
*Offset 0x0195 - GT PLL voltage offset Core PLL voltage offset.*
  - UINT8 [RingPllVoltageOffset](#)  
*Offset 0x0196 - Ring PLL voltage offset Core PLL voltage offset.*
  - UINT8 [SaPllVoltageOffset](#)  
*Offset 0x0197 - System Agent PLL voltage offset Core PLL voltage offset.*
  - UINT8 [McPllVoltageOffset](#)  
*Offset 0x0198 - Memory Controller PLL voltage offset Core PLL voltage offset.*
  - UINT8 [BclkAdaptiveVoltage](#)  
*Offset 0x0199 - BCLK Adaptive Voltage Enable When enabled, the CPU V/F curves are aware of BCLK frequency when calculated.*
  - UINT8 [Avx2RatioOffset](#)  
*Offset 0x019A - AVX2 Ratio Offset 0(Default)= No Offset.*
  - UINT8 [Avx3RatioOffset](#)  
*Offset 0x019B - AVX3 Ratio Offset 0(Default)= No Offset.*
  - UINT8 [TjMaxOffset](#)  
*Offset 0x019C - TjMax Offset TjMax offset. Specified value here is clipped by pCode (125 - TjMax Offset) to support TjMax in the range of 62 to 115 deg Celsius.*
  - UINT8 [FivrFaults](#)  
*Offset 0x019D - Fivr Faults Fivr Faults; 0: Disabled; 1: **Enabled**.*
  - UINT8 [FivrEfficiency](#)  
*Offset 0x019E - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; 1: **Enabled**.*
  - UINT8 [UnusedUpdSpace7](#)  
*Offset 0x019F.*
  - UINT16 [VcclnVoltageOverride](#)  
*Offset 0x01A0 - Vccln Voltage Override This will override Vccln output voltage level to the voltage value specified.*
  - UINT8 [Avx2VoltageScaleFactor](#)  
*Offset 0x01A2 - Avx2 Voltage Guardband Scaling Factor AVX2 Voltage Guardband Scale factor applied to AVX2 workloads.*
  - UINT8 [Avx512VoltageScaleFactor](#)  
*Offset 0x01A3 - Avx512 Voltage Guardband Scaling Factor AVX512 Voltage Guardband Scale factor applied to AVX512 workloads.*
  - UINT8 [NonCoreHighVoltageMode](#)  
*Offset 0x01A4 - Non-Core High Voltage Mode Enable High Voltage Mode in the non-core FIVR domains (Ring/GT).*
  - UINT8 [CoreHighVoltageMode](#)  
*Offset 0x01A5 - Core High Voltage Mode Enable High Voltage Mode in the core FIVR Domains.*
  - UINT8 [PerCoreRatioLimit](#) [8]  
*Offset 0x01A6 - Per Core Ratio Limit Per Core Ratio Limit.*
  - UINT8 [FivrTdc](#)  
*Offset 0x01AE - FIVR TDC Enable or Disable FIVR TDC from PCODE.*
  - UINT8 [FullRangeMultiplierUnlockEn](#)
-

- Offset 0x01AF - Full Range Multiplier unlock enable Enable or Disable communication between Punit and Core in 100MHz granularity.
- UINT8 [SaPllFreqOverride](#)  
Offset 0x01B0 - SA PLL Freq override Enable or Disable SA PLL Freq override to 1600MHz instead of 3200MHz on Desktop.
  - UINT8 [XhciPllOverride](#)  
Offset 0x01B1 - XHCI PLL override Enable or Disable XHCI PLL override to use TMU PLL instead of SA PLL.
  - UINT8 [FivrPs](#)  
Offset 0x01B2 - FIVR PS Enable or Disable FIVR PS.
  - UINT8 [FivrProtection](#)  
Offset 0x01B3 - FIVR PROTECTION Enable or Disable FIVR overvoltage and overcurrent protection.
  - UINT8 [TschwFixup](#)  
Offset 0x01B4 - TSC HW Fixup Enable or Disable Core HW Fixup during TSC copy from PMA and APIC.
  - UINT8 [UnusedUpdSpace8](#)  
Offset 0x01B5.
  - UINT16 [VccinVrMaxVoltage](#)  
Offset 0x01B6 - VccIN VR MAX Voltage The new VccIN VR MAX Voltage to allow requesting in U3.13V format.
  - UINT8 [PvdRatioThreshold](#)  
Offset 0x01B8 - Post Divider (PVD) Ratio Threshold PVD Ratio Threshold.
  - UINT8 [HyperThreading](#)  
Offset 0x01B9 - Hyper Threading Enable/Disable Enable or Disable Hyper Threading; 0: Disable; **1: Enable** \$EN\_↔ DIS.
  - UINT8 [BootFrequency](#)  
Offset 0x01BA - Boot frequency Sets the boot frequency starting from reset vector.
  - UINT8 [ActiveCoreCount](#)  
Offset 0x01BB - Number of active cores Number of active cores(Depends on Number of cores).
  - UINT8 [FclkFrequency](#)  
Offset 0x01BC - Processor Early Power On Configuration FCLK setting **0: 800 MHz (ULT/ULX)**.
  - UINT8 [JtagC10PowerGateDisable](#)  
Offset 0x01BD - Set JTAG power in C10 and deeper power states False: JTAG is power gated in C10 state.
  - UINT8 [BistOnReset](#)  
Offset 0x01BE - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.
  - UINT8 [VmxEnable](#)  
Offset 0x01BF - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable**.
  - UINT8 [CpuRatio](#)  
Offset 0x01C0 - CPU ratio value CPU ratio value.
  - UINT8 [TmeEnable](#)  
Offset 0x01C1 - Enable or Disable TME Enable or Disable TME; **0: Disable**; 1: Enable.
  - UINT8 [CpuCrashLogEnable](#)  
Offset 0x01C2 - Enable CPU CrashLog Enable or Disable CPU CrashLog; 0: Disable; **1: Enable**.
  - UINT8 [DebugInterfaceEnable](#)  
Offset 0x01C3 - 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 0x01C4 - CPU Run Control Lock Lock or Unlock CPU Run Control; 0: Disable; **1: Enable**.
  - UINT8 [SkipMplnitPreMem](#)  
Offset 0x01C5 - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SilicionInit API.
  - UINT8 [CpuPreMemRsvd](#) [13]  
Offset 0x01C6.
  - UINT8 [SkipStopPbet](#)  
Offset 0x01D3 - Skip Stop PBET Timer Enable/Disable Skip Stop PBET Timer; **0: Disable**; 1: Enable \$EN\_DIS.
-

- UINT8 [EnableC6Dram](#)  
*Offset 0x01D4 - C6DRAM power gating feature This policy indicates whether or not BIOS should allocate PRMRR memory for C6DRAM power gating feature.*
  - UINT8 [BiosGuard](#)  
*Offset 0x01D5 - BiosGuard Enable/Disable.*
  - UINT8 [BiosGuardToolsInterface](#)  
*Offset 0x01D6.*
  - UINT8 [EnableSgx](#)  
*Offset 0x01D7 - EnableSgx Enable/Disable.*
  - UINT8 [Txt](#)  
*Offset 0x01D8 - Txt Enable/Disable.*
  - UINT8 [UnusedUpdSpace9](#) [3]  
*Offset 0x01D9.*
  - UINT32 [PrmrrSize](#)  
*Offset 0x01DC - PrmrrSize Enable/Disable.*
  - UINT8 [TxtAcheckRequest](#)  
*Offset 0x01E0 - TxtAcheckRequest Enable/Disable.*
  - UINT8 [UnusedUpdSpace10](#)  
*Offset 0x01E1.*
  - UINT16 [BiosSize](#)  
*Offset 0x01E2 - BiosSize Enable/Disable.*
  - UINT32 [SinitMemorySize](#)  
*Offset 0x01E4 - SinitMemorySize Enable/Disable.*
  - UINT32 [TxtHeapMemorySize](#)  
*Offset 0x01E8 - TxtHeapMemorySize Enable/Disable.*
  - UINT8 [UnusedUpdSpace11](#) [4]  
*Offset 0x01EC.*
  - UINT64 [TxtDprMemoryBase](#)  
*Offset 0x01F0 - TxtDprMemoryBase Enable/Disable.*
  - UINT32 [TxtDprMemorySize](#)  
*Offset 0x01F8 - TxtDprMemorySize Enable/Disable.*
  - UINT32 [BiosAcmBase](#)  
*Offset 0x01FC - BiosAcmBase Enable/Disable.*
  - UINT32 [BiosAcmSize](#)  
*Offset 0x0200 - BiosAcmSize Enable/Disable.*
  - UINT32 [TgaSize](#)  
*Offset 0x0204 - TgaSize Enable/Disable.*
  - UINT64 [TxtLcpPdBase](#)  
*Offset 0x0208 - TxtLcpPdBase Enable/Disable.*
  - UINT64 [TxtLcpPdSize](#)  
*Offset 0x0210 - TxtLcpPdSize Enable/Disable.*
  - UINT32 [ApStartupBase](#)  
*Offset 0x0218 - ApStartupBase Enable/Disable.*
  - UINT8 [IsTPMPresence](#)  
*Offset 0x021C - IsTPMPresence IsTPMPresence default values.*
  - UINT8 [SecurityPreMemRsvd](#) [16]  
*Offset 0x021D.*
  - UINT8 [UnusedUpdSpace12](#) [3]  
*Offset 0x022D.*
  - UINT32 [ledSize](#)
-

- Offset 0x0230 - Intel Enhanced Debug Intel Enhanced Debug (IED): 0=Disabled, 0x400000=Enabled and 4MB S←  
MRAM occupied 0 : Disable, 0x400000 : Enable.
- UINT8 [UserBd](#)

Offset 0x0234 - Board Type MrcBoardType, Options are 0=Mobile/Mobile Halo, 1=Desktop/DT Halo, 5=ULT/ULX/←  
Mobile Halo, 7=UP Server 0:Mobile/Mobile Halo, 1:Desktop/DT Halo, 5:ULT/ULX/Mobile Halo, 7:UP Server.
  - UINT8 [X2ApicOptOut](#)

Offset 0x0235 - State of X2APIC\_OPT\_OUT bit in the DMAR table 0=Disable/Clear, 1=Enable/Set \$EN\_DIS.
  - UINT8 [DmaControlGuarantee](#)

Offset 0x0236 - State of DMA\_CONTROL\_GUARANTEE bit in the DMAR table 0=Disable/Clear, 1=Enable/Set \$E←  
N\_DIS.
  - UINT8 [UnusedUpdSpace13](#) [1]

Offset 0x0237.
  - UINT32 [VtdBaseAddress](#) [9]

Offset 0x0238 - Base addresses for VT-d function MMIO access Base addresses for VT-d MMIO access per VT-d  
engine.
  - UINT8 [VtdDisable](#)

Offset 0x025C - Disable VT-d 0=Enable/FALSE(VT-d enabled), 1=Disable/TRUE (VT-d disabled) \$EN\_DIS.
  - UINT8 [IgdDvmt50PreAlloc](#)

Offset 0x025D - Internal Graphics Pre-allocated Memory Size of memory preallocated for internal graphics.
  - UINT8 [InternalGfx](#)

Offset 0x025E - Internal Graphics Enable/disable internal graphics.
  - UINT8 [ApertureSize](#)

Offset 0x025F - Aperture Size Select the Aperture Size.
  - UINT8 [PrimaryDisplay](#)

Offset 0x0260 - Selection of the primary display device 0=iGFX, 1=PEG, 2=PCIe Graphics on PCH, 3(Default)=AUTO,  
4=Hybrid Graphics 0:iGFX, 1:PEG, 2:PCIe Graphics on PCH, 3:AUTO, 4:Hybrid Graphics.
  - UINT8 [UnusedUpdSpace14](#) [3]

Offset 0x0261.
  - UINT32 [GttMmAdr](#)

Offset 0x0264 - Temporary MMIO address for GTTMMADR The reference code will use this as Temporary MM←  
IO address space to access GTTMMADR Registers.Platform should provide conflict free Temporary MMIO Range:  
GttMmAdr to (GttMmAdr + 2MB MMIO + 6MB Reserved + GttSize).
  - UINT32 [GmAdr](#)

Offset 0x0268 - 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).
  - UINT16 [GttSize](#)

Offset 0x026C - Selection of iGFX GTT Memory size 1=2MB, 2=4MB, 3=8MB, Default is 3 1:2MB, 2:4MB, 3:8MB.
  - UINT8 [PsmiRegionSize](#)

Offset 0x026E - 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 [GtPsmiSupport](#)

Offset 0x026F - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.
  - UINT8 [PanelPowerEnable](#)

Offset 0x0270 - Panel Power Enable Control for enabling/disabling VDD force bit (Required only for early enabling of  
eDP panel).
  - UINT8 [RootPortIndex](#)

Offset 0x0271 - PCIe root port Function number for Hybrid Graphics dGPU Root port Index number to indicate which  
PCIe root port has dGPU.
  - UINT8 [UnusedUpdSpace15](#) [2]

Offset 0x0272.
  - UINT32 [SaRtd3Pcie0Gpio](#) [24]
-

- Offset 0x0274 - Hybrid Graphics GPIO information for PEG 0 Switchable Graphics GPIO information for PEG 0, for Reset, power and wake GPIOs.*
- UINT32 [SaRtd3Pcie1Gpio](#) [24]
 

*Offset 0x02D4 - Hybrid Graphics GPIO information for PEG 1 Hybrid Graphics GPIO information for PEG 1, for Reset, power and wake GPIOs.*
  - UINT32 [SaRtd3Pcie2Gpio](#) [24]
 

*Offset 0x0334 - Hybrid Graphics GPIO information for PEG 2 Hybrid Graphics GPIO information for PEG 2, for Reset, power and wake GPIOs.*
  - UINT32 [SaRtd3Pcie3Gpio](#) [24]
 

*Offset 0x0394 - Hybrid Graphics GPIO information for PEG 3 Hybrid Graphics GPIO information for PEG 3, for Reset, power and wake GPIOs.*
  - UINT16 [HgDelayAfterPwrEn](#)

*Offset 0x03F4 - HG dGPU Power Delay HG dGPU delay interval after power enabling: 0=Minimal, 1000=Maximum, default is 300=300 microseconds.*
  - UINT16 [HgDelayAfterHoldReset](#)

*Offset 0x03F6 - HG dGPU Reset Delay HG dGPU delay interval for Reset complete: 0=Minimal, 1000=Maximum, default is 100=100 microseconds.*
  - UINT16 [MmioSizeAdjustment](#)

*Offset 0x03F8 - 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.*
  - UINT16 [MmioSize](#)

*Offset 0x03FA - MMIO Size Size of MMIO space reserved for devices.*
  - UINT32 [TsegSize](#)

*Offset 0x03FC - Tseg Size Size of SMRAM memory reserved.*
  - UINT8 [TxtImplemented](#)

*Offset 0x0400 - Enable/Disable MRC TXT dependency When enabled MRC execution will wait for TXT initialization to be done first.*
  - UINT8 [SkipExtGfxScan](#)

*Offset 0x0401 - Skip external display device scanning Enable: Do not scan for external display device, Disable (Default): Scan external display devices \$EN\_DIS.*
  - UINT8 [BdatEnable](#)

*Offset 0x0402 - Generate BIOS Data ACPI Table Enable: Generate BDAT for MRC RMT or SA PCIe data.*
  - UINT8 [BdatTestType](#)

*Offset 0x0403 - BdatTestType Indicates the type of Memory Training data to populate into the BDAT ACPI table.*
  - UINT8 [ScanExtGfxForLegacyOpRom](#)

*Offset 0x0404 - 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 0x0405 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.*
  - UINT8 [DmiGen3ProgramStaticEq](#)

*Offset 0x0406 - Enable/Disable DMI GEN3 Static EQ Phase1 programming Program DMI Gen3 EQ Phase1 Static Presets.*
  - UINT8 [Peg0Enable](#)

*Offset 0x0407 - Enable/Disable PEG 0 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.*
  - UINT8 [Peg1Enable](#)

*Offset 0x0408 - Enable/Disable PEG 1 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.*
  - UINT8 [Peg2Enable](#)

*Offset 0x0409 - Enable/Disable PEG 2 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.*
-

- [UINT8 Peg3Enable](#)  
*Offset 0x040A - Enable/Disable PEG 3 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.*
  - [UINT8 Peg0MaxLinkSpeed](#)  
*Offset 0x040B - PEG 0 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.*
  - [UINT8 Peg1MaxLinkSpeed](#)  
*Offset 0x040C - PEG 1 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.*
  - [UINT8 Peg2MaxLinkSpeed](#)  
*Offset 0x040D - PEG 2 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.*
  - [UINT8 Peg3MaxLinkSpeed](#)  
*Offset 0x040E - PEG 3 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.*
  - [UINT8 Peg0MaxLinkWidth](#)  
*Offset 0x040F - PEG 0 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4, (0x4): Limit Link to x8 0:Auto, 1:x1, 2:x2, 3:x4, 4:x8.*
  - [UINT8 Peg1MaxLinkWidth](#)  
*Offset 0x0410 - PEG 1 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4 0:Auto, 1:x1, 2:x2, 3:x4.*
  - [UINT8 Peg2MaxLinkWidth](#)  
*Offset 0x0411 - PEG 2 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2 0:Auto, 1:x1, 2:x2.*
  - [UINT8 Peg3MaxLinkWidth](#)  
*Offset 0x0412 - PEG 3 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2 0:Auto, 1:x1, 2:x2.*
  - [UINT8 Peg0PowerDownUnusedLanes](#)  
*Offset 0x0413 - Power down unused lanes on PEG 0 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.*
  - [UINT8 Peg1PowerDownUnusedLanes](#)  
*Offset 0x0414 - Power down unused lanes on PEG 1 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.*
  - [UINT8 Peg2PowerDownUnusedLanes](#)  
*Offset 0x0415 - Power down unused lanes on PEG 2 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.*
  - [UINT8 Peg3PowerDownUnusedLanes](#)  
*Offset 0x0416 - Power down unused lanes on PEG 3 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.*
  - [UINT8 InitPcieAspmAfterOprom](#)  
*Offset 0x0417 - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.*
  - [UINT8 PegDisableSpreadSpectrumClocking](#)  
*Offset 0x0418 - PCIe Disable Spread Spectrum Clocking PCIe Disable Spread Spectrum Clocking.*
  - [UINT8 DmiGen3RootPortPreset \[8\]](#)  
*Offset 0x0419 - DMI Gen3 Root port preset values per lane Used for programming DMI Gen3 preset values per lane.*
  - [UINT8 DmiGen3EndPointPreset \[8\]](#)  
*Offset 0x0421 - DMI Gen3 End port preset values per lane Used for programming DMI Gen3 preset values per lane.*
  - [UINT8 DmiGen3EndPointHint \[8\]](#)
-

- Offset 0x0429 - DMI Gen3 End port Hint values per lane Used for programming DMI Gen3 Hint values per lane.*

    - UINT8 [DmiGen3RxCtlePeaking](#) [4]
      - Offset 0x0431 - DMI Gen3 RxCTLEp per-Bundle control Range: 0-15, 0 is default for each bundle, must be specified based upon platform design.*
    - UINT8 [PegGen3RxCtlePeaking](#) [10]
      - Offset 0x0435 - PEG Gen3 RxCTLEp per-Bundle control Range: 0-15, 12 is default for each bundle, must be specified based upon platform design.*
    - UINT8 [UnusedUpdSpace16](#)
      - Offset 0x043F.*
    - UINT32 [PegDataPtr](#)
      - Offset 0x0440 - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA\_PEG\_DATA) and platform code can save/restore this data to skip preset search in the following boots.*
    - UINT8 [PegGpioData](#) [28]
      - Offset 0x0444 - PEG PERST# GPIO information The reference code will use the information in this structure in order to reset PCIe Gen3 devices during equalization, if necessary.*
    - UINT8 [DmiDeEmphasis](#)
      - Offset 0x0460 - DeEmphasis control for DMI DeEmphasis control for DMI.*
    - UINT8 [PegRootPortHPE](#) [4]
      - Offset 0x0461 - PCIe Hot Plug Enable/Disable per port 0(Default): Disable, 1: Enable.*
    - UINT8 [DmiMaxLinkSpeed](#)
      - Offset 0x0465 - 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 0x0466 - DMI Equalization Phase 2 DMI Equalization Phase 2.*
    - UINT8 [DmiGen3EqPh3Method](#)
      - Offset 0x0467 - DMI Gen3 Equalization Phase3 DMI Gen3 Equalization Phase3.*
    - UINT8 [Peg0Gen3EqPh2Enable](#)
      - Offset 0x0468 - Phase2 EQ enable on the PEG 0:1:0.*
    - UINT8 [Peg1Gen3EqPh2Enable](#)
      - Offset 0x0469 - Phase2 EQ enable on the PEG 0:1:1.*
    - UINT8 [Peg2Gen3EqPh2Enable](#)
      - Offset 0x046A - Phase2 EQ enable on the PEG 0:1:2.*
    - UINT8 [Peg3Gen3EqPh2Enable](#)
      - Offset 0x046B - Phase2 EQ enable on the PEG 0:1:3.*
    - UINT8 [Peg0Gen3EqPh3Method](#)
      - Offset 0x046C - Phase3 EQ method on the PEG 0:1:0.*
    - UINT8 [Peg1Gen3EqPh3Method](#)
      - Offset 0x046D - Phase3 EQ method on the PEG 0:1:1.*
    - UINT8 [Peg2Gen3EqPh3Method](#)
      - Offset 0x046E - Phase3 EQ method on the PEG 0:1:2.*
    - UINT8 [Peg3Gen3EqPh3Method](#)
      - Offset 0x046F - Phase3 EQ method on the PEG 0:1:3.*
    - UINT8 [PegGen3ProgramStaticEq](#)
      - Offset 0x0470 - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program PEG Gen3 EQ Phase1 Static Presets.*
    - UINT8 [Gen3SwEqAlwaysAttempt](#)
      - Offset 0x0471 - PEG Gen3 SwEq Always Attempt Gen3 Software Equalization will be executed every boot.*
    - UINT8 [Gen3SwEqNumberOfPresets](#)
      - Offset 0x0472 - Select number of TxEq presets to test in the PCIe/DMI SwEq Select number of TxEq presets to test in the PCIe/DMI SwEq.*
    - UINT8 [Gen3SwEqEnableVocTest](#)
-

- Offset 0x0473 - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.
- UINT8 [PegRxCemTestingMode](#)  
Offset 0x0474 - PCIe Rx Compliance Testing Mode Disabled(0x0)(Default): Normal Operation - Disable PCIe Rx Compliance testing, Enabled(0x1): PCIe Rx Compliance Test Mode - PEG controller is in Rx Compliance Testing Mode; it should only be set when doing PCIe compliance testing \$EN\_DIS.
  - UINT8 [PegRxCemLoopbackLane](#)  
Offset 0x0475 - PCIe Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specified Lane (0 - 15) will be used for RxCEMLoopback.
  - UINT8 [PegGenerateBdatMarginTable](#)  
Offset 0x0476 - Generate PCIe BDAT Margin Table Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.
  - UINT8 [PegRxCemNonProtocolAwareness](#)  
Offset 0x0477 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.
  - UINT8 [PegGen3RxCtleOverride](#)  
Offset 0x0478 - PCIe Override RxCTLE Disable(0x0)(Default): Normal Operation - RxCTLE adaptive behavior enabled, Enable(0x1): Override RxCTLE - Disable RxCTLE adaptive behavior to keep the configured RxCTLE peak values unmodified \$EN\_DIS.
  - UINT8 [PegGen3RootPortPreset](#) [20]  
Offset 0x0479 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.
  - UINT8 [PegGen3EndPointPreset](#) [20]  
Offset 0x048D - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.
  - UINT8 [PegGen3EndPointHint](#) [20]  
Offset 0x04A1 - PEG Gen3 End port Hint values per lane Used for programming PEG Gen3 Hint values per lane.
  - UINT8 [UnusedUpdSpace17](#)  
Offset 0x04B5.
  - UINT16 [Gen3SwEqJitterDwellTime](#)  
Offset 0x04B6 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.
  - UINT16 [Gen3SwEqJitterErrorTarget](#)  
Offset 0x04B8 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.
  - UINT16 [Gen3SwEqVocDwellTime](#)  
Offset 0x04BA - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.
  - UINT16 [Gen3SwEqVocErrorTarget](#)  
Offset 0x04BC - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.
  - UINT8 [SalpuEnable](#)  
Offset 0x04BE - Enable/Disable SA IPU Enable(Default): Enable SA IPU, Disable: Disable SA IPU \$EN\_DIS.
  - UINT8 [SalpulmrConfiguration](#)  
Offset 0x04BF - IPU IMR Configuration 0:IPU Camera, 1:IPU Gen Default is 0 0:IPU Camera, 1:IPU Gen.
  - UINT8 [ImguClkOutEn](#) [5]  
Offset 0x04C0 - IMGU CLKOUT Configuration The configuration of IMGU CLKOUT, 0: Disable;1: **Enable**.
  - UINT8 [CpuTraceHubMode](#)  
Offset 0x04C5 - 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.
  - UINT8 [CpuTraceHubMemReg0Size](#)  
Offset 0x04C6 - CPU Trace Hub Memory Region 0 CPU Trace Hub Memory Region 0, The available memory size is : 0MB, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.
  - UINT8 [CpuTraceHubMemReg1Size](#)  
Offset 0x04C7 - CPU Trace Hub Memory Region 1 CPU Trace Hub Memory Region 1.
  - UINT8 [SaOcSupport](#)  
Offset 0x04C8 - Enable/Disable SA OcSupport Enable: Enable SA OcSupport, Disable(Default): Disable SA OcSupport \$EN\_DIS.
-

- UINT8 [GtVoltageMode](#)  
*Offset 0x04C9 - GT slice Voltage Mode 0(Default): Adaptive, 1: Override 0: Adaptive, 1: Override.*
  - UINT8 [GtMaxOcRatio](#)  
*Offset 0x04CA - Maximum GTs turbo ratio override 0(Default)=Minimal/Auto, 42=Maximum.*
  - UINT8 [UnusedUpdSpace18](#)  
*Offset 0x04CB.*
  - UINT16 [GtVoltageOffset](#)  
*Offset 0x04CC - The voltage offset applied to GT slice 0(Default)=Minimal, 1000=Maximum.*
  - UINT16 [GtVoltageOverride](#)  
*Offset 0x04CE - The GT slice voltage override which is applied to the entire range of GT frequencies 0(Default)=Minimal, 2000=Maximum.*
  - UINT16 [GtExtraTurboVoltage](#)  
*Offset 0x04D0 - adaptive voltage applied during turbo frequencies 0(Default)=Minimal, 2000=Maximum.*
  - UINT16 [SaVoltageOffset](#)  
*Offset 0x04D2 - voltage offset applied to the SA 0(Default)=Minimal, 1000=Maximum.*
  - UINT8 [RealtimeMemoryTiming](#)  
*Offset 0x04D4 - Realtime Memory Timing 0(Default): Disabled, 1: Enabled.*
  - UINT8 [TcsslbtPcie0En](#)  
*Offset 0x04D5 - TCSS Thunderbolt PCIE Root Port 0 Enable Set TCSS Thunderbolt PCIE Root Port 0.*
  - UINT8 [TcsslbtPcie1En](#)  
*Offset 0x04D6 - TCSS Thunderbolt PCIE Root Port 1 Enable Set TCSS Thunderbolt PCIE Root Port 1.*
  - UINT8 [TcsslbtPcie2En](#)  
*Offset 0x04D7 - TCSS Thunderbolt PCIE Root Port 2 Enable Set TCSS Thunderbolt PCIE Root Port 2.*
  - UINT8 [TcsslbtPcie3En](#)  
*Offset 0x04D8 - TCSS Thunderbolt PCIE Root Port 3 Enable Set TCSS Thunderbolt PCIE Root Port 3.*
  - UINT8 [TcssXhciEn](#)  
*Offset 0x04D9 - TCSS USB HOST (xHCI) Enable Set TCSS XHCI.*
  - UINT8 [TcssXdcien](#)  
*Offset 0x04DA - TCSS USB DEVICE (xDCI) Enable Set TCSS XDCI.*
  - UINT8 [TcssDma0En](#)  
*Offset 0x04DB - TCSS DMA0 Enable Set TCSS DMA0.*
  - UINT8 [TcssDma1En](#)  
*Offset 0x04DC - TCSS DMA1 Enable Set TCSS DMA1.*
  - UINT8 [PcieMultipleSegmentEnabled](#)  
*Offset 0x04DD - This is policy to control iTBT PCIe Multiple Segment setting.*
  - UINT8 [CridEnable](#)  
*Offset 0x04DE - Enable/Disable SA CRID Enable: SA CRID, Disable (Default): SA CRID \$EN\_DIS.*
  - UINT8 [UsbTcPortEnPreMem](#)  
*Offset 0x04DF - TCSS USB Port Enable Bitmap for per port enabling.*
  - UINT8 [MemBootMode](#)  
*Offset 0x04E0 - Mem Boot Mode 0: BOOT\_MODE\_1LM(Default), 1: BOOT\_MODE\_2LM, 2: BOOT\_MODE\_PROVISION 0: BOOT\_MODE\_1LM, 1: BOOT\_MODE\_2LM, 2: BOOT\_MODE\_PROVISION.*
  - UINT8 [Peg3Aspm](#)  
*Offset 0x04E1 - PCIe ASPM programming will happen in relation to the Oprom This option is specifically needed for ASPM configuration in 2LM feature 0:Disabled, 1:L0, 2:L1, 3:L0L1, 4:Auto.*
  - UINT8 [MfvcWrrArb](#)  
*Offset 0x04E2 - MFVC WRR VC Arbitration 0: DEFAULT\_PHASES(Default), 1: PROGRAM\_128PHASES 0: DEFAULT\_PHASES, 1: PROGRAM\_128PHASES.*
  - UINT8 [Vcld\\_7\\_0](#) [16]  
*Offset 0x04E3 - Vcld\_7\_0 values Select VC ID for arbitration.*
  - UINT8 [SetHwParameters](#)
-

- Offset 0x04F3 - Set Hw Parameters enable/disable 1: enable, 0: disable, Enable/disable setting of HW parameters \$EN\_DIS.
- UINT16 [Ltr\\_L1D2\\_ThVal](#)  
Offset 0x04F4 - LTR L1.2 Threshold Value LTR L1.2 Threshold Value.
  - UINT8 [Ltr\\_L1D2\\_ThScale](#)  
Offset 0x04F6 - LTR L1.2 Threshold Scale LTR L1.2 Threshold Scale.
  - UINT8 [SysPwrState](#)  
Offset 0x04F7 - system power state system power state indicates the platform power state.
  - UINT8 [MediaDeathNotification](#)  
Offset 0x04F8 - Media Death Notification Enable/Disable 1: enable, 0: disable, Enable/disable for Media Death Notification \$EN\_DIS.
  - UINT8 [HealthLogNotification](#)  
Offset 0x04F9 - Health Log Notification Enable/Disable 1: enable, 0: disable, Enable/disable for Health Log Notification \$EN\_DIS.
  - UINT8 [TempBelowThrottleNotification](#)  
Offset 0x04FA - Temp crosses below TempThrottle Notification Enable/Disable 1: enable, 0: disable, Enable/disable for Temp crosses below TempThrottle Notification \$EN\_DIS.
  - UINT8 [TempAboveThrottleNotification](#)  
Offset 0x04FB - Temp crosses above TempThrottle Notification Enable/Disable 1: enable, 0: disable, Enable/disable for Temp crosses above TempThrottle Notification \$EN\_DIS.
  - UINT8 [MissingCommitBitNotification](#)  
Offset 0x04FC - Missing Commit Bit Notification Enable/Disable 1: enable, 0: disable, Enable/disable for Missing Commit Bit Notification \$EN\_DIS.
  - UINT8 [NVMeHoldDisableBit](#)  
Offset 0x04FD - NVMeHoldDisableBit 1: enable, 0: disable, Enable/disable for NVMeHoldDisableBit \$EN\_DIS.
  - UINT8 [PegImrEnable](#)  
Offset 0x04FE - PEG IMR support This option configures the IMR support for PEG.
  - UINT8 [PegImrRpSelection](#)  
Offset 0x04FF - PEG Root port number for IMR.
  - UINT16 [PegImrSize](#)  
Offset 0x0500 - PEG IMR size The size of IMR to be allocated for PEG EndPoint device.
  - UINT8 [EnableAbove4GBMmio](#)  
Offset 0x0502 - Enable above 4GB MMIO resource support Enable/disable above 4GB MMIO resource support \$EN\_DIS.
  - UINT8 [LoadMgUcFw](#)  
Offset 0x0503 - Control Load MG uC FW Enable/disable Load MG uC FW \$EN\_DIS.
  - UINT8 [ITbtVtdEnable](#)  
Offset 0x0504 - Enable/Disable ITbtVtd Disabled(0x0): Disable ITbtVtd, Enabled(0x1): Enable ITbtVtd 0:Disable, 1:Enable.
  - UINT8 [UnusedUpdSpace19](#) [3]  
Offset 0x0505.
  - UINT32 [SaPcieRpEnableMask](#)  
Offset 0x0508 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.
  - UINT8 [SaPcieRpLinkDownGpios](#)  
Offset 0x050C - Assertion on Link Down GPIOs GPIO Assertion on Link Down.
  - UINT8 [SaPreMemRsvd](#) [29]  
Offset 0x050D.
  - UINT8 [HeciTimeouts](#)  
Offset 0x052A - HECI Timeouts 0: Disable, 1: Enable (Default) timeout check for HECI \$EN\_DIS.
  - UINT8 [DidInitStat](#)  
Offset 0x052B - 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 0x052C - CPU Replaced Polling Disable Test, 0: disable, 1: enable, Setting this option disables CPU replacement polling loop \$EN\_DIS.
- UINT8 [SendDidMsg](#)

Offset 0x052D - 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 0x052E - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.
  - UINT8 [SkipMbpHob](#)

Offset 0x052F - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.
  - UINT8 [HeciCommunication2](#)

Offset 0x0530 - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.
  - UINT8 [KtDeviceEnable](#)

Offset 0x0531 - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.
  - UINT8 [UnusedUpdSpace20](#) [2]

Offset 0x0532.
  - UINT32 [Heci1BarAddress](#)

Offset 0x0534 - HECI1 BAR address BAR address of HECI1.
  - UINT32 [Heci2BarAddress](#)

Offset 0x0538 - HECI2 BAR address BAR address of HECI2.
  - UINT32 [Heci3BarAddress](#)

Offset 0x053C - HECI3 BAR address BAR address of HECI3.
  - UINT8 [MePreMemRsvd](#) [16]

Offset 0x0540.
  - UINT8 [PchTraceHubMode](#)

Offset 0x0550 - PCH Trace Hub Mode Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software or 'Disable' trace hub functionality.
  - UINT8 [PchTraceHubMemReg0Size](#)

Offset 0x0551 - PCH Trace Hub Memory Region 0 buffer Size Specify size of Pch trace memory region 0 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.
  - UINT8 [PchTraceHubMemReg1Size](#)

Offset 0x0552 - PCH Trace Hub Memory Region 1 buffer Size Specify size of Pch trace memory region 1 buffer, the size can be 0, 1MB, 8MB, 64MB, 128MB, 256MB, 512MB.
  - UINT8 [SmbusEnable](#)

Offset 0x0553 - Enable SMBus Enable/disable SMBus controller.
  - UINT8 [SmbusArpEnable](#)

Offset 0x0554 - Enable SMBus ARP support Enable SMBus ARP support.
  - UINT8 [SmbusDynamicPowerGating](#)

Offset 0x0555 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.
  - UINT8 [SmbusSpdWriteDisable](#)

Offset 0x0556 - SMBUS SPD Write Disable Set/Clear Smbus SPD Write Disable.
  - UINT8 [PchSmbAlertEnable](#)

Offset 0x0557 - Enable SMBus Alert Pin Enable SMBus Alert Pin.
  - UINT16 [PchSmbusIoBase](#)

Offset 0x0558 - SMBUS Base Address SMBUS Base Address (IO space).
  - UINT8 [PchNumRsvdSmbusAddresses](#)

Offset 0x055A - Number of RsvdSmbusAddressTable.
  - UINT8 [UnusedUpdSpace21](#)

Offset 0x055B.
  - UINT32 [RsvdSmbusAddressTablePtr](#)

Offset 0x055C - Point of RsvdSmbusAddressTable Array of addresses reserved for non-ARP-capable SMBus devices.
  - UINT8 [DciEn](#)
-

- Offset 0x0560 - DCI Enable Determine if to enable DCI debug from host \$EN\_DIS.*

  - UINT8 [DciModphyPg](#)

*Offset 0x0561 - Enable DCI ModPHY Pwoer Gate Enable ModPHY Pwoer Gate when DCI is enabled \$EN\_DIS.*
  - UINT8 [DciDbcMode](#)

*Offset 0x0562 - 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.*
  - UINT8 [DciUsb3TypecUfpDbg](#)

*Offset 0x0563 - 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.*
  - UINT32 [PcieRpEnableMask](#)

*Offset 0x0564 - Enable PCIE RP Mask Enable/disable PCIE Root Ports.*
  - UINT8 [PcieImrEnabled](#)

*Offset 0x0568 - Enable PCIe IMR 0:Disable, 1:Enable \$EN\_DIS.*
  - UINT8 [UnusedUpdSpace22](#)

*Offset 0x0569.*
  - UINT16 [PcieImrSize](#)

*Offset 0x056A - Size of PCIe IMR.*
  - UINT8 [ImrRpSelection](#)

*Offset 0x056C - Root port number for IMR.*
  - UINT8 [PchPcieHsioRxSetCtleEnable](#) [24]

*Offset 0x056D - Enable PCH HSIO PCIE Rx Set Ctle Enable PCH PCIe Gen 3 Set CTLE Value.*
  - UINT8 [PchPcieHsioRxSetCtle](#) [24]

*Offset 0x0585 - PCH HSIO PCIE Rx Set Ctle Value PCH PCIe Gen 3 Set CTLE Value.*
  - UINT8 [PchPcieHsioTxGen1DownscaleAmpEnable](#) [24]

*Offset 0x059D - Enble PCH HSIO PCIE TX Gen 1 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen1DownscaleAmp](#) [24]

*Offset 0x05B5 - 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 0x05CD - Enable PCH HSIO PCIE TX Gen 2 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen2DownscaleAmp](#) [24]

*Offset 0x05E5 - 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 0x05FD - Enable PCH HSIO PCIE TX Gen 3 Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen3DownscaleAmp](#) [24]

*Offset 0x0615 - 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 0x062D - Enable PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment Setting value override 0↔: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen1DeEmph](#) [24]

*Offset 0x0645 - 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 0x065D - Enable PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen2DeEmph3p5](#) [24]

- Offset 0x0675 - 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 0x068D - Enable PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.*
  - UINT8 [PchPcieHsioTxGen2DeEmph6p0](#) [24]
 

*Offset 0x06A5 - 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 0x06BD - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↔ : Disable; 1: Enable.*
  - UINT8 [PchSataHsioRxGen1EqBoostMag](#) [8]
 

*Offset 0x06C5 - 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 0x06CD - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↔ : Disable; 1: Enable.*
  - UINT8 [PchSataHsioRxGen2EqBoostMag](#) [8]
 

*Offset 0x06D5 - 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 0x06DD - Enable PCH HSIO SATA Receiver Equalization Boost Magnitude Adjustment Value override 0↔ : Disable; 1: Enable.*
  - UINT8 [PchSataHsioRxGen3EqBoostMag](#) [8]
 

*Offset 0x06E5 - 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 0x06ED - Enable PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen1DownscaleAmp](#) [8]
 

*Offset 0x06F5 - 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 0x06FD - Enable PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen2DownscaleAmp](#) [8]
 

*Offset 0x0705 - 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 0x070D - Enable PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen3DownscaleAmp](#) [8]
 

*Offset 0x0715 - 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 0x071D - Enable PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen1DeEmph](#) [8]
 

*Offset 0x0725 - 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 0x072D - Enable PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen2DeEmph](#) [8]
-

- Offset 0x0735 - 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 0x073D - Enable PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting value override 0: Disable; 1: Enable.*
  - UINT8 [PchSataHsioTxGen3DeEmph](#) [8]
 

*Offset 0x0745 - 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 [ChipsetInitMessage](#)

*Offset 0x074D - ChipsetInit HECI message DEPRECATED \$EN\_DIS.*
  - UINT8 [BypassPhySyncReset](#)

*Offset 0x074E - Bypass ChipsetInit sync reset.*
  - UINT8 [PchLpcEnhancePort8xhDecoding](#)

*Offset 0x074F - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.*
  - UINT8 [PchPort80Route](#)

*Offset 0x0750 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.*
  - UINT8 [WdtDisableAndLock](#)

*Offset 0x0751 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.*
  - UINT8 [PchHdaEnable](#)

*Offset 0x0752 - Enable Intel HD Audio (Azalia) 0: Disable, 1: Enable (Default) Azalia controller \$EN\_DIS.*
  - UINT8 [PchIshEnable](#)

*Offset 0x0753 - Enable PCH ISH Controller 0: Disable, 1: Enable (Default) ISH Controller \$EN\_DIS.*
  - UINT8 [PlatformDebugConsent](#)

*Offset 0x0754 - Platform Debug Consent To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type.*
  - UINT8 [PcdDebugInterfaceFlags](#)

*Offset 0x0755 - Debug Interfaces Debug Interfaces.*
  - UINT8 [SerialIoUartDebugControllerNumber](#)

*Offset 0x0756 - Serial Io Uart Debug Controller Number Select SerialIo Uart Controller for debug.*
  - UINT8 [SerialIoUartDebugAutoFlow](#)

*Offset 0x0757 - Serial Io Uart Debug Auto Flow Enables UART hardware flow control, CTS and RTS lines.*
  - UINT32 [SerialIoUartDebugBaudRate](#)

*Offset 0x0758 - Serial Io Uart Debug BaudRate Set default BaudRate Supported from 0 - default to 6000000.*
  - UINT8 [SerialIoUartDebugParity](#)

*Offset 0x075C - Serial Io Uart Debug Parity Set default Parity.*
  - UINT8 [SerialIoUartDebugStopBits](#)

*Offset 0x075D - Serial Io Uart Debug Stop Bits Set default stop bits.*
  - UINT8 [SerialIoUartDebugDataBits](#)

*Offset 0x075E - Serial Io Uart Debug Data Bits Set default word length.*
  - UINT8 [PcdIsaSerialUartBase](#)

*Offset 0x075F - ISA Serial Base selection Select ISA Serial Base address.*
  - UINT8 [PcdSerialDebugBaudRate](#)

*Offset 0x0760 - PcdSerialDebugBaudRate Baud Rate for Serial Debug Messages.*
  - UINT8 [UnusedUpdSpace23](#)

*Offset 0x0761.*
  - UINT16 [PostCodeOutputPort](#)

*Offset 0x0762 - Post Code Output Port This option configures Post Code Output Port.*
  - UINT8 [PchPreMemRsvd](#) [32]
 

*Offset 0x0764.*
  - UINT8 [WRDSEQT](#)

*Offset 0x0784 - Write Drive Strength/Equalization 2D Enables/Disable Write Drive Strength/Equalization 2D \$EN\_↔DIS.*
-

- UINT8 [UnusedUpdSpace24](#) [4]  
*Offset 0x0785.*
- UINT8 [ReservedFspmUpd](#) [15]  
*Offset 0x0789.*

### 12.7.1 Detailed Description

Fsp M Configuration.

Definition at line 56 of file FspmUpd.h.

### 12.7.2 Member Data Documentation

#### 12.7.2.1 ActiveCoreCount

UINT8 FSP\_M\_CONFIG::ActiveCoreCount

Offset 0x01BB - 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 1572 of file FspmUpd.h.

#### 12.7.2.2 ApertureSize

UINT8 FSP\_M\_CONFIG::ApertureSize

Offset 0x025F - Aperture Size Select the Aperture Size.

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

Definition at line 1826 of file FspmUpd.h.

#### 12.7.2.3 ApStartupBase

UINT32 FSP\_M\_CONFIG::ApStartupBase

Offset 0x0218 - ApStartupBase Enable/Disable.

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

Definition at line 1753 of file FspmUpd.h.

#### 12.7.2.4 Avx2RatioOffset

UINT8 FSP\_M\_CONFIG::Avx2RatioOffset

Offset 0x019A - 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 1423 of file FspmUpd.h.

---

### 12.7.2.5 Avx2VoltageScaleFactor

UINT8 FSP\_M\_CONFIG::Avx2VoltageScaleFactor

Offset 0x01A2 - Avx2 Voltage Guardband Scaling Factor AVX2 Voltage Guardband Scale factor applied to AVX2 workloads.

Range is 0-200 in 1/100 units, where a value of 125 would apply a 1.25 scale factor.

Definition at line 1463 of file FspmUpd.h.

### 12.7.2.6 Avx3RatioOffset

UINT8 FSP\_M\_CONFIG::Avx3RatioOffset

Offset 0x019B - 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 1429 of file FspmUpd.h.

### 12.7.2.7 Avx512VoltageScaleFactor

UINT8 FSP\_M\_CONFIG::Avx512VoltageScaleFactor

Offset 0x01A3 - Avx512 Voltage Guardband Scaling Factor AVX512 Voltage Guardband Scale factor applied to AVX512 workloads.

Range is 0-200 in 1/100 units, where a value of 125 would apply a 1.25 scale factor.

Definition at line 1469 of file FspmUpd.h.

### 12.7.2.8 BclkAdaptiveVoltage

UINT8 FSP\_M\_CONFIG::BclkAdaptiveVoltage

Offset 0x0199 - 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 1417 of file FspmUpd.h.

### 12.7.2.9 BdatEnable

UINT8 FSP\_M\_CONFIG::BdatEnable

Offset 0x0402 - 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 1955 of file FspmUpd.h.

---

### 12.7.2.10 BdatTestType

UINT8 FSP\_M\_CONFIG::BdatTestType

Offset 0x0403 - 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 1961 of file FspmUpd.h.

### 12.7.2.11 BiosAcmBase

UINT32 FSP\_M\_CONFIG::BiosAcmBase

Offset 0x01FC - BiosAcmBase Enable/Disable.

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

Definition at line 1728 of file FspmUpd.h.

### 12.7.2.12 BiosAcmSize

UINT32 FSP\_M\_CONFIG::BiosAcmSize

Offset 0x0200 - BiosAcmSize Enable/Disable.

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

Definition at line 1733 of file FspmUpd.h.

### 12.7.2.13 BiosGuard

UINT8 FSP\_M\_CONFIG::BiosGuard

Offset 0x01D5 - BiosGuard Enable/Disable.

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

Definition at line 1659 of file FspmUpd.h.

### 12.7.2.14 BiosSize

UINT16 FSP\_M\_CONFIG::BiosSize

Offset 0x01E2 - BiosSize Enable/Disable.

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

Definition at line 1699 of file FspmUpd.h.

### 12.7.2.15 BistOnReset

UINT8 FSP\_M\_CONFIG::BistOnReset

Offset 0x01BE - BIST on Reset Enable or Disable BIST on Reset; **0: Disable**; 1: Enable.

---

\$EN\_DIS

Definition at line 1592 of file FspmUpd.h.

#### 12.7.2.16 BootFrequency

UINT8 FSP\_M\_CONFIG::BootFrequency

Offset 0x01BA - 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 1565 of file FspmUpd.h.

#### 12.7.2.17 BypassPhySyncReset

UINT8 FSP\_M\_CONFIG::BypassPhySyncReset

Offset 0x074E - Bypass ChipsetInit sync reset.

DEPRECATED \$EN\_DIS

Definition at line 3019 of file FspmUpd.h.

#### 12.7.2.18 ChHashEnable

UINT8 FSP\_M\_CONFIG::ChHashEnable

Offset 0x010A - Ch Hash Support Enable/Disable Channel Hash Support.

NOTE: ONLY if Memory interleaved Mode \$EN\_DIS

Definition at line 759 of file FspmUpd.h.

#### 12.7.2.19 ChHashInterleaveBit

UINT8 FSP\_M\_CONFIG::ChHashInterleaveBit

Offset 0x0120 - 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 875 of file FspmUpd.h.

#### 12.7.2.20 ChHashMask

UINT16 FSP\_M\_CONFIG::ChHashMask

Offset 0x0122 - 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 885 of file FspmUpd.h.

#### 12.7.2.21 CkeRankMapping

UINT8 FSP\_M\_CONFIG::CkeRankMapping

Offset 0x0159 - 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 1139 of file FspmUpd.h.

#### 12.7.2.22 CleanMemory

UINT8 FSP\_M\_CONFIG::CleanMemory

Offset 0x0099 - 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 142 of file FspmUpd.h.

#### 12.7.2.23 CmdRanksTerminated

UINT8 FSP\_M\_CONFIG::CmdRanksTerminated

Offset 0x016E - 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 1275 of file FspmUpd.h.

#### 12.7.2.24 CoreHighVoltageMode

UINT8 FSP\_M\_CONFIG::CoreHighVoltageMode

Offset 0x01A5 - Core High Voltage Mode Enable High Voltage Mode in the core FIVR Domains.

Used for LN2 cold boot mitigation. **0 - Disable**, 1 - Enable \$EN\_DIS

Definition at line 1483 of file FspmUpd.h.

#### 12.7.2.25 CoreMaxOcRatio

UINT8 FSP\_M\_CONFIG::CoreMaxOcRatio

Offset 0x0183 - 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 1326 of file FspmUpd.h.

#### 12.7.2.26 CorePllVoltageOffset

UINT8 FSP\_M\_CONFIG::CorePllVoltageOffset

Offset 0x0194 - Core PLL voltage offset Core PLL voltage offset.

**0: No offset.** Range 0-63

Definition at line 1390 of file FspmUpd.h.

#### 12.7.2.27 CoreVoltageAdaptive

UINT16 FSP\_M\_CONFIG::CoreVoltageAdaptive

Offset 0x0190 - 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 1380 of file FspmUpd.h.

#### 12.7.2.28 CoreVoltageMode

UINT8 FSP\_M\_CONFIG::CoreVoltageMode

Offset 0x0184 - Core voltage mode Core voltage mode; **0: Adaptive**; 1: Override.

\$EN\_DIS

Definition at line 1332 of file FspmUpd.h.

#### 12.7.2.29 CoreVoltageOverride

UINT16 FSP\_M\_CONFIG::CoreVoltageOverride

Offset 0x018E - 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 1374 of file FspmUpd.h.

#### 12.7.2.30 CpuCrashLogEnable

UINT8 FSP\_M\_CONFIG::CpuCrashLogEnable

Offset 0x01C2 - Enable CPU CrashLog Enable or Disable CPU CrashLog; 0: Disable; **1: Enable.**

\$EN\_DIS

Definition at line 1615 of file FspmUpd.h.

---

### 12.7.2.31 CpuRatio

UINT8 FSP\_M\_CONFIG::CpuRatio

Offset 0x01C0 - CPU ratio value CPU ratio value.

Valid Range 0 to 63

Definition at line 1603 of file FspmUpd.h.

### 12.7.2.32 CpuTraceHubMemReg0Size

UINT8 FSP\_M\_CONFIG::CpuTraceHubMemReg0Size

Offset 0x04C6 - 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 2395 of file FspmUpd.h.

### 12.7.2.33 CpuTraceHubMemReg1Size

UINT8 FSP\_M\_CONFIG::CpuTraceHubMemReg1Size

Offset 0x04C7 - 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 2402 of file FspmUpd.h.

### 12.7.2.34 CpuTraceHubMode

UINT8 FSP\_M\_CONFIG::CpuTraceHubMode

Offset 0x04C5 - 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 2388 of file FspmUpd.h.

### 12.7.2.35 DciUsb3TypecUfpDbg

UINT8 FSP\_M\_CONFIG::DciUsb3TypecUfpDbg

Offset 0x0563 - 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 2821 of file FspmUpd.h.

---

### 12.7.2.36 Ddr4OneDpc

UINT8 FSP\_M\_CONFIG::Ddr4OneDpc

Offset 0x00B4 - Ddr4OneDpc DDR4 1DPC performance feature for 2R DIMMs.

Can be enabled on DIMM0 or DIMM1 only, or on both (default) 0: Disabled, 1: Enabled on DIMM0 only, 2: Enabled on DIMM1 only, 3: Enabled

Definition at line 289 of file FspmUpd.h.

### 12.7.2.37 DdrFreqLimit

UINT16 FSP\_M\_CONFIG::DdrFreqLimit

Offset 0x009E - 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 172 of file FspmUpd.h.

### 12.7.2.38 DdrSpeedControl

UINT8 FSP\_M\_CONFIG::DdrSpeedControl

Offset 0x00AE - DDR Speed Control DDR Frequency and Gear control for all SAGV points.

0:Auto, 1:Manual

Definition at line 252 of file FspmUpd.h.

### 12.7.2.39 DebugInterfaceLockEnable

UINT8 FSP\_M\_CONFIG::DebugInterfaceLockEnable

Offset 0x01C4 - CPU Run Control Lock Lock or Unlock CPU Run Control; 0: Disable; **1: Enable.**

\$EN\_DIS

Definition at line 1628 of file FspmUpd.h.

### 12.7.2.40 DisableDimmChannel0

UINT8 FSP\_M\_CONFIG::DisableDimmChannel0

Offset 0x00A0 - 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 178 of file FspmUpd.h.

---

#### 12.7.2.41 DisableDimmChannel1

UINT8 FSP\_M\_CONFIG::DisableDimmChannel1

Offset 0x00A1 - 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 184 of file FspmUpd.h.

#### 12.7.2.42 DisableMessageCheck

UINT8 FSP\_M\_CONFIG::DisableMessageCheck

Offset 0x052E - Check HECI message before send Test, 0: disable, 1: enable, Enable/Disable message check.

\$EN\_DIS

Definition at line 2683 of file FspmUpd.h.

#### 12.7.2.43 DmiDeEmphasis

UINT8 FSP\_M\_CONFIG::DmiDeEmphasis

Offset 0x0460 - DeEmphasis control for DMI DeEmphasis control for DMI.

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

Definition at line 2156 of file FspmUpd.h.

#### 12.7.2.44 DmiGen3EndPointHint

UINT8 FSP\_M\_CONFIG::DmiGen3EndPointHint[8]

Offset 0x0429 - 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 2123 of file FspmUpd.h.

#### 12.7.2.45 DmiGen3EndPointPreset

UINT8 FSP\_M\_CONFIG::DmiGen3EndPointPreset[8]

Offset 0x0421 - 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 2118 of file FspmUpd.h.

#### 12.7.2.46 DmiGen3EqPh2Enable

UINT8 FSP\_M\_CONFIG::DmiGen3EqPh2Enable

---

Offset 0x0466 - 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 2175 of file FspmUpd.h.

#### 12.7.2.47 DmiGen3EqPh3Method

UINT8 FSP\_M\_CONFIG::DmiGen3EqPh3Method

Offset 0x0467 - 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 2185 of file FspmUpd.h.

#### 12.7.2.48 DmiGen3ProgramStaticEq

UINT8 FSP\_M\_CONFIG::DmiGen3ProgramStaticEq

Offset 0x0406 - 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 1981 of file FspmUpd.h.

#### 12.7.2.49 DmiGen3RootPortPreset

UINT8 FSP\_M\_CONFIG::DmiGen3RootPortPreset [8]

Offset 0x0419 - 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 2113 of file FspmUpd.h.

#### 12.7.2.50 EnableC6Dram

UINT8 FSP\_M\_CONFIG::EnableC6Dram

Offset 0x01D4 - 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 1653 of file FspmUpd.h.

### 12.7.2.51 EnableSgx

UINT8 FSP\_M\_CONFIG::EnableSgx

Offset 0x01D7 - EnableSgx Enable/Disable.

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

Definition at line 1669 of file FspmUpd.h.

### 12.7.2.52 EnCmdRate

UINT8 FSP\_M\_CONFIG::EnCmdRate

Offset 0x015C - Command Rate Support CMD Rate and Limit Support Option.

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

Definition at line 1155 of file FspmUpd.h.

### 12.7.2.53 EpgEnable

UINT8 FSP\_M\_CONFIG::EpgEnable

Offset 0x015E - Energy Performance Gain Enable/disable(default) Energy Performance Gain.

\$EN\_DIS

Definition at line 1167 of file FspmUpd.h.

### 12.7.2.54 FClkFrequency

UINT8 FSP\_M\_CONFIG::FClkFrequency

Offset 0x01BC - 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 1579 of file FspmUpd.h.

### 12.7.2.55 FivrEfficiency

UINT8 FSP\_M\_CONFIG::FivrEfficiency

Offset 0x019E - Fivr Efficiency Fivr Efficiency Management; 0: Disabled; **1: Enabled.**

\$EN\_DIS

Definition at line 1447 of file FspmUpd.h.

### 12.7.2.56 FivrFaults

UINT8 FSP\_M\_CONFIG::FivrFaults

---

Offset 0x019D - Fivr Faults Fivr Faults; 0: Disabled; 1: **Enabled**.

\$EN\_DIS

Definition at line 1441 of file FspmUpd.h.

#### 12.7.2.57 FivrProtection

UINT8 FSP\_M\_CONFIG::FivrProtection

Offset 0x01B3 - FIVR PROTECTION Enable or Disable FIVR overvoltage and overcurrent protection.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1529 of file FspmUpd.h.

#### 12.7.2.58 FivrPs

UINT8 FSP\_M\_CONFIG::FivrPs

Offset 0x01B2 - FIVR PS Enable or Disable FIVR PS.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1522 of file FspmUpd.h.

#### 12.7.2.59 FivrTdc

UINT8 FSP\_M\_CONFIG::FivrTdc

Offset 0x01AE - FIVR TDC Enable or Disable FIVR TDC from PCODE.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1495 of file FspmUpd.h.

#### 12.7.2.60 ForceOltmOrRefresh2x

UINT8 FSP\_M\_CONFIG::ForceOltmOrRefresh2x

Offset 0x016C - Force OLTM or 2X Refresh when needed Disabled(Default): = Force OLTM.

Enabled: = Force 2x Refresh. \$EN\_DIS

Definition at line 1263 of file FspmUpd.h.

#### 12.7.2.61 FreqSaGvLow

UINT16 FSP\_M\_CONFIG::FreqSaGvLow

Offset 0x00AA - 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 239 of file FspmUpd.h.

#### 12.7.2.62 FreqSaGvMid

UINT16 FSP\_M\_CONFIG::FreqSaGvMid

Offset 0x00AC - 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 246 of file FspmUpd.h.

#### 12.7.2.63 FullRangeMultiplierUnlockEn

UINT8 FSP\_M\_CONFIG::FullRangeMultiplierUnlockEn

Offset 0x01AF - Full Range Multiplier unlock enable Enable or Disable communication between Punit and Core in 100MHz granularity.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1502 of file FspmUpd.h.

#### 12.7.2.64 Gen3SwEqAlwaysAttempt

UINT8 FSP\_M\_CONFIG::Gen3SwEqAlwaysAttempt

Offset 0x0471 - PEG Gen3 SwEq Always Attempt Gen3 Software Equalization will be executed every boot.

Disabled(0x0)(Default): Reuse EQ settings saved/restored from NVRAM whenever possible, Enabled(0x1): Re-test and generate new EQ values every boot, not recommended 0:Disable, 1:Enable

Definition at line 2268 of file FspmUpd.h.

#### 12.7.2.65 Gen3SwEqEnableVocTest

UINT8 FSP\_M\_CONFIG::Gen3SwEqEnableVocTest

Offset 0x0473 - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.

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

Definition at line 2286 of file FspmUpd.h.

#### 12.7.2.66 Gen3SwEqJitterDwellTime

UINT16 FSP\_M\_CONFIG::Gen3SwEqJitterDwellTime

Offset 0x04B6 - Jitter Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 1000.

---

**Warning**

Do not change from the default

Definition at line 2348 of file FspmUpd.h.

**12.7.2.67 Gen3SwEqJitterErrorTarget**

UINT16 FSP\_M\_CONFIG::Gen3SwEqJitterErrorTarget

Offset 0x04B8 - Jitter Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 1.

**Warning**

Do not change from the default

Definition at line 2353 of file FspmUpd.h.

**12.7.2.68 Gen3SwEqNumberOfPresets**

UINT8 FSP\_M\_CONFIG::Gen3SwEqNumberOfPresets

Offset 0x0472 - Select number of TxEq presets to test in the PCIe/DMI SwEq Select number of TxEq presets to test in the PCIe/DMI SwEq.

P7,P3,P5(0x0): Test Presets 7, 3, and 5, P0-P9(0x1): Test Presets 0-9, Auto(0x2)(Default): Use the current default method (Default)Auto will test Presets 7, 3, and 5. It is possible for this default to change over time;using Auto will ensure Reference Code always uses the latest default settings 0:P7 P3 P5, 1:P0 to P9, 2:Auto

Definition at line 2278 of file FspmUpd.h.

**12.7.2.69 Gen3SwEqVocDwellTime**

UINT16 FSP\_M\_CONFIG::Gen3SwEqVocDwellTime

Offset 0x04BA - VOC Dwell Time for PCIe Gen3 Software Equalization Range: 0-65535, default is 10000.

**Warning**

Do not change from the default

Definition at line 2358 of file FspmUpd.h.

**12.7.2.70 Gen3SwEqVocErrorTarget**

UINT16 FSP\_M\_CONFIG::Gen3SwEqVocErrorTarget

Offset 0x04BC - VOC Error Target for PCIe Gen3 Software Equalization Range: 0-65535, default is 2.

**Warning**

Do not change from the default

Definition at line 2363 of file FspmUpd.h.

---

### 12.7.2.71 GmAdr

UINT32 FSP\_M\_CONFIG::GmAdr

Offset 0x0268 - 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 1852 of file FspmUpd.h.

### 12.7.2.72 GtPllVoltageOffset

UINT8 FSP\_M\_CONFIG::GtPllVoltageOffset

Offset 0x0195 - GT PLL voltage offset Core PLL voltage offset.

**0: No offset.** Range 0-63

Definition at line 1395 of file FspmUpd.h.

### 12.7.2.73 GtPsmiSupport

UINT8 FSP\_M\_CONFIG::GtPsmiSupport

Offset 0x026F - Selection of PSMI Support On/Off 0(Default) = FALSE, 1 = TRUE.

When TRUE, it will allow the PSMI Support \$EN\_DIS

Definition at line 1870 of file FspmUpd.h.

### 12.7.2.74 GttMmAdr

UINT32 FSP\_M\_CONFIG::GttMmAdr

Offset 0x0264 - 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 1844 of file FspmUpd.h.

### 12.7.2.75 HeciCommunication2

UINT8 FSP\_M\_CONFIG::HeciCommunication2

Offset 0x0530 - HECI2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECI2 Device from PCI space.

\$EN\_DIS

Definition at line 2695 of file FspmUpd.h.

#### 12.7.2.76 HobBufferSize

UINT8 FSP\_M\_CONFIG::HobBufferSize

Offset 0x00D2 - 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 430 of file FspmUpd.h.

#### 12.7.2.77 HotThresholdCh0Dimm0

UINT8 FSP\_M\_CONFIG::HotThresholdCh0Dimm0

Offset 0x0138 - Hot 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 972 of file FspmUpd.h.

#### 12.7.2.78 HotThresholdCh0Dimm1

UINT8 FSP\_M\_CONFIG::HotThresholdCh0Dimm1

Offset 0x0139 - Hot 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 977 of file FspmUpd.h.

#### 12.7.2.79 HotThresholdCh1Dimm0

UINT8 FSP\_M\_CONFIG::HotThresholdCh1Dimm0

Offset 0x013A - Hot 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 982 of file FspmUpd.h.

#### 12.7.2.80 HotThresholdCh1Dimm1

UINT8 FSP\_M\_CONFIG::HotThresholdCh1Dimm1

Offset 0x013B - Hot 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 987 of file FspmUpd.h.

---

### 12.7.2.81 Idd3n

UINT16 FSP\_M\_CONFIG::Idd3n

Offset 0x0126 - 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 902 of file FspmUpd.h.

### 12.7.2.82 Idd3p

UINT16 FSP\_M\_CONFIG::Idd3p

Offset 0x0128 - 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 908 of file FspmUpd.h.

### 12.7.2.83 IgdDvmt50PreAlloc

UINT8 FSP\_M\_CONFIG::IgdDvmt50PreAlloc

Offset 0x025D - 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 1814 of file FspmUpd.h.

### 12.7.2.84 ImguClkOutEn

UINT8 FSP\_M\_CONFIG::ImguClkOutEn[5]

Offset 0x04C0 - IMGU CLKOUT Configuration The configuration of IMGU CLKOUT, 0: Disable;1: **Enable**.

\$EN\_DIS

Definition at line 2381 of file FspmUpd.h.

### 12.7.2.85 ImrRpSelection

UINT8 FSP\_M\_CONFIG::ImrRpSelection

Offset 0x056C - Root port number for IMR.

Root port number for IMR.

Definition at line 2847 of file FspmUpd.h.

### 12.7.2.86 InitPcieAspmAfterOprom

UINT8 FSP\_M\_CONFIG::InitPcieAspmAfterOprom

---

Offset 0x0417 - 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 2101 of file FspmUpd.h.

#### 12.7.2.87 InternalGfx

UINT8 FSP\_M\_CONFIG::InternalGfx

Offset 0x025E - Internal Graphics Enable/disable internal graphics.

\$EN\_DIS

Definition at line 1820 of file FspmUpd.h.

#### 12.7.2.88 IsvtIoPort

UINT8 FSP\_M\_CONFIG::IsvtIoPort

Offset 0x00D1 - ISVT IO Port Address ISVT IO Port Address.

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

Definition at line 423 of file FspmUpd.h.

#### 12.7.2.89 JtagC10PowerGateDisable

UINT8 FSP\_M\_CONFIG::JtagC10PowerGateDisable

Offset 0x01BD - 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 1586 of file FspmUpd.h.

#### 12.7.2.90 KtDeviceEnable

UINT8 FSP\_M\_CONFIG::KtDeviceEnable

Offset 0x0531 - Enable KT device Test, 0: disable, 1: enable, Enable or Disable KT device.

\$EN\_DIS

Definition at line 2701 of file FspmUpd.h.

#### 12.7.2.91 LockPTMregs

UINT8 FSP\_M\_CONFIG::LockPTMregs

Offset 0x0405 - Lock PCU Thermal Management registers Lock PCU Thermal Management registers.

---

Enable(Default)=1, Disable=0 \$EN\_DIS

Definition at line 1974 of file FspmUpd.h.

#### 12.7.2.92 MarginLimitCheck

UINT8 FSP\_M\_CONFIG::MarginLimitCheck

Offset 0x00EE - Margin Limit Check Margin Limit Check.

Choose level of margin check 0:Disable, 1:L1, 2:L2, 3:Both

Definition at line 598 of file FspmUpd.h.

#### 12.7.2.93 McPllVoltageOffset

UINT8 FSP\_M\_CONFIG::McPllVoltageOffset

Offset 0x0198 - Memory Controller PLL voltage offset Core PLL voltage offset.

**0: No offset.** Range 0-63

Definition at line 1410 of file FspmUpd.h.

#### 12.7.2.94 MemoryTrace

UINT8 FSP\_M\_CONFIG::MemoryTrace

Offset 0x0109 - Memory Trace Enable Memory Trace of Ch 0 to Ch 1 using Stacked Mode.

Both channels must be of equal size. This option may change TOLUD and REMAP values as needed. \$EN\_DIS

Definition at line 753 of file FspmUpd.h.

#### 12.7.2.95 MmioSize

UINT16 FSP\_M\_CONFIG::MmioSize

Offset 0x03FA - MMIO Size Size of MMIO space reserved for devices.

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

Definition at line 1929 of file FspmUpd.h.

#### 12.7.2.96 NonCoreHighVoltageMode

UINT8 FSP\_M\_CONFIG::NonCoreHighVoltageMode

Offset 0x01A4 - Non-Core High Voltage Mode Enable High Voltage Mode in the non-core FIVR domains (Ring/GT).

Used for LN2 cold boot mitigation. **0 - Disable**, 1 - Enable \$EN\_DIS

Definition at line 1476 of file FspmUpd.h.

---

### 12.7.2.97 OcLock

UINT8 FSP\_M\_CONFIG::OcLock

Offset 0x0182 - Over clocking Lock Over clocking Lock Enable/Disable; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 1320 of file FspmUpd.h.

### 12.7.2.98 PanelPowerEnable

UINT8 FSP\_M\_CONFIG::PanelPowerEnable

Offset 0x0270 - 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 1877 of file FspmUpd.h.

### 12.7.2.99 PcdDebugInterfaceFlags

UINT8 FSP\_M\_CONFIG::PcdDebugInterfaceFlags

Offset 0x0755 - Debug Interfaces Debug Interfaces.

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

Definition at line 3066 of file FspmUpd.h.

### 12.7.2.100 PcdIsaSerialUartBase

UINT8 FSP\_M\_CONFIG::PcdIsaSerialUartBase

Offset 0x075F - ISA Serial Base selection Select ISA Serial Base address.

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

Definition at line 3109 of file FspmUpd.h.

### 12.7.2.101 PcdSerialDebugBaudRate

UINT8 FSP\_M\_CONFIG::PcdSerialDebugBaudRate

Offset 0x0760 - 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 3115 of file FspmUpd.h.

### 12.7.2.102 PcdSerialDebugLevel

UINT8 FSP\_M\_CONFIG::PcdSerialDebugLevel

---

Offset 0x0098 - 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 136 of file FspmUpd.h.

#### 12.7.2.103 PchLpcEnhancePort8xhDecoding

```
UINT8 FSP_M_CONFIG::PchLpcEnhancePort8xhDecoding
```

Offset 0x074F - PCH LPC Enhance the port 8xh decoding Original LPC only decodes one byte of port 80h.

\$EN\_DIS

Definition at line 3025 of file FspmUpd.h.

#### 12.7.2.104 PchNumRsvdSmbusAddresses

```
UINT8 FSP_M_CONFIG::PchNumRsvdSmbusAddresses
```

Offset 0x055A - Number of RsvdSmbusAddressTable.

The number of elements in the RsvdSmbusAddressTable.

Definition at line 2786 of file FspmUpd.h.

#### 12.7.2.105 PchPort80Route

```
UINT8 FSP_M_CONFIG::PchPort80Route
```

Offset 0x0750 - PCH Port80 Route Control where the Port 80h cycles are sent, 0: LPC; 1: PCI.

\$EN\_DIS

Definition at line 3031 of file FspmUpd.h.

#### 12.7.2.106 PchSmbAlertEnable

```
UINT8 FSP_M_CONFIG::PchSmbAlertEnable
```

Offset 0x0557 - Enable SMBus Alert Pin Enable SMBus Alert Pin.

\$EN\_DIS

Definition at line 2776 of file FspmUpd.h.

#### 12.7.2.107 PchTraceHubMemReg0Size

```
UINT8 FSP_M_CONFIG::PchTraceHubMemReg0Size
```

Offset 0x0551 - 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 2738 of file FspmUpd.h.

#### 12.7.2.108 PchTraceHubMemReg1Size

UINT8 FSP\_M\_CONFIG::PchTraceHubMemReg1Size

Offset 0x0552 - 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 2745 of file FspmUpd.h.

#### 12.7.2.109 PchTraceHubMode

UINT8 FSP\_M\_CONFIG::PchTraceHubMode

Offset 0x0550 - 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 2731 of file FspmUpd.h.

#### 12.7.2.110 PcieImrSize

UINT16 FSP\_M\_CONFIG::PcieImrSize

Offset 0x056A - Size of PCIe IMR.

Size of PCIe IMR in megabytes

Definition at line 2842 of file FspmUpd.h.

#### 12.7.2.111 PcieMultipleSegmentEnabled

UINT8 FSP\_M\_CONFIG::PcieMultipleSegmentEnabled

Offset 0x04DD - 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 2505 of file FspmUpd.h.

#### 12.7.2.112 PcieRpEnableMask

UINT32 FSP\_M\_CONFIG::PcieRpEnableMask

Offset 0x0564 - 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 2827 of file FspmUpd.h.

#### 12.7.2.113 Peg0Gen3EqPh2Enable

UINT8 FSP\_M\_CONFIG::Peg0Gen3EqPh2Enable

Offset 0x0468 - Phase2 EQ enable on the PEG 0:1:0.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2192 of file FspmUpd.h.

#### 12.7.2.114 Peg0Gen3EqPh3Method

UINT8 FSP\_M\_CONFIG::Peg0Gen3EqPh3Method

Offset 0x046C - Phase3 EQ method on the PEG 0:1:0.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2223 of file FspmUpd.h.

#### 12.7.2.115 Peg1Gen3EqPh2Enable

UINT8 FSP\_M\_CONFIG::Peg1Gen3EqPh2Enable

Offset 0x0469 - Phase2 EQ enable on the PEG 0:1:1.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2199 of file FspmUpd.h.

#### 12.7.2.116 Peg1Gen3EqPh3Method

UINT8 FSP\_M\_CONFIG::Peg1Gen3EqPh3Method

Offset 0x046D - Phase3 EQ method on the PEG 0:1:1.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2233 of file FspmUpd.h.

---

### 12.7.2.117 Peg2Gen3EqPh2Enable

UINT8 FSP\_M\_CONFIG::Peg2Gen3EqPh2Enable

Offset 0x046A - Phase2 EQ enable on the PEG 0:1:2.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2206 of file FspmUpd.h.

### 12.7.2.118 Peg2Gen3EqPh3Method

UINT8 FSP\_M\_CONFIG::Peg2Gen3EqPh3Method

Offset 0x046E - Phase3 EQ method on the PEG 0:1:2.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2243 of file FspmUpd.h.

### 12.7.2.119 Peg3Gen3EqPh2Enable

UINT8 FSP\_M\_CONFIG::Peg3Gen3EqPh2Enable

Offset 0x046B - Phase2 EQ enable on the PEG 0:1:3.

Phase2 EQ enable on the PEG 0:1:0. Disabled(0x0): Disable phase 2, Enabled(0x1): Enable phase 2, Auto(0x2)(Default): Use the current default method 0:Disable, 1:Enable, 2:Auto

Definition at line 2213 of file FspmUpd.h.

### 12.7.2.120 Peg3Gen3EqPh3Method

UINT8 FSP\_M\_CONFIG::Peg3Gen3EqPh3Method

Offset 0x046F - Phase3 EQ method on the PEG 0:1:3.

PEG Gen3 Equalization Phase3. Auto(0x0)(Default): Use the current default method, HwEq(0x1): Use Adaptive Hardware Equalization, SwEq(0x2): Use Adaptive Software Equalization (Implemented in BIOS Reference Code), Static(0x3): Use the Static EQs provided in DmiGen3EndPointPreset array for Phase1 AND Phase3 (Instead of just Phase1), Disabled(0x4): Bypass Equalization Phase 3 0:Auto, 1:HwEq, 2:SwEq, 3:StaticEq, 4:BypassPhase3

Definition at line 2253 of file FspmUpd.h.

### 12.7.2.121 PegDataPtr

UINT32 FSP\_M\_CONFIG::PegDataPtr

Offset 0x0440 - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA\_PEG\_DATA) and platform code can save/restore this data to skip preset search in the following boots.

Range: 0-0xFFFFFFFF, default is 0

---

Definition at line 2144 of file FspmUpd.h.

#### 12.7.2.122 PegDisableSpreadSpectrumClocking

UINT8 FSP\_M\_CONFIG::PegDisableSpreadSpectrumClocking

Offset 0x0418 - PCIe Disable Spread Spectrum Clocking PCIe Disable Spread Spectrum Clocking.

Normal Operation(0x0)(Default) - SSC enabled, Disable SSC(0x1) - Disable SSC per platform design or for compliance testing 0:Normal Operation, 1:Disable SSC

Definition at line 2108 of file FspmUpd.h.

#### 12.7.2.123 PegGen3EndPointHint

UINT8 FSP\_M\_CONFIG::PegGen3EndPointHint [20]

Offset 0x04A1 - PEG Gen3 End port Hint values per lane Used for programming PEG Gen3 Hint values per lane.

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

Definition at line 2339 of file FspmUpd.h.

#### 12.7.2.124 PegGen3EndPointPreset

UINT8 FSP\_M\_CONFIG::PegGen3EndPointPreset [20]

Offset 0x048D - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.

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

Definition at line 2334 of file FspmUpd.h.

#### 12.7.2.125 PegGen3ProgramStaticEq

UINT8 FSP\_M\_CONFIG::PegGen3ProgramStaticEq

Offset 0x0470 - Enable/Disable PEG GEN3 Static EQ Phase1 programming Program PEG Gen3 EQ Phase1 Static Presets.

Disabled(0x0): Disable EQ Phase1 Static Presets Programming, Enabled(0x1)(Default): Enable EQ Phase1 Static Presets Programming \$EN\_DIS

Definition at line 2260 of file FspmUpd.h.

#### 12.7.2.126 PegGen3RootPortPreset

UINT8 FSP\_M\_CONFIG::PegGen3RootPortPreset [20]

Offset 0x0479 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.

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

---

Definition at line 2329 of file FspmUpd.h.

#### 12.7.2.127 PegGenerateBdatMarginTable

UINT8 FSP\_M\_CONFIG::PegGenerateBdatMarginTable

Offset 0x0476 - Generate PCIe BDAT Margin Table Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

Disabled(0x0)(Default): Normal Operation - Disable PCIe BDAT margin data generation, Enable(0x1): Generate PCIe BDAT margin data \$EN\_DIS

Definition at line 2307 of file FspmUpd.h.

#### 12.7.2.128 PegImrEnable

UINT8 FSP\_M\_CONFIG::PegImrEnable

Offset 0x04FE - PEG IMR support This option configures the IMR support for PEG.

(def=Disable) \$EN\_DIS

Definition at line 2602 of file FspmUpd.h.

#### 12.7.2.129 PegImrRpSelection

UINT8 FSP\_M\_CONFIG::PegImrRpSelection

Offset 0x04FF - PEG Root port number for IMR.

PEG Root port number for IMR.

Definition at line 2607 of file FspmUpd.h.

#### 12.7.2.130 PegRxCemLoopbackLane

UINT8 FSP\_M\_CONFIG::PegRxCemLoopbackLane

Offset 0x0475 - PCIe Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specified Lane (0 - 15) will be used for RxCEMLoopback.

Default is Lane 0

Definition at line 2299 of file FspmUpd.h.

#### 12.7.2.131 PegRxCemNonProtocolAwareness

UINT8 FSP\_M\_CONFIG::PegRxCemNonProtocolAwareness

Offset 0x0477 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

Disabled(0x0)(Default): Normal Operation - Disable non-protocol awareness, Enable(0x1): Non-Protocol Awareness Enabled - Enable non-protocol awareness for compliance testing \$EN\_DIS

---

Definition at line 2316 of file FspmUpd.h.

#### 12.7.2.132 PerCoreRatioLimit

UINT8 FSP\_M\_CONFIG::PerCoreRatioLimit[8]

Offset 0x01A6 - Per Core Ratio Limit Per Core Ratio Limit.

Range 0 - 120. **Default = 0**, no BIOS programming of per core ratio.

Definition at line 1489 of file FspmUpd.h.

#### 12.7.2.133 PlatformDebugConsent

UINT8 FSP\_M\_CONFIG::PlatformDebugConsent

Offset 0x0754 - 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 0:Disabled, 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 3060 of file FspmUpd.h.

#### 12.7.2.134 PrmrrSize

UINT32 FSP\_M\_CONFIG::PrmrrSize

Offset 0x01DC - PrmrrSize Enable/Disable.

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

Definition at line 1684 of file FspmUpd.h.

#### 12.7.2.135 ProbelessTrace

UINT8 FSP\_M\_CONFIG::ProbelessTrace

Offset 0x00B5 - 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 296 of file FspmUpd.h.

#### 12.7.2.136 PvdRatioThreshold

UINT8 FSP\_M\_CONFIG::PvdRatioThreshold

Offset 0x01B8 - Post Divider (PVD) Ratio Threshold PVD Ratio Threshold.

**0: No offset.** Range 0-63

---

Definition at line 1551 of file FspmUpd.h.

#### 12.7.2.137 PwdwnIdleCounter

UINT8 FSP\_M\_CONFIG::PwdwnIdleCounter

Offset 0x016D - 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 1269 of file FspmUpd.h.

#### 12.7.2.138 RankInterleave

UINT8 FSP\_M\_CONFIG::RankInterleave

Offset 0x0107 - 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 740 of file FspmUpd.h.

#### 12.7.2.139 Ratio

UINT8 FSP\_M\_CONFIG::Ratio

Offset 0x00BB - 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 330 of file FspmUpd.h.

#### 12.7.2.140 RealtimeMemoryTiming

UINT8 FSP\_M\_CONFIG::RealtimeMemoryTiming

Offset 0x04D4 - 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 2450 of file FspmUpd.h.

#### 12.7.2.141 RefClk

UINT8 FSP\_M\_CONFIG::RefClk

Offset 0x00BA - Memory Reference Clock 100MHz, 133MHz.

0:133MHz, 1:100MHz

Definition at line 323 of file FspmUpd.h.

---

#### 12.7.2.142 RetrainOnFastFail

UINT8 FSP\_M\_CONFIG::RetrainOnFastFail

Offset 0x0171 - Retrain on Fast Fail Restart MRC in Cold mode if SW MemTest fails during Fast flow.

Default = Enabled \$EN\_DIS

Definition at line 1292 of file FspmUpd.h.

#### 12.7.2.143 RhSolution

UINT8 FSP\_M\_CONFIG::RhSolution

Offset 0x015F - Row Hammer Solution Type of method used to prevent Row Hammer.

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

Definition at line 1173 of file FspmUpd.h.

#### 12.7.2.144 RingDownBin

UINT8 FSP\_M\_CONFIG::RingDownBin

Offset 0x0186 - 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 1345 of file FspmUpd.h.

#### 12.7.2.145 RingMaxOcRatio

UINT8 FSP\_M\_CONFIG::RingMaxOcRatio

Offset 0x0185 - 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 1338 of file FspmUpd.h.

#### 12.7.2.146 RingPllVoltageOffset

UINT8 FSP\_M\_CONFIG::RingPllVoltageOffset

Offset 0x0196 - Ring PLL voltage offset Core PLL voltage offset.

**0: No offset.** Range 0-63

Definition at line 1400 of file FspmUpd.h.

#### 12.7.2.147 RingVoltageAdaptive

UINT16 FSP\_M\_CONFIG::RingVoltageAdaptive

---

Offset 0x018A - 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 1363 of file FspmUpd.h.

#### 12.7.2.148 RingVoltageMode

UINT8 FSP\_M\_CONFIG::RingVoltageMode

Offset 0x0187 - Ring voltage mode Ring voltage mode; **0: Adaptive**; 1: Override.

\$EN\_DIS

Definition at line 1351 of file FspmUpd.h.

#### 12.7.2.149 RingVoltageOffset

UINT16 FSP\_M\_CONFIG::RingVoltageOffset

Offset 0x018C - Ring Turbo voltage Offset The voltage offset applied to the ring while operating in turbo mode.

Valid Range 0 to 1000

Definition at line 1368 of file FspmUpd.h.

#### 12.7.2.150 RingVoltageOverride

UINT16 FSP\_M\_CONFIG::RingVoltageOverride

Offset 0x0188 - 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 1357 of file FspmUpd.h.

#### 12.7.2.151 RMT

UINT8 FSP\_M\_CONFIG::RMT

Offset 0x00ED - Rank Margin Tool Enable/disable Rank Margin Tool.

\$EN\_DIS

Definition at line 592 of file FspmUpd.h.

#### 12.7.2.152 RMTBIT

UINT8 FSP\_M\_CONFIG::RMTBIT

Offset 0x0172 - Rank Margin Tool Per Bit Enable/disable Rank Margin Tool Per Bit.

\$EN\_DIS

---

Definition at line 1298 of file FspmUpd.h.

#### 12.7.2.153 RMTLoopCount

UINT8 FSP\_M\_CONFIG::RMTLoopCount

Offset 0x016F - RMTLoopCount Specifies the Loop Count to be used during Rank Margin Tool Testing.

0 - AUTO

Definition at line 1280 of file FspmUpd.h.

#### 12.7.2.154 RmtPerTask

UINT8 FSP\_M\_CONFIG::RmtPerTask

Offset 0x00A5 - 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 210 of file FspmUpd.h.

#### 12.7.2.155 SafeMode

UINT8 FSP\_M\_CONFIG::SafeMode

Offset 0x00B3 - 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 282 of file FspmUpd.h.

#### 12.7.2.156 SaGv

UINT8 FSP\_M\_CONFIG::SaGv

Offset 0x009C - 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 161 of file FspmUpd.h.

#### 12.7.2.157 SaPcieRpEnableMask

UINT32 FSP\_M\_CONFIG::SaPcieRpEnableMask

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

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

Definition at line 2640 of file FspmUpd.h.

---

### 12.7.2.158 SaPcieRpLinkDownGpios

UINT8 FSP\_M\_CONFIG::SaPcieRpLinkDownGpios

Offset 0x050C - 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 2647 of file FspmUpd.h.

### 12.7.2.159 SaPllFreqOverride

UINT8 FSP\_M\_CONFIG::SaPllFreqOverride

Offset 0x01B0 - SA PLL Freq override Enable or Disable SA PLL Freq override to 1600MHz instead of 3200MHz on Desktop.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1509 of file FspmUpd.h.

### 12.7.2.160 SaPllVoltageOffset

UINT8 FSP\_M\_CONFIG::SaPllVoltageOffset

Offset 0x0197 - System Agent PLL voltage offset Core PLL voltage offset.

**0: No offset.** Range 0-63

Definition at line 1405 of file FspmUpd.h.

### 12.7.2.161 ScanExtGfxForLegacyOpRom

UINT8 FSP\_M\_CONFIG::ScanExtGfxForLegacyOpRom

Offset 0x0404 - 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 1968 of file FspmUpd.h.

### 12.7.2.162 ScramblerSupport

UINT8 FSP\_M\_CONFIG::ScramblerSupport

Offset 0x00B2 - Scrambler Support This option enables data scrambling in memory.

\$EN\_DIS

Definition at line 276 of file FspmUpd.h.

---

**12.7.2.163 SerialIoUartDebugAutoFlow**

UINT8 FSP\_M\_CONFIG::SerialIoUartDebugAutoFlow

Offset 0x0757 - Serial Io Uart Debug Auto Flow Enables UART hardware flow control, CTS and RTS lines.

\$EN\_DIS

Definition at line 3079 of file FspmUpd.h.

**12.7.2.164 SerialIoUartDebugBaudRate**

UINT32 FSP\_M\_CONFIG::SerialIoUartDebugBaudRate

Offset 0x0758 - Serial Io Uart Debug BaudRate Set default BaudRate Supported from 0 - default to 6000000.

Recommended values 9600, 19200, 57600, 115200, 460800, 921600, 1500000, 1843200, 3000000, 3686400, 6000000

Definition at line 3085 of file FspmUpd.h.

**12.7.2.165 SerialIoUartDebugControllerNumber**

UINT8 FSP\_M\_CONFIG::SerialIoUartDebugControllerNumber

Offset 0x0756 - Serial Io Uart Debug Controller Number Select SerialIo Uart Controller for debug.

Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 3073 of file FspmUpd.h.

**12.7.2.166 SerialIoUartDebugDataBits**

UINT8 FSP\_M\_CONFIG::SerialIoUartDebugDataBits

Offset 0x075E - Serial Io Uart Debug Data Bits Set default word length.

0: Default, 5,6,7,8 5:5BITS, 6:6BITS, 7:7BITS, 8:8BITS

Definition at line 3103 of file FspmUpd.h.

**12.7.2.167 SerialIoUartDebugParity**

UINT8 FSP\_M\_CONFIG::SerialIoUartDebugParity

Offset 0x075C - Serial Io Uart Debug Parity Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 3091 of file FspmUpd.h.

**12.7.2.168 SerialIoUartDebugStopBits**

UINT8 FSP\_M\_CONFIG::SerialIoUartDebugStopBits

---

Offset 0x075D - Serial Io Uart Debug Stop Bits Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 3097 of file FspmUpd.h.

#### 12.7.2.169 SinitMemorySize

UINT32 FSP\_M\_CONFIG::SinitMemorySize

Offset 0x01E4 - SinitMemorySize Enable/Disable.

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

Definition at line 1704 of file FspmUpd.h.

#### 12.7.2.170 SkipMbpHob

UINT8 FSP\_M\_CONFIG::SkipMbpHob

Offset 0x052F - Skip MBP HOB Test, 0: disable, 1: enable, Enable/Disable MOB HOB.

\$EN\_DIS

Definition at line 2689 of file FspmUpd.h.

#### 12.7.2.171 SkipMplnitPreMem

UINT8 FSP\_M\_CONFIG::SkipMpInitPreMem

Offset 0x01C5 - 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 1635 of file FspmUpd.h.

#### 12.7.2.172 SmbusArpEnable

UINT8 FSP\_M\_CONFIG::SmbusArpEnable

Offset 0x0554 - Enable SMBus ARP support Enable SMBus ARP support.

\$EN\_DIS

Definition at line 2757 of file FspmUpd.h.

#### 12.7.2.173 SmbusDynamicPowerGating

UINT8 FSP\_M\_CONFIG::SmbusDynamicPowerGating

Offset 0x0555 - Smbus dynamic power gating Disable or Enable Smbus dynamic power gating.

\$EN\_DIS

Definition at line 2763 of file FspmUpd.h.

---

#### 12.7.2.174 SmbusEnable

UINT8 FSP\_M\_CONFIG::SmbusEnable

Offset 0x0553 - Enable SMBus Enable/disable SMBus controller.

\$EN\_DIS

Definition at line 2751 of file FspmUpd.h.

#### 12.7.2.175 SmbusSpdWriteDisable

UINT8 FSP\_M\_CONFIG::SmbusSpdWriteDisable

Offset 0x0556 - 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 2770 of file FspmUpd.h.

#### 12.7.2.176 SpdAddressTable

UINT8 FSP\_M\_CONFIG::SpdAddressTable[4]

Offset 0x0050 - Spd Address Tabl Specify SPD Address table for CH0D0/CH0D1/CH1D0&CH1D1.

MemorySpdPtr will be used if SPD Address is 00

Definition at line 82 of file FspmUpd.h.

#### 12.7.2.177 SpdProfileSelected

UINT8 FSP\_M\_CONFIG::SpdProfileSelected

Offset 0x00B7 - 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 310 of file FspmUpd.h.

#### 12.7.2.178 TcssDma0En

UINT8 FSP\_M\_CONFIG::TcssDma0En

Offset 0x04DB - TCSS DMA0 Enable Set TCSS DMA0.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2492 of file FspmUpd.h.

---

**12.7.2.179 TcssDma1En**

UINT8 FSP\_M\_CONFIG::TcssDma1En

Offset 0x04DC - TCSS DMA1 Enable Set TCSS DMA1.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2498 of file FspmUpd.h.

**12.7.2.180 TcssItbtPcie0En**

UINT8 FSP\_M\_CONFIG::TcssItbtPcie0En

Offset 0x04D5 - TCSS Thunderbolt PCIE Root Port 0 Enable Set TCSS Thunderbolt PCIE Root Port 0.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2456 of file FspmUpd.h.

**12.7.2.181 TcssItbtPcie1En**

UINT8 FSP\_M\_CONFIG::TcssItbtPcie1En

Offset 0x04D6 - TCSS Thunderbolt PCIE Root Port 1 Enable Set TCSS Thunderbolt PCIE Root Port 1.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2462 of file FspmUpd.h.

**12.7.2.182 TcssItbtPcie2En**

UINT8 FSP\_M\_CONFIG::TcssItbtPcie2En

Offset 0x04D7 - TCSS Thunderbolt PCIE Root Port 2 Enable Set TCSS Thunderbolt PCIE Root Port 2.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2468 of file FspmUpd.h.

**12.7.2.183 TcssItbtPcie3En**

UINT8 FSP\_M\_CONFIG::TcssItbtPcie3En

Offset 0x04D8 - TCSS Thunderbolt PCIE Root Port 3 Enable Set TCSS Thunderbolt PCIE Root Port 3.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 2474 of file FspmUpd.h.

**12.7.2.184 TcssXdcIEn**

UINT8 FSP\_M\_CONFIG::TcssXdcIEn

Offset 0x04DA - 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 2486 of file FspmUpd.h.

#### 12.7.2.185 TcssXhciEn

UINT8 FSP\_M\_CONFIG::TcssXhciEn

Offset 0x04D9 - 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 2480 of file FspmUpd.h.

#### 12.7.2.186 TgaSize

UINT32 FSP\_M\_CONFIG::TgaSize

Offset 0x0204 - TgaSize Enable/Disable.

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

Definition at line 1738 of file FspmUpd.h.

#### 12.7.2.187 ThrtCkeMinTmr

UINT8 FSP\_M\_CONFIG::ThrtCkeMinTmr

Offset 0x0158 - 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 1133 of file FspmUpd.h.

#### 12.7.2.188 ThrtCkeMinTmrLpddr

UINT8 FSP\_M\_CONFIG::ThrtCkeMinTmrLpddr

Offset 0x0170 - Throttler CKEMin Timer for LPDDR LPDDR Timer value for CKEMin, range[255;0].

Req'd min of SC\_ROUND\_T + BYTE\_LENGTH (4). Dfault is 0x40

Definition at line 1286 of file FspmUpd.h.

#### 12.7.2.189 TjMaxOffset

UINT8 FSP\_M\_CONFIG::TjMaxOffset

Offset 0x019C - 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 1435 of file FspmUpd.h.

---

### 12.7.2.190 TmeEnable

UINT8 FSP\_M\_CONFIG::TmeEnable

Offset 0x01C1 - Enable or Disable TME Enable or Disable TME; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 1609 of file FspmUpd.h.

### 12.7.2.191 TrainTrace

UINT8 FSP\_M\_CONFIG::TrainTrace

Offset 0x00A4 - 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 203 of file FspmUpd.h.

### 12.7.2.192 tRTP

UINT8 FSP\_M\_CONFIG::tRTP

Offset 0x00C9 - 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 380 of file FspmUpd.h.

### 12.7.2.193 TschwFixup

UINT8 FSP\_M\_CONFIG::TschwFixup

Offset 0x01B4 - TSC HW Fixup Enable or Disable Core HW Fixup during TSC copy from PMA and APIC.

**0: Disable**. 1: Enable. \$EN\_DIS

Definition at line 1536 of file FspmUpd.h.

### 12.7.2.194 TsegSize

UINT32 FSP\_M\_CONFIG::TsegSize

Offset 0x03FC - Tseg Size Size of SMRAM memory reserved.

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

Definition at line 1935 of file FspmUpd.h.

### 12.7.2.195 TsodAlarmwindowLockBit

UINT8 FSP\_M\_CONFIG::TsodAlarmwindowLockBit

Offset 0x0167 - 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 1229 of file FspmUpd.h.

#### 12.7.2.196 TsodCriticalEventOnly

UINT8 FSP\_M\_CONFIG::TsodCriticalEventOnly

Offset 0x0165 - Critical event only Disable:Trips on alarm or critical.

Enable:Trips only if criticaal temperature is reached \$EN\_DIS

Definition at line 1215 of file FspmUpd.h.

#### 12.7.2.197 TsodCriticaltripLockBit

UINT8 FSP\_M\_CONFIG::TsodCriticaltripLockBit

Offset 0x0168 - 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 1236 of file FspmUpd.h.

#### 12.7.2.198 TsodEventMode

UINT8 FSP\_M\_CONFIG::TsodEventMode

Offset 0x0163 - Event mode Disable:Comparator mode.

Enable:Interrupt mode \$EN\_DIS

Definition at line 1201 of file FspmUpd.h.

#### 12.7.2.199 TsodEventOutputControl

UINT8 FSP\_M\_CONFIG::TsodEventOutputControl

Offset 0x0166 - Event output control Disable:Event output disable.

Enable:Event output enabled \$EN\_DIS

Definition at line 1222 of file FspmUpd.h.

#### 12.7.2.200 TsodEventPolarity

UINT8 FSP\_M\_CONFIG::TsodEventPolarity

Offset 0x0164 - EVENT polarity Disable:Active LOW.

---

Enable:Active HIGH \$EN\_DIS

Definition at line 1208 of file FspmUpd.h.

#### 12.7.2.201 TsodManualEnable

UINT8 FSP\_M\_CONFIG::TsodManualEnable

Offset 0x016B - 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 1256 of file FspmUpd.h.

#### 12.7.2.202 TsodShutdownMode

UINT8 FSP\_M\_CONFIG::TsodShutdownMode

Offset 0x0169 - Shutdown mode Disable:Temperature sensor enable.

Enable:Temperature sensor disable \$EN\_DIS

Definition at line 1243 of file FspmUpd.h.

#### 12.7.2.203 TsodTcritMax

UINT8 FSP\_M\_CONFIG::TsodTcritMax

Offset 0x0162 - 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 1194 of file FspmUpd.h.

#### 12.7.2.204 Txt

UINT8 FSP\_M\_CONFIG::Txt

Offset 0x01D8 - Txt Enable/Disable.

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

Definition at line 1675 of file FspmUpd.h.

#### 12.7.2.205 TxtAcheckRequest

UINT8 FSP\_M\_CONFIG::TxtAcheckRequest

Offset 0x01E0 - TxtAcheckRequest Enable/Disable.

---

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

Definition at line 1690 of file FspmUpd.h.

#### 12.7.2.206 TxtDprMemoryBase

UINT64 FSP\_M\_CONFIG::TxtDprMemoryBase

Offset 0x01F0 - TxtDprMemoryBase Enable/Disable.

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

Definition at line 1718 of file FspmUpd.h.

#### 12.7.2.207 TxtDprMemorySize

UINT32 FSP\_M\_CONFIG::TxtDprMemorySize

Offset 0x01F8 - TxtDprMemorySize Enable/Disable.

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

Definition at line 1723 of file FspmUpd.h.

#### 12.7.2.208 TxtHeapMemorySize

UINT32 FSP\_M\_CONFIG::TxtHeapMemorySize

Offset 0x01E8 - TxtHeapMemorySize Enable/Disable.

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

Definition at line 1709 of file FspmUpd.h.

#### 12.7.2.209 TxtImplemented

UINT8 FSP\_M\_CONFIG::TxtImplemented

Offset 0x0400 - 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 1942 of file FspmUpd.h.

#### 12.7.2.210 TxtLcpPdBase

UINT64 FSP\_M\_CONFIG::TxtLcpPdBase

Offset 0x0208 - TxtLcpPdBase Enable/Disable.

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

Definition at line 1743 of file FspmUpd.h.

---

#### 12.7.2.211 TxtLcpPdSize

UINT64 FSP\_M\_CONFIG::TxtLcpPdSize

Offset 0x0210 - TxtLcpPdSize Enable/Disable.

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

Definition at line 1748 of file FspmUpd.h.

#### 12.7.2.212 UserBudgetEnable

UINT8 FSP\_M\_CONFIG::UserBudgetEnable

Offset 0x0161 - User Manual Budget Disabled: Configuration of memories will defined the Budget value.

Enabled: User Input will be used. \$EN\_DIS

Definition at line 1187 of file FspmUpd.h.

#### 12.7.2.213 UserThresholdEnable

UINT8 FSP\_M\_CONFIG::UserThresholdEnable

Offset 0x0160 - User Manual Threshold Disabled: Predefined threshold will be used.

Enabled: User Input will be used. \$EN\_DIS

Definition at line 1180 of file FspmUpd.h.

#### 12.7.2.214 VccInVoltageOverride

UINT16 FSP\_M\_CONFIG::VccInVoltageOverride

Offset 0x01A0 - VccIn Voltage Override This will override VccIn output voltage level to the voltage value specified.

Valid Range 0 to 3000

Definition at line 1457 of file FspmUpd.h.

#### 12.7.2.215 VccinVrMaxVoltage

UINT16 FSP\_M\_CONFIG::VccinVrMaxVoltage

Offset 0x01B6 - VccIN VR MAX Voltage The new VccIN VR MAX Voltage to allow requesting in U3.13V format.

Valid Range is in U3.13 from 0 to 7999V.

Definition at line 1546 of file FspmUpd.h.

---

### 12.7.2.216 VddVoltage

UINT16 FSP\_M\_CONFIG::VddVoltage

Offset 0x00B8 - 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 317 of file FspmUpd.h.

### 12.7.2.217 VmxEnable

UINT8 FSP\_M\_CONFIG::VmxEnable

Offset 0x01BF - Enable or Disable VMX Enable or Disable VMX; 0: Disable; **1: Enable.**

\$EN\_DIS

Definition at line 1598 of file FspmUpd.h.

### 12.7.2.218 WarmThresholdCh0Dimm0

UINT8 FSP\_M\_CONFIG::WarmThresholdCh0Dimm0

Offset 0x0134 - 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 952 of file FspmUpd.h.

### 12.7.2.219 WarmThresholdCh0Dimm1

UINT8 FSP\_M\_CONFIG::WarmThresholdCh0Dimm1

Offset 0x0135 - 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 957 of file FspmUpd.h.

### 12.7.2.220 WarmThresholdCh1Dimm0

UINT8 FSP\_M\_CONFIG::WarmThresholdCh1Dimm0

Offset 0x0136 - 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 962 of file FspmUpd.h.

### 12.7.2.221 WarmThresholdCh1Dimm1

UINT8 FSP\_M\_CONFIG::WarmThresholdCh1Dimm1

---

Offset 0x0137 - Warm Threshold Ch1 Dimm1 range[255;0]=[31.875;0] in W for OLTm, [127.5;0] in C for CLTM.

Default is 255

Definition at line 967 of file FspmUpd.h.

#### 12.7.2.222 WdtDisableAndLock

```
UINT8 FSP_M_CONFIG::WdtDisableAndLock
```

Offset 0x0751 - Disable and Lock Watch Dog Register Set 1 to clear WDT status, then disable and lock WDT registers.

\$EN\_DIS

Definition at line 3037 of file FspmUpd.h.

#### 12.7.2.223 XhciPllOverride

```
UINT8 FSP_M_CONFIG::XhciPllOverride
```

Offset 0x01B1 - XHCI PLL override Enable or Disable XHCI PLL override to use TMU PLL instead of SA PLL.

**0: Disable.** 1: Enable. \$EN\_DIS

Definition at line 1516 of file FspmUpd.h.

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

- [FspmUpd.h](#)

## 12.8 FSP\_M\_RESTRICTED\_CONFIG Struct Reference

Fsp M Restricted Configuration.

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

### Public Attributes

- [UINT32 Signature](#)  
*Offset 0x0798.*
- [UINT8 AsyncOdtDis](#)  
*Offset 0x079C - Asynchronous ODT This option configures the Memory Controller Asynchronous ODT control 0→:Enabled, 1:Disabled.*
- [UINT8 PowerDownMode](#)  
*Offset 0x079D - Power Down Mode This option controls command bus tristating during idle periods 0x0:No Power Down, 0x1:APD, 0x6:PPD DLL OFF, 0xFF:Auto.*
- [UINT8 WeaklockEn](#)  
*Offset 0x079E - DLL Weak Lock Support Enables/Disable DLL Weak Lock Support \$EN\_DIS.*
- [UINT8 Force1Dpc](#)  
*Offset 0x079F - Force 1 DPC config Enables/Disable Force 1 DPC config \$EN\_DIS.*
- [UINT8 ForceSingleRank](#)  
*Offset 0x07A0 - Fore Single Rank config Enables/Disable Fore Single Rank config \$EN\_DIS.*
- [UINT8 PerBankRefresh](#)  
*Offset 0x07A1 - PerBankRefresh Control of Per Bank Refresh feature for LPDDR DRAMs \$EN\_DIS.*

- UINT16 [SrefCfgIdleTmr](#)  
*Offset 0x07A2 - SelfRefresh IdleTimer SelfRefresh IdleTimer, Default is 512.*
- UINT8 [OpportunisticRead](#)  
*Offset 0x07A4 - Opportunistic Read Enables/Disable Opportunistic Read (Def= Enable) \$EN\_DIS.*
- UINT8 [MemStackMode](#)  
*Offset 0x07A5 - Stacked Mode Memory Stacked Mode Support (Def = Disable) \$EN\_DIS.*
- UINT8 [StackModeChBit](#)  
*Offset 0x07A6 - Stacked Mode Ch Bit Channel hash bit used during Stacked Mode(Def= BIT28) 0:BIT28, 1:BIT29, 2:BIT30, 3:BIT31, 4:BIT32, 5:BIT33, 6:BIT34.*
- UINT8 [LowMemChannel](#)  
*Offset 0x07A7 - Low Memory Channel Selecting which Physical Channel is mapped to low memory when Stacked Mode is used.*
- UINT8 [Disable2CycleBypass](#)  
*Offset 0x07A8 - Cycle Bypass Support Enables/Disable Cycle Bypass Support(Def=Disable) \$EN\_DIS.*
- UINT8 [MCREGOFFSET](#)  
*Offset 0x07A9 - MC Register Offset Apply user offsets to select MC registers(Def=Disable) \$EN\_DIS.*
- UINT8 [CAVrefCtlOffset](#)  
*Offset 0x07AA - CA Vref Ctl Offset Offset to be applied to DDRDATA7CH1\_CR\_DDRCRVREFADJUST1.CAVref 0:-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.*
- UINT8 [Ch0VrefCtlOffset](#)  
*Offset 0x07AB - Ch0 DQ Vref Ctrl Offset Offset to be applied to DDRDATA7CH1\_CR\_DDRCRVREFADJUST1.↔ Ch0VrefCtl 0:-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.*
- UINT8 [Ch1VrefCtlOffset](#)  
*Offset 0x07AC - Ch1 DQ Vref Ctrl Offset Offset to be applied to DDRDATA7CH1\_CR\_DDRCRVREFADJUST1.↔ Ch1VrefCtl 0:-12,1:-11, 2:-10, 3:-9, 4:-8, 5:-7, 6:-6, 7:-5, 8:-4, 9:-3, 10:-2, 11:-1, 12:0, 13:+1, 14:+2, 15:+3, 16:+4, 17:+5, 18:+6, 19:+7, 20:+8, 21:+9, 22:+10, 23:+11, 24:+12, 0xFF:RANDOM.*
- UINT8 [Ch0ClkPiCodeOffset](#)  
*Offset 0x07AD - Ch0 Clk PI Code Offset Offset to be applied to DDRCLKCH0\_CR\_DDRCRCLKPICODE.PiSetting↔ Rank[0-3] 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.*
- UINT8 [Ch1ClkPiCodeOffset](#)  
*Offset 0x07AE - Ch1 Clk PI Code Offset Offset to be applied to DDRCLKCH1\_CR\_DDRCRCLKPICODE.PiSetting↔ Rank[0-3] 0:-6,1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.*
- UINT8 [Ch0RcvEnOffset](#)  
*Offset 0x07AF - Ch0 RcvEn Offset Offset to be applied to DDRDATAACH0\_CR\_DDRCRDATAOFFSETTRAIN.RcvEn 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch1RcvEnOffset](#)  
*Offset 0x07B0 - Ch1 RcvEn Offset Offset to be applied to DDRDATAACH1\_CR\_DDRCRDATAOFFSETTRAIN.RcvEn 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch0RxDqsOffset](#)  
*Offset 0x07B1 - Ch0 Rx Dqs Offset Offset to be applied to DDRDATAACH0\_CR\_DDRCRDATAOFFSETTRAIN.Rx↔ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch1RxDqsOffset](#)  
*Offset 0x07B2 - Ch1 Rx Dqs Offset Offset to be applied to DDRDATAACH1\_CR\_DDRCRDATAOFFSETTRAIN.Rx↔ DqsOffset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch0TxDqOffset](#)  
*Offset 0x07B3 - Ch0 Tx Dq Offset Offset to be applied to DDRDATAACH0\_CR\_DDRCRDATAOFFSETTRAIN.TxDq↔ Offset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch1TxDqOffset](#)  
*Offset 0x07B4 - Ch1 Tx Dq Offset Offset to be applied to DDRDATAACH1\_CR\_DDRCRDATAOFFSETTRAIN.TxDq↔ Offset 0:-3,1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch0TxDqsOffset](#)

- Offset 0x07B5 - Ch0 Tx Dqs Offset Offset to be applied to DDRDACH0\_CR\_DDRCRDATAOFFSETTRAIN.Tx↔ DqsOffset 0:-3, 1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
- UINT8 [Ch1TxDqsOffset](#)  
*Offset 0x07B6 - Ch1 Tx Dqs Offset Offset to be applied to DDRDACH1\_CR\_DDRCRDATAOFFSETTRAIN.Tx↔ DqsOffset 0:-3, 1:-2, 2:-1, 3:0, 4:1, 5:2, 6:3, 0xFF:RANDOM.*
  - UINT8 [Ch0VrefOffset](#)  
*Offset 0x07B7 - Ch0 Vref Offset Offset to be applied to DDRDACH0\_CR\_DDRCRDATAOFFSETTRAIN.VrefOffset 0:-6, 1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.*
  - UINT8 [Ch1VrefOffset](#)  
*Offset 0x07B8 - Ch1 Vref Offset Offset to be applied to DDRDACH1\_CR\_DDRCRDATAOFFSETTRAIN.VrefOffset 0:-6, 1:-5, 2:-4, 3:-3, 4:-2, 5:-1, 6:0, 7:1, 8:2, 9:3, 10:4, 11:5, 12:6, 0xFF:RANDOM.*
  - UINT8 [tRRSG](#)  
*Offset 0x07B9 - tRRSG Delay between Read-to-Read commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tRRDG](#)  
*Offset 0x07BA - tRRDG Delay between Read-to-Read commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tRRDR](#)  
*Offset 0x07BB - tRRDR Delay between Read-to-Read commands in different Ranks.*
  - UINT8 [tRRDD](#)  
*Offset 0x07BC - tRRDD Delay between Read-to-Read commands in different DIMMs.*
  - UINT8 [tWRSG](#)  
*Offset 0x07BD - tWRSG Delay between Write-to-Read commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tWRDG](#)  
*Offset 0x07BE - tWRDG Delay between Write-to-Read commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tWRDR](#)  
*Offset 0x07BF - tWRDR Delay between Write-to-Read commands in different Ranks.*
  - UINT8 [tWRDD](#)  
*Offset 0x07C0 - tWRDD Delay between Write-to-Read commands in different DIMMs.*
  - UINT8 [tWWSG](#)  
*Offset 0x07C1 - tWWSG Delay between Write-to-Write commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tWWDG](#)  
*Offset 0x07C2 - tWWDG Delay between Write-to-Write commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tWWDR](#)  
*Offset 0x07C3 - tWWDR Delay between Write-to-Write commands in different Ranks.*
  - UINT8 [tWWDD](#)  
*Offset 0x07C4 - tWWDD Delay between Write-to-Write commands in different DIMMs.*
  - UINT8 [tRWSG](#)  
*Offset 0x07C5 - tRWSG Delay between Read-to-Write commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tRWDG](#)  
*Offset 0x07C6 - tRWDG Delay between Read-to-Write commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.*
  - UINT8 [tRWDR](#)  
*Offset 0x07C7 - tRWDR Delay between Read-to-Write commands in different Ranks.*
  - UINT8 [tRWDD](#)  
*Offset 0x07C8 - tRWDD Delay between Read-to-Write commands in different DIMMs.*
  - UINT8 [ScramClockGateAB](#)  
*Offset 0x07C9 - Clock Gate AB Clock Gate AB 0:Disable, 1:2 Cycles, 2:3 Cycles, 3:4 Cycles.*
-

- UINT8 [ScramClockGateC](#)  
*Offset 0x07CA - Clock Gate C Select which Row swizzle algorithm to use during Row Hammer test 0:Disable, 1:2 Cycles, 2:4 Cycles, 3:8 Cycles.*
  - UINT8 [ScramEnableDbiAB](#)  
*Offset 0x07CB - Enable DBI AB Enable DBI AB \$EN\_DIS.*
  - UINT8 [Interpreter](#)  
*Offset 0x07CC - MRC Interpreter Select CMOS location match of DD01 or Ctrl-Break key or force entry 0:CMOS, 1:Break, 2:Force.*
  - UINT8 [IoOdtMode](#)  
*Offset 0x07CD - ODT mode ODT mode 0:Default, 1:Ctt, 2:Vtt, 3:Vddq, 4:Vss,5:Max.*
  - UINT8 [TestMenuDprLock](#)  
*Offset 0x07CE - Lock DPR register Lock DPR register.*
  - UINT8 [LoadValidationFv](#)  
*Offset 0x07CF - LoadValidationFv Enable: Enable loading of ValidationFV, Disable(Default) \$EN\_DIS.*
  - UINT8 [PrefetchNonPrefetchRatio](#)  
*Offset 0x07D0 - Prefetch NonPrefetch Ratio 0: All prefetch, 1: Seven of Eight Prefetch, 2: Three of Four Prefetch, 3: Half Prefetch Half Non-Prefetch(Default), 4: Three of Four Non-Prefetch, 5: Seven of Eight Prefetch, 6: All Non-prefetch 0: All prefetch, 1: Seven of Eight Prefetch, 2: Three of Four Prefetch, 3: Half Prefetch Half Non-Prefetch, 4: Three of Four Non-Prefetch, 5: Seven of Eight Prefetch, 6: All Non-prefetch.*
  - UINT8 [PcuDdrVoltage](#)  
*Offset 0x07D1 - Override for PCU\_CR\_DDR\_VOLTAGE Setting PCU\_CR\_DDR\_VOLTAGE.*
  - UINT8 [SaRestrictedSvPolicyEnable](#)  
*Offset 0x07D2 - SvPolicyEnable Enable: SV policy is enabled, Disable(Default): SV policy is disabled \$EN\_DIS.*
  - UINT8 [ForceUnlockAes](#)  
*Offset 0x07D3 - Force Unlock AES 0(Default)=Disable, 1=Enable \$EN\_DIS.*
  - UINT8 [UnlockMchbarCtrlRegs](#)  
*Offset 0x07D4 - Unlock MCHBAR control registers Unlock MCHBAR control registers; 0: disable, 1: enable \$EN\_DIS.*
  - UINT8 [ForceTxtEnable](#)  
*Offset 0x07D5 - Force TXT Enable Force TXT Enable; 0: disable, 1: enable \$EN\_DIS.*
  - UINT8 [UnusedUpdSpace25](#) [2]  
*Offset 0x07D6.*
  - UINT64 [MsegSize](#)  
*Offset 0x07D8 - MSEG Size MSEG Size.*
  - UINT8 [XmCliEnable](#)  
*Offset 0x07E0 - CpuSvBootMode Enable: FlexCon is enabled, Disble(Default): FlexCon is disabled \$EN\_DIS.*
  - UINT8 [SaTestSamplePartStatusOverride](#)  
*Offset 0x07E1 - Sa Test Sample Part Status Override 0-Passthrough, 1-Production part, 2-Preproduction part.*
  - UINT8 [SaTestGrunitClockGating](#)  
*Offset 0x07E2 - Sa Test Grunit ClockGating Enable Sa Test Grunit ClockGating \$EN\_DIS.*
  - UINT8 [SaTestDmiCapRegLock](#)  
*Offset 0x07E3 - Sa Test Dmi Cap Reg Lock DMI Capability Register Lock.*
  - UINT8 [SaTestDmiMaxPayloadSize](#)  
*Offset 0x07E4 - Sa Test Dmi Max Payload Size DMI Max Payload Size.*
  - UINT8 [SaPcieVcLimLock](#)  
*Offset 0x07E5 - Sa Pcie VcLim Lock Lock bit.*
  - UINT8 [SaPcieVCmCmpLim](#)  
*Offset 0x07E6 - Sa Pcie VCm Cmp Lim VCm Completions override.*
  - UINT8 [SaPcieVCmPLim](#)  
*Offset 0x07E7 - Sa Pcie VCm PLim posted VCm Requests override.*
  - UINT8 [SaPcieVCmNpLim](#)  
*Offset 0x07E8 - Sa Pcie VCm NpLim non-posted VCm Requests override.*
  - UINT8 [SaLagunaCreditWA](#)
-

- Offset 0x07E9 - Sa Laguna Credit WA Laguna Credit WA.*

    - UINT8 [SaSvDmiComplianceDeemphasis](#)
      - Offset 0x07EA - Sa Sv Dmi Compliance Deemphasis SvDmiComplianceDeemphasis.*
    - UINT8 [UnusedUpdSpace26](#)
      - Offset 0x07EB.*
    - UINT16 [SaSvRemapBaseOverride](#)
      - Offset 0x07EC - Sa Sv Remap Base Override SvRemapBaseOverride.*
    - UINT8 [SaSystemAgentClockGatingEnable](#)
      - Offset 0x07EE - Sa System Agent ClockGating Enable SystemAgentClockGatingEnable.*
    - UINT8 [SaPciePllShutdownEnable](#)
      - Offset 0x07EF - Sa Pcie Pll Shutdown Enable PciePllShutdownEnable.*
    - UINT8 [SaSV\\_DMI\\_GEN1\\_halt](#)
      - Offset 0x07F0 - Sa SV\_DMI\_GEN1\_halt SV\_DMI\_GEN1\_halt.*
    - UINT8 [SaSV\\_nFTS\\_DMI\\_auto](#)
      - Offset 0x07F1 - Sa SV\_nFTS\_DMI\_auto SV\_nFTS\_DMI\_auto.*
    - UINT8 [SaSvDMI\\_nFTS](#)
      - Offset 0x07F2 - Sa Sv DMI\_nFTS SvDMI\_nFTS.*
    - UINT8 [SanFTS\\_auto](#)
      - Offset 0x07F3 - Sa nFTS\_auto nFTS\_auto.*
    - UINT8 [SanFTS\\_gen3\\_auto](#)
      - Offset 0x07F4 - Sa nFTS\_gen3\_auto nFTS\_gen3\_auto.*
    - UINT8 [SaSVIAER](#)
      - Offset 0x07F5 - Sa SVIAER SVIAER.*
    - UINT8 [SaSvScramblerDmi](#)
      - Offset 0x07F6 - Sa Sv Scrambler Dmi SvScramblerDmi.*
    - UINT8 [SaSvDmiSerr](#)
      - Offset 0x07F7 - Sa Sv Dmi Serr SvDmiSerr.*
    - UINT8 [SaSvPEG\\_nFTS](#) [4]
      - Offset 0x07F8 - Sa SvPEG\_nFTS SvPEG\_nFTS.*
    - UINT8 [SaSvPEG\\_gen3\\_ccFTS](#) [4]
      - Offset 0x07FC - Sa SvPEG\_gen3\_ccFTS SvPEG\_gen3\_ccFTS.*
    - UINT8 [SaSvPEG\\_gen3\\_nccFTS](#) [4]
      - Offset 0x0800 - Sa SvPEG\_gen3\_nccFTS SvPEG\_gen3\_nccFTS.*
    - UINT8 [SaSvScramblerPeg](#) [4]
      - Offset 0x0804 - Sa Sv Scrambler Peg SvScramblerPeg.*
    - UINT8 [SaSvScramblerPegGen3](#) [4]
      - Offset 0x0808 - Sa Sv Scrambler Peg Gen3 SvScramblerPegGen3.*
    - UINT8 [SaSvPegSerr](#) [4]
      - Offset 0x080C - Sa Sv Peg Serr SvPegSerr.*
    - UINT8 [SaTestTxClkGating](#)
      - Offset 0x0810 - Sa Test Tx ClkGating TestTxClkGating.*
    - UINT8 [SaTestRxClkGating](#)
      - Offset 0x0811 - Sa Test Rx ClkGating TestRxClkGating.*
    - UINT8 [SaTestLowPwrMode](#)
      - Offset 0x0812 - Sa Test Low Pwr Mode TestLowPwrMode.*
    - UINT8 [SaSrMode](#)
      - Offset 0x0813 - Sa Sr Mode SrMode.*
    - UINT8 [SaSrSeq](#)
      - Offset 0x0814 - Sa Sr Seq SrSeq.*
    - UINT8 [SaBurstSpacing](#)
      - Offset 0x0815 - Sa Burst Spacing BurstSpacing.*
-

- UINT8 [SaCpuSvBootMode](#)  
*Offset 0x0816 - Cpu Sv Boot Mode 0: Auto (Default), 1: Commercial boot mode, 2: SV boot mode, 3: SV boot JTAG mode with SB loop, 4: SV boot JTAG mode without SB loop 0: Auto , 1: Commercial boot mode, 2: SV boot mode, 3: SV boot JTAG mode with SB loop, 4: SV boot JTAG mode without SB loop.*
  - UINT8 [UnusedUpdSpace27](#)  
*Offset 0x0817.*
  - UINT32 [FmhcDevLtr](#)  
*Offset 0x0818 - Fmhc Device LTR FmhcDevLtr.*
  - UINT8 [FmhcSkipLock](#)  
*Offset 0x081C - Far skip lock FmhcSkipLock.*
  - UINT8 [UnusedUpdSpace28](#) [3]  
*Offset 0x081D.*
  - UINT32 [FmhcCcrdc](#)  
*Offset 0x0820 - Fmhc CMI Credit control FmhcCcrdc.*
  - UINT8 [FmRwrr](#)  
*Offset 0x0824 - Far Memory Read Weighted Round Robin FMRWRR.*
  - UINT8 [FmWwrr](#)  
*Offset 0x0825 - Far Memory Write Weighted Round Robin FMWWRR.*
  - UINT8 [Fmwrr](#)  
*Offset 0x0826 - Far Memory Weighted Round Robin FMWRR.*
  - UINT8 [Swrr](#)  
*Offset 0x0827 - Storage Weighted Round Robin SWRR.*
  - UINT16 [PartialWriteTimeout](#)  
*Offset 0x0828 - Partial Write time out in micro sec PartialWriteTimeout.*
  - UINT8 [MdmEn](#)  
*Offset 0x082A - Multipurpose buffer Mode enable/disable 1: enable, 0: disable \$EN\_DIS.*
  - UINT8 [InOrdExe](#)  
*Offset 0x082B - In order execution enable/disable 1: enable, 0: disable \$EN\_DIS.*
  - UINT8 [Dis2kRdC](#)  
*Offset 0x082C - Disable 2K read cache 1: enable, 0: disable \$EN\_DIS.*
  - UINT8 [UnusedUpdSpace29](#)  
*Offset 0x082D.*
  - UINT16 [Tmt1](#)  
*Offset 0x082E - Thermal Management Temperature 1 TMT1.*
  - UINT16 [Tmt2](#)  
*Offset 0x0830 - Thermal Management Temperature 2 TMT2.*
  - UINT8 [HeciCommunication](#)  
*Offset 0x0832 - HECI Communication Test, 0: POR, 1: enable, 2: disable, Disables HECI communication causing ME to enter error state.*
  - UINT8 [HeciCommunication3](#)  
*Offset 0x0833 - HECI3 Interface Communication Test, 0: POR, 1: enable, 2: disable, Adds or Removes HECI3 Device from PCI space.*
  - UINT8 [HostResetNotification](#)  
*Offset 0x0834 - Notification test for Host Reset Test, 0: POR, 1: enable, 2: disable, Enable test for notification when Host Reset \$EN\_DIS.*
  - UINT8 [ManufRstAndHaltOnS3Resume](#)  
*Offset 0x0835 - Send Manufacturing Reset And Halt On S3 Resume Test, 0: POR, 1: enable, 2: disable, Enable sending Manufacturing Reset and Halt on S3 Resume \$EN\_DIS.*
  - UINT8 [ModPhySelection](#)  
*Offset 0x0836 - ModPhy Selection Policy DEPRECATED.*
  - UINT8 [PchTestDmiTranCoOverEn](#) [4]  
*Offset 0x0837 - Dmi Test Tran Co Over En Enable/Disable Lane Transmitter Coefficient.*
-

- UUINT8 [PchTestDmiTranCoOverPostCur](#) [4]  
*Offset 0x083B - Dmi Test Tran Co Over Post Cur Lane Transmitter Post-Cursor Coefficient Override.*
- UUINT8 [PchTestDmiTranCoOverPreCur](#) [4]  
*Offset 0x083F - Dmi Test Tran Co Over Pre Cur Lane Transmitter Pre-Cursor Coefficient Override.*
- UUINT8 [PchTestDmiUpPortTranPreset](#) [4]  
*Offset 0x0843 - Dmi Test Up Port Tran Preset Upstream Port Lane Transmitter Preset.*
- UUINT8 [PchTestDmiUpPortTranPresetEn](#)  
*Offset 0x0847 - Dmi Test UpPort Tran Preset En 0: POR setting, 1: force enable, 2: force disable.*
- UUINT8 [PchTestDmiRtlepceb](#)  
*Offset 0x0848 - Dmi Test Rtlepceb DMI Remote Transmit Link Equalization Preset/Coefficient Evaluation Bypass (RTLEPCEB).*
- UUINT8 [PchTestDmiMeUmaRootSpaceCheck](#)  
*Offset 0x0849 - DMI ME UMA Root Space Check DMI IOSF Root Space attribute check for RS3 for cycles targeting MEUMA.*
- UUINT8 [DisableResets](#)  
*Offset 0x084A - Disable Reset This option disable/enable reset functionality.*
- UUINT8 [UnusedUpdSpace30](#) [6]  
*Offset 0x084B.*
- UUINT8 [ReservedFspmRestrictedUpd](#) [15]  
*Offset 0x0851.*

### 12.8.1 Detailed Description

Fsp M Restricted Configuration.

Definition at line 3147 of file FspmUpd.h.

### 12.8.2 Member Data Documentation

#### 12.8.2.1 DisableResets

UUINT8 FSP\_M\_RESTRICTED\_CONFIG::DisableResets

Offset 0x084A - Disable Reset This option disable/enable reset functionality.

(Default==POR) 0:Platform POR, 1: Enable, 2: Disable

Definition at line 3840 of file FspmUpd.h.

#### 12.8.2.2 HeciCommunication

UUINT8 FSP\_M\_RESTRICTED\_CONFIG::HeciCommunication

Offset 0x0832 - HECI Communication Test, 0: POR, 1: enable, 2: disable, Disables HECI communication causing ME to enter error state.

\$EN\_DIS

Definition at line 3774 of file FspmUpd.h.

### 12.8.2.3 HeciCommunication3

UINT8 FSP\_M\_RESTRICTED\_CONFIG::HeciCommunication3

Offset 0x0833 - HECI3 Interface Communication Test, 0: POR, 1: enable, 2: disable, Adds or Removes HECI3 Device from PCI space.

\$EN\_DIS

Definition at line 3780 of file FspmUpd.h.

### 12.8.2.4 LowMemChannel

UINT8 FSP\_M\_RESTRICTED\_CONFIG::LowMemChannel

Offset 0x07A7 - Low Memory Channel Selecting which Physical Channel is mapped to low memory when Stacked Mode is used.

0:Channel A, 1:Channel B, 0xFF:Auto

Definition at line 3216 of file FspmUpd.h.

### 12.8.2.5 MsegSize

UINT64 FSP\_M\_RESTRICTED\_CONFIG::MsegSize

Offset 0x07D8 - MSEG Size MSEG Size.

Valid values 0 : 512K , 1 : 1M , 2 : 1.5M , 3 : 2M , 4 : 2.4M , 5 : 3M 0 : 512K , 1 : 1M , 2 : 1.5M , 3 : 2M , 4 : 2.4M , 5 : 3M

Definition at line 3503 of file FspmUpd.h.

### 12.8.2.6 PchTestDmiMeUmaRootSpaceCheck

UINT8 FSP\_M\_RESTRICTED\_CONFIG::PchTestDmiMeUmaRootSpaceCheck

Offset 0x0849 - DMI ME UMA Root Space Check DMI IOSF Root Space attribute check for RS3 for cycles targeting MEUMA.

0: POR, 1: enable, 2: disable

Definition at line 3834 of file FspmUpd.h.

### 12.8.2.7 PcuDdrVoltage

UINT8 FSP\_M\_RESTRICTED\_CONFIG::PcuDdrVoltage

Offset 0x07D1 - Override for PCU\_CR\_DDR\_VOLTAGE Setting PCU\_CR\_DDR\_VOLTAGE.

0xFF:Auto 6:1.1V 7:1.2V

Definition at line 3469 of file FspmUpd.h.

---

### 12.8.2.8 TestMenuDprLock

UINT8 FSP\_M\_RESTRICTED\_CONFIG::TestMenuDprLock

Offset 0x07CE - Lock DPR register Lock DPR register.

**0: Platform POR** ; 1: Enable; 2: Disable 0:Platform POR, 1: Enable, 2: Disable

Definition at line 3448 of file FspmUpd.h.

### 12.8.2.9 tRRDD

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRRDD

Offset 0x07BC - tRRDD Delay between Read-to-Read commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3346 of file FspmUpd.h.

### 12.8.2.10 tRRDG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRRDG

Offset 0x07BA - tRRDG Delay between Read-to-Read commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3336 of file FspmUpd.h.

### 12.8.2.11 tRRDR

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRRDR

Offset 0x07BB - tRRDR Delay between Read-to-Read commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3341 of file FspmUpd.h.

### 12.8.2.12 tRRSG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRRSG

Offset 0x07B9 - tRRSG Delay between Read-to-Read commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3330 of file FspmUpd.h.

### 12.8.2.13 tRWDD

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRWDD

---

Offset 0x07C8 - tRWDD Delay between Read-to-Write commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3412 of file FspmUpd.h.

#### 12.8.2.14 tRWDG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRWDG

Offset 0x07C6 - tRWDG Delay between Read-to-Write commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3402 of file FspmUpd.h.

#### 12.8.2.15 tRWDR

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRWDR

Offset 0x07C7 - tRWDR Delay between Read-to-Write commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3407 of file FspmUpd.h.

#### 12.8.2.16 tRWSG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tRWSG

Offset 0x07C5 - tRWSG Delay between Read-to-Write commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3396 of file FspmUpd.h.

#### 12.8.2.17 tWRDD

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWRDD

Offset 0x07C0 - tWRDD Delay between Write-to-Read commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3368 of file FspmUpd.h.

#### 12.8.2.18 tWRDG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWRDG

Offset 0x07BE - tWRDG Delay between Write-to-Read commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

---

0-Auto, Range 4-54.

Definition at line 3358 of file FspmUpd.h.

#### 12.8.2.19 tWRDR

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWRDR

Offset 0x07BF - tWRDR Delay between Write-to-Read commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3363 of file FspmUpd.h.

#### 12.8.2.20 tWRSG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWRSG

Offset 0x07BD - tWRSG Delay between Write-to-Read commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-86.

Definition at line 3352 of file FspmUpd.h.

#### 12.8.2.21 tWWDD

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWWDD

Offset 0x07C4 - tWWDD Delay between Write-to-Write commands in different DIMMs.

0-Auto, Range 4-54.

Definition at line 3390 of file FspmUpd.h.

#### 12.8.2.22 tWWDG

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWWDG

Offset 0x07C2 - tWWDG Delay between Write-to-Write commands in different Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3380 of file FspmUpd.h.

#### 12.8.2.23 tWWDR

UINT8 FSP\_M\_RESTRICTED\_CONFIG::tWWDR

Offset 0x07C3 - tWWDR Delay between Write-to-Write commands in different Ranks.

0-Auto, Range 4-54.

Definition at line 3385 of file FspmUpd.h.

---

## 12.8.2.24 tWWSG

```
UINT8 FSP_M_RESTRICTED_CONFIG::tWWSG
```

Offset 0x07C1 - tWWSG Delay between Write-to-Write commands in the same Bank Group for DDR4 or Same Rank for DDR3/LPDDR3.

0-Auto, Range 4-54.

Definition at line 3374 of file FspmUpd.h.

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

- [FspmUpd.h](#)

## 12.9 FSP\_S\_CONFIG Struct Reference

Fsp S Configuration.

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

## Public Attributes

- [UINT8 SiCsmFlag](#)  
*Offset 0x0020 - Si Config CSM Flag.*
- [UINT8 UnusedUpdSpace0](#) [3]  
*Offset 0x0021.*
- [UINT32 SiSsidTablePtr](#)  
*Offset 0x0024.*
- [UINT16 SiNumberOfSsidTableEntry](#)  
*Offset 0x0028.*
- [UINT8 SiPostMemRsvd](#) [16]  
*Offset 0x002A.*
- [UINT8 UnusedUpdSpace1](#) [2]  
*Offset 0x003A.*
- [UINT32 MicrocodeRegionBase](#)  
*Offset 0x003C - MicrocodeRegionBase Memory Base of Microcode Updates.*
- [UINT32 MicrocodeRegionSize](#)  
*Offset 0x0040 - MicrocodeRegionSize Size of Microcode Updates.*
- [UINT8 TxtEnable](#)  
*Offset 0x0044 - Enable or Disable TXT Enable or Disable TXT; 0: Disable; 1: **Enable**.*
- [UINT8 AesEnable](#)  
*Offset 0x0045 - Advanced Encryption Standard (AES) feature Enable or Disable Advanced Encryption Standard (AES) feature; 0: Disable; 1: **Enable \$EN\_DIS**.*
- [UINT8 SkipMplnit](#)  
*Offset 0x0046 - Skip Multi-Processor Initialization When this is skipped, boot loader must initialize processors before SilicionInit API.*
- [UINT8 PpinSupport](#)  
*Offset 0x0047 - PpinSupport to view Protected Processor Inventory Number Enable or Disable or Auto (Based on End of Manufacturing flag.*
- [UINT8 TurboMode](#)  
*Offset 0x0048 - Turbo Mode Enable/Disable Turbo mode.*

- UINT8 [Psi3Enable](#)  
*Offset 0x0049 - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; 1: Enable.*
  - UINT8 [Psi4Enable](#)  
*Offset 0x004A - Power State 4 enable/disable PCODE MMIO Mailbox: Power State 4 enable/disable; 0: Disable; 1: Enable.For all VR Indexes.*
  - UINT8 [ImonSlope](#)  
*Offset 0x004B - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.*
  - UINT8 [ImonOffset](#)  
*Offset 0x004C - Imon offset correction PCODE MMIO Mailbox: Imon offset correction.*
  - UINT8 [VrConfigEnable](#)  
*Offset 0x004D - Enable/Disable BIOS configuration of VR Enable/Disable BIOS configuration of VR; 0: Disable; 1: Enable.For all VR Indexes.*
  - UINT8 [TdcEnable](#)  
*Offset 0x004E - Thermal Design Current enable/disable PCODE MMIO Mailbox: Thermal Design Current enable/disable; 0: Disable; 1: Enable.For all VR Indexes.*
  - UINT8 [TdcTimeWindow](#)  
*Offset 0x004F - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.*
  - UINT8 [TdcLock](#)  
*Offset 0x0050 - Thermal Design Current Lock PCODE MMIO Mailbox: Thermal Design Current Lock; 0: Disable; 1: Enable.For all VR Indexes.*
  - UINT8 [UnusedUpdSpace2](#)  
*Offset 0x0051.*
  - UINT16 [TdcPowerLimit](#)  
*Offset 0x0052 - Thermal Design Current current limit PCODE MMIO Mailbox: Thermal Design Current current limit.*
  - UINT16 [AcLoadline](#)  
*Offset 0x0054 - AcLoadline PCODE MMIO Mailbox: AcLoadline in 1/100 mOhms (ie.*
  - UINT16 [DcLoadline](#)  
*Offset 0x0056 - DcLoadline PCODE MMIO Mailbox: DcLoadline in 1/100 mOhms (ie.*
  - UINT16 [Psi1Threshold](#)  
*Offset 0x0058 - Power State 1 Threshold current PCODE MMIO Mailbox: Power State 1 current cutoff in 1/4 Amp increments.*
  - UINT16 [Psi2Threshold](#)  
*Offset 0x005A - Power State 2 Threshold current PCODE MMIO Mailbox: Power State 2 current cutoff in 1/4 Amp increments.*
  - UINT16 [Psi3Threshold](#)  
*Offset 0x005C - Power State 3 Threshold current PCODE MMIO Mailbox: Power State 3 current cutoff in 1/4 Amp increments.*
  - UINT16 [IccMax](#)  
*Offset 0x005E - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.*
  - UINT16 [VrVoltageLimit](#)  
*Offset 0x0060 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.*
  - UINT8 [PsysSlope](#)  
*Offset 0x0062 - Platform Psys slope correction PCODE MMIO Mailbox: Platform Psys slope correction.*
  - UINT8 [PsysOffset](#)  
*Offset 0x0063 - Platform Psys offset correction PCODE MMIO Mailbox: Platform Psys offset correction.*
  - UINT8 [AcousticNoiseMitigation](#)  
*Offset 0x0064 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.*
  - UINT8 [PreWake](#)  
*Offset 0x0065 - Pre Wake Randomization time PCODE MMIO Mailbox: Acoustic Mitigation Range.Defines the maximum pre-wake randomization time in micro ticks.This can be programmed only if AcousticNoiseMitigation is enabled.*
  - UINT8 [RampUp](#)
-

Offset 0x0066 - Ramp Up Randomization time PCODE MMIO Mailbox: Acoustic Mitigation Range. Defines the maximum Ramp Up randomization time in micro ticks. This can be programmed only if AcousticNoiseMitigation is enabled. Range 0-255 **0**.

- UINT8 [RampDown](#)

Offset 0x0067 - Ramp Down Randomization time PCODE MMIO Mailbox: Acoustic Mitigation Range. Defines the maximum Ramp Down randomization time in micro ticks. This can be programmed only if AcousticNoiseMitigation is enabled. Range 0-255 **0**.

- UINT8 [FastPkgCRampDisableFivr](#)

Offset 0x0068 - 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 0x0069 - 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 [SendVrMbxCmd](#)

Offset 0x006A - Enable VR specific mailbox command VR specific mailbox commands.

- UINT8 [UnusedUpdSpace3](#)

Offset 0x006B.

- UINT16 [FivrRfiFrequency](#)

Offset 0x006C - FIVR RFI Frequency PCODE MMIO Mailbox: Set the desired RFI frequency, in increments of 100→ KHz.

- UINT8 [FivrSpreadSpectrum](#)

Offset 0x006E - FIVR RFI Spread Spectrum PCODE MMIO Mailbox: FIVR RFI Spread Spectrum, in 0.1% increments.

- UINT8 [EnableMinVoltageOverride](#)

Offset 0x006F - Enable or Disable Minimum Voltage Override Enable or disable Minimum Voltage overrides ; **0: Disable**; 1: Enable.

- UINT16 [MinVoltageC8](#)

Offset 0x0070 - Min Voltage for C8 PCODE MMIO Mailbox: Minimum voltage for C8.

- UINT16 [MinVoltageRuntime](#)

Offset 0x0072 - Min Voltage for Runtime PCODE MMIO Mailbox: Minimum voltage for runtime.

- UINT8 [MlcStreamerPrefetcher](#)

Offset 0x0074 - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; **0: Disable**; **1: Enable**.

- UINT8 [MlcSpatialPrefetcher](#)

Offset 0x0075 - Enable or Disable MLC Spatial Prefetcher Enable or Disable MLC Spatial Prefetcher; **0: Disable**; **1: Enable** \$EN\_DIS.

- UINT8 [MonitorMwaitEnable](#)

Offset 0x0076 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; **0: Disable**; **1: Enable**.

- UINT8 [ProcessorTraceOutputScheme](#)

Offset 0x0077 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.

- UINT8 [ProcessorTraceEnable](#)

Offset 0x0078 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

- UINT8 [UnusedUpdSpace4](#) [7]

Offset 0x0079.

- UINT64 [ProcessorTraceMemBase](#)

Offset 0x0080 - Base of memory region allocated for Processor Trace Base address of memory region allocated for Processor Trace.

- UINT32 [ProcessorTraceMemLength](#)

Offset 0x0088 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.

- UINT8 [VoltageOptimization](#)

Offset 0x008C - Enable or Disable Voltage Optimization feature Enable or Disable Voltage Optimization feature 0: Disable; **1: Enable** \$EN\_DIS.

- UINT8 [ThreeStrikeCounterDisable](#)

Offset 0x008D - 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 [MachineCheckEnable](#)

Offset 0x008E - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.

- UINT8 [ApldleManner](#)

Offset 0x008F - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.

- UINT8 [OneCoreRatioLimit](#)

Offset 0x0090 - 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 0x0091 - 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 0x0092 - 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 0x0093 - 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 [FiveCoreRatioLimit](#)

Offset 0x0094 - 5-Core Ratio Limit 5-Core Ratio Limit: For XE part: LFM to 255, For overclocking 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 0x0095 - 6-Core Ratio Limit 6-Core Ratio Limit: For XE part: LFM to 255, For overclocking 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 0x0096 - 7-Core Ratio Limit 7-Core Ratio Limit: For XE part: LFM to 255, For overclocking 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 0x0097 - 8-Core Ratio Limit 8-Core Ratio Limit: For XE part: LFM to 255, For overclocking 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 [Hwp](#)

Offset 0x0098 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

- UINT8 [HdcControl](#)

Offset 0x0099 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

- UINT8 [PowerLimit1Time](#)

Offset 0x009A - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.

- UINT8 [PowerLimit2](#)

Offset 0x009B - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

- UINT8 [TurboPowerLimitLock](#)

Offset 0x009C - Turbo settings Lock Lock all Turbo settings Enable/Disable; **0: Disable** , 1: Enable \$EN\_DIS.

- UINT8 [PowerLimit3Time](#)

Offset 0x009D - Package PL3 time window Package PL3 time window range for this policy from 0 to 64ms.

- UINT8 [PowerLimit3DutyCycle](#)  
*Offset 0x009E - Package PL3 Duty Cycle Package PL3 Duty Cycle; Valid Range is 0 to 100.*
- UINT8 [PowerLimit3Lock](#)  
*Offset 0x009F - Package PL3 Lock Package PL3 Lock Enable/Disable; **0: Disable** ; **1: Enable** \$EN\_DIS.*
- UINT8 [PowerLimit4Lock](#)  
*Offset 0x00A0 - Package PL4 Lock Package PL4 Lock Enable/Disable; **0: Disable** ; **1: Enable** \$EN\_DIS.*
- UINT8 [TccActivationOffset](#)  
*Offset 0x00A1 - TCC Activation Offset TCC Activation Offset.*
- UINT8 [TccOffsetClamp](#)  
*Offset 0x00A2 - 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 0x00A3 - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; **1: Enabled**.*
- UINT32 [PowerLimit1](#)  
*Offset 0x00A4 - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.*
- UINT32 [PowerLimit2Power](#)  
*Offset 0x00A8 - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.*
- UINT32 [PowerLimit3](#)  
*Offset 0x00AC - Package PL3 power limit Package PL3 power limit.*
- UINT32 [PowerLimit4](#)  
*Offset 0x00B0 - Package PL4 power limit Package PL4 power limit.*
- UINT32 [TccOffsetTimeWindowForRatl](#)  
*Offset 0x00B4 - Tcc Offset Time Window for RATL Package PL4 power limit.*
- UINT8 [HwpInterruptControl](#)  
*Offset 0x00B8 - 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 [EnableIbpm](#)  
*Offset 0x00B9 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.*
- UINT8 [EnableIbpmDriver](#)  
*Offset 0x00BA - Intel Turbo Boost Max Technology 3.0 Driver Intel Turbo Boost Max Technology 3.0 Driver **0**↔ : **Disabled**; **1: Enabled** \$EN\_DIS.*
- UINT8 [EnablePerCorePState](#)  
*Offset 0x00BB - Enable or Disable Per Core P State OS control Enable or Disable Per Core P State OS control.*
- UINT8 [EnableHwpAutoPerCorePstate](#)  
*Offset 0x00BC - 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 0x00BD - Enable or Disable HwP Autonomous EPP Grouping Enable or Disable HwP Autonomous EPP Grouping.*
- UINT8 [EnableEpbPeciOverride](#)  
*Offset 0x00BE - Enable or Disable EPB override over PECI Enable or Disable EPB override over PECI.*
- UINT8 [EnableFastMsrHwpReq](#)  
*Offset 0x00BF - Enable or Disable Fast MSR for IA32\_HWP\_REQUEST Enable or Disable Fast MSR for IA32\_H↔ WP\_REQUEST.*
- UINT8 [MinRingRatioLimit](#)  
*Offset 0x00C0 - Minimum Ring ratio limit override Minimum Ring ratio limit override.*
- UINT8 [MaxRingRatioLimit](#)  
*Offset 0x00C1 - Maximum Ring ratio limit override Maximum Ring ratio limit override.*
- UINT8 [NumberOfEntries](#)  
*Offset 0x00C2 - 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 0x00C3 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.*
  - UINT8 [Custom2PowerLimit1Time](#)  
*Offset 0x00C4 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.*
  - UINT8 [Custom3PowerLimit1Time](#)  
*Offset 0x00C5 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.*
  - UINT8 [Custom1TurboActivationRatio](#)  
*Offset 0x00C6 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.*
  - UINT8 [Custom2TurboActivationRatio](#)  
*Offset 0x00C7 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.*
  - UINT8 [Custom3TurboActivationRatio](#)  
*Offset 0x00C8 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.*
  - UINT8 [ConfigTdpLock](#)  
*Offset 0x00C9 - ConfigTdp mode settings Lock Lock the ConfigTdp mode settings from runtime changes; **0: Disable**; 1: Enable \$EN\_DIS.*
  - UINT8 [ConfigTdpBios](#)  
*Offset 0x00CA - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.*
  - UINT8 [MaxRatio](#)  
*Offset 0x00CB - Max P-State Ratio Max P-State Ratio, Valid Range 0 to 0x7F.*
  - UINT8 [StateRatio](#) [40]  
*Offset 0x00CC - P-state ratios for custom P-state table P-state ratios for custom P-state table.*
  - UINT32 [Custom1PowerLimit1](#)  
*Offset 0x00F4 - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.*
  - UINT32 [Custom1PowerLimit2](#)  
*Offset 0x00F8 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.*
  - UINT32 [Custom2PowerLimit1](#)  
*Offset 0x00FC - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.*
  - UINT32 [Custom2PowerLimit2](#)  
*Offset 0x0100 - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.*
  - UINT32 [Custom3PowerLimit1](#)  
*Offset 0x0104 - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.*
  - UINT32 [Custom3PowerLimit2](#)  
*Offset 0x0108 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.*
  - UINT8 [PsysPowerLimit1](#)  
*Offset 0x010C - PL1 Enable value PL1 Enable value to limit average platform power.*
  - UINT8 [PsysPowerLimit1Time](#)  
*Offset 0x010D - 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 0x010E - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.*
  - UINT8 [UnusedUpdSpace5](#)  
*Offset 0x010F.*
  - UINT16 [PsysPmax](#)
-

- Offset 0x0110 - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.*

    - UINT8 [UnusedUpdSpace6](#) [2]
      - Offset 0x0112.*
    - UINT32 [PsysPowerLimit1 Power](#)
      - Offset 0x0114 - Platform PL1 power Platform PL1 power.*
    - UINT32 [PsysPowerLimit2Power](#)
      - Offset 0x0118 - Platform PL2 power Platform PL2 power.*
    - UINT8 [Eist](#)
      - Offset 0x011C - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.*
    - UINT8 [EnergyEfficientPState](#)
      - Offset 0x011D - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.*
    - UINT8 [EnergyEfficientTurbo](#)
      - Offset 0x011E - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.*
    - UINT8 [TStates](#)
      - Offset 0x011F - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.*
    - UINT8 [BiProcHot](#)
      - Offset 0x0120 - Enable or Disable Bi-Directional PROCHOT# Enable or Disable Bi-Directional PROCHOT#; 0: Disable; 1: **Enable** \$EN\_DIS.*
    - UINT8 [DisableProcHotOut](#)
      - Offset 0x0121 - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; 1: **Enable**.*
    - UINT8 [ProcHotResponse](#)
      - Offset 0x0122 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.*
    - UINT8 [DisableVrThermalAlert](#)
      - Offset 0x0123 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; **0: Disable**; 1: Enable.*
    - UINT8 [AutoThermalReporting](#)
      - Offset 0x0124 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; 1: **Enable**.*
    - UINT8 [ThermalMonitor](#)
      - Offset 0x0125 - Enable or Disable Thermal Monitor Enable or Disable Thermal Monitor; 0: Disable; 1: **Enable** \$EN\_DIS.*
    - UINT8 [Cx](#)
      - Offset 0x0126 - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).*
    - UINT8 [PmgCstCfgCtrlLock](#)
      - Offset 0x0127 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; 1: **Enable**.*
    - UINT8 [C1e](#)
      - Offset 0x0128 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.*
    - UINT8 [C1StateAutoDemotion](#)
      - Offset 0x0129 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.*
    - UINT8 [C1StateUnDemotion](#)
      - Offset 0x012A - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.*
    - UINT8 [PkgCStateDemotion](#)
      - Offset 0x012B - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.*
    - UINT8 [PkgCStateUnDemotion](#)
      - Offset 0x012C - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.*
    - UINT8 [CStatePreWake](#)
      - Offset 0x012D - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.*
    - UINT8 [TimedMwait](#)
      - Offset 0x012E - Enable or Disable TimedMwait Support.*
-

- UINT8 [CstCfgCtrlIoMwaitRedirection](#)  
Offset 0x012F - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.
- UINT8 [PkgCStateLimit](#)  
Offset 0x0130 - Set the Max Pkg Cstate Set the Max Pkg Cstate.
- UINT8 [CstateLatencyControl1TimeUnit](#)  
Offset 0x0131 - TimeUnit for C-State Latency Control1 TimeUnit for C-State Latency Control1; Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.
- UINT8 [CstateLatencyControl2TimeUnit](#)  
Offset 0x0132 - TimeUnit for C-State Latency Control2 TimeUnit for C-State Latency Control2; Valid values 0 - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.
- UINT8 [CstateLatencyControl3TimeUnit](#)  
Offset 0x0133 - 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 0x0134 - TimeUnit for C-State Latency Control4 Time - 1ns , 1 - 32ns , 2 - 1024ns , 3 - 32768ns , 4 - 1048576ns , 5 - 33554432ns.
- UINT8 [CstateLatencyControl5TimeUnit](#)  
Offset 0x0135 - 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 0x0136 - Interrupt Redirection Mode Select Interrupt Redirection Mode Select.0: Fixed priority; 1: Round robin; 2: Hash vector; 7: No change.
- UINT8 [ProcHotLock](#)  
Offset 0x0137 - Lock procbot configuration Lock procbot configuration Enable/Disable; **0: Disable**; 1: Enable \$EN↔\_DIS.
- UINT8 [RaceToHalt](#)  
Offset 0x0138 - Race To Halt Enable/Disable Race To Halt feature.
- UINT8 [ConfigTdpLevel](#)  
Offset 0x0139 - Configuration for boot TDP selection Configuration for boot TDP selection; **0: TDP Nominal**; 1: TDP Down; 2: TDP Up; 0xFF : Deactivate.
- UINT16 [CstateLatencyControl1Irtl](#)  
Offset 0x013A - 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 0x013C - 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 0x013E - 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 0x0140 - 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 0x0142 - Interrupt Response Time Limit of C-State LatencyControl5 Interrupt Response Time Limit of C-State LatencyControl5. Range of value 0 to 0x3FF.
- UINT8 [StateRatioMax16](#) [16]  
Offset 0x0144 - P-state ratios for max 16 version of custom P-state table P-state ratios for max 16 version of custom P-state table.
- UINT32 [CpuBistData](#)  
Offset 0x0154 - CpuBistData Pointer CPU BIST Data.
- UINT32 [CpuMpPpi](#)  
Offset 0x0158 - CpuMpPpi Pointer for CpuMpPpi.
- UINT32 [CpuMpHob](#)

- Offset 0x015C - CpuMphob Pointer for CpuMphob.*

    - UINT8 [CpuPostMemRsvd](#) [16]
      - Offset 0x0160.*
    - UINT64 [BgpdtHash](#) [4]
      - Offset 0x0170 - BgpdtHash[4] BgpdtHash values.*
    - UINT32 [BiosGuardAttr](#)
      - Offset 0x0190 - BiosGuardAttr BiosGuardAttr default values.*
    - UINT8 [UnusedUpdSpace7](#) [4]
      - Offset 0x0194.*
    - UINT64 [BiosGuardModulePtr](#)
      - Offset 0x0198 - BiosGuardModulePtr BiosGuardModulePtr default values.*
    - UINT64 [SendEcCmd](#)
      - Offset 0x01A0 - SendEcCmd SendEcCmd function pointer.*
    - UINT8 [EcCmdProvisionEav](#)
      - Offset 0x01A8 - EcCmdProvisionEav Ephemeral Authorization Value default values.*
    - UINT8 [EcCmdLock](#)
      - Offset 0x01A9 - EcCmdLock EcCmdLock default values.*
    - UINT8 [UnusedUpdSpace8](#) [6]
      - Offset 0x01AA.*
    - UINT64 [SgxEpoch0](#)
      - Offset 0x01B0 - SgxEpoch0 SgxEpoch0 default values.*
    - UINT64 [SgxEpoch1](#)
      - Offset 0x01B8 - SgxEpoch1 SgxEpoch1 default values.*
    - UINT8 [SgxSinitNvsData](#)
      - Offset 0x01C0 - SgxSinitNvsData SgxSinitNvsData default values.*
    - UINT8 [SgxSinitDataFromTpm](#)
      - Offset 0x01C1 - SgxSinitDataFromTpm SgxSinitDataFromTpm default values.*
    - UINT8 [SecurityPostMemRsvd](#) [16]
      - Offset 0x01C2.*
    - UINT8 [Device4Enable](#)
      - Offset 0x01D2 - Enable Device 4 Enable/disable Device 4 \$EN\_DIS.*
    - UINT8 [CridEnable](#)
      - Offset 0x01D3 - Enable/Disable SA CRID Enable: SA CRID, Disable (Default): SA CRID \$EN\_DIS.*
    - UINT8 [SkipPamLock](#)
      - Offset 0x01D4 - Skip PAM register lock Enable: PAM register will not be locked by RC, platform code should lock it, Disable(Default): PAM registers will be locked by RC \$EN\_DIS.*
    - UINT8 [EdramTestMode](#)
      - Offset 0x01D5 - 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 [DmiAspm](#)
      - Offset 0x01D6 - DMI ASPM 0=Disable, 1:L0s, 2:L1, 3(Default)=L0sL1 0:Disable, 1:L0s, 2:L1, 3:L0sL1.*
    - UINT8 [DmiExtSync](#)
      - Offset 0x01D7 - DMI Extended Sync Control Enable: Enable DMI Extended Sync Control, Disable(Default): Disable DMI Extended Sync Control \$EN\_DIS.*
    - UINT8 [Dmilot](#)
      - Offset 0x01D8 - DMI IOT Control Enable: Enable DMI IOT Control, Disable(Default): Disable DMI IOT Control \$EN\_DIS.*
    - UINT8 [PegDeEmphasis](#) [4]
      - Offset 0x01D9 - PCIe DeEmphasis control per root port 0: -6dB, 1(Default): -3.5dB 0:-6dB, 1:-3.5dB.*
    - UINT8 [PegSlotPowerLimitValue](#) [4]
      - Offset 0x01DD - PCIe Slot Power Limit value per root port Slot power limit value per root port.*
-

- UINTE8 [PegSlotPowerLimitScale](#) [4]
  - Offset 0x01E1 - PCIe Slot Power Limit scale per root port Slot power limit scale per root port 0:1.0x, 1:0.1x, 2:0.01x, 3:0x001x.*
- UINTE8 [UnusedUpdSpace9](#) [1]
  - Offset 0x01E5.*
- UINTE16 [PegPhysicalSlotNumber](#) [4]
  - Offset 0x01E6 - PCIe Physical Slot Number per root port Physical Slot Number per root port.*
- UINTE8 [PegMaxPayload](#) [4]
  - Offset 0x01EE - PEG Max Payload size per root port 0xFF(Default):Auto, 0x1: Force 128B, 0x2: Force 256B 0xFF: Auto, 0x1: Force 128B, 0x2: Force 256B.*
- UINTE8 [UnusedUpdSpace10](#) [2]
  - Offset 0x01F2.*
- UINTE32 [GraphicsConfigPtr](#)
  - Offset 0x01F4 - Graphics Configuration Ptr Points to VBT.*
- UINTE32 [LogoPtr](#)
  - Offset 0x01F8 - Logo Pointer Points to PEI Display Logo Image.*
- UINTE32 [LogoSize](#)
  - Offset 0x01FC - Logo Size Size of PEI Display Logo Image.*
- UINTE32 [BltBufferAddress](#)
  - Offset 0x0200 - Blt Buffer Address Address of Blt buffer.*
- UINTE32 [BltBufferSize](#)
  - Offset 0x0204 - Blt Buffer Size Size of Blt Buffer, is equal to PixelWidth \* PixelHeight \* 4 bytes (the size of EFI\_G $\leftarrow$ RAPHICS\_OUTPUT\_BLT\_PIXEL)*
- UINTE8 [PavpEnable](#)
  - Offset 0x0208 - Enable/Disable PavpEnable Enable(Default): Enable PavpEnable, Disable: Disable PavpEnable \$ $\leftarrow$ EN\_DIS.*
- UINTE8 [CdClock](#)
  - Offset 0x0209 - CdClock Frequency selection 0=307.2 Mhz, 1=312 Mhz, 2=552 Mhz, 3=556.8 Mhz, 4=648 Mhz, 5(Default)= 652.8 Mhz 0: 307.2 Mhz, 1: 312 Mhz, 2: 552 Mhz, 3: 556.8 Mhz, 4: 648 Mhz, 5: 652.8 Mhz.*
- UINTE8 [PeiGraphicsPeimInit](#)
  - Offset 0x020A - Enable/Disable PeiGraphicsPeimInit Enable: Enable PeiGraphicsPeimInit, Disable(Default): Disable PeiGraphicsPeimInit \$EN\_DIS.*
- UINTE8 [RenderStandby](#)
  - Offset 0x020B - Enable/Disable IGFX RenderStandby Enable(Default): Enable IGFX RenderStandby, Disable: Disable IGFX RenderStandby \$EN\_DIS.*
- UINTE8 [PmSupport](#)
  - Offset 0x020C - Enable/Disable IGFX PmSupport Enable(Default): Enable IGFX PmSupport, Disable: Disable IGFX PmSupport \$EN\_DIS.*
- UINTE8 [CdynmaxClampEnable](#)
  - Offset 0x020D - Enable/Disable CdynmaxClamp Enable: Enable CdynmaxClamp, Disable(Default): Disable CdynmaxClamp \$EN\_DIS.*
- UINTE8 [GtFreqMax](#)
  - Offset 0x020E - 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.*
- UINTE8 [DisableTurboGt](#)
  - Offset 0x020F - Disable Turbo GT 0=Disable: GT frequency is not limited, 1=Enable: Disables Turbo GT frequency \$EN\_DIS.*
- UINTE8 [SkipCdClockInit](#)

- Offset 0x0210 - Enable/Disable CdClock Init Enable: Skip Full CD clock initialization, Disable(Default): Initialize the full CD clock if not initialized by Gfx PEIM \$EN\_DIS.
- UINT8 [DdiPortAConfig](#)  
Offset 0x0211 - 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 0x0212 - Enable or disable HPD of DDI port B 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPortCHpd](#)  
Offset 0x0213 - Enable or disable HPD of DDI port C 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPort1Hpd](#)  
Offset 0x0214 - Enable or disable HPD of DDI port 1 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPort2Hpd](#)  
Offset 0x0215 - Enable or disable HPD of DDI port 2 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPort3Hpd](#)  
Offset 0x0216 - Enable or disable HPD of DDI port 3 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPort4Hpd](#)  
Offset 0x0217 - Enable or disable HPD of DDI port 4 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPortBDdc](#)  
Offset 0x0218 - Enable or disable DDC of DDI port B 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPortCDdc](#)  
Offset 0x0219 - Enable or disable DDC of DDI port C 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [DdiPort1Ddc](#)  
Offset 0x021A - Enable DDC setting of DDI Port 1 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.
  - UINT8 [DdiPort2Ddc](#)  
Offset 0x021B - Enable DDC setting of DDI Port 2 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.
  - UINT8 [DdiPort3Ddc](#)  
Offset 0x021C - Enable DDC setting of DDI Port 3 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.
  - UINT8 [DdiPort4Ddc](#)  
Offset 0x021D - Enable DDC setting of DDI Port 4 0=Disable, 1=DDC(Default) 0: Disable, 1: DDC.
  - UINT8 [GnaEnable](#)  
Offset 0x021E - Enable or disable GNA device 0=Disable, 1(Default)=Enable \$EN\_DIS.
  - UINT8 [UsbOverride](#)  
Offset 0x021F - USB override in IOM This policy will enable/disable USB Connect override in IOM \$EN\_DIS.
  - UINT8 [VccSt](#)  
Offset 0x0220 - VCCST request for IOM This policy will enable/disable VCCST and also decides if message would be replayed in S4/S5 \$EN\_DIS.
  - UINT8 [D3HotEnable](#)  
Offset 0x0221 - Enable D3 Hot in TCSS This policy will enable/disable D3 hot support in IOM \$EN\_DIS.
  - UINT8 [D3ColdEnable](#)  
Offset 0x0222 - Enable D3 Cold in TCSS This policy will enable/disable D3 cold support in IOM \$EN\_DIS.
  - UINT8 [PmcPdEnable](#)  
Offset 0x0223 - Enable/Disable PMC-PD Solution This policy will enable/disable PMC-PD Solution vs EC-TCPC Solution \$EN\_DIS.
  - UINT8 [PtmEnabled](#) [4]  
Offset 0x0224 - Enable/Disable PTM This policy will enable/disable Precision Time Measurement for TCSS PCIe Root Ports \$EN\_DIS.
  - UINT8 [VmdEnable](#)  
Offset 0x0228 - Enable VMD controller Enable/disable to VMD controller.
  - UINT8 [VmdPortA](#)  
Offset 0x0229 - Enable VMD portA Support Enable/disable to VMD portA Support.
  - UINT8 [VmdPortB](#)  
Offset 0x022A - Enable VMD portB Support Enable/disable to VMD portB Support.
-

- UINT8 [VmdPortC](#)  
*Offset 0x022B - Enable VMD portC Support Enable/disable to VMD portC Support.*
  - UINT8 [VmdPortD](#)  
*Offset 0x022C - Enable VMD portD Support Enable/disable to VMD portD Support.*
  - UINT8 [VmdCfgBarSz](#)  
*Offset 0x022D - VMD Config Bar size Set The VMD Config Bar Size.*
  - UINT8 [VmdCfgBarAttr](#)  
*Offset 0x022E - 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 0x022F - VMD Mem Bar1 size Set The VMD Mem Bar1 Size.*
  - UINT8 [VmdMemBar1Attr](#)  
*Offset 0x0230 - 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 0x0231 - VMD Mem Bar2 size Set The VMD Mem Bar2 Size.*
  - UINT8 [VmdMemBar2Attr](#)  
*Offset 0x0232 - 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 [UnusedUpdSpace11](#) [1]  
*Offset 0x0233.*
  - UINT32 [IomTypeCPortPadCfg](#) [8]  
*Offset 0x0234 - 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.*
  - UINT16 [TcssAuxOri](#)  
*Offset 0x0254 - TCSS Aux Orientation Override Enable Bits 0, 2, ...*
  - UINT16 [TcssHslOri](#)  
*Offset 0x0256 - TCSS HSL Orientation Override Enable Bits 0, 2, ...*
  - UINT8 [PchUsbOverCurrentEnable](#)  
*Offset 0x0258 - 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 [CpuUsb3OverCurrentPin](#) [8]  
*Offset 0x0259 - CPU USB3 Port Over Current Pin Describe the specific over current pin number of USBC Port N.*
  - UINT8 [UsbTcPortEn](#)  
*Offset 0x0261 - TCSS USB Port Enable Bits 0, 1, ...*
  - UINT8 [UnusedUpdSpace12](#) [2]  
*Offset 0x0262.*
  - UINT32 [IclAxITbtDmaUuid](#) [2]  
*Offset 0x0264 - ITBT DMA UUID TCSS DMA1, DMA2 UUID Number.*
  - UINT8 [ITbtPcieRootPortEn](#) [4]  
*Offset 0x026C - ITBT Root Port Enable ITBT Root Port Enable, 0:Disable, 1:Enable 0:Disable, 1:Enable.*
  - UINT16 [ITbtForcePowerOnTimeoutInMs](#)  
*Offset 0x0270 - ITBTForcePowerOn Timeout value ITBTForcePowerOn value.*
  - UINT16 [ITbtConnectTopologyTimeoutInMs](#)  
*Offset 0x0272 - ITbtConnectTopology Timeout value ITbtConnectTopologyTimeout value.*
  - UINT8 [TcssXhciEnableComplianceMode](#)  
*Offset 0x0274 - TcssXhciEnableComplianceMode Set Compliance Mode.*
  - UINT8 [TcssLoopbackModeBitMap](#)  
*Offset 0x0275 - TcssLoopbackModeBitMap Set Loopback Mode Bit Map.*
-

- UINT8 [SaPcieEqPh3LaneParamCm](#) [4]  
*Offset 0x0276 - PCIE Eq Ph3 Lane Param Cm SA\_PCIE\_EQ\_LANE\_PARAM.*
  - UINT8 [SaPcieEqPh3LaneParamCp](#) [4]  
*Offset 0x027A - PCIE Eq Ph3 Lane Param Cp SA\_PCIE\_EQ\_LANE\_PARAM.*
  - UINT8 [SaPcieDisableRootPortClockGating](#)  
*Offset 0x027E - PCIE Disable RootPort Clock Gating Describes whether the PCI Express Clock Gating for each root port is enabled by platform modules.*
  - UINT8 [SaPcieComplianceTestMode](#)  
*Offset 0x027F - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.*
  - UINT8 [SaPcieEnablePeerMemoryWrite](#)  
*Offset 0x0280 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.*
  - UINT8 [SaPcieRpFunctionSwap](#)  
*Offset 0x0281 - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.*
  - UINT8 [UnusedUpdSpace13](#) [2]  
*Offset 0x0282.*
  - UINT32 [SaPcieDeviceOverrideTablePtr](#)  
*Offset 0x0284 - Pch PCIE device override table pointer The PCIe device table is being used to override PCIe device ASPM settings.*
  - UINT8 [SaPcieRpHotPlug](#) [4]  
*Offset 0x0288 - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.*
  - UINT8 [SaPcieRpPmSci](#) [4]  
*Offset 0x028C - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.*
  - UINT8 [SaPcieRpTransmitterHalfSwing](#) [4]  
*Offset 0x0290 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.*
  - UINT8 [SaPcieRpAcsEnabled](#) [4]  
*Offset 0x0294 - PCIE RP Access Control Services Extended Capability Enable/Disable PCIE RP Access Control Services Extended Capability.*
  - UINT8 [SaPcieRpAdvancedErrorReporting](#) [4]  
*Offset 0x0298 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.*
  - UINT8 [SaPcieRpUnsupportedRequestReport](#) [4]  
*Offset 0x029C - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.*
  - UINT8 [SaPcieRpFatalErrorReport](#) [4]  
*Offset 0x02A0 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.*
  - UINT8 [SaPcieRpNoFatalErrorReport](#) [4]  
*Offset 0x02A4 - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.*
  - UINT8 [SaPcieRpCorrectableErrorReport](#) [4]  
*Offset 0x02A8 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.*
  - UINT8 [SaPcieRpSystemErrorOnFatalError](#) [4]  
*Offset 0x02AC - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.*
  - UINT8 [SaPcieRpSystemErrorOnNonFatalError](#) [4]  
*Offset 0x02B0 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.*
  - UINT8 [SaPcieRpSystemErrorOnCorrectableError](#) [4]  
*Offset 0x02B4 - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.*
  - UINT8 [SaPcieRpMaxPayload](#) [4]  
*Offset 0x02B8 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH\_PCIE\_MAX\_PAYLOAD.*
  - UINT32 [SaPcieRpDpcMask](#)
-

- Offset 0x02BC - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.*

    - UINT32 [SaPcieRpDpcExtensionsMask](#)
  - Offset 0x02C0 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.*

    - UINT8 [SaPcieRpSlotImplemented](#) [4]
  - Offset 0x02C4 - PCH PCIe root port connection type 0: built-in device, 1:slot.*

    - UINT8 [SaPcieRpPcieSpeed](#) [4]
  - Offset 0x02C8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.*

    - UINT8 [SaPcieRpGen3EqPh3Method](#) [4]
  - Offset 0x02CC - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH\_PCIE\_EQ\_METHOD).*

    - UINT8 [SaPcieRpPhysicalSlotNumber](#) [4]
  - Offset 0x02D0 - PCIE RP Physical Slot Number Indicates the slot number for the root port.*

    - UINT8 [SaPcieRpAspm](#) [4]
  - Offset 0x02D4 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH\_PCIE\_ASPM\_CONTROL).*

    - UINT8 [SaPcieRpL1Substates](#) [4]
  - Offset 0x02D8 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: SA\_PCIE\_L1SUBSTATES\_CONTROL).*

    - UINT8 [SaPcieRpLtrEnable](#) [4]
  - Offset 0x02DC - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.*

    - UINT8 [SaPcieRpLtrConfigLock](#) [4]
  - Offset 0x02E0 - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.*

    - UINT32 [SaPcieRpPtmMask](#)
  - Offset 0x02E4 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.*

    - UINT16 [SaPcieRpDetectTimeoutMs](#) [4]
  - Offset 0x02E8 - 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.*

    - UINT16 [SaPcieRpLtrMaxSnoopLatency](#) [4]
  - Offset 0x02F0 - PCIE RP Ltr Max Snoop Latency Test, Latency Tolerance Reporting, Max Snoop Latency.*

    - UINT16 [SaPcieRpLtrMaxNoSnoopLatency](#) [4]
  - Offset 0x02F8 - PCIE RP Ltr Max No Snoop Latency Test, Latency Tolerance Reporting, Max Non-Snoop Latency.*

    - UINT8 [SaPcieRpSnoopLatencyOverrideMode](#) [4]
  - Offset 0x0300 - PCIE RP Snoop Latency Override Mode Test, Latency Tolerance Reporting, Snoop Latency Override Mode.*

    - UINT8 [SaPcieRpSnoopLatencyOverrideMultiplier](#) [4]
  - Offset 0x0304 - PCIE RP Snoop Latency Override Multiplier Test, Latency Tolerance Reporting, Snoop Latency Override Multiplier.*

    - UINT16 [SaPcieRpSnoopLatencyOverrideValue](#) [4]
  - Offset 0x0308 - PCIE RP Snoop Latency Override Value Test, Latency Tolerance Reporting, Snoop Latency Override Value.*

    - UINT8 [SaPcieRpNonSnoopLatencyOverrideMode](#) [4]
  - Offset 0x0310 - PCIE RP Non Snoop Latency Override Mode Test, Latency Tolerance Reporting, Non-Snoop Latency Override Mode.*

    - UINT8 [SaPcieRpNonSnoopLatencyOverrideMultiplier](#) [4]
  - Offset 0x0314 - PCIE RP Non Snoop Latency Override Multiplier Test, Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.*

    - UINT16 [SaPcieRpNonSnoopLatencyOverrideValue](#) [4]
  - Offset 0x0318 - PCIE RP Non Snoop Latency Override Value Test, Latency Tolerance Reporting, Non-Snoop Latency Override Value.*

    - UINT8 [SaPcieRpUptp](#) [4]
  - Offset 0x0320 - PCIE RP Upstream Port Transmitter Preset Test, Used during Gen3 Link Equalization.*

    - UINT8 [SaPcieRpDptp](#) [4]
  - Offset 0x0324 - PCIE RP Downstream Port Transmitter Preset Test, Used during Gen3 Link Equalization.*

    - UINT8 [SaPostMemRsvd](#) [7]
-

- Offset 0x0328.
  - UINT8 [Heci3Enabled](#)
    - Offset 0x032F - HECI3 state The HECI3 state from Mbp for reference in S3 path or when MbpHob is not installed.
  - UINT8 [MeUnconfigOnRtcClear](#)
    - Offset 0x0330 - ME Unconfig on RTC clear 0: Disable ME Unconfig On Rtc Clear.
  - UINT8 [EndOfPostMessage](#)
    - Offset 0x0331 - End of Post message Test, Send End of Post message.
  - UINT8 [DisableD0I3SettingForHeci](#)
    - Offset 0x0332 - D0I3 Setting for HECI Disable Test, 0: disable, 1: enable, Setting this option disables setting D0I3 bit for all HECI devices \$EN\_DIS.
  - UINT8 [MctpBroadcastCycle](#)
    - Offset 0x0333 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.
  - UINT8 [MePostMemRsvd](#) [10]
    - Offset 0x0334.
  - UINT8 [AmtEnabled](#)
    - Offset 0x033E - AMT Switch Enable/Disable.
  - UINT8 [WatchDog](#)
    - Offset 0x033F - WatchDog Timer Switch Enable/Disable.
  - UINT8 [AsfEnabled](#)
    - Offset 0x0340 - ASF Switch Enable/Disable.
  - UINT8 [FwProgress](#)
    - Offset 0x0341 - PET Progress Enable/Disable.
  - UINT16 [WatchDogTimerOs](#)
    - Offset 0x0342 - OS Timer 16 bits Value, Set OS watchdog timer.
  - UINT16 [WatchDogTimerBios](#)
    - Offset 0x0344 - BIOS Timer 16 bits Value, Set BIOS watchdog timer.
  - UINT8 [ManageabilityMode](#)
    - Offset 0x0346 - Manageability Mode set by Mebx Enable/Disable.
  - UINT8 [AmtSolEnabled](#)
    - Offset 0x0347 - SOL Switch Enable/Disable.
  - UINT8 [RemoteAssistance](#)
    - Offset 0x0348 - Remote Assistance Trigger Availablilty Enable/Disable.
  - UINT8 [AmtKvmEnabled](#)
    - Offset 0x0349 - KVM Switch Enable/Disable.
  - UINT8 [ForcMebxSyncUp](#)
    - Offset 0x034A - MEBX execution Enable/Disable.
  - UINT8 [AmtPostMemRsvd](#) [10]
    - Offset 0x034B.
  - UINT8 [SerialloSpi0CsPolarity](#) [2]
    - Offset 0x0355 - SPI0 Chip Select Polarity Sets polarity for each chip Select.
  - UINT8 [SerialloSpi1CsPolarity](#) [2]
    - Offset 0x0357 - SPI1 Chip Select Polarity Sets polarity for each chip Select.
  - UINT8 [SerialloSpi2CsPolarity](#) [2]
    - Offset 0x0359 - SPI2 Chip Select Polarity Sets polarity for each chip Select.
  - UINT8 [SerialloSpi0CsEnable](#) [2]
    - Offset 0x035B - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.
  - UINT8 [SerialloSpi1CsEnable](#) [2]
    - Offset 0x035D - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.
  - UINT8 [SerialloSpi2CsEnable](#) [2]
    - Offset 0x035F - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.
  - UINT8 [SerialloSpiMode](#) [3]
-

- Offset 0x0361 - SPIn Device Mode Selects SPI operation mode.*

    - UINT8 [SerialloSpiDefaultCsOutput](#) [3]
      - Offset 0x0364 - SPIn Default Chip Select Output Sets Default CS as Output.*
    - UINT8 [PchSerialloI2cPadsTermination](#) [6]
      - Offset 0x0367 - 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,I2C2,I2C3,I2C4,I2C5 pads termination respectively.*
    - UINT8 [SerialloI2cMode](#) [6]
      - Offset 0x036D - I2Cn Device Mode Selects I2c operation mode.*
    - UINT8 [SerialloUartMode](#) [3]
      - Offset 0x0373 - UARTn Device Mode Selects Uart operation mode.*
    - UINT8 [UnusedUpdSpace14](#) [2]
      - Offset 0x0376.*
    - UINT32 [SerialloUartBaudRate](#) [3]
      - Offset 0x0378 - Default BaudRate for each Serial IO UART Set default BaudRate Supported from 0 - default to 6000000.*
    - UINT8 [SerialloUartParity](#) [3]
      - Offset 0x0384 - Default ParityType for each Serial IO UART Set default Parity.*
    - UINT8 [SerialloUartDataBits](#) [3]
      - Offset 0x0387 - Default DataBits for each Serial IO UART Set default word length.*
    - UINT8 [SerialloUartStopBits](#) [3]
      - Offset 0x038A - Default StopBits for each Serial IO UART Set default stop bits.*
    - UINT8 [SerialloUartPowerGating](#) [3]
      - Offset 0x038D - Power Gating mode for each Serial IO UART that works in COM mode Set Power Gating.*
    - UINT8 [SerialloUartDmaEnable](#) [3]
      - Offset 0x0390 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.*
    - UINT8 [SerialloUartAutoFlow](#) [3]
      - Offset 0x0393 - Enables UART hardware flow control, CTS and RTS lines Enables UART hardware flow control, CTS and RTS lines.*
    - UINT8 [UnusedUpdSpace15](#) [2]
      - Offset 0x0396.*
    - UINT32 [SerialloUartRxPinMux](#) [3]
      - Offset 0x0398 - SerialloUartRxPinMux Select Seriallo Uart Rx pin muxing.*
    - UINT32 [SerialloUartTxPinMux](#) [3]
      - Offset 0x03A4 - SerialloUartTxPinMux Select Seriallo Uart Tx pin muxing.*
    - UINT32 [SerialloUartRtsPinMux](#) [3]
      - Offset 0x03B0 - SerialloUartRtsPinMux Select Seriallo Uart Rts pin muxing.*
    - UINT32 [SerialloUartCtsPinMux](#) [3]
      - Offset 0x03BC - SerialloUartCtsPinMux Select Seriallo Uart Cts pin muxing.*
    - UINT8 [SerialloDebugUartNumber](#)
      - Offset 0x03C8 - UART Number For Debug Purpose UART number for debug purpose.*
    - UINT8 [PchLanEnable](#)
      - Offset 0x03C9 - Enable LAN Enable/disable LAN controller.*
    - UINT8 [PchLanLtrEnable](#)
      - Offset 0x03CA - Enable PCH Lan LTR capability of PCH internal LAN 0: Disable; 1: Enable.*
    - UINT8 [PchHdaDspEnable](#)
      - Offset 0x03CB - Enable HD Audio DSP Enable/disable HD Audio DSP feature.*
    - UINT8 [PchHdaPme](#)
      - Offset 0x03CC - Enable Pme Enable Azalia wake-on-ring.*
    - UINT8 [PchHdaVcType](#)
      - Offset 0x03CD - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.*
-

- UINT8 [PchHdaLinkFrequency](#)  
*Offset 0x03CE - HD Audio Link Frequency HDA Link Freq (PCH\_HDAUDIO\_LINK\_FREQUENCY enum): 0: 6MHz, 1: 12MHz, 2: 24MHz.*
  - UINT8 [PchHdaIDispLinkFrequency](#)  
*Offset 0x03CF - iDisp-Link Frequency iDisp-Link Freq (PCH\_HDAUDIO\_LINK\_FREQUENCY enum): 4: 96MHz, 3: 48MHz.*
  - UINT8 [PchHdaIDispLinkTmode](#)  
*Offset 0x03D0 - 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 0x03D1 - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).*
  - UINT8 [PchHdaIDispCodecDisconnect](#)  
*Offset 0x03D2 - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.*
  - UINT8 [PchHdaCodecSxWakeCapability](#)  
*Offset 0x03D3 - PCH HDA Codec Sx Wake Capability Capability to detect wake initiated by a codec in Sx.*
  - UINT16 [PchHdaResetWaitTimer](#)  
*Offset 0x03D4 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.*
  - UINT8 [PchHdaVerbTableEntryNum](#)  
*Offset 0x03D6 - PCH HDA Verb Table Entry Number Number of Entries in Verb Table.*
  - UINT8 [UnusedUpdSpace16](#)  
*Offset 0x03D7.*
  - UINT32 [PchHdaVerbTablePtr](#)  
*Offset 0x03D8 - PCH HDA Verb Table Pointer Pointer to Array of pointers to Verb Table.*
  - UINT8 [PchHdaAudioLinkHda](#)  
*Offset 0x03DC - Enable HD Audio Link Enable/disable HD Audio Link.*
  - UINT8 [PchHdaAudioLinkDmic0](#)  
*Offset 0x03DD - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.*
  - UINT8 [PchHdaAudioLinkDmic1](#)  
*Offset 0x03DE - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.*
  - UINT8 [PchHdaAudioLinkSsp0](#)  
*Offset 0x03DF - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.*
  - UINT8 [PchHdaAudioLinkSsp1](#)  
*Offset 0x03E0 - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.*
  - UINT8 [PchHdaAudioLinkSsp2](#)  
*Offset 0x03E1 - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.*
  - UINT8 [PchHdaAudioLinkSsp3](#)  
*Offset 0x03E2 - Enable HD Audio SSP3 Link Enable/disable HD Audio SSP3/I2S link.*
  - UINT8 [PchHdaAudioLinkSsp4](#)  
*Offset 0x03E3 - Enable HD Audio SSP4 Link Enable/disable HD Audio SSP4/I2S link.*
  - UINT8 [PchHdaAudioLinkSsp5](#)  
*Offset 0x03E4 - Enable HD Audio SSP5 Link Enable/disable HD Audio SSP5/I2S link.*
  - UINT8 [PchHdaAudioLinkSndw1](#)  
*Offset 0x03E5 - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.*
  - UINT8 [PchHdaAudioLinkSndw2](#)  
*Offset 0x03E6 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.*
  - UINT8 [PchHdaAudioLinkSndw3](#)  
*Offset 0x03E7 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.*
  - UINT8 [PchHdaAudioLinkSndw4](#)  
*Offset 0x03E8 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.*
  - UINT8 [CnviMode](#)
-

- Offset 0x03E9 - CNVi Configuration This option allows for automatic detection of Connectivity Solution.*

    - UINT8 [CnviBtCore](#)
      - Offset 0x03EA - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.*
    - UINT8 [CnviBtAudioOffload](#)
      - Offset 0x03EB - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.*
    - UINT8 [CnviMfUart1Type](#)
      - Offset 0x03EC - CNVi MfUart1 Type This option configures Uart type which connects to MfUart1 0:ISH Uart0, 1↔:SerialIO Uart2, 2:Uart over external pads.*
    - UINT8 [UnusedUpdSpace17](#) [3]
      - Offset 0x03ED.*
    - UINT32 [CnviRfResetPinMux](#)
      - Offset 0x03F0 - CNVi RF\_RESET pin muxing Select CNVi RF\_RESET# pin depending on board routing.*
    - UINT32 [CnviClkreqPinMux](#)
      - Offset 0x03F4 - CNVi CLKREQ pin muxing Select CNVi CLKREQ pin depending on board routing.*
    - UINT8 [PchEspilgmrEnable](#)
      - Offset 0x03F8 - Espi Lgmr Memory Range decode This option enables or disables espi lgmr \$EN\_DIS.*
    - UINT8 [PchEspibmeMasterSlaveEnabled](#)
      - Offset 0x03F9 - PCH eSPI Master and Slave BME enabled PCH eSPI Master and Slave BME enabled \$EN\_DIS.*
    - UINT8 [PchEspihostC10ReportEnable](#)
      - Offset 0x03FA - Enable Host C10 reporting through eSPI Enable/disable Host C10 reporting to Slave via eSPI Virtual Wire.*
    - UINT8 [ScsSdCardEnabled](#)
      - Offset 0x03FB - Enable SdCard Controller Enable/disable SD Card Controller.*
    - UINT8 [SdCardPowerEnableActiveHigh](#)
      - Offset 0x03FC - SdCard power enable polarity Choose SD\_PWREN# polarity 0: Active low, 1: Active high.*
    - UINT8 [SdCardOverrideDefaultDll](#)
      - Offset 0x03FD - SdCard override default DLL Enable/Disable override on default DLL values \$EN\_DIS.*
    - UINT8 [SdCardSdr50RxDelay125ps](#)
      - Offset 0x03FE - SdCard SDR50 delay Value of the delay for SDR50 speed in 125ps multiple.*
    - UINT8 [SdCardDdr50RxDelay125ps](#)
      - Offset 0x03FF - SdCard DDR50 delay Value of the delay for DDR50 speed in 125ps multiple.*
    - UINT8 [ScsEmmcEnabled](#)
      - Offset 0x0400 - Enable eMMC Controller Enable/disable eMMC Controller.*
    - UINT8 [ScsEmmchS400Enabled](#)
      - Offset 0x0401 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.*
    - UINT8 [PchScsEmmchS400DIIDataValid](#)
      - Offset 0x0402 - Set HS400 Tuning Data Valid Set if HS400 Tuning Data Valid.*
    - UINT8 [PchScsEmmchS400RxStrobeDll1](#)
      - Offset 0x0403 - Rx Strobe Delay Control Rx Strobe Delay Control - Rx Strobe Delay DLL 1 (HS400 Mode).*
    - UINT8 [PchScsEmmchS400TxDataDll](#)
      - Offset 0x0404 - Tx Data Delay Control Tx Data Delay Control 1 - Tx Data Delay (HS400 Mode).*
    - UINT8 [UfsEnable](#) [2]
      - Offset 0x0405 - UFS enable/disable Tx Data Delay Control 1 - Tx Data Delay (HS400 Mode).*
    - UINT8 [PchlshSpiGpioAssign](#)
      - Offset 0x0407 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.*
    - UINT8 [PchlshUart0GpioAssign](#)
      - Offset 0x0408 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.*
    - UINT8 [PchlshUart1GpioAssign](#)
      - Offset 0x0409 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.*
    - UINT8 [PchlshI2c0GpioAssign](#)
      - Offset 0x040A - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.*
-

- UINT8 [PchIshI2c1GpioAssign](#)  
*Offset 0x040B - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshI2c2GpioAssign](#)  
*Offset 0x040C - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp0GpioAssign](#)  
*Offset 0x040D - Enable PCH ISH GP\_0 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp1GpioAssign](#)  
*Offset 0x040E - Enable PCH ISH GP\_1 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp2GpioAssign](#)  
*Offset 0x040F - Enable PCH ISH GP\_2 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp3GpioAssign](#)  
*Offset 0x0410 - Enable PCH ISH GP\_3 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp4GpioAssign](#)  
*Offset 0x0411 - Enable PCH ISH GP\_4 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp5GpioAssign](#)  
*Offset 0x0412 - Enable PCH ISH GP\_5 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp6GpioAssign](#)  
*Offset 0x0413 - Enable PCH ISH GP\_6 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshGp7GpioAssign](#)  
*Offset 0x0414 - Enable PCH ISH GP\_7 GPIO pin assigned 0: Disable; 1: Enable.*
  - UINT8 [PchIshPdtUnlock](#)  
*Offset 0x0415 - PCH ISH PDT Unlock Msg 0: False; 1: True.*
  - UINT8 [SataEnable](#)  
*Offset 0x0416 - Enable SATA Enable/disable SATA controller.*
  - UINT8 [SataTestMode](#)  
*Offset 0x0417 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.*
  - UINT8 [SataSalpSupport](#)  
*Offset 0x0418 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.*
  - UINT8 [SataPwrOptEnable](#)  
*Offset 0x0419 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.*
  - UINT8 [EsataSpeedLimit](#)  
*Offset 0x041A - PCH Sata eSATA Speed Limit When enabled, BIOS will configure the PxSCTL.SPD to 2 to limit the eSATA port speed.*
  - UINT8 [SataLedEnable](#)  
*Offset 0x041B - SATA LED SATA LED indicating SATA controller activity.*
  - UINT8 [SataMode](#)  
*Offset 0x041C - SATA Mode Select SATA controller working mode.*
  - UINT8 [SataSpeedLimit](#)  
*Offset 0x041D - PCH Sata Speed Limit Indicates the maximum speed the SATA controller can support 0h: Pch↔SataSpeedDefault.*
  - UINT8 [SataPortsEnable](#) [8]  
*Offset 0x041E - Enable SATA ports Enable/disable SATA ports.*
  - UINT8 [SataPortsHotPlug](#) [8]  
*Offset 0x0426 - Enable SATA Port HotPlug Enable SATA Port HotPlug.*
  - UINT8 [SataPortsInterlockSw](#) [8]  
*Offset 0x042E - Enable SATA Port Interlock Sw Enable SATA Port Interlock Sw.*
  - UINT8 [SataPortsExternal](#) [8]  
*Offset 0x0436 - Enable SATA Port External Enable SATA Port External.*
  - UINT8 [SataPortsSpinUp](#) [8]  
*Offset 0x043E - Enable SATA Port SpinUp Enable the COMRESET initialization Sequence to the device.*
  - UINT8 [SataPortsSolidStateDrive](#) [8]
-

- Offset 0x0446 - Enable SATA Port Solid State Drive 0: HDD; 1: SSD.*

  - UINT8 [SataPortsDevSlp](#) [8]
    - Offset 0x044E - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.*
  - UINT8 [SataPortsEnableDitoConfig](#) [8]
    - Offset 0x0456 - Enable SATA Port Enable Dito Config Enable DEVSLP Idle Timeout settings (DmVal, DitoVal).*
  - UINT8 [SataPortsDmVal](#) [8]
    - Offset 0x045E - Enable SATA Port DmVal DITO multiplier.*
  - UINT16 [SataPortsDitoVal](#) [8]
    - Offset 0x0466 - Enable SATA Port DmVal DEVSLP Idle Timeout (DITO), Default is 625.*
  - UINT8 [SataPortsZpOdd](#) [8]
    - Offset 0x0476 - Enable SATA Port ZpOdd Support zero power ODD.*
  - UINT8 [SataRstRaidDeviceld](#)
    - Offset 0x047E - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.*
  - UINT8 [SataRstRaid0](#)
    - Offset 0x047F - PCH Sata Rst Raid0 RAID0.*
  - UINT8 [SataRstRaid1](#)
    - Offset 0x0480 - PCH Sata Rst Raid1 RAID1.*
  - UINT8 [SataRstRaid10](#)
    - Offset 0x0481 - PCH Sata Rst Raid10 RAID10.*
  - UINT8 [SataRstRaid5](#)
    - Offset 0x0482 - PCH Sata Rst Raid5 RAID5.*
  - UINT8 [SataRstIrrt](#)
    - Offset 0x0483 - PCH Sata Rst Irrt Intel Rapid Recovery Technology.*
  - UINT8 [SataRstOromUiBanner](#)
    - Offset 0x0484 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.*
  - UINT8 [SataRstOromUiDelay](#)
    - Offset 0x0485 - 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 0x0486 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.*
  - UINT8 [SataRstLedLocate](#)
    - Offset 0x0487 - 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 0x0488 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.*
  - UINT8 [SataRstSmartStorage](#)
    - Offset 0x0489 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.*
  - UINT8 [SataRstInterrupt](#)
    - Offset 0x048A - SATA RST Interrupt Mode Allows to choose which interrupts will be implemented by SATA controller in RAID mode.*
  - UINT8 [SataRstOptaneMemory](#)
    - Offset 0x048B - PCH Sata Rst Optane Memory Optane Memory \$EN\_DIS.*
  - UINT8 [SataRstLegacyOrom](#)
    - Offset 0x048C - PCH SATA use RST Legacy OROM Use PCH SATA RST Legacy OROM when CSM is Enabled \$EN\_DIS.*
  - UINT8 [SataRstCpuAttachedStorage](#)
    - Offset 0x048D - PCH Sata Rst CPU Attached Storage CPU Attached Storage \$EN\_DIS.*
  - UINT8 [SataRstPcieEnable](#) [3]
    - Offset 0x048E - PCH Sata Rst Pcie Storage Remap enable Enable Intel RST for PCIe Storage remapping.*
  - UINT8 [SataRstPcieStoragePort](#) [3]
    - Offset 0x0491 - PCH Sata Rst Pcie Storage Port Intel RST for PCIe Storage remapping - PCIe Port Selection (1-based, 0 = autodetect).*

- UINT8 [SataRstPcieDeviceResetDelay](#) [3]  
*Offset 0x0494 - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.*
  - UINT8 [SataP0T1M](#)  
*Offset 0x0497 - Port 0 T1 Multipler Port 0 T1 Multipler.*
  - UINT8 [SataP0T2M](#)  
*Offset 0x0498 - Port 0 T2 Multipler Port 0 T2 Multipler.*
  - UINT8 [SataP0T3M](#)  
*Offset 0x0499 - Port 0 T3 Multipler Port 0 T3 Multipler.*
  - UINT8 [SataP0TDisp](#)  
*Offset 0x049A - Port 0 Tdispatch Port 0 Tdispatch.*
  - UINT8 [SataP1T1M](#)  
*Offset 0x049B - Port 1 T1 Multipler Port 1 T1 Multipler.*
  - UINT8 [SataP1T2M](#)  
*Offset 0x049C - Port 1 T2 Multipler Port 1 T2 Multipler.*
  - UINT8 [SataP1T3M](#)  
*Offset 0x049D - Port 1 T3 Multipler Port 1 T3 Multipler.*
  - UINT8 [SataP1TDisp](#)  
*Offset 0x049E - Port 1 Tdispatch Port 1 Tdispatch.*
  - UINT8 [SataP0Tinact](#)  
*Offset 0x049F - Port 0 Tinactive Port 0 Tinactive.*
  - UINT8 [SataP0TDispFinit](#)  
*Offset 0x04A0 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.*
  - UINT8 [SataP1Tinact](#)  
*Offset 0x04A1 - Port 1 Tinactive Port 1 Tinactive.*
  - UINT8 [SataP1TDispFinit](#)  
*Offset 0x04A2 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.*
  - UINT8 [SataThermalSuggestedSetting](#)  
*Offset 0x04A3 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.*
  - UINT8 [PchEnableComplianceMode](#)  
*Offset 0x04A4 - Enable xHCI Compliance Mode Compliance Mode can be enabled for testing through this option but this is disabled by default.*
  - UINT8 [UsbPdoProgramming](#)  
*Offset 0x04A5 - USB PDO Programming Enable/disable PDO programming for USB in PEI phase.*
  - UINT8 [PchEnableDbcObs](#)  
*Offset 0x04A6 - USB Overcurrent Override for Dbc This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option.*
  - UINT8 [PchXhciOcLock](#)  
*Offset 0x04A7 - 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 [PortUsb20Enable](#) [16]  
*Offset 0x04A8 - Enable USB2 ports Enable/disable per USB2 ports.*
  - UINT8 [Usb2OverCurrentPin](#) [16]  
*Offset 0x04B8 - USB2 Port Over Current Pin Describe the specific over current pin number of USB 2.0 Port N.*
  - UINT8 [PortUsb30Enable](#) [10]  
*Offset 0x04C8 - Enable USB3 ports Enable/disable per USB3 ports.*
  - UINT8 [Usb3OverCurrentPin](#) [10]  
*Offset 0x04D2 - USB3 Port Over Current Pin Describe the specific over current pin number of USB 3.0 Port N.*
  - UINT8 [XdcIEnable](#)  
*Offset 0x04DC - Enable xDCI controller Enable/disable to xDCI controller.*
  - UINT8 [Usb2PhyPetxiset](#) [16]
-

- Offset 0x04DD - USB Per Port HS Preemphasis Bias USB Per Port HS Preemphasis Bias.*

  - UINT8 [Usb2PhyTxiset](#) [16]
    - Offset 0x04ED - USB Per Port HS Transmitter Bias USB Per Port HS Transmitter Bias.*
  - UINT8 [Usb2PhyPredeemp](#) [16]
    - Offset 0x04FD - USB Per Port HS Transmitter Emphasis USB Per Port HS Transmitter Emphasis.*
  - UINT8 [Usb2PhyPehalfbit](#) [16]
    - Offset 0x050D - USB Per Port Half Bit Pre-emphasis USB Per Port Half Bit Pre-emphasis.*
  - UINT8 [Usb3HsioTxDeEmphEnable](#) [10]
    - Offset 0x051D - 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 0x0527 - 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 0x0531 - 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 0x053B - USB 3.0 TX Output Downscale Amplitude Adjustment USB 3.0 TX Output Downscale Amplitude Adjustment, HSIO\_TX\_DWORD8[21:16], **Default = 00h**.*
  - UINT8 [PcieRpHotPlug](#) [24]
    - Offset 0x0545 - Enable PCIE RP HotPlug Indicate whether the root port is hot plug available.*
  - UINT8 [PcieRpPmSci](#) [24]
    - Offset 0x055D - Enable PCIE RP Pm Sci Indicate whether the root port power manager SCI is enabled.*
  - UINT8 [PcieRpTransmitterHalfSwing](#) [24]
    - Offset 0x0575 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.*
  - UINT8 [PcieRpClkReqDetect](#) [24]
    - Offset 0x058D - Enable PCIE RP Clk Req Detect Probe CLKREQ# signal before enabling CLKREQ# based power management.*
  - UINT8 [PcieRpAdvancedErrorReporting](#) [24]
    - Offset 0x05A5 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.*
  - UINT8 [PcieRpUnsupportedRequestReport](#) [24]
    - Offset 0x05BD - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.*
  - UINT8 [PcieRpFatalErrorReport](#) [24]
    - Offset 0x05D5 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.*
  - UINT8 [PcieRpNoFatalErrorReport](#) [24]
    - Offset 0x05ED - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.*
  - UINT8 [PcieRpCorrectableErrorReport](#) [24]
    - Offset 0x0605 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.*
  - UINT8 [PcieRpSystemErrorOnFatalError](#) [24]
    - Offset 0x061D - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.*
  - UINT8 [PcieRpSystemErrorOnNonFatalError](#) [24]
    - Offset 0x0635 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.*
  - UINT8 [PcieRpSystemErrorOnCorrectableError](#) [24]
    - Offset 0x064D - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.*
  - UINT8 [PcieRpMaxPayload](#) [24]
    - Offset 0x0665 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH\_PCIE\_MAX\_↔PAYLOAD.*
  - UINT8 [UnusedUpdSpace18](#) [3]
    - Offset 0x067D.*
  - UINT32 [PcieRpDpcMask](#)

- Offset 0x0680 - DPC for PCIE RP Mask Enable/disable Downstream Port Containment for PCIE Root Ports.*

    - UUINT32 [PcieRpDpcExtensionsMask](#)
      - Offset 0x0684 - DPC Extensions PCIE RP Mask Enable/disable DPC Extensions for PCIE Root Ports.*
    - UUINT32 [PcieRpPtmMask](#)
      - Offset 0x0688 - PTM for PCIE RP Mask Enable/disable Precision Time Measurement for PCIE Root Ports.*
    - UUINT8 [PcieRpPcieSpeed](#) [24]
      - Offset 0x068C - PCIE RP Pcie Speed Determines each PCIE Port speed capability.*
    - UUINT8 [PcieRpGen3EqPh3Method](#) [24]
      - Offset 0x06A4 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH\_PCIE\_EQ\_METHOD).*
    - UUINT8 [PcieRpPhysicalSlotNumber](#) [24]
      - Offset 0x06BC - PCIE RP Physical Slot Number Indicates the slot number for the root port.*
    - UUINT8 [PcieRpSlotImplemented](#) [24]
      - Offset 0x06D4 - PCH PCIe root port connection type 0: built-in device, 1:slot.*
    - UUINT8 [PcieRpCompletionTimeout](#) [24]
      - Offset 0x06EC - PCIE RP Completion Timeout The root port completion timeout(see: PCH\_PCIE\_COMPLETION\_TIMEOUT).*
    - UUINT8 [PcieRpAspm](#) [24]
      - Offset 0x0704 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH\_PCIE\_ASPM\_CONTROL).*
    - UUINT8 [PcieRpL1Substates](#) [24]
      - Offset 0x071C - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH\_PCIE\_L1SUBSTATES\_CONTROL).*
    - UUINT8 [PcieRpLtrEnable](#) [24]
      - Offset 0x0734 - PCIE RP Ltr Enable Latency Tolerance Reporting Mechanism.*
    - UUINT8 [PcieRpLtrConfigLock](#) [24]
      - Offset 0x074C - PCIE RP Ltr Config Lock 0: Disable; 1: Enable.*
    - UUINT8 [PcieRpAcSEnabled](#) [24]
      - Offset 0x0764 - PCIE RP Access Control Services Extended Capability Enable/Disable PCIE RP Access Control Services Extended Capability.*
    - UUINT8 [PcieRpEnableCpm](#) [24]
      - Offset 0x077C - 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.*
    - UUINT16 [PcieRpDetectTimeoutMs](#) [24]
      - Offset 0x0794 - 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.*
    - UUINT16 [PcieRpLtrMaxSnoopLatency](#) [24]
      - Offset 0x07C4 - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.*
    - UUINT16 [PcieRpLtrMaxNoSnoopLatency](#) [24]
      - Offset 0x07F4 - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.*
    - UUINT8 [PcieRpSnoopLatencyOverrideMode](#) [24]
      - Offset 0x0824 - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.*
    - UUINT8 [PcieRpSnoopLatencyOverrideMultiplier](#) [24]
      - Offset 0x083C - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.*
    - UUINT16 [PcieRpSnoopLatencyOverrideValue](#) [24]
      - Offset 0x0854 - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.*
    - UUINT8 [PcieRpNonSnoopLatencyOverrideMode](#) [24]
      - Offset 0x0884 - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.*
    - UUINT8 [PcieRpNonSnoopLatencyOverrideMultiplier](#) [24]
-

- Offset 0x089C - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.*
- UINT16 [PcieRpNonSnoopLatencyOverrideValue](#) [24]
 

*Offset 0x08B4 - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.*
  - UINT8 [PcieRpSlotPowerLimitScale](#) [24]
 

*Offset 0x08E4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.*
  - UINT16 [PcieRpSlotPowerLimitValue](#) [24]
 

*Offset 0x08FC - PCIE RP Slot Power Limit Value Specifies upper limit on power supply by slot.*
  - UINT8 [PcieRpUptp](#) [24]
 

*Offset 0x092C - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.*
  - UINT8 [PcieRpDptp](#) [24]
 

*Offset 0x0944 - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.*
  - UINT8 [PcieClkSrcUsage](#) [16]
 

*Offset 0x095C - 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 0x096C - ClkReq-to-ClkSrc mapping Number of ClkReq signal assigned to ClkSrc.*
  - UINT8 [PcieEqPh3LaneParamCm](#) [24]
 

*Offset 0x097C - PCIE Eq Ph3 Lane Param Cm PCH\_PCIE\_EQ\_LANE\_PARAM.*
  - UINT8 [PcieEqPh3LaneParamCp](#) [24]
 

*Offset 0x0994 - PCIE Eq Ph3 Lane Param Cp PCH\_PCIE\_EQ\_LANE\_PARAM.*
  - UINT8 [PcieSwEqCoeffListCm](#) [5]
 

*Offset 0x09AC - PCIE Sw Eq CoeffList Cm PCH\_PCIE\_EQ\_PARAM.*
  - UINT8 [PcieSwEqCoeffListCp](#) [5]
 

*Offset 0x09B1 - PCIE Sw Eq CoeffList Cp PCH\_PCIE\_EQ\_PARAM.*
  - UINT8 [PcieEnablePort8xhDecode](#)

*Offset 0x09B6 - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.*
  - UINT8 [PchPciePort8xhDecodePortIndex](#)

*Offset 0x09B7 - PCIE Port8xh Decode Port Index The Index of PCIe Port that is selected for Port8xh Decode (0 Based).*
  - UINT8 [PcieEnablePeerMemoryWrite](#)

*Offset 0x09B8 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.*
  - UINT8 [PcieComplianceTestMode](#)

*Offset 0x09B9 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.*
  - UINT8 [PcieRpFunctionSwap](#)

*Offset 0x09BA - PCIE Rp Function Swap Allows BIOS to use root port function number swapping when root port of function 0 is disabled.*
  - UINT8 [NumOfDevIntConfig](#)

*Offset 0x09BB - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.*
  - UINT32 [DevIntConfigPtr](#)

*Offset 0x09BC - Address of PCH\_DEVICE\_INTERRUPT\_CONFIG table.*
  - UINT8 [PxRcConfig](#) [8]
 

*Offset 0x09C0 - PIRQx to IRQx Map Config PIRQx to IRQx mapping.*
  - UINT8 [GpioIrqRoute](#)

*Offset 0x09C8 - Select GPIO IRQ Route GPIO IRQ Select.*
  - UINT8 [ScilrqSelect](#)

*Offset 0x09C9 - Select ScilrqSelect SCI IRQ Select.*
  - UINT8 [TcolrqSelect](#)
-

- Offset 0x09CA - Select TcolrqSelect TCO IRQ Select.*

  - UINT8 [TcolrqEnable](#)
- Offset 0x09CB - Enable/Disable Tco IRQ Enable/disable TCO IRQ \$EN\_DIS.*

  - UINT8 [PchLockDownGlobalSmi](#)
- Offset 0x09CC - Enable LOCKDOWN SMI Enable SMI\_LOCK bit to prevent writes to the Global SMI Enable bit.*

  - UINT8 [PchLockDownBiosInterface](#)
- Offset 0x09CD - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.*

  - UINT8 [PchLockDownBiosLock](#)
- Offset 0x09CE - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:RegD←→Ch[5]) for the BIOS region protection.*

  - UINT8 [PchLockDownRtcMemoryLock](#)
- Offset 0x09CF - RTC CMOS MEMORY LOCK Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and lower 128-byte bank of RTC RAM.*

  - UINT8 [PchUnlockGpioPads](#)
- Offset 0x09D0 - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.*

  - UINT8 [PchPwrOptEnable](#)
- Offset 0x09D1 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.*

  - UINT8 [PchDmiAspmCtrl](#)
- Offset 0x09D2 - Pch Dmi Aspm Ctrl ASPM configuration on the PCH side of the DMI/OPI Link.*

  - UINT8 [PchWriteProtectionEnable](#) [5]
- Offset 0x09D3 - PCH Flash Protection Ranges Write Enble Write or erase is blocked by hardware.*

  - UINT8 [PchReadProtectionEnable](#) [5]
- Offset 0x09D8 - PCH Flash Protection Ranges Read Enble Read is blocked by hardware.*

  - UINT8 [UnusedUpdSpace19](#) [1]
- Offset 0x09DD.*

  - UINT16 [PchProtectedRangeLimit](#) [5]
- Offset 0x09DE - 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 0x09E8 - PCH Protect Range Base Left shifted address by 12 bits with address bits 11:0 are assumed to be 0.*

  - UINT8 [PchIoApicEntry24\\_119](#)
- Offset 0x09F2 - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.*

  - UINT8 [Enable8254ClockGating](#)
- Offset 0x09F3 - Enable 8254 Static Clock Gating Set 8254CGE=1 is required for SLP\_S0 support.*

  - UINT8 [Enable8254ClockGatingOnS3](#)
- Offset 0x09F4 - Enable 8254 Static Clock Gating On S3 This is only applicable when Enable8254ClockGating is disabled.*

  - UINT8 [PchIoApicId](#)
- Offset 0x09F5 - PCH Io Apic ID This member determines IOAPIC ID.*

  - UINT8 [PchSbAccessUnlock](#)
- Offset 0x09F6 - PCH Unlock SideBand access The SideBand PortID mask for certain end point (e.g.*

  - UINT8 [PchCrid](#)
- Offset 0x09F7 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.*

  - UINT8 [PchPmPmeB0S5Dis](#)
- Offset 0x09F8 - 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 [PchPmWolEnableOverride](#)
- Offset 0x09F9 - 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 0x09FA - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.*

    - UINT8 [PchPmWoWlanEnable](#)
      - Offset 0x09FB - PCH Pm WoW lan Enable Determine if WLAN wake from Sx, corresponds to the HOST\_WLAN\_PP\_EN bit in the PWRM\_CFG3 register.*
    - UINT8 [PchPmWoWlanDeepSxEnable](#)
      - Offset 0x09FC - 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 0x09FD - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.*
    - UINT8 [PchPmDeepSxPol](#)
      - Offset 0x09FE - PCH Pm Deep Sx Pol Deep Sx Policy.*
    - UINT8 [PchPmSlpS3MinAssert](#)
      - Offset 0x09FF - PCH Pm Slp S3 Min Assert SLP\_S3 Minimum Assertion Width Policy.*
    - UINT8 [PchPmSlpS4MinAssert](#)
      - Offset 0x0A00 - PCH Pm Slp S4 Min Assert SLP\_S4 Minimum Assertion Width Policy.*
    - UINT8 [PchPmSlpSusMinAssert](#)
      - Offset 0x0A01 - PCH Pm Slp Sus Min Assert SLP\_SUS Minimum Assertion Width Policy.*
    - UINT8 [PchPmSlpAMinAssert](#)
      - Offset 0x0A02 - PCH Pm Slp A Min Assert SLP\_A Minimum Assertion Width Policy.*
    - UINT8 [PchPmSlpStrchSusUp](#)
      - Offset 0x0A03 - PCH Pm Slp Strch Sus Up Enable SLP\_X Stretching After SUS Well Power Up.*
    - UINT8 [PchPmSlpLanLowDc](#)
      - Offset 0x0A04 - PCH Pm Slp Lan Low Dc Enable/Disable SLP\_LAN# Low on DC Power.*
    - UINT8 [PchPmPwrBtnOverridePeriod](#)
      - Offset 0x0A05 - PCH Pm Pwr Btn Override Period PCH power button override period.*
    - UINT8 [PchPmDisableEnergyReport](#)
      - Offset 0x0A06 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.*
    - UINT8 [PchPmDisableDsxAcPresentPullDown](#)
      - Offset 0x0A07 - 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 0x0A08 - PCH Pm Disable Native Power Button Power button native mode disable.*
    - UINT8 [UnusedUpdSpace20](#) [3]
      - Offset 0x0A09.*
    - UINT32 [PmcPowerButtonDebounce](#)
      - Offset 0x0A0C - Power button debounce configuration Debounce time for PWRBTN in microseconds.*
    - UINT8 [PchPmSlpS0Enable](#)
      - Offset 0x0A10 - PCH Pm Slp S0 Enable Indicates whether SLP\_S0# is to be asserted when PCH reaches idle state.*
    - UINT8 [PchPmMeWakeSts](#)
      - Offset 0x0A11 - PCH Pm ME\_WAKE\_STS Clear the ME\_WAKE\_STS bit in the Power and Reset Status (PRSTS) register.*
    - UINT8 [PchPmWolOvrWkSts](#)
      - Offset 0x0A12 - PCH Pm WOL\_OVR\_WK\_STS Clear the WOL\_OVR\_WK\_STS bit in the Power and Reset Status (PRSTS) register.*
    - UINT8 [EnableTcoTimer](#)
      - Offset 0x0A13 - Enable TCO timer.*
    - UINT8 [PchPmVrAlert](#)
      - Offset 0x0A14 - 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 [PchPmPwrCycDur](#)
      - Offset 0x0A15 - PCH Pm Reset Power Cycle Duration Could be customized in the unit of second.*
    - UINT8 [PchPmPciePIIScc](#)
-

- Offset 0x0A16 - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.*

    - UINT8 [PchPmS0i3Support](#)
  - Offset 0x0A17 - S0i3 support S0i3 platform support.*

    - UINT8 [SlpS0Override](#)
  - Offset 0x0A18 - SLP\_S0# Override Enabled will toggle SLP\_S0# assertion  
Disabled will enable SLP\_S0# assertion when debug is enabled.*

    - UINT8 [SlpS0DisQForDebug](#)
  - Offset 0x0A19 - S0ix Override Settings 'No Change' will keep PMC BWG settings.*

    - UINT8 [PmcDbgMsgEn](#)
  - Offset 0x0A1A - 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 [PsOnEnable](#)
  - Offset 0x0A1B - Enable PS\_ON.*

    - UINT8 [PmcCpuC10GatePinEnable](#)
  - Offset 0x0A1C - 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 [PmcModPhySusPgEnable](#)
  - Offset 0x0A1D - ModPHY SUS Power Domain Dynamic Gating Enable/Disable ModPHY SUS Power Domain Dy-  
namic Gating.*

    - UINT8 [PmcUsb2PhySusPgEnable](#)
  - Offset 0x0A1E - 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 [PmcOsIdleEnable](#)
  - Offset 0x0A1F - OS IDLE Mode Enable Enable/Disable OS Idle Mode (PCH-N only) \$EN\_DIS.*

    - UINT8 [PmcCrashLogEnable](#)
  - Offset 0x0A20 - Enable PMC CrashLog Enable or Disable PMC CrashLog; 0: Disable; 1: **Enable**.*

    - UINT8 [PchHotEnable](#)
  - Offset 0x0A21 - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.*

    - UINT16 [PchT0Level](#)
  - Offset 0x0A22 - Thermal Throttling Custimized T0Level Value Custimized T0Level value.*

    - UINT16 [PchT1Level](#)
  - Offset 0x0A24 - Thermal Throttling Custimized T1Level Value Custimized T1Level value.*

    - UINT16 [PchT2Level](#)
  - Offset 0x0A26 - Thermal Throttling Custimized T2Level Value Custimized T2Level value.*

    - UINT8 [PchTTEnable](#)
  - Offset 0x0A28 - Enable The Thermal Throttle Enable the thermal throttle function.*

    - UINT8 [PchTTState13Enable](#)
  - Offset 0x0A29 - 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 0x0A2A - Thermal Throttle Lock Thermal Throttle Lock.*

    - UINT8 [TTSuggestedSetting](#)
  - Offset 0x0A2B - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.*

    - UINT8 [TTCrossThrottling](#)
  - Offset 0x0A2C - Enable PCH Cross Throttling Enable/Disable PCH Cross Throttling \$EN\_DIS.*

    - UINT8 [PchDmiTsawEn](#)
  - Offset 0x0A2D - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.*

    - UINT8 [DmiSuggestedSetting](#)
  - Offset 0x0A2E - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.*

    - UINT8 [DmiTS0TW](#)
  - Offset 0x0A2F - Thermal Sensor 0 Target Width Thermal Sensor 0 Target Width.*

    - UINT8 [DmiTS1TW](#)
-

- Offset 0x0A30 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.*

    - UINT8 [DmiTS2TW](#)
  - Offset 0x0A31 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.*

    - UINT8 [DmiTS3TW](#)
  - Offset 0x0A32 - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.*

    - UINT8 [PchMemoryThrottlingEnable](#)
  - Offset 0x0A33 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.*

    - UINT8 [PchMemoryPmsyncEnable](#) [2]
  - Offset 0x0A34 - Memory Thermal Throttling Enable Memory Thermal Throttling.*

    - UINT8 [PchMemoryC0TransmitEnable](#) [2]
  - Offset 0x0A36 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.*

    - UINT8 [PchMemoryPinSelection](#) [2]
  - Offset 0x0A38 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.*

    - UINT16 [PchTemperatureHotLevel](#)
  - Offset 0x0A3A - Thermal Device Temperature Decides the temperature.*

    - UINT8 [PchFivrExtV1p05RailEnabledStates](#)
  - Offset 0x0A3C - 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 [UnusedUpdSpace21](#)
  - Offset 0x0A3D.*

    - UINT16 [PchFivrExtV1p05RailVoltage](#)
  - Offset 0x0A3E - 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 0x0A40 - External V1P05 Icc Max Value Granularity of this setting is 1mA and maximal possible value is 200mA.*

    - UINT8 [PchFivrExtVnnRailEnabledStates](#)
  - Offset 0x0A41 - 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 0x0A42 - 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 0x0A44 - 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 0x0A45 - 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 0x0A46 - 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 0x0A48 - 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 0x0A49 - Transition time in microseconds from Low Current Mode Voltage to High Current Mode Voltage This field has 1us resolution.*

    - UINT8 [PchFivrVccinAuxRetToHighCurModeVolTranTime](#)
  - Offset 0x0A4A - Transition time in microseconds from Retention Mode Voltage to High Current Mode Voltage This field has 1us resolution.*

    - UINT8 [PchFivrVccinAuxRetToLowCurModeVolTranTime](#)
  - Offset 0x0A4B - Transition time in microseconds from Retention Mode Voltage to Low Current Mode Voltage This field has 1us resolution.*
-

- UUINT16 [PchFivrVccinAuxOffToHighCurModeVolTranTime](#)  
*Offset 0x0A4C - Transition time in microseconds from Off (0V) to High Current Mode Voltage This field has 1us resolution.*
- UUINT8 [PchFivrDynPm](#)  
*Offset 0x0A4E - FIVR Dynamic Power Management Enable/Disable FIVR Dynamic Power Management.*
- UUINT8 [UnusedUpdSpace22](#)  
*Offset 0x0A4F.*
- UUINT32 [TraceHubMemBase](#)  
*Offset 0x0A50 - 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.*
- UUINT8 [PchPostMemRsvd](#) [64]  
*Offset 0x0A54.*
- UUINT8 [ReservedFpsUpd](#) [12]  
*Offset 0x0A94.*

### 12.9.1 Detailed Description

Fsp S Configuration.

Definition at line 86 of file FspUpd.h.

### 12.9.2 Member Data Documentation

#### 12.9.2.1 AcLoadline

UUINT16 FSP\_S\_CONFIG::AcLoadline

Offset 0x0054 - 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 218 of file FspUpd.h.

#### 12.9.2.2 AcousticNoiseMitigation

UUINT8 FSP\_S\_CONFIG::AcousticNoiseMitigation

Offset 0x0064 - Acoustic Noise Mitigation feature Enable or Disable Acoustic Noise Mitigation feature.

This has to be enabled to program slew rate configuration for all VR domains, Pre Wake, Ramp Up and, Ramp Down times. **0: Disabled; 1: Enabled** \$EN\_DIS

Definition at line 269 of file FspUpd.h.

#### 12.9.2.3 AmtEnabled

UUINT8 FSP\_S\_CONFIG::AmtEnabled

Offset 0x033E - AMT Switch Enable/Disable.

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

Definition at line 1797 of file FspUpd.h.

#### 12.9.2.4 AmtKvmEnabled

UINT8 FSP\_S\_CONFIG::AmtKvmEnabled

Offset 0x0349 - KVM Switch Enable/Disable.

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

Definition at line 1852 of file FspUpd.h.

#### 12.9.2.5 AmtSolEnabled

UINT8 FSP\_S\_CONFIG::AmtSolEnabled

Offset 0x0347 - SOL Switch Enable/Disable.

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

Definition at line 1840 of file FspUpd.h.

#### 12.9.2.6 ApIdleManner

UINT8 FSP\_S\_CONFIG::ApIdleManner

Offset 0x008F - 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 418 of file FspUpd.h.

#### 12.9.2.7 AsfEnabled

UINT8 FSP\_S\_CONFIG::AsfEnabled

Offset 0x0340 - ASF Switch Enable/Disable.

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

Definition at line 1809 of file FspUpd.h.

#### 12.9.2.8 AutoThermalReporting

UINT8 FSP\_S\_CONFIG::AutoThermalReporting

Offset 0x0124 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; 1: **Enable**.

\$EN\_DIS

Definition at line 842 of file FspUpd.h.

---

### 12.9.2.9 C1e

UINT8 FSP\_S\_CONFIG::C1e

Offset 0x0128 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

0: Disable; 1: **Enable** \$EN\_DIS

Definition at line 866 of file FspsUpd.h.

### 12.9.2.10 C1StateAutoDemotion

UINT8 FSP\_S\_CONFIG::C1StateAutoDemotion

Offset 0x0129 - Enable or Disable C1 Cstate Demotion Enable or Disable C1 Cstate Demotion.

Disable; 1: **Enable** \$EN\_DIS

Definition at line 872 of file FspsUpd.h.

### 12.9.2.11 C1StateUnDemotion

UINT8 FSP\_S\_CONFIG::C1StateUnDemotion

Offset 0x012A - Enable or Disable C1 Cstate UnDemotion Enable or Disable C1 Cstate UnDemotion.

Disable; 1: **Enable** \$EN\_DIS

Definition at line 878 of file FspsUpd.h.

### 12.9.2.12 CnviBtAudioOffload

UINT8 FSP\_S\_CONFIG::CnviBtAudioOffload

Offset 0x03EB - CNVi BT Audio Offload Enable/Disable BT Audio Offload, Default is DISABLE.

0: DISABLE, 1: ENABLE \$EN\_DIS

Definition at line 2185 of file FspsUpd.h.

### 12.9.2.13 CnviBtCore

UINT8 FSP\_S\_CONFIG::CnviBtCore

Offset 0x03EA - CNVi BT Core Enable/Disable CNVi BT Core, Default is ENABLE.

0: DISABLE, 1: ENABLE \$EN\_DIS

Definition at line 2179 of file FspsUpd.h.

### 12.9.2.14 CnviClkreqPinMux

UINT32 FSP\_S\_CONFIG::CnviClkreqPinMux

Offset 0x03F4 - CNVi CLKREQ pin muxing Select CNVi CLKREQ pin depending on board routing.

---

ICP-LP: GPP\_A9 = 0x2640E609(default) or GPP\_F5 = 0x2645E605. ICP-H: 0. ICP-N: GPP\_H13 = 0x2746E60D(default) or GPP\_H2 = 0x3746E602. Refer to GPIO\_\*\_MUXING\_CNVI\_MODEM\_CLKREQ\_\* in GpioPins\*.h.  
 Definition at line 2209 of file FspUpd.h.

#### 12.9.2.15 CnviMode

UINT8 FSP\_S\_CONFIG::CnviMode

Offset 0x03E9 - 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 2173 of file FspUpd.h.

#### 12.9.2.16 CnviRfResetPinMux

UINT32 FSP\_S\_CONFIG::CnviRfResetPinMux

Offset 0x03F0 - CNVi RF\_RESET pin muxing Select CNVi RF\_RESET# pin depending on board routing.

ICP-LP: GPP\_A8 = 0x2640E408(default) or GPP\_F4 = 0x1645E404. ICP-H: 0. ICP-N: GPP\_H12 = 0x2746E40C(default) or GPP\_H1 = 0x3746E401. Refer to GPIO\_\*\_MUXING\_CNVI\_RF\_RESET\_\* in GpioPins\*.h.

Definition at line 2202 of file FspUpd.h.

#### 12.9.2.17 ConfigTdpBios

UINT8 FSP\_S\_CONFIG::ConfigTdpBios

Offset 0x00CA - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 693 of file FspUpd.h.

#### 12.9.2.18 CpuMpHob

UINT32 FSP\_S\_CONFIG::CpuMpHob

Offset 0x015C - CpuMpHob Pointer for CpuMpHob.

This is optional data buffer for CpuMpPpi usage.

Definition at line 1019 of file FspUpd.h.

#### 12.9.2.19 CStatePreWake

UINT8 FSP\_S\_CONFIG::CStatePreWake

Offset 0x012D - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

0: Disable; **1: Enable** \$EN\_DIS

Definition at line 896 of file FspsUpd.h.

#### 12.9.2.20 CstCfgCtrlIoMwaitRedirection

UINT8 FSP\_S\_CONFIG::CstCfgCtrlIoMwaitRedirection

Offset 0x012F - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; **1: Enable**.

\$EN\_DIS

Definition at line 908 of file FspsUpd.h.

#### 12.9.2.21 Custom1PowerLimit1

UINT32 FSP\_S\_CONFIG::Custom1PowerLimit1

Offset 0x00F4 - 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 711 of file FspsUpd.h.

#### 12.9.2.22 Custom1PowerLimit1Time

UINT8 FSP\_S\_CONFIG::Custom1PowerLimit1Time

Offset 0x00C3 - 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 656 of file FspsUpd.h.

#### 12.9.2.23 Custom1PowerLimit2

UINT32 FSP\_S\_CONFIG::Custom1PowerLimit2

Offset 0x00F8 - 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 717 of file FspsUpd.h.

#### 12.9.2.24 Custom1TurboActivationRatio

UINT8 FSP\_S\_CONFIG::Custom1TurboActivationRatio

Offset 0x00C6 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

Valid Range 0 to 255

Definition at line 671 of file FspsUpd.h.

---

### 12.9.2.25 Custom2PowerLimit1

UINT32 FSP\_S\_CONFIG::Custom2PowerLimit1

Offset 0x00FC - 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 723 of file FspsUpd.h.

### 12.9.2.26 Custom2PowerLimit1Time

UINT8 FSP\_S\_CONFIG::Custom2PowerLimit1Time

Offset 0x00C4 - 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 661 of file FspsUpd.h.

### 12.9.2.27 Custom2PowerLimit2

UINT32 FSP\_S\_CONFIG::Custom2PowerLimit2

Offset 0x0100 - 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 729 of file FspsUpd.h.

### 12.9.2.28 Custom2TurboActivationRatio

UINT8 FSP\_S\_CONFIG::Custom2TurboActivationRatio

Offset 0x00C7 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

Valid Range 0 to 255

Definition at line 676 of file FspsUpd.h.

### 12.9.2.29 Custom3PowerLimit1

UINT32 FSP\_S\_CONFIG::Custom3PowerLimit1

Offset 0x0104 - 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 735 of file FspsUpd.h.

---

### 12.9.2.30 Custom3PowerLimit1Time

UINT8 FSP\_S\_CONFIG::Custom3PowerLimit1Time

Offset 0x00C5 - 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 666 of file FspsUpd.h.

### 12.9.2.31 Custom3PowerLimit2

UINT32 FSP\_S\_CONFIG::Custom3PowerLimit2

Offset 0x0108 - 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 741 of file FspsUpd.h.

### 12.9.2.32 Custom3TurboActivationRatio

UINT8 FSP\_S\_CONFIG::Custom3TurboActivationRatio

Offset 0x00C8 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

Valid Range 0 to 255

Definition at line 681 of file FspsUpd.h.

### 12.9.2.33 Cx

UINT8 FSP\_S\_CONFIG::Cx

Offset 0x0126 - 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 854 of file FspsUpd.h.

### 12.9.2.34 DcLoadline

UINT16 FSP\_S\_CONFIG::DcLoadline

Offset 0x0056 - 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 224 of file FspsUpd.h.

### 12.9.2.35 DevIntConfigPtr

UINT32 FSP\_S\_CONFIG::DevIntConfigPtr

---

Offset 0x09BC - Address of PCH\_DEVICE\_INTERRUPT\_CONFIG table.

The address of the table of PCH\_DEVICE\_INTERRUPT\_CONFIG.

Definition at line 3053 of file FspUpd.h.

#### 12.9.2.36 DisableProcHotOut

UINT8 FSP\_S\_CONFIG::DisableProcHotOut

Offset 0x0121 - 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 824 of file FspUpd.h.

#### 12.9.2.37 DisableVrThermalAlert

UINT8 FSP\_S\_CONFIG::DisableVrThermalAlert

Offset 0x0123 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; 0: **Disable**; 1: Enable.

\$EN\_DIS

Definition at line 836 of file FspUpd.h.

#### 12.9.2.38 DmiSuggestedSetting

UINT8 FSP\_S\_CONFIG::DmiSuggestedSetting

Offset 0x0A2E - DMI Thermal Sensor Suggested Setting DMT thermal sensor suggested representative values.

\$EN\_DIS

Definition at line 3477 of file FspUpd.h.

#### 12.9.2.39 DmiTS0TW

UINT8 FSP\_S\_CONFIG::DmiTS0TW

Offset 0x0A2F - Thermal Sensor 0 Target Width Thermal Sensor 0 Target Width.

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

Definition at line 3483 of file FspUpd.h.

#### 12.9.2.40 DmiTS1TW

UINT8 FSP\_S\_CONFIG::DmiTS1TW

Offset 0x0A30 - Thermal Sensor 1 Target Width Thermal Sensor 1 Target Width.

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

Definition at line 3489 of file FspUpd.h.

---

#### 12.9.2.41 DmiTS2TW

UINT8 FSP\_S\_CONFIG::DmiTS2TW

Offset 0x0A31 - Thermal Sensor 2 Target Width Thermal Sensor 2 Target Width.

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

Definition at line 3495 of file FspUpd.h.

#### 12.9.2.42 DmiTS3TW

UINT8 FSP\_S\_CONFIG::DmiTS3TW

Offset 0x0A32 - Thermal Sensor 3 Target Width Thermal Sensor 3 Target Width.

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

Definition at line 3501 of file FspUpd.h.

#### 12.9.2.43 EcCmdLock

UINT8 FSP\_S\_CONFIG::EcCmdLock

Offset 0x01A9 - EcCmdLock EcCmdLock default values.

Locks Ephemeral Authorization Value sent previously

Definition at line 1059 of file FspUpd.h.

#### 12.9.2.44 EcCmdProvisionEav

UINT8 FSP\_S\_CONFIG::EcCmdProvisionEav

Offset 0x01A8 - EcCmdProvisionEav Ephemeral Authorization Value default values.

Provisions an ephemeral shared secret to the EC

Definition at line 1054 of file FspUpd.h.

#### 12.9.2.45 Eist

UINT8 FSP\_S\_CONFIG::Eist

Offset 0x011C - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

0: Disable; 1: **Enable** \$EN\_DIS

Definition at line 792 of file FspUpd.h.

---

#### 12.9.2.46 Enable8254ClockGating

UINT8 FSP\_S\_CONFIG::Enable8254ClockGating

Offset 0x09F3 - 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 3164 of file FspUpd.h.

#### 12.9.2.47 Enable8254ClockGatingOnS3

UINT8 FSP\_S\_CONFIG::Enable8254ClockGatingOnS3

Offset 0x09F4 - Enable 8254 Static Clock Gating On S3 This is only applicable when Enable8254ClockGating is disabled.

FSP will do the 8254 CGE programming on S3 resume when Enable8254ClockGatingOnS3 is enabled. This avoids the SMI requirement for the programming. \$EN\_DIS

Definition at line 3172 of file FspUpd.h.

#### 12.9.2.48 EnableEpbPeciOverride

UINT8 FSP\_S\_CONFIG::EnableEpbPeciOverride

Offset 0x00BE - Enable or Disable EPB override over PECl Enable or Disable EPB override over PECl.

**0: Disable; 1: Enable** \$EN\_DIS

Definition at line 627 of file FspUpd.h.

#### 12.9.2.49 EnableFastMsrHwpReq

UINT8 FSP\_S\_CONFIG::EnableFastMsrHwpReq

Offset 0x00BF - 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 633 of file FspUpd.h.

#### 12.9.2.50 EnableHwpAutoEppGrouping

UINT8 FSP\_S\_CONFIG::EnableHwpAutoEppGrouping

Offset 0x00BD - Enable or Disable HwP Autonomous EPP Grouping Enable or Disable HwP Autonomous EPP Grouping.

**0: Disable; 1: Enable** \$EN\_DIS

Definition at line 621 of file FspUpd.h.

---

#### 12.9.2.51 EnableHwpAutoPerCorePstate

UINT8 FSP\_S\_CONFIG::EnableHwpAutoPerCorePstate

Offset 0x00BC - 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 615 of file FspsUpd.h.

#### 12.9.2.52 EnableItbm

UINT8 FSP\_S\_CONFIG::EnableItbm

Offset 0x00B9 - Intel Turbo Boost Max Technology 3.0 Intel Turbo Boost Max Technology 3.0.

0: Disabled; **1: Enabled** \$EN\_DIS

Definition at line 596 of file FspsUpd.h.

#### 12.9.2.53 EnableMinVoltageOverride

UINT8 FSP\_S\_CONFIG::EnableMinVoltageOverride

Offset 0x006F - Enable or Disable Minimum Voltage Override Enable or disable Minimum Voltage overrides ; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 335 of file FspsUpd.h.

#### 12.9.2.54 EnablePerCorePState

UINT8 FSP\_S\_CONFIG::EnablePerCorePState

Offset 0x00BB - 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 608 of file FspsUpd.h.

#### 12.9.2.55 EnableTcoTimer

UINT8 FSP\_S\_CONFIG::EnableTcoTimer

Offset 0x0A13 - 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 3324 of file FspsUpd.h.

---

### 12.9.2.56 EndOfPostMessage

UINT8 FSP\_S\_CONFIG::EndOfPostMessage

Offset 0x0331 - 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 1774 of file FspUpd.h.

### 12.9.2.57 EnergyEfficientPState

UINT8 FSP\_S\_CONFIG::EnergyEfficientPState

Offset 0x011D - 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 799 of file FspUpd.h.

### 12.9.2.58 EnergyEfficientTurbo

UINT8 FSP\_S\_CONFIG::EnergyEfficientTurbo

Offset 0x011E - 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 806 of file FspUpd.h.

### 12.9.2.59 EsataSpeedLimit

UINT8 FSP\_S\_CONFIG::EsataSpeedLimit

Offset 0x041A - 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 2409 of file FspUpd.h.

### 12.9.2.60 FastPkgCRampDisableFivr

UINT8 FSP\_S\_CONFIG::FastPkgCRampDisableFivr

Offset 0x0068 - 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 297 of file FspUpd.h.

---

### 12.9.2.61 FivrRfiFrequency

UINT16 FSP\_S\_CONFIG::FivrRfiFrequency

Offset 0x006C - 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 323 of file FspsUpd.h.

### 12.9.2.62 FivrSpreadSpectrum

UINT8 FSP\_S\_CONFIG::FivrSpreadSpectrum

Offset 0x006E - 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 329 of file FspsUpd.h.

### 12.9.2.63 ForcMebxSyncUp

UINT8 FSP\_S\_CONFIG::ForcMebxSyncUp

Offset 0x034A - MEBX execution Enable/Disable.

0: Disable, 1: enable, Force MEBX execution \$EN\_DIS

Definition at line 1858 of file FspsUpd.h.

### 12.9.2.64 FwProgress

UINT8 FSP\_S\_CONFIG::FwProgress

Offset 0x0341 - PET Progress Enable/Disable.

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

Definition at line 1816 of file FspsUpd.h.

### 12.9.2.65 GpioIrqRoute

UINT8 FSP\_S\_CONFIG::GpioIrqRoute

Offset 0x09C8 - Select GPIO IRQ Route GPIO IRQ Select.

The valid value is 14 or 15.

Definition at line 3065 of file FspsUpd.h.

---

### 12.9.2.66 HdcControl

UINT8 FSP\_S\_CONFIG::HdcControl

Offset 0x0099 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

0: Disabled; **1: Enabled** 2-3:Reserved \$EN\_DIS

Definition at line 491 of file FspsUpd.h.

### 12.9.2.67 Heci3Enabled

UINT8 FSP\_S\_CONFIG::Heci3Enabled

Offset 0x032F - 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 1759 of file FspsUpd.h.

### 12.9.2.68 Hwp

UINT8 FSP\_S\_CONFIG::Hwp

Offset 0x0098 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

0: Disable; **1: Enable**; 2-3:Reserved \$EN\_DIS

Definition at line 485 of file FspsUpd.h.

### 12.9.2.69 HwpInterruptControl

UINT8 FSP\_S\_CONFIG::HwpInterruptControl

Offset 0x00B8 - 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 590 of file FspsUpd.h.

### 12.9.2.70 IccMax

UINT16 FSP\_S\_CONFIG::IccMax

Offset 0x005E - Icc Max limit PCODE MMIO Mailbox: VR Icc Max limit.

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

Definition at line 244 of file FspsUpd.h.

### 12.9.2.71 ImonOffset

UINT8 FSP\_S\_CONFIG::ImonOffset

---

Offset 0x004C - 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 178 of file FspUpd.h.

#### 12.9.2.72 ImonSlope

```
UINT8 FSP_S_CONFIG::ImonSlope
```

Offset 0x004B - 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 172 of file FspUpd.h.

#### 12.9.2.73 IomTypeCPortPadCfg

```
UINT32 FSP_S_CONFIG::IomTypeCPortPadCfg[8]
```

Offset 0x0234 - 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: Icl = IceLake)

Definition at line 1451 of file FspUpd.h.

#### 12.9.2.74 ITbtConnectTopologyTimeoutInMs

```
UINT16 FSP_S_CONFIG::ITbtConnectTopologyTimeoutInMs
```

Offset 0x0272 - ITbtConnectTopology Timeout value ITbtConnectTopologyTimeout value.

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

Definition at line 1505 of file FspUpd.h.

#### 12.9.2.75 ITbtForcePowerOnTimeoutInMs

```
UINT16 FSP_S_CONFIG::ITbtForcePowerOnTimeoutInMs
```

Offset 0x0270 - ITBTForcePowerOn Timeout value ITBTForcePowerOn value.

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

Definition at line 1499 of file FspUpd.h.

#### 12.9.2.76 MachineCheckEnable

```
UINT8 FSP_S_CONFIG::MachineCheckEnable
```

Offset 0x008E - 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 412 of file FspsUpd.h.

#### 12.9.2.77 ManageabilityMode

UINT8 FSP\_S\_CONFIG::ManageabilityMode

Offset 0x0346 - Manageability Mode set by Mebx Enable/Disable.

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

Definition at line 1834 of file FspsUpd.h.

#### 12.9.2.78 MaxRingRatioLimit

UINT8 FSP\_S\_CONFIG::MaxRingRatioLimit

Offset 0x00C1 - Maximum Ring ratio limit override Maximum Ring ratio limit override.

**0: Hardware defaults.** Range: 0 - Max turbo ratio limit

Definition at line 645 of file FspsUpd.h.

#### 12.9.2.79 MctpBroadcastCycle

UINT8 FSP\_S\_CONFIG::MctpBroadcastCycle

Offset 0x0333 - Mctp Broadcast Cycle Test, Determine if MCTP Broadcast is enabled **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 1787 of file FspsUpd.h.

#### 12.9.2.80 MeUnconfigOnRtcClear

UINT8 FSP\_S\_CONFIG::MeUnconfigOnRtcClear

Offset 0x0330 - 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 1767 of file FspsUpd.h.

#### 12.9.2.81 MinRingRatioLimit

UINT8 FSP\_S\_CONFIG::MinRingRatioLimit

Offset 0x00C0 - Minimum Ring ratio limit override Minimum Ring ratio limit override.

**0: Hardware defaults.** Range: 0 - Max turbo ratio limit

Definition at line 639 of file FspsUpd.h.

---

### 12.9.2.82 MinVoltageC8

UINT16 FSP\_S\_CONFIG::MinVoltageC8

Offset 0x0070 - Min Voltage for C8 PCODE MMIO Mailbox: Minimum voltage for C8.

Valid if EnableMinVoltageOverride =

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

Definition at line 341 of file FspsUpd.h.

### 12.9.2.83 MinVoltageRuntime

UINT16 FSP\_S\_CONFIG::MinVoltageRuntime

Offset 0x0072 - Min Voltage for Runtime PCODE MMIO Mailbox: Minimum voltage for runtime.

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

Definition at line 347 of file FspsUpd.h.

### 12.9.2.84 MlcStreamerPrefetcher

UINT8 FSP\_S\_CONFIG::MlcStreamerPrefetcher

Offset 0x0074 - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0↔ : Disable; **1: Enable.**

\$EN\_DIS

Definition at line 353 of file FspsUpd.h.

### 12.9.2.85 MonitorMwaitEnable

UINT8 FSP\_S\_CONFIG::MonitorMwaitEnable

Offset 0x0076 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; **1: Enable.**

\$EN\_DIS

Definition at line 365 of file FspsUpd.h.

### 12.9.2.86 NumberOfEntries

UINT8 FSP\_S\_CONFIG::NumberOfEntries

Offset 0x00C2 - 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 651 of file FspsUpd.h.

---

### 12.9.2.87 NumOfDevIntConfig

UINT8 FSP\_S\_CONFIG::NumOfDevIntConfig

Offset 0x09BB - Number of DevIntConfig Entry Number of Device Interrupt Configuration Entry.

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

Definition at line 3048 of file FspUpd.h.

### 12.9.2.88 OneCoreRatioLimit

UINT8 FSP\_S\_CONFIG::OneCoreRatioLimit

Offset 0x0090 - 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 425 of file FspUpd.h.

### 12.9.2.89 PchCrid

UINT8 FSP\_S\_CONFIG::PchCrid

Offset 0x09F7 - PCH Compatibility Revision ID This member describes whether or not the CRID feature of PCH should be enabled.

\$EN\_DIS

Definition at line 3190 of file FspUpd.h.

### 12.9.2.90 PchDmiAspmCtrl

UINT8 FSP\_S\_CONFIG::PchDmiAspmCtrl

Offset 0x09D2 - 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 3125 of file FspUpd.h.

### 12.9.2.91 PchDmiTsawEn

UINT8 FSP\_S\_CONFIG::PchDmiTsawEn

Offset 0x0A2D - DMI Thermal Sensor Autonomous Width Enable DMI Thermal Sensor Autonomous Width Enable.

\$EN\_DIS

Definition at line 3471 of file FspUpd.h.

---

### 12.9.2.92 PchEnableComplianceMode

UINT8 FSP\_S\_CONFIG::PchEnableComplianceMode

Offset 0x04A4 - 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 2669 of file FspUpd.h.

### 12.9.2.93 PchEnableDbcObs

UINT8 FSP\_S\_CONFIG::PchEnableDbcObs

Offset 0x04A6 - 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 2683 of file FspUpd.h.

### 12.9.2.94 PchEspHostC10ReportEnable

UINT8 FSP\_S\_CONFIG::PchEspHostC10ReportEnable

Offset 0x03FA - Enable Host C10 reporting through eSPI Enable/disable Host C10 reporting to Slave via eSPI Virtual Wire.

\$EN\_DIS

Definition at line 2227 of file FspUpd.h.

### 12.9.2.95 PchFivrDynPm

UINT8 FSP\_S\_CONFIG::PchFivrDynPm

Offset 0x0A4E - FIVR Dynamic Power Management Enable/Disable FIVR Dynamic Power Management.

\$EN\_DIS

Definition at line 3608 of file FspUpd.h.

### 12.9.2.96 PchFivrExtVnnRailSxEnabledStates

UINT8 FSP\_S\_CONFIG::PchFivrExtVnnRailSxEnabledStates

Offset 0x0A45 - 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 3567 of file FspUpd.h.

---

### 12.9.2.97 PchFivrExtVnnRailSxIccMax

UINT8 FSP\_S\_CONFIG::PchFivrExtVnnRailSxIccMax

Offset 0x0A48 - 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 3579 of file FspUpd.h.

### 12.9.2.98 PchFivrExtVnnRailSxVoltage

UINT16 FSP\_S\_CONFIG::PchFivrExtVnnRailSxVoltage

Offset 0x0A46 - 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 3573 of file FspUpd.h.

### 12.9.2.99 PchFivrVccinAuxLowToHighCurModeVolTranTime

UINT8 FSP\_S\_CONFIG::PchFivrVccinAuxLowToHighCurModeVolTranTime

Offset 0x0A49 - 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 3585 of file FspUpd.h.

### 12.9.2.100 PchFivrVccinAuxOffToHighCurModeVolTranTime

UINT16 FSP\_S\_CONFIG::PchFivrVccinAuxOffToHighCurModeVolTranTime

Offset 0x0A4C - 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 3602 of file FspUpd.h.

### 12.9.2.101 PchFivrVccinAuxRetToHighCurModeVolTranTime

UINT8 FSP\_S\_CONFIG::PchFivrVccinAuxRetToHighCurModeVolTranTime

Offset 0x0A4A - 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 3591 of file FspUpd.h.

---

**12.9.2.102 PchFivrVccinAuxRetToLowCurModeVolTranTime**

UINT8 FSP\_S\_CONFIG::PchFivrVccinAuxRetToLowCurModeVolTranTime

Offset 0x0A4B - 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 3597 of file FspUpd.h.

**12.9.2.103 PchHdaAudioLinkDmic0**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkDmic0

Offset 0x03DD - Enable HD Audio DMIC0 Link Enable/disable HD Audio DMIC0 link.

Muxed with SNDW4. \$EN\_DIS

Definition at line 2100 of file FspUpd.h.

**12.9.2.104 PchHdaAudioLinkDmic1**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkDmic1

Offset 0x03DE - Enable HD Audio DMIC1 Link Enable/disable HD Audio DMIC1 link.

Muxed with SNDW3. \$EN\_DIS

Definition at line 2106 of file FspUpd.h.

**12.9.2.105 PchHdaAudioLinkHda**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkHda

Offset 0x03DC - Enable HD Audio Link Enable/disable HD Audio Link.

Muxed with SSP0/SSP1/SNDW1. \$EN\_DIS

Definition at line 2094 of file FspUpd.h.

**12.9.2.106 PchHdaAudioLinkSndw1**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSndw1

Offset 0x03E5 - Enable HD Audio SoundWire#1 Link Enable/disable HD Audio SNDW1 link.

Muxed with HDA. \$EN\_DIS

Definition at line 2148 of file FspUpd.h.

**12.9.2.107 PchHdaAudioLinkSndw2**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSndw2

---

Offset 0x03E6 - Enable HD Audio SoundWire#2 Link Enable/disable HD Audio SNDW2 link.  
Muxed with SSP1. \$EN\_DIS  
Definition at line 2154 of file FspUpd.h.

#### 12.9.2.108 PchHdaAudioLinkSndw3

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSndw3

Offset 0x03E7 - Enable HD Audio SoundWire#3 Link Enable/disable HD Audio SNDW3 link.  
Muxed with DMIC1. \$EN\_DIS  
Definition at line 2160 of file FspUpd.h.

#### 12.9.2.109 PchHdaAudioLinkSndw4

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSndw4

Offset 0x03E8 - Enable HD Audio SoundWire#4 Link Enable/disable HD Audio SNDW4 link.  
Muxed with DMIC0. \$EN\_DIS  
Definition at line 2166 of file FspUpd.h.

#### 12.9.2.110 PchHdaAudioLinkSsp0

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp0

Offset 0x03DF - Enable HD Audio SSP0 Link Enable/disable HD Audio SSP0/I2S link.  
Muxed with HDA. \$EN\_DIS  
Definition at line 2112 of file FspUpd.h.

#### 12.9.2.111 PchHdaAudioLinkSsp1

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp1

Offset 0x03E0 - Enable HD Audio SSP1 Link Enable/disable HD Audio SSP1/I2S link.  
Muxed with HDA/SNDW2. \$EN\_DIS  
Definition at line 2118 of file FspUpd.h.

#### 12.9.2.112 PchHdaAudioLinkSsp2

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp2

Offset 0x03E1 - Enable HD Audio SSP2 Link Enable/disable HD Audio SSP2/I2S link.  
\$EN\_DIS  
Definition at line 2124 of file FspUpd.h.

---

**12.9.2.113 PchHdaAudioLinkSsp3**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp3

Offset 0x03E2 - Enable HD Audio SSP3 Link Enable/disable HD Audio SSP3/I2S link.

\$EN\_DIS

Definition at line 2130 of file FspUpd.h.

**12.9.2.114 PchHdaAudioLinkSsp4**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp4

Offset 0x03E3 - Enable HD Audio SSP4 Link Enable/disable HD Audio SSP4/I2S link.

\$EN\_DIS

Definition at line 2136 of file FspUpd.h.

**12.9.2.115 PchHdaAudioLinkSsp5**

UINT8 FSP\_S\_CONFIG::PchHdaAudioLinkSsp5

Offset 0x03E4 - Enable HD Audio SSP5 Link Enable/disable HD Audio SSP5/I2S link.

\$EN\_DIS

Definition at line 2142 of file FspUpd.h.

**12.9.2.116 PchHdaDspEnable**

UINT8 FSP\_S\_CONFIG::PchHdaDspEnable

Offset 0x03CB - Enable HD Audio DSP Enable/disable HD Audio DSP feature.

\$EN\_DIS

Definition at line 2021 of file FspUpd.h.

**12.9.2.117 PchHdaDspUaaCompliance**

UINT8 FSP\_S\_CONFIG::PchHdaDspUaaCompliance

Offset 0x03D1 - 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 2058 of file FspUpd.h.

**12.9.2.118 PchHdaIDispCodecDisconnect**

UINT8 FSP\_S\_CONFIG::PchHdaIDispCodecDisconnect

---

Offset 0x03D2 - iDisplay Audio Codec disconnection 0: Not disconnected, enumerable, 1: Disconnected SDI, not enumerable.

\$EN\_DIS

Definition at line 2064 of file FspUpd.h.

#### 12.9.2.119 PchHdaDispLinkFrequency

UINT8 FSP\_S\_CONFIG::PchHdaIDispLinkFrequency

Offset 0x03CF - iDisp-Link Frequency iDisp-Link Freq (PCH\_HDAUDIO\_LINK\_FREQUENCY enum): 4: 96MHz, 3: 48MHz.

4: 96MHz, 3: 48MHz

Definition at line 2045 of file FspUpd.h.

#### 12.9.2.120 PchHdaLinkFrequency

UINT8 FSP\_S\_CONFIG::PchHdaLinkFrequency

Offset 0x03CE - 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 2039 of file FspUpd.h.

#### 12.9.2.121 PchHdaPme

UINT8 FSP\_S\_CONFIG::PchHdaPme

Offset 0x03CC - Enable Pme Enable Azalia wake-on-ring.

\$EN\_DIS

Definition at line 2027 of file FspUpd.h.

#### 12.9.2.122 PchHdaResetWaitTimer

UINT16 FSP\_S\_CONFIG::PchHdaResetWaitTimer

Offset 0x03D4 - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds. Default is 600.

Definition at line 2074 of file FspUpd.h.

#### 12.9.2.123 PchHdaVcType

UINT8 FSP\_S\_CONFIG::PchHdaVcType

Offset 0x03CD - VC Type Virtual Channel Type Select: 0: VC0, 1: VC1.

---

0: VC0, 1: VC1

Definition at line 2033 of file FspUpd.h.

#### 12.9.2.124 PchHotEnable

UINT8 FSP\_S\_CONFIG::PchHotEnable

Offset 0x0A21 - PCHHOT# pin Enable PCHHOT# pin assertion when temperature is higher than PchHotLevel.

0: disable, 1: enable \$EN\_DIS

Definition at line 3419 of file FspUpd.h.

#### 12.9.2.125 PchIoApicEntry24\_119

UINT8 FSP\_S\_CONFIG::PchIoApicEntry24\_119

Offset 0x09F2 - Enable PCH Io Apic Entry 24-119 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 3156 of file FspUpd.h.

#### 12.9.2.126 PchIoApicId

UINT8 FSP\_S\_CONFIG::PchIoApicId

Offset 0x09F5 - PCH Io Apic ID This member determines IOAPIC ID.

Default is 0x02.

Definition at line 3177 of file FspUpd.h.

#### 12.9.2.127 PchIshGp0GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshGp0GpioAssign

Offset 0x040D - Enable PCH ISH GP\_0 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2331 of file FspUpd.h.

#### 12.9.2.128 PchIshGp1GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshGp1GpioAssign

Offset 0x040E - Enable PCH ISH GP\_1 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2337 of file FspUpd.h.

---

**12.9.2.129 PchIshGp2GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp2GpioAssign

Offset 0x040F - Enable PCH ISH GP\_2 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2343 of file FspUpd.h.

**12.9.2.130 PchIshGp3GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp3GpioAssign

Offset 0x0410 - Enable PCH ISH GP\_3 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2349 of file FspUpd.h.

**12.9.2.131 PchIshGp4GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp4GpioAssign

Offset 0x0411 - Enable PCH ISH GP\_4 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2355 of file FspUpd.h.

**12.9.2.132 PchIshGp5GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp5GpioAssign

Offset 0x0412 - Enable PCH ISH GP\_5 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2361 of file FspUpd.h.

**12.9.2.133 PchIshGp6GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp6GpioAssign

Offset 0x0413 - Enable PCH ISH GP\_6 GPIO pin assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2367 of file FspUpd.h.

**12.9.2.134 PchIshGp7GpioAssign**

UINT8 FSP\_S\_CONFIG::PchIshGp7GpioAssign

Offset 0x0414 - Enable PCH ISH GP\_7 GPIO pin assigned 0: Disable; 1: Enable.

---

\$EN\_DIS

Definition at line 2373 of file FspUpd.h.

#### 12.9.2.135 PchIshI2c0GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshI2c0GpioAssign

Offset 0x040A - Enable PCH ISH I2C0 GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2313 of file FspUpd.h.

#### 12.9.2.136 PchIshI2c1GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshI2c1GpioAssign

Offset 0x040B - Enable PCH ISH I2C1 GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2319 of file FspUpd.h.

#### 12.9.2.137 PchIshI2c2GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshI2c2GpioAssign

Offset 0x040C - Enable PCH ISH I2C2 GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2325 of file FspUpd.h.

#### 12.9.2.138 PchIshPdtUnlock

UINT8 FSP\_S\_CONFIG::PchIshPdtUnlock

Offset 0x0415 - PCH ISH PDT Unlock Msg 0: False; 1: True.

\$EN\_DIS

Definition at line 2379 of file FspUpd.h.

#### 12.9.2.139 PchIshSpiGpioAssign

UINT8 FSP\_S\_CONFIG::PchIshSpiGpioAssign

Offset 0x0407 - Enable PCH ISH SPI GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2295 of file FspUpd.h.

---

#### 12.9.2.140 PchIshUart0GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshUart0GpioAssign

Offset 0x0408 - Enable PCH ISH UART0 GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2301 of file FspUpd.h.

#### 12.9.2.141 PchIshUart1GpioAssign

UINT8 FSP\_S\_CONFIG::PchIshUart1GpioAssign

Offset 0x0409 - Enable PCH ISH UART1 GPIO pins assigned 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2307 of file FspUpd.h.

#### 12.9.2.142 PchLanEnable

UINT8 FSP\_S\_CONFIG::PchLanEnable

Offset 0x03C9 - Enable LAN Enable/disable LAN controller.

\$EN\_DIS

Definition at line 2009 of file FspUpd.h.

#### 12.9.2.143 PchLanLtrEnable

UINT8 FSP\_S\_CONFIG::PchLanLtrEnable

Offset 0x03CA - Enable PCH Lan LTR capability of PCH internal LAN 0: Disable; 1: Enable.

\$EN\_DIS

Definition at line 2015 of file FspUpd.h.

#### 12.9.2.144 PchLockDownBiosInterface

UINT8 FSP\_S\_CONFIG::PchLockDownBiosInterface

Offset 0x09CD - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

\$EN\_DIS

Definition at line 3093 of file FspUpd.h.

#### 12.9.2.145 PchLockDownBiosLock

UINT8 FSP\_S\_CONFIG::PchLockDownBiosLock

---

Offset 0x09CE - Enable LOCKDOWN BIOS LOCK Enable the BIOS Lock feature and set EISS bit (D31:F5:Reg↔ DCh[5]) for the BIOS region protection.

\$EN\_DIS

Definition at line 3100 of file FspUpd.h.

#### 12.9.2.146 PchLockDownGlobalSmi

UINT8 FSP\_S\_CONFIG::PchLockDownGlobalSmi

Offset 0x09CC - Enable LOCKDOWN SMI Enable SMI\_LOCK bit to prevent writes to the Global SMI Enable bit.

\$EN\_DIS

Definition at line 3087 of file FspUpd.h.

#### 12.9.2.147 PchLockDownRtcMemoryLock

UINT8 FSP\_S\_CONFIG::PchLockDownRtcMemoryLock

Offset 0x09CF - 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 3107 of file FspUpd.h.

#### 12.9.2.148 PchMemoryThrottlingEnable

UINT8 FSP\_S\_CONFIG::PchMemoryThrottlingEnable

Offset 0x0A33 - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.

\$EN\_DIS

Definition at line 3507 of file FspUpd.h.

#### 12.9.2.149 PchPmDeepSxPol

UINT8 FSP\_S\_CONFIG::PchPmDeepSxPol

Offset 0x09FE - PCH Pm Deep Sx Pol Deep Sx Policy.

\$EN\_DIS

Definition at line 3233 of file FspUpd.h.

#### 12.9.2.150 PchPmDisableDsxAcPresentPulldown

UINT8 FSP\_S\_CONFIG::PchPmDisableDsxAcPresentPulldown

Offset 0x0A07 - PCH Pm Disable Dsx Ac Present Pulldown When Disable, PCH will internal pull down AC\_PRE↔ SENT in deep SX and during G3 exit.

---

\$EN\_DIS

Definition at line 3282 of file FspUpd.h.

#### 12.9.2.151 PchPmDisableEnergyReport

UINT8 FSP\_S\_CONFIG::PchPmDisableEnergyReport

Offset 0x0A06 - PCH Energy Reporting Disable/Enable PCH to CPU energy report feature.

\$EN\_DIS

Definition at line 3276 of file FspUpd.h.

#### 12.9.2.152 PchPmDisableNativePowerButton

UINT8 FSP\_S\_CONFIG::PchPmDisableNativePowerButton

Offset 0x0A08 - PCH Pm Disable Native Power Button Power button native mode disable.

\$EN\_DIS

Definition at line 3288 of file FspUpd.h.

#### 12.9.2.153 PchPmLanWakeFromDeepSx

UINT8 FSP\_S\_CONFIG::PchPmLanWakeFromDeepSx

Offset 0x09FD - PCH Pm Lan Wake From DeepSx Determine if enable LAN to wake from deep Sx.

\$EN\_DIS

Definition at line 3227 of file FspUpd.h.

#### 12.9.2.154 PchPmMeWakeSts

UINT8 FSP\_S\_CONFIG::PchPmMeWakeSts

Offset 0x0A11 - PCH Pm ME\_WAKE\_STS Clear the ME\_WAKE\_STS bit in the Power and Reset Status (PRSTS) register.

\$EN\_DIS

Definition at line 3310 of file FspUpd.h.

#### 12.9.2.155 PchPmPciePllSsc

UINT8 FSP\_S\_CONFIG::PchPmPciePllSsc

Offset 0x0A16 - PCH Pm Pcie Pll Ssc Specifies the Pcie Pll Spread Spectrum Percentage.

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

Definition at line 3343 of file FspUpd.h.

---

**12.9.2.156 PchPmPcieWakeFromDeepSx**

UINT8 FSP\_S\_CONFIG::PchPmPcieWakeFromDeepSx

Offset 0x09FA - PCH Pm Pcie Wake From DeepSx Determine if enable PCIe to wake from deep Sx.

\$EN\_DIS

Definition at line 3208 of file FspUpd.h.

**12.9.2.157 PchPmPmeB0S5Dis**

UINT8 FSP\_S\_CONFIG::PchPmPmeB0S5Dis

Offset 0x09F8 - 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 3196 of file FspUpd.h.

**12.9.2.158 PchPmPwrBtnOverridePeriod**

UINT8 FSP\_S\_CONFIG::PchPmPwrBtnOverridePeriod

Offset 0x0A05 - 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 3270 of file FspUpd.h.

**12.9.2.159 PchPmPwrCycDur**

UINT8 FSP\_S\_CONFIG::PchPmPwrCycDur

Offset 0x0A15 - 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 3337 of file FspUpd.h.

**12.9.2.160 PchPmS0i3Support**

UINT8 FSP\_S\_CONFIG::PchPmS0i3Support

Offset 0x0A17 - S0i3 support S0i3 platform support.

When enabled ASL code is used to determine if platform can go to S0i2 or S0i3 state. 0:Disable(S0i2 only), 1:Enable (Runtime in ASL) \$EN\_DIS

Definition at line 3350 of file FspUpd.h.

**12.9.2.161 PchPmSlpAMinAssert**

UINT8 FSP\_S\_CONFIG::PchPmSlpAMinAssert

---

Offset 0x0A02 - PCH Pm Slp A Min Assert SLP\_A Minimum Assertion Width Policy.

Default is PchSlpA2s.

Definition at line 3253 of file FspUpd.h.

#### 12.9.2.162 PchPmSlpLanLowDc

UINT8 FSP\_S\_CONFIG::PchPmSlpLanLowDc

Offset 0x0A04 - PCH Pm Slp Lan Low Dc Enable/Disable SLP\_LAN# Low on DC Power.

\$EN\_DIS

Definition at line 3265 of file FspUpd.h.

#### 12.9.2.163 PchPmSlpS0Enable

UINT8 FSP\_S\_CONFIG::PchPmSlpS0Enable

Offset 0x0A10 - PCH Pm Slp S0 Enable Indicates whether SLP\_S0# is to be asserted when PCH reaches idle state.

\$EN\_DIS

Definition at line 3304 of file FspUpd.h.

#### 12.9.2.164 PchPmSlpS3MinAssert

UINT8 FSP\_S\_CONFIG::PchPmSlpS3MinAssert

Offset 0x09FF - PCH Pm Slp S3 Min Assert SLP\_S3 Minimum Assertion Width Policy.

Default is PchSlpS350ms.

Definition at line 3238 of file FspUpd.h.

#### 12.9.2.165 PchPmSlpS4MinAssert

UINT8 FSP\_S\_CONFIG::PchPmSlpS4MinAssert

Offset 0x0A00 - PCH Pm Slp S4 Min Assert SLP\_S4 Minimum Assertion Width Policy.

Default is PchSlpS44s.

Definition at line 3243 of file FspUpd.h.

#### 12.9.2.166 PchPmSlpStrchSusUp

UINT8 FSP\_S\_CONFIG::PchPmSlpStrchSusUp

Offset 0x0A03 - PCH Pm Slp Strch Sus Up Enable SLP\_X Stretching After SUS Well Power Up.

\$EN\_DIS

Definition at line 3259 of file FspUpd.h.

---

**12.9.2.167 PchPmSlpSusMinAssert**

UINT8 FSP\_S\_CONFIG::PchPmSlpSusMinAssert

Offset 0x0A01 - PCH Pm Slp Sus Min Assert SLP\_SUS Minimum Assertion Width Policy.

Default is PchSlpSus4s.

Definition at line 3248 of file FspUpd.h.

**12.9.2.168 PchPmVrAlert**

UINT8 FSP\_S\_CONFIG::PchPmVrAlert

Offset 0x0A14 - 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 3331 of file FspUpd.h.

**12.9.2.169 PchPmWolEnableOverride**

UINT8 FSP\_S\_CONFIG::PchPmWolEnableOverride

Offset 0x09F9 - 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 3202 of file FspUpd.h.

**12.9.2.170 PchPmWolOvrWkSts**

UINT8 FSP\_S\_CONFIG::PchPmWolOvrWkSts

Offset 0x0A12 - 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 3316 of file FspUpd.h.

**12.9.2.171 PchPmWoWlanDeepSxEnable**

UINT8 FSP\_S\_CONFIG::PchPmWoWlanDeepSxEnable

Offset 0x09FC - 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 3221 of file FspUpd.h.

---

#### 12.9.2.172 PchPmWoWlanEnable

UINT8 FSP\_S\_CONFIG::PchPmWoWlanEnable

Offset 0x09FB - 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 3214 of file FspUpd.h.

#### 12.9.2.173 PchPwrOptEnable

UINT8 FSP\_S\_CONFIG::PchPwrOptEnable

Offset 0x09D1 - Enable Power Optimizer Enable DMI Power Optimizer on PCH side.

\$EN\_DIS

Definition at line 3119 of file FspUpd.h.

#### 12.9.2.174 PchSbAccessUnlock

UINT8 FSP\_S\_CONFIG::PchSbAccessUnlock

Offset 0x09F6 - 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 3184 of file FspUpd.h.

#### 12.9.2.175 PchScsEmmcHs400D11DataValid

UINT8 FSP\_S\_CONFIG::PchScsEmmcHs400D11DataValid

Offset 0x0402 - Set HS400 Tuning Data Valid Set if HS400 Tuning Data Valid.

\$EN\_DIS

Definition at line 2273 of file FspUpd.h.

#### 12.9.2.176 PchSerialIoI2cPadsTermination

UINT8 FSP\_S\_CONFIG::PchSerialIoI2cPadsTermination[6]

Offset 0x0367 - PCH SerialIo I2C Pads Termination 0x0: Hardware default, 0x1: None, 0x13: 1kOhm weak pull-up, 0x15: 5kOhm weak pull-up, 0x19: 20kOhm weak pull-up - Enable/disable SerialIo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5 pads termination respectively.

One byte for each controller, byte0 for I2C0, byte1 for I2C1, and so on.

Definition at line 1915 of file FspUpd.h.

---

**12.9.2.177 PchTTEnable**

UINT8 FSP\_S\_CONFIG::PchTTEnable

Offset 0x0A28 - Enable The Thermal Throttle Enable the thermal throttle function.

\$EN\_DIS

Definition at line 3440 of file FspUpd.h.

**12.9.2.178 PchTTLock**

UINT8 FSP\_S\_CONFIG::PchTTLock

Offset 0x0A2A - Thermal Throttle Lock Thermal Throttle Lock.

\$EN\_DIS

Definition at line 3453 of file FspUpd.h.

**12.9.2.179 PchTTState13Enable**

UINT8 FSP\_S\_CONFIG::PchTTState13Enable

Offset 0x0A29 - 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 3447 of file FspUpd.h.

**12.9.2.180 PchUnlockGpioPads**

UINT8 FSP\_S\_CONFIG::PchUnlockGpioPads

Offset 0x09D0 - Unlock all GPIO pads Force all GPIO pads to be unlocked for debug purpose.

\$EN\_DIS

Definition at line 3113 of file FspUpd.h.

**12.9.2.181 PchXhciOcLock**

UINT8 FSP\_S\_CONFIG::PchXhciOcLock

Offset 0x04A7 - 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 2690 of file FspUpd.h.

---

### 12.9.2.182 PcieComplianceTestMode

UINT8 FSP\_S\_CONFIG::PcieComplianceTestMode

Offset 0x09B9 - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

\$EN\_DIS

Definition at line 3035 of file FspUpd.h.

### 12.9.2.183 PcieEnablePeerMemoryWrite

UINT8 FSP\_S\_CONFIG::PcieEnablePeerMemoryWrite

Offset 0x09B8 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

\$EN\_DIS

Definition at line 3029 of file FspUpd.h.

### 12.9.2.184 PcieEnablePort8xhDecode

UINT8 FSP\_S\_CONFIG::PcieEnablePort8xhDecode

Offset 0x09B6 - 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 3018 of file FspUpd.h.

### 12.9.2.185 PcieEqPh3LaneParamCm

UINT8 FSP\_S\_CONFIG::PcieEqPh3LaneParamCm[24]

Offset 0x097C - PCIE Eq Ph3 Lane Param Cm PCH\_PCIE\_EQ\_LANE\_PARAM.

Coefficient C-1.

Definition at line 2996 of file FspUpd.h.

### 12.9.2.186 PcieEqPh3LaneParamCp

UINT8 FSP\_S\_CONFIG::PcieEqPh3LaneParamCp[24]

Offset 0x0994 - PCIE Eq Ph3 Lane Param Cp PCH\_PCIE\_EQ\_LANE\_PARAM.

Coefficient C+1.

Definition at line 3001 of file FspUpd.h.

---

**12.9.2.187 PcieRpAspm**

UINT8 FSP\_S\_CONFIG::PcieRpAspm[24]

Offset 0x0704 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH\_PCIE\_ASPM\_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 2886 of file FspUpd.h.

**12.9.2.188 PcieRpCompletionTimeout**

UINT8 FSP\_S\_CONFIG::PcieRpCompletionTimeout[24]

Offset 0x06EC - PCIE RP Completion Timeout The root port completion timeout(see: PCH\_PCIE\_COMPLETION\_TIMEOUT).

Default is PchPcieCompletionTO\_Default.

Definition at line 2880 of file FspUpd.h.

**12.9.2.189 PcieRpDpcExtensionsMask**

UINT32 FSP\_S\_CONFIG::PcieRpDpcExtensionsMask

Offset 0x0684 - 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 2847 of file FspUpd.h.

**12.9.2.190 PcieRpDpcMask**

UINT32 FSP\_S\_CONFIG::PcieRpDpcMask

Offset 0x0680 - 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 2841 of file FspUpd.h.

**12.9.2.191 PcieRpDptp**

UINT8 FSP\_S\_CONFIG::PcieRpDptp[24]

Offset 0x0944 - PCIE RP Downstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 2980 of file FspUpd.h.

**12.9.2.192 PcieRpFunctionSwap**

UINT8 FSP\_S\_CONFIG::PcieRpFunctionSwap

---

Offset 0x09BA - 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 3042 of file FspUpd.h.

#### 12.9.2.193 PcieRpGen3EqPh3Method

UINT8 FSP\_S\_CONFIG::PcieRpGen3EqPh3Method[24]

Offset 0x06A4 - 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 2865 of file FspUpd.h.

#### 12.9.2.194 PcieRpL1Substates

UINT8 FSP\_S\_CONFIG::PcieRpL1Substates[24]

Offset 0x071C - 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 2892 of file FspUpd.h.

#### 12.9.2.195 PcieRpPcieSpeed

UINT8 FSP\_S\_CONFIG::PcieRpPcieSpeed[24]

Offset 0x068C - 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 2859 of file FspUpd.h.

#### 12.9.2.196 PcieRpPhysicalSlotNumber

UINT8 FSP\_S\_CONFIG::PcieRpPhysicalSlotNumber[24]

Offset 0x06BC - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 2870 of file FspUpd.h.

#### 12.9.2.197 PcieRpPtmMask

UINT32 FSP\_S\_CONFIG::PcieRpPtmMask

Offset 0x0688 - 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 2853 of file FspUpd.h.

#### 12.9.2.198 PcieRpSlotPowerLimitScale

UINT8 FSP\_S\_CONFIG::PcieRpSlotPowerLimitScale[24]

Offset 0x08E4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

Leave as 0 to set to default.

Definition at line 2965 of file FspUpd.h.

#### 12.9.2.199 PcieRpSlotPowerLimitValue

UINT16 FSP\_S\_CONFIG::PcieRpSlotPowerLimitValue[24]

Offset 0x08FC - PCIE RP Slot Power Limit Value Specifies upper limit on power supply by slot.

Leave as 0 to set to default.

Definition at line 2970 of file FspUpd.h.

#### 12.9.2.200 PcieRpUptp

UINT8 FSP\_S\_CONFIG::PcieRpUptp[24]

Offset 0x092C - PCIE RP Upstream Port Transmitter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 2975 of file FspUpd.h.

#### 12.9.2.201 PcieSwEqCoeffListCm

UINT8 FSP\_S\_CONFIG::PcieSwEqCoeffListCm[5]

Offset 0x09AC - PCIE Sw Eq CoeffList Cm PCH\_PCIE\_EQ\_PARAM.

Coefficient C-1.

Definition at line 3006 of file FspUpd.h.

#### 12.9.2.202 PcieSwEqCoeffListCp

UINT8 FSP\_S\_CONFIG::PcieSwEqCoeffListCp[5]

Offset 0x09B1 - PCIE Sw Eq CoeffList Cp PCH\_PCIE\_EQ\_PARAM.

Coefficient C+1.

Definition at line 3011 of file FspUpd.h.

---

### 12.9.2.203 PkgCStateDemotion

UINT8 FSP\_S\_CONFIG::PkgCStateDemotion

Offset 0x012B - Enable or Disable Package Cstate Demotion Enable or Disable Package Cstate Demotion.

0: Disable; **1: Enable** \$EN\_DIS

Definition at line 884 of file FspsUpd.h.

### 12.9.2.204 PkgCStateLimit

UINT8 FSP\_S\_CONFIG::PkgCStateLimit

Offset 0x0130 - 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 915 of file FspsUpd.h.

### 12.9.2.205 PkgCStateUnDemotion

UINT8 FSP\_S\_CONFIG::PkgCStateUnDemotion

Offset 0x012C - Enable or Disable Package Cstate UnDemotion Enable or Disable Package Cstate UnDemotion.

0: Disable; **1: Enable** \$EN\_DIS

Definition at line 890 of file FspsUpd.h.

### 12.9.2.206 PmcCpuC10GatePinEnable

UINT8 FSP\_S\_CONFIG::PmcCpuC10GatePinEnable

Offset 0x0A1C - 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 3387 of file FspsUpd.h.

### 12.9.2.207 PmcCrashLogEnable

UINT8 FSP\_S\_CONFIG::PmcCrashLogEnable

Offset 0x0A20 - Enable PMC CrashLog Enable or Disable PMC CrashLog; 0: Disable; **1: Enable.**

\$EN\_DIS

Definition at line 3413 of file FspsUpd.h.

### 12.9.2.208 PmcDbgMsgEn

UINT8 FSP\_S\_CONFIG::PmcDbgMsgEn

---

Offset 0x0A1A - 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 3372 of file FspUpd.h.

#### 12.9.2.209 PmcModPhySusPgEnable

UINT8 FSP\_S\_CONFIG::PmcModPhySusPgEnable

Offset 0x0A1D - 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 3394 of file FspUpd.h.

#### 12.9.2.210 PmcPowerButtonDebounce

UINT32 FSP\_S\_CONFIG::PmcPowerButtonDebounce

Offset 0x0A0C - 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 3298 of file FspUpd.h.

#### 12.9.2.211 PmgCstCfgCtrlLock

UINT8 FSP\_S\_CONFIG::PmgCstCfgCtrlLock

Offset 0x0127 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; 1: **Enable**. \$EN\_DIS

Definition at line 860 of file FspUpd.h.

#### 12.9.2.212 PortUsb20Enable

UINT8 FSP\_S\_CONFIG::PortUsb20Enable[16]

Offset 0x04A8 - 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 2696 of file FspUpd.h.

#### 12.9.2.213 PortUsb30Enable

UINT8 FSP\_S\_CONFIG::PortUsb30Enable[10]

Offset 0x04C8 - 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 2707 of file FspsUpd.h.

#### 12.9.2.214 PowerLimit1

UINT32 FSP\_S\_CONFIG::PowerLimit1

Offset 0x00A4 - 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 560 of file FspsUpd.h.

#### 12.9.2.215 PowerLimit1Time

UINT8 FSP\_S\_CONFIG::PowerLimit1Time

Offset 0x009A - 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 497 of file FspsUpd.h.

#### 12.9.2.216 PowerLimit2

UINT8 FSP\_S\_CONFIG::PowerLimit2

Offset 0x009B - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

0 : Disable; 1: **Enable** \$EN\_DIS

Definition at line 503 of file FspsUpd.h.

#### 12.9.2.217 PowerLimit2Power

UINT32 FSP\_S\_CONFIG::PowerLimit2Power

Offset 0x00A8 - 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 566 of file FspsUpd.h.

#### 12.9.2.218 PowerLimit3

UINT32 FSP\_S\_CONFIG::PowerLimit3

Offset 0x00AC - 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 572 of file FspsUpd.h.

---

#### 12.9.2.219 PowerLimit4

UINT32 FSP\_S\_CONFIG::PowerLimit4

Offset 0x00B0 - Package PL4 power limit Package PL4 power limit.

Units are based on POWER\_MGMT\_CONFIG.CustomPowerUnit.Valid Range 0 to 1023875 in Step size of 125

Definition at line 578 of file FspsUpd.h.

#### 12.9.2.220 PpinSupport

UINT8 FSP\_S\_CONFIG::PpinSupport

Offset 0x0047 - 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 148 of file FspsUpd.h.

#### 12.9.2.221 PreWake

UINT8 FSP\_S\_CONFIG::PreWake

Offset 0x0065 - Pre Wake Randomization time PCODE MMIO Mailbox: Acoustic Mitigation Range.Defines the maximum pre-wake randomization time in micro ticks.This can be programmed only if AcousticNoiseMitigation is enabled.

Range 0-255 0.

Definition at line 276 of file FspsUpd.h.

#### 12.9.2.222 ProcessorTraceEnable

UINT8 FSP\_S\_CONFIG::ProcessorTraceEnable

Offset 0x0078 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 377 of file FspsUpd.h.

#### 12.9.2.223 ProcessorTraceMemBase

UINT64 FSP\_S\_CONFIG::ProcessorTraceMemBase

Offset 0x0080 - 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 387 of file FspsUpd.h.

---

#### 12.9.2.224 ProcessorTraceMemLength

UINT32 FSP\_S\_CONFIG::ProcessorTraceMemLength

Offset 0x0088 - Memory region allocation for Processor Trace Length in bytes of memory region allocated for Processor Trace.

Processor Trace requires 2<sup>N</sup> alignment and size in bytes per thread, from 4KB to 128MB. **0: Disable**

Definition at line 393 of file FspUpd.h.

#### 12.9.2.225 ProcessorTraceOutputScheme

UINT8 FSP\_S\_CONFIG::ProcessorTraceOutputScheme

Offset 0x0077 - 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 371 of file FspUpd.h.

#### 12.9.2.226 ProcHotResponse

UINT8 FSP\_S\_CONFIG::ProcHotResponse

Offset 0x0122 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable; 1: Enable.**

\$EN\_DIS

Definition at line 830 of file FspUpd.h.

#### 12.9.2.227 Psi1Threshold

UINT16 FSP\_S\_CONFIG::Psi1Threshold

Offset 0x0058 - 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 229 of file FspUpd.h.

#### 12.9.2.228 Psi2Threshold

UINT16 FSP\_S\_CONFIG::Psi2Threshold

Offset 0x005A - 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 234 of file FspUpd.h.

---

#### 12.9.2.229 Psi3Enable

UINT8 FSP\_S\_CONFIG::Psi3Enable

Offset 0x0049 - Power State 3 enable/disable PCODE MMIO Mailbox: Power State 3 enable/disable; 0: Disable; **1: Enable.**

For all VR Indexes

Definition at line 160 of file FspUpd.h.

#### 12.9.2.230 Psi3Threshold

UINT16 FSP\_S\_CONFIG::Psi3Threshold

Offset 0x005C - 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 239 of file FspUpd.h.

#### 12.9.2.231 PsOnEnable

UINT8 FSP\_S\_CONFIG::PsOnEnable

Offset 0x0A1B - 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 3380 of file FspUpd.h.

#### 12.9.2.232 PsysOffset

UINT8 FSP\_S\_CONFIG::PsysOffset

Offset 0x0063 - 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 261 of file FspUpd.h.

#### 12.9.2.233 PsysPmax

UINT16 FSP\_S\_CONFIG::PsysPmax

Offset 0x0110 - 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 770 of file FspUpd.h.

---

#### 12.9.2.234 PsysPowerLimit1

UINT8 FSP\_S\_CONFIG::PsysPowerLimit1

Offset 0x010C - PL1 Enable value PL1 Enable value to limit average platform power.

**0: Disable**; 1: Enable. \$EN\_DIS

Definition at line 747 of file FspsUpd.h.

#### 12.9.2.235 PsysPowerLimit1Power

UINT32 FSP\_S\_CONFIG::PsysPowerLimit1Power

Offset 0x0114 - 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 780 of file FspsUpd.h.

#### 12.9.2.236 PsysPowerLimit2

UINT8 FSP\_S\_CONFIG::PsysPowerLimit2

Offset 0x010E - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

**0: Disable**; 1: Enable. \$EN\_DIS

Definition at line 760 of file FspsUpd.h.

#### 12.9.2.237 PsysPowerLimit2Power

UINT32 FSP\_S\_CONFIG::PsysPowerLimit2Power

Offset 0x0118 - 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 786 of file FspsUpd.h.

#### 12.9.2.238 PsysSlope

UINT8 FSP\_S\_CONFIG::PsysSlope

Offset 0x0062 - 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 255 of file FspsUpd.h.

#### 12.9.2.239 PxCrConfig

UINT8 FSP\_S\_CONFIG::PxCrConfig[8]

Offset 0x09C0 - 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 3060 of file FspUpd.h.

#### 12.9.2.240 RaceToHalt

UINT8 FSP\_S\_CONFIG::RaceToHalt

Offset 0x0138 - 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 964 of file FspUpd.h.

#### 12.9.2.241 RemoteAssistance

UINT8 FSP\_S\_CONFIG::RemoteAssistance

Offset 0x0348 - Remote Assistance Trigger Availablilty Enable/Disable.

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

Definition at line 1846 of file FspUpd.h.

#### 12.9.2.242 SaPcieComplianceTestMode

UINT8 FSP\_S\_CONFIG::SaPcieComplianceTestMode

Offset 0x027F - PCIE Compliance Test Mode Compliance Test Mode shall be enabled when using Compliance Load Board.

\$EN\_DIS

Definition at line 1540 of file FspUpd.h.

#### 12.9.2.243 SaPcieDeviceOverrideTablePtr

UINT32 FSP\_S\_CONFIG::SaPcieDeviceOverrideTablePtr

Offset 0x0284 - 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 1564 of file FspUpd.h.

#### 12.9.2.244 SaPcieDisableRootPortClockGating

UINT8 FSP\_S\_CONFIG::SaPcieDisableRootPortClockGating

Offset 0x027E - 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 1534 of file FspUpd.h.

#### 12.9.2.245 SaPcieEnablePeerMemoryWrite

UINT8 FSP\_S\_CONFIG::SaPcieEnablePeerMemoryWrite

Offset 0x0280 - PCIE Enable Peer Memory Write This member describes whether Peer Memory Writes are enabled on the platform.

\$EN\_DIS

Definition at line 1546 of file FspUpd.h.

#### 12.9.2.246 SaPcieEqPh3LaneParamCm

UINT8 FSP\_S\_CONFIG::SaPcieEqPh3LaneParamCm[4]

Offset 0x0276 - PCIE Eq Ph3 Lane Param Cm SA\_PCIE\_EQ\_LANE\_PARAM.

Coefficient C-1.

Definition at line 1522 of file FspUpd.h.

#### 12.9.2.247 SaPcieEqPh3LaneParamCp

UINT8 FSP\_S\_CONFIG::SaPcieEqPh3LaneParamCp[4]

Offset 0x027A - PCIE Eq Ph3 Lane Param Cp SA\_PCIE\_EQ\_LANE\_PARAM.

Coefficient C+1.

Definition at line 1527 of file FspUpd.h.

#### 12.9.2.248 SaPcieRpAspm

UINT8 FSP\_S\_CONFIG::SaPcieRpAspm[4]

Offset 0x02D4 - PCIE RP Aspm The ASPM configuration of the root port (see: PCH\_PCIE\_ASPM\_CONTROL).

Default is PchPcieAspmAutoConfig.

Definition at line 1669 of file FspUpd.h.

#### 12.9.2.249 SaPcieRpDpcExtensionsMask

UINT32 FSP\_S\_CONFIG::SaPcieRpDpcExtensionsMask

Offset 0x02C0 - 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 1641 of file FspUpd.h.

---

#### 12.9.2.250 SaPcieRpDpcMask

UINT32 FSP\_S\_CONFIG::SaPcieRpDpcMask

Offset 0x02BC - 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 1635 of file FspUpd.h.

#### 12.9.2.251 SaPcieRpDptp

UINT8 FSP\_S\_CONFIG::SaPcieRpDptp[4]

Offset 0x0324 - PCIE RP Downstream Port Transmitter Preset Test, Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 1748 of file FspUpd.h.

#### 12.9.2.252 SaPcieRpFunctionSwap

UINT8 FSP\_S\_CONFIG::SaPcieRpFunctionSwap

Offset 0x0281 - 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 1553 of file FspUpd.h.

#### 12.9.2.253 SaPcieRpGen3EqPh3Method

UINT8 FSP\_S\_CONFIG::SaPcieRpGen3EqPh3Method[4]

Offset 0x02CC - 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 1658 of file FspUpd.h.

#### 12.9.2.254 SaPcieRpL1Substates

UINT8 FSP\_S\_CONFIG::SaPcieRpL1Substates[4]

Offset 0x02D8 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: SA\_PCIE\_L1SUB\_STATES\_CONTROL).

Default is SaPcieL1SubstatesL1\_1\_2.

Definition at line 1675 of file FspUpd.h.

---

**12.9.2.255 SaPcieRpPcieSpeed**

```
UINT8 FSP_S_CONFIG::SaPcieRpPcieSpeed[4]
```

Offset 0x02C8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.

0: Auto; 1: Gen1; 2: Gen2; 3: Gen3 (see: SA\_PCIE\_SPEED).

Definition at line 1652 of file FspUpd.h.

**12.9.2.256 SaPcieRpPhysicalSlotNumber**

```
UINT8 FSP_S_CONFIG::SaPcieRpPhysicalSlotNumber[4]
```

Offset 0x02D0 - PCIE RP Physical Slot Number Indicates the slot number for the root port.

Default is the value as root port index.

Definition at line 1663 of file FspUpd.h.

**12.9.2.257 SaPcieRpPtmMask**

```
UINT32 FSP_S_CONFIG::SaPcieRpPtmMask
```

Offset 0x02E4 - 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 1691 of file FspUpd.h.

**12.9.2.258 SaPcieRpUtp**

```
UINT8 FSP_S_CONFIG::SaPcieRpUtp[4]
```

Offset 0x0320 - PCIE RP Upstream Port Transmitter Preset Test, Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 1743 of file FspUpd.h.

**12.9.2.259 SataEnable**

```
UINT8 FSP_S_CONFIG::SataEnable
```

Offset 0x0416 - Enable SATA Enable/disable SATA controller.

\$EN\_DIS

Definition at line 2385 of file FspUpd.h.

**12.9.2.260 SataLedEnable**

```
UINT8 FSP_S_CONFIG::SataLedEnable
```

Offset 0x041B - SATA LED SATA LED indicating SATA controller activity.

---

0: disable, 1: enable \$EN\_DIS

Definition at line 2415 of file FspUpd.h.

#### 12.9.2.261 SataMode

UINT8 FSP\_S\_CONFIG::SataMode

Offset 0x041C - SATA Mode Select SATA controller working mode.

0:AHCI, 1:RAID

Definition at line 2421 of file FspUpd.h.

#### 12.9.2.262 SataP0TDispFinit

UINT8 FSP\_S\_CONFIG::SataP0TDispFinit

Offset 0x04A0 - Port 0 Alternate Fast Init Tdispatch Port 0 Alternate Fast Init Tdispatch.

\$EN\_DIS

Definition at line 2645 of file FspUpd.h.

#### 12.9.2.263 SataP1TDispFinit

UINT8 FSP\_S\_CONFIG::SataP1TDispFinit

Offset 0x04A2 - Port 1 Alternate Fast Init Tdispatch Port 1 Alternate Fast Init Tdispatch.

\$EN\_DIS

Definition at line 2656 of file FspUpd.h.

#### 12.9.2.264 SataPortsDevSlp

UINT8 FSP\_S\_CONFIG::SataPortsDevSlp[8]

Offset 0x044E - 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 2463 of file FspUpd.h.

#### 12.9.2.265 SataPortsDmVal

UINT8 FSP\_S\_CONFIG::SataPortsDmVal[8]

Offset 0x045E - Enable SATA Port DmVal DITO multiplier.

Default is 15.

Definition at line 2473 of file FspUpd.h.

---

**12.9.2.266 SataPortsEnable**

```
UINT8 FSP_S_CONFIG::SataPortsEnable[8]
```

Offset 0x041E - Enable SATA ports Enable/disable SATA ports.

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

Definition at line 2432 of file FspUpd.h.

**12.9.2.267 SataPwrOptEnable**

```
UINT8 FSP_S_CONFIG::SataPwrOptEnable
```

Offset 0x0419 - PCH Sata Pwr Opt Enable SATA Power Optimizer on PCH side.

\$EN\_DIS

Definition at line 2403 of file FspUpd.h.

**12.9.2.268 SataRstHddUnlock**

```
UINT8 FSP_S_CONFIG::SataRstHddUnlock
```

Offset 0x0486 - PCH Sata Rst Hdd Unlock Indicates that the HDD password unlock in the OS is enabled.

\$EN\_DIS

Definition at line 2536 of file FspUpd.h.

**12.9.2.269 SataRstInterrupt**

```
UINT8 FSP_S_CONFIG::SataRstInterrupt
```

Offset 0x048A - 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 2561 of file FspUpd.h.

**12.9.2.270 SataRstIrrt**

```
UINT8 FSP_S_CONFIG::SataRstIrrt
```

Offset 0x0483 - PCH Sata Rst Irrt Intel Rapid Recovery Technology.

\$EN\_DIS

Definition at line 2519 of file FspUpd.h.

**12.9.2.271 SataRstIrrtOnly**

```
UINT8 FSP_S_CONFIG::SataRstIrrtOnly
```

---

Offset 0x0488 - PCH Sata Rst Irrt Only Allow only IRRT drives to span internal and external ports.

\$EN\_DIS

Definition at line 2549 of file FspUpd.h.

#### 12.9.2.272 SataRstLedLocate

UINT8 FSP\_S\_CONFIG::SataRstLedLocate

Offset 0x0487 - 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 2543 of file FspUpd.h.

#### 12.9.2.273 SataRstOromUiBanner

UINT8 FSP\_S\_CONFIG::SataRstOromUiBanner

Offset 0x0484 - PCH Sata Rst Orom Ui Banner OROM UI and BANNER.

\$EN\_DIS

Definition at line 2525 of file FspUpd.h.

#### 12.9.2.274 SataRstPcieDeviceResetDelay

UINT8 FSP\_S\_CONFIG::SataRstPcieDeviceResetDelay[3]

Offset 0x0494 - PCH Sata Rst Pcie Device Reset Delay PCIe Storage Device Reset Delay in milliseconds.

Default value is 100ms

Definition at line 2594 of file FspUpd.h.

#### 12.9.2.275 SataRstRaid0

UINT8 FSP\_S\_CONFIG::SataRstRaid0

Offset 0x047F - PCH Sata Rst Raid0 RAID0.

\$EN\_DIS

Definition at line 2495 of file FspUpd.h.

#### 12.9.2.276 SataRstRaid1

UINT8 FSP\_S\_CONFIG::SataRstRaid1

Offset 0x0480 - PCH Sata Rst Raid1 RAID1.

\$EN\_DIS

Definition at line 2501 of file FspUpd.h.

---

**12.9.2.277 SataRstRaid10**

UINT8 FSP\_S\_CONFIG::SataRstRaid10

Offset 0x0481 - PCH Sata Rst Raid10 RAID10.

\$EN\_DIS

Definition at line 2507 of file FspUpd.h.

**12.9.2.278 SataRstRaid5**

UINT8 FSP\_S\_CONFIG::SataRstRaid5

Offset 0x0482 - PCH Sata Rst Raid5 RAID5.

\$EN\_DIS

Definition at line 2513 of file FspUpd.h.

**12.9.2.279 SataRstRaidDeviceId**

UINT8 FSP\_S\_CONFIG::SataRstRaidDeviceId

Offset 0x047E - PCH Sata Rst Raid Alternate Id Enable RAID Alternate ID.

\$EN\_DIS

Definition at line 2489 of file FspUpd.h.

**12.9.2.280 SataRstSmartStorage**

UINT8 FSP\_S\_CONFIG::SataRstSmartStorage

Offset 0x0489 - PCH Sata Rst Smart Storage RST Smart Storage caching Bit.

\$EN\_DIS

Definition at line 2555 of file FspUpd.h.

**12.9.2.281 SataSalpSupport**

UINT8 FSP\_S\_CONFIG::SataSalpSupport

Offset 0x0418 - Enable SATA SALP Support Enable/disable SATA Aggressive Link Power Management.

\$EN\_DIS

Definition at line 2397 of file FspUpd.h.

---

**12.9.2.282 SataTestMode**

UINT8 FSP\_S\_CONFIG::SataTestMode

Offset 0x0417 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

\$EN\_DIS

Definition at line 2391 of file FspUpd.h.

**12.9.2.283 SataThermalSuggestedSetting**

UINT8 FSP\_S\_CONFIG::SataThermalSuggestedSetting

Offset 0x04A3 - Sata Thermal Throttling Suggested Setting Sata Thermal Throttling Suggested Setting.

\$EN\_DIS

Definition at line 2662 of file FspUpd.h.

**12.9.2.284 ScIrqSelect**

UINT8 FSP\_S\_CONFIG::SciIrqSelect

Offset 0x09C9 - Select ScIrqSelect SCI IRQ Select.

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

Definition at line 3070 of file FspUpd.h.

**12.9.2.285 ScsEmmcEnabled**

UINT8 FSP\_S\_CONFIG::ScsEmmcEnabled

Offset 0x0400 - Enable eMMC Controller Enable/disable eMMC Controller.

\$EN\_DIS

Definition at line 2261 of file FspUpd.h.

**12.9.2.286 ScsEmmcHs400Enabled**

UINT8 FSP\_S\_CONFIG::ScsEmmcHs400Enabled

Offset 0x0401 - Enable eMMC HS400 Mode Enable eMMC HS400 Mode.

\$EN\_DIS

Definition at line 2267 of file FspUpd.h.

**12.9.2.287 ScsSdCardEnabled**

UINT8 FSP\_S\_CONFIG::ScsSdCardEnabled

Offset 0x03FB - Enable SdCard Controller Enable/disable SD Card Controller.

---

\$EN\_DIS

Definition at line 2233 of file FspUpd.h.

#### 12.9.2.288 SendEcCmd

UINT64 FSP\_S\_CONFIG::SendEcCmd

Offset 0x01A0 - 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 1049 of file FspUpd.h.

#### 12.9.2.289 SendVrMbxCmd

UINT8 FSP\_S\_CONFIG::SendVrMbxCmd

Offset 0x006A - 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 312 of file FspUpd.h.

#### 12.9.2.290 SerialIoDebugUartNumber

UINT8 FSP\_S\_CONFIG::SerialIoDebugUartNumber

Offset 0x03C8 - UART Number For Debug Purpose UART number for debug purpose.

0:UART0, 1: UART1, 2:UART2. Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:UART0, 1:UART1, 2:UART2

Definition at line 2003 of file FspUpd.h.

#### 12.9.2.291 SerialIoI2cMode

UINT8 FSP\_S\_CONFIG::SerialIoI2cMode[6]

Offset 0x036D - I2Cn Device Mode Selects I2c operation mode.

N represents controller index: I2c0, I2c1, ... Available modes: 0:SerialIoI2cDisabled, 1:SerialIoI2cPci, 2:SerialIoI2cHidden

Definition at line 1921 of file FspUpd.h.

#### 12.9.2.292 SerialIoSpi0CsEnable

UINT8 FSP\_S\_CONFIG::SerialIoSpi0CsEnable[2]

Offset 0x035B - SPI0 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 1885 of file FspUpd.h.

#### 12.9.2.293 SerialIoSpi0CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi0CsPolarity[2]
```

Offset 0x0355 - SPI0 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 1868 of file FspUpd.h.

#### 12.9.2.294 SerialIoSpi1CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsEnable[2]
```

Offset 0x035D - SPI1 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 1890 of file FspUpd.h.

#### 12.9.2.295 SerialIoSpi1CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi1CsPolarity[2]
```

Offset 0x0357 - SPI1 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 1874 of file FspUpd.h.

#### 12.9.2.296 SerialIoSpi2CsEnable

```
UINT8 FSP_S_CONFIG::SerialIoSpi2CsEnable[2]
```

Offset 0x035F - SPI2 Chip Select Enable 0:Disabled, 1:Enabled.

Enables GPIO for CS0 or CS1 if it is Enabled

Definition at line 1895 of file FspUpd.h.

#### 12.9.2.297 SerialIoSpi2CsPolarity

```
UINT8 FSP_S_CONFIG::SerialIoSpi2CsPolarity[2]
```

Offset 0x0359 - SPI2 Chip Select Polarity Sets polarity for each chip Select.

Available options: 0:PchSerialIoCsActiveLow, 1:PchSerialIoCsActiveHigh

Definition at line 1880 of file FspUpd.h.

---

### 12.9.2.298 SerialIoSpiDefaultCsOutput

UINT8 FSP\_S\_CONFIG::SerialIoSpiDefaultCsOutput[3]

Offset 0x0364 - 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 1907 of file FspUpd.h.

### 12.9.2.299 SerialIoSpiMode

UINT8 FSP\_S\_CONFIG::SerialIoSpiMode[3]

Offset 0x0361 - SPIn Device Mode Selects SPI operation mode.

N represents controller index: SPI0, SPI1, ... Available modes: 0:SerialIoSpiDisabled, 1:SerialIoSpiPci, 2:SerialIoSpiHidden

Definition at line 1901 of file FspUpd.h.

### 12.9.2.300 SerialIoUartCtsPinMux

UINT32 FSP\_S\_CONFIG::SerialIoUartCtsPinMux[3]

Offset 0x03BC - SerialIoUartCtsPinMux Select SerialIo Uart Cts pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_CTS\* for possible values.

Definition at line 1996 of file FspUpd.h.

### 12.9.2.301 SerialIoUartDataBits

UINT8 FSP\_S\_CONFIG::SerialIoUartDataBits[3]

Offset 0x0387 - Default DataBits for each Serial IO UART Set default word length.

0: Default, 5,6,7,8

Definition at line 1947 of file FspUpd.h.

### 12.9.2.302 SerialIoUartDmaEnable

UINT8 FSP\_S\_CONFIG::SerialIoUartDmaEnable[3]

Offset 0x0390 - Enable Dma for each Serial IO UART that supports it Set DMA/PIO mode.

0: Disabled, 1: Enabled

Definition at line 1963 of file FspUpd.h.

### 12.9.2.303 SerialIoUartMode

UINT8 FSP\_S\_CONFIG::SerialIoUartMode[3]

---

Offset 0x0373 - UARTn Device Mode Selects Uart operation mode.

N represents controller index: Uart0, Uart1, ... Available modes: 0:SerialIoUartDisabled, 1:SerialIoUartPci, 2:SerialIoUartHidden, 3:SerialIoUartCom, 4:SerialIoUartSkiplnit

Definition at line 1928 of file FspUpd.h.

#### 12.9.2.304 SerialIoUartParity

```
UINT8 FSP_S_CONFIG::SerialIoUartParity[3]
```

Offset 0x0384 - Default ParityType for each Serial IO UART Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 1942 of file FspUpd.h.

#### 12.9.2.305 SerialIoUartPowerGating

```
UINT8 FSP_S_CONFIG::SerialIoUartPowerGating[3]
```

Offset 0x038D - 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 1958 of file FspUpd.h.

#### 12.9.2.306 SerialIoUartRtsPinMux

```
UINT32 FSP_S_CONFIG::SerialIoUartRtsPinMux[3]
```

Offset 0x03B0 - SerialIoUartRtsPinMux Select SerialIo Uart Rts pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_RTS\* for possible values.

Definition at line 1990 of file FspUpd.h.

#### 12.9.2.307 SerialIoUartRxPinMux

```
UINT32 FSP_S_CONFIG::SerialIoUartRxPinMux[3]
```

Offset 0x0398 - SerialIoUartRxPinMux Select SerialIo Uart Rx pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_RX\* for possible values.

Definition at line 1978 of file FspUpd.h.

#### 12.9.2.308 SerialIoUartStopBits

```
UINT8 FSP_S_CONFIG::SerialIoUartStopBits[3]
```

Offset 0x038A - Default StopBits for each Serial IO UART Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 1953 of file FspUpd.h.

---

### 12.9.2.309 SerialIoUartTxPinMux

UINT32 FSP\_S\_CONFIG::SerialIoUartTxPinMux[3]

Offset 0x03A4 - SerialIoUartTxPinMux Select SerialIo Uart Tx pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_TX\* for possible values.

Definition at line 1984 of file FspUpd.h.

### 12.9.2.310 SiCsmFlag

UINT8 FSP\_S\_CONFIG::SiCsmFlag

Offset 0x0020 - Si Config CSM Flag.

Platform specific common policies that used by several silicon components. CSM status flag. \$EN\_DIS

Definition at line 92 of file FspUpd.h.

### 12.9.2.311 SkipMpInit

UINT8 FSP\_S\_CONFIG::SkipMpInit

Offset 0x0046 - 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 141 of file FspUpd.h.

### 12.9.2.312 SlowSlewRateForFivr

UINT8 FSP\_S\_CONFIG::SlowSlewRateForFivr

Offset 0x0069 - 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 304 of file FspUpd.h.

### 12.9.2.313 SlpS0DisQForDebug

UINT8 FSP\_S\_CONFIG::SlpS0DisQForDebug

Offset 0x0A19 - 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 3365 of file FspUpd.h.

---

#### 12.9.2.314 SlpS0Override

UINT8 FSP\_S\_CONFIG::SlpS0Override

Offset 0x0A18 - 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 3357 of file FspUpd.h.

#### 12.9.2.315 StateRatio

UINT8 FSP\_S\_CONFIG::StateRatio[40]

Offset 0x00CC - 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 705 of file FspUpd.h.

#### 12.9.2.316 StateRatioMax16

UINT8 FSP\_S\_CONFIG::StateRatioMax16[16]

Offset 0x0144 - 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 1004 of file FspUpd.h.

#### 12.9.2.317 TccActivationOffset

UINT8 FSP\_S\_CONFIG::TccActivationOffset

Offset 0x00A1 - 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 539 of file FspUpd.h.

#### 12.9.2.318 TccOffsetClamp

UINT8 FSP\_S\_CONFIG::TccOffsetClamp

Offset 0x00A2 - 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 547 of file FspsUpd.h.

#### 12.9.2.319 TccOffsetLock

UINT8 FSP\_S\_CONFIG::TccOffsetLock

Offset 0x00A3 - 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 554 of file FspsUpd.h.

#### 12.9.2.320 TccOffsetTimeWindowForRatl

UINT32 FSP\_S\_CONFIG::TccOffsetTimeWindowForRatl

Offset 0x00B4 - Tcc Offset Time Window for RATL Package PL4 power limit.

Units are based on POWER\_MGMT\_CONFIG.CustomPowerUnit.Valid Range 0 to 1023875 in Step size of 125

Definition at line 584 of file FspsUpd.h.

#### 12.9.2.321 TcolrqSelect

UINT8 FSP\_S\_CONFIG::TcoIrqSelect

Offset 0x09CA - Select TcolrqSelect TCO IRQ Select.

The valid value is 9, 10, 11, 20, 21, 22, 23.

Definition at line 3075 of file FspsUpd.h.

#### 12.9.2.322 TcssAuxOri

UINT16 FSP\_S\_CONFIG::TcssAuxOri

Offset 0x0254 - TCSS Aux Orientation Override Enable Bits 0, 2, ...

10 control override enables, bits 1, 3, ... 11 control overrides

Definition at line 1456 of file FspsUpd.h.

#### 12.9.2.323 TcssHslOri

UINT16 FSP\_S\_CONFIG::TcssHslOri

Offset 0x0256 - TCSS HSL Orientation Override Enable Bits 0, 2, ...

10 control override enables, bits 1, 3, ... 11 control overrides

Definition at line 1461 of file FspsUpd.h.

---

#### 12.9.2.324 TcssLoopbackModeBitMap

UINT8 FSP\_S\_CONFIG::TcssLoopbackModeBitMap

Offset 0x0275 - TcssLoopbackModeBitMap Set Loopback Mode Bit Map.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 1517 of file FspUpd.h.

#### 12.9.2.325 TcssXhciEnableComplianceMode

UINT8 FSP\_S\_CONFIG::TcssXhciEnableComplianceMode

Offset 0x0274 - TcssXhciEnableComplianceMode Set Compliance Mode.

0:Disabled 1:Enabled \$EN\_DIS

Definition at line 1511 of file FspUpd.h.

#### 12.9.2.326 TdcPowerLimit

UINT16 FSP\_S\_CONFIG::TdcPowerLimit

Offset 0x0052 - 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 212 of file FspUpd.h.

#### 12.9.2.327 TdcTimeWindow

UINT8 FSP\_S\_CONFIG::TdcTimeWindow

Offset 0x004F - 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 196 of file FspUpd.h.

#### 12.9.2.328 ThreeStrikeCounterDisable

UINT8 FSP\_S\_CONFIG::ThreeStrikeCounterDisable

Offset 0x008D - 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 406 of file FspUpd.h.

#### 12.9.2.329 TimedMwait

UINT8 FSP\_S\_CONFIG::TimedMwait

---

Offset 0x012E - Enable or Disable TimedMwait Support.

Enable or Disable TimedMwait Support. **0: Disable**; 1: Enable \$EN\_DIS

Definition at line 902 of file FspUpd.h.

#### 12.9.2.330 TStates

UINT8 FSP\_S\_CONFIG::TStates

Offset 0x011F - Enable or Disable T states Enable or Disable T states; **0: Disable**; 1: Enable.

\$EN\_DIS

Definition at line 812 of file FspUpd.h.

#### 12.9.2.331 TTSuggestedSetting

UINT8 FSP\_S\_CONFIG::TTSuggestedSetting

Offset 0x0A2B - Thermal Throttling Suggested Setting Thermal Throttling Suggested Setting.

\$EN\_DIS

Definition at line 3459 of file FspUpd.h.

#### 12.9.2.332 TurboMode

UINT8 FSP\_S\_CONFIG::TurboMode

Offset 0x0048 - Turbo Mode Enable/Disable Turbo mode.

0: disable, 1: enable \$EN\_DIS

Definition at line 154 of file FspUpd.h.

#### 12.9.2.333 TxtEnable

UINT8 FSP\_S\_CONFIG::TxtEnable

Offset 0x0044 - Enable or Disable TXT Enable or Disable TXT; 0: Disable; **1: Enable**.

\$EN\_DIS

Definition at line 128 of file FspUpd.h.

#### 12.9.2.334 UfsEnable

UINT8 FSP\_S\_CONFIG::UfsEnable[2]

Offset 0x0405 - UFS enable/disable Tx Data Delay Control 1 - Tx Data Delay (HS400 Mode).

\$EN\_DIS

Definition at line 2289 of file FspUpd.h.

---

### 12.9.2.335 Usb2PhyPehalfbit

UINT8 FSP\_S\_CONFIG::Usb2PhyPehalfbit[16]

Offset 0x050D - 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 2742 of file FspUpd.h.

### 12.9.2.336 Usb2PhyPetxiset

UINT8 FSP\_S\_CONFIG::Usb2PhyPetxiset[16]

Offset 0x04DD - 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 2724 of file FspUpd.h.

### 12.9.2.337 Usb2PhyPredeemp

UINT8 FSP\_S\_CONFIG::Usb2PhyPredeemp[16]

Offset 0x04FD - 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 2736 of file FspUpd.h.

### 12.9.2.338 Usb2PhyTxiset

UINT8 FSP\_S\_CONFIG::Usb2PhyTxiset[16]

Offset 0x04ED - 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 2730 of file FspUpd.h.

### 12.9.2.339 Usb3HsioTxDeEmph

UINT8 FSP\_S\_CONFIG::Usb3HsioTxDeEmph[10]

Offset 0x0527 - 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 2754 of file FspUpd.h.

---

#### 12.9.2.340 Usb3HsioTxDeEmphEnable

UINT8 FSP\_S\_CONFIG::Usb3HsioTxDeEmphEnable[10]

Offset 0x051D - 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 2748 of file FspUpd.h.

#### 12.9.2.341 Usb3HsioTxDownscaleAmp

UINT8 FSP\_S\_CONFIG::Usb3HsioTxDownscaleAmp[10]

Offset 0x053B - 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 2766 of file FspUpd.h.

#### 12.9.2.342 Usb3HsioTxDownscaleAmpEnable

UINT8 FSP\_S\_CONFIG::Usb3HsioTxDownscaleAmpEnable[10]

Offset 0x0531 - 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 2760 of file FspUpd.h.

#### 12.9.2.343 UsbPdoProgramming

UINT8 FSP\_S\_CONFIG::UsbPdoProgramming

Offset 0x04A5 - 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 2676 of file FspUpd.h.

#### 12.9.2.344 UsbTcPortEn

UINT8 FSP\_S\_CONFIG::UsbTcPortEn

Offset 0x0261 - TCSS USB Port Enable Bits 0, 1, ...

max Type C port control enables

Definition at line 1478 of file FspUpd.h.

---

**12.9.2.345 VmdEnable**

UINT8 FSP\_S\_CONFIG::VmdEnable

Offset 0x0228 - Enable VMD controller Enable/disable to VMD controller.

\$EN\_DIS

Definition at line 1383 of file FspUpd.h.

**12.9.2.346 VmdPortA**

UINT8 FSP\_S\_CONFIG::VmdPortA

Offset 0x0229 - Enable VMD portA Support Enable/disable to VMD portA Support.

\$EN\_DIS

Definition at line 1389 of file FspUpd.h.

**12.9.2.347 VmdPortB**

UINT8 FSP\_S\_CONFIG::VmdPortB

Offset 0x022A - Enable VMD portB Support Enable/disable to VMD portB Support.

\$EN\_DIS

Definition at line 1395 of file FspUpd.h.

**12.9.2.348 VmdPortC**

UINT8 FSP\_S\_CONFIG::VmdPortC

Offset 0x022B - Enable VMD portC Support Enable/disable to VMD portC Support.

\$EN\_DIS

Definition at line 1401 of file FspUpd.h.

**12.9.2.349 VmdPortD**

UINT8 FSP\_S\_CONFIG::VmdPortD

Offset 0x022C - Enable VMD portD Support Enable/disable to VMD portD Support.

\$EN\_DIS

Definition at line 1407 of file FspUpd.h.

**12.9.2.350 VrVoltageLimit**

UINT16 FSP\_S\_CONFIG::VrVoltageLimit

Offset 0x0060 - VR Voltage Limit PCODE MMIO Mailbox: VR Voltage Limit.

---

Range is 0-7999mV.

Definition at line 249 of file FspUpd.h.

#### 12.9.2.351 WatchDog

UINT8 FSP\_S\_CONFIG::WatchDog

Offset 0x033F - WatchDog Timer Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable WatchDog timer. \$EN\_DIS

Definition at line 1803 of file FspUpd.h.

#### 12.9.2.352 WatchDogTimerBios

UINT16 FSP\_S\_CONFIG::WatchDogTimerBios

Offset 0x0344 - BIOS Timer 16 bits Value, Set BIOS watchdog timer.

\$EN\_DIS

Definition at line 1828 of file FspUpd.h.

#### 12.9.2.353 WatchDogTimerOs

UINT16 FSP\_S\_CONFIG::WatchDogTimerOs

Offset 0x0342 - OS Timer 16 bits Value, Set OS watchdog timer.

\$EN\_DIS

Definition at line 1822 of file FspUpd.h.

#### 12.9.2.354 XdciEnable

UINT8 FSP\_S\_CONFIG::XdciEnable

Offset 0x04DC - Enable xDCI controller Enable/disable to xDCI controller.

\$EN\_DIS

Definition at line 2718 of file FspUpd.h.

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

- [FspUpd.h](#)

## 12.10 FSP\_S\_RESTRICTED\_CONFIG Struct Reference

Fsp S Restricted Configuration.

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

---

## Public Attributes

- UUINT32 [Signature](#)  
*Offset 0x0AA0.*
  - UUINT8 [SiSvPolicyEnable](#)  
*Offset 0x0AA4 - Si Config SvPolicyEnable.*
  - UUINT8 [HsleWorkaround](#)  
*Offset 0x0AA5 - Si Config HsleWorkaround Enable/Disable HSLE model specific workarounds \$EN\_DIS.*
  - UUINT8 [SgxDebugMode](#)  
*Offset 0x0AA6 - SgxDebugMode SgxDebugMode default values.*
  - UUINT8 [SvLtEnable](#)  
*Offset 0x0AA7 - SvLtEnable SvLtEnable default values.*
  - UUINT64 [EpcOffset](#)  
*Offset 0x0AA8 - EpcOffset EpcOffset default values.*
  - UUINT64 [EpcLength](#)  
*Offset 0x0AB0 - EpcLength EpcLength default values.*
  - UUINT8 [SgxLCP](#)  
*Offset 0x0AB8 - SgxLCP SgxLCP default values.*
  - UUINT8 [UnusedUpdSpace23](#) [7]  
*Offset 0x0AB9.*
  - UUINT64 [SgxLEPubKeyHash0](#)  
*Offset 0x0AC0 - EpcLength EpcLength default values.*
  - UUINT64 [SgxLEPubKeyHash1](#)  
*Offset 0x0AC8 - EpcLength EpcLength default values.*
  - UUINT64 [SgxLEPubKeyHash2](#)  
*Offset 0x0AD0 - EpcLength EpcLength default values.*
  - UUINT64 [SgxLEPubKeyHash3](#)  
*Offset 0x0AD8 - EpcLength EpcLength default values.*
  - UUINT8 [SecurityRestrictedRsvd](#) [3]  
*Offset 0x0AE0.*
  - UUINT8 [SaTestMplIOffSen](#)  
*Offset 0x0AE3 - Sa Test MplIOffSen TestMplIOffSen.*
  - UUINT8 [SaTestMdllIOffSen](#)  
*Offset 0x0AE4 - Sa Test MdllIOffSen TestMdllIOffSen.*
  - UUINT8 [SaTestModeEdramInternal](#)  
*Offset 0x0AE5 - Sa Test Mode Edram Internal Edram Enable Option.*
  - UUINT8 [SaTestSecurityLock](#)  
*Offset 0x0AE6 - Sa Test Security Lock Enable/Disable Security lock.*
  - UUINT8 [SaClearCorrUnCorrErrEnable](#)  
*Offset 0x0AE7 - Sa Clear CorrUnCorrErr Enable Clear CorrUnCorrErr Enable \$EN\_DIS.*
  - UUINT8 [SaPeg0CompletionTimeout](#)  
*Offset 0x0AE8 - Sa Peg0 Completion Timeout Peg0 Completion Timeout.*
  - UUINT8 [SaPeg1CompletionTimeout](#)  
*Offset 0x0AE9 - Sa Peg1 Completion Timeout Peg1 Completion Timeout.*
  - UUINT8 [SaPeg2CompletionTimeout](#)  
*Offset 0x0AEA - Sa Peg2 Completion Timeout Peg2 Completion Timeout.*
  - UUINT8 [SaPeg3CompletionTimeout](#)  
*Offset 0x0AEB - Sa Peg3 Completion Timeout Peg3 Completion Timeout.*
  - UUINT8 [SaTestPegAspmL0sAggression](#) [4]  
*Offset 0x0AEC - Sa Test Peg Aspm L0s Aggression Test Peg Aspm L0s Aggression.*
  - UUINT8 [SaSvPegArifen](#) [4]
-

- Offset 0x0AF0 - Sa SvPegArifen SvPegArifen.*
  - UINT8 [SaSvPegComplianceDeemphasis](#) [4]
    - Offset 0x0AF4 - Sa Sv Peg Compliance Deemphasis SvPegComplianceDeemphasis.*
  - UINT8 [SaSvPegTxLnStaggeringMode](#) [4]
    - Offset 0x0AF8 - Sa Sv Peg TxLn Staggering Mode SvPegTxLnStaggeringMode.*
  - UINT8 [SaSvPegTxLaneStaggeringInterval](#) [4]
    - Offset 0x0AFC - Sa Sv Peg TxLane Staggering Interval SvPegTxLaneStaggeringInterval.*
  - UINT8 [SaSvPegRxLnStaggeringMode](#) [4]
    - Offset 0x0B00 - Sa Sv Peg RxLn Staggering Mode SvPegRxLnStaggeringMode.*
  - UINT8 [SaSvPegRxLaneStaggeringInterval](#) [4]
    - Offset 0x0B04 - Sa Sv Peg RxLane Staggering Interval SvPegRxLaneStaggeringInterval.*
  - UINT8 [SaTestForceWake](#)
    - Offset 0x0B08 - Sa Graphics Pei Test Force Wake Test Force Wake.*
  - UINT8 [SaTestGfxPause](#)
    - Offset 0x0B09 - Sa Graphics Pei Test Gfx Pause Test Gfx Pause.*
  - UINT8 [SaTestGraphicsFreqModify](#)
    - Offset 0x0B0A - Sa Graphics Pei Test Graphics Freq Modify Test Graphics Freq Modify.*
  - UINT8 [SaTestPmLock](#)
    - Offset 0x0B0B - Sa Graphics Pei Test PmLock Test PmLock.*
  - UINT8 [SaTestPavpHeavyMode](#)
    - Offset 0x0B0C - Sa Graphics Pei Test Pavp Heavy Mode Test Pavp Heavy Mode.*
  - UINT8 [SaTestDopClockGating](#)
    - Offset 0x0B0D - Sa Graphics Pei Test Dop ClockGating Test Dop ClockGating.*
  - UINT8 [SaTestUnsolicitedAttackOverride](#)
    - Offset 0x0B0E - Sa Graphics Pei Test Unsolicited Attack Override Test Unsolicited Attack Override.*
  - UINT8 [SaTestWOPCMSupport](#)
    - Offset 0x0B0F - Sa Graphics Pei Test WOPCM Support Test WOPCM Support.*
  - UINT8 [SaTestPavpAsmf](#)
    - Offset 0x0B10 - Sa Graphics Pei Test Pavp Asmf Test Pavp Asmf.*
  - UINT8 [SaTestUnitLevelClockGating](#)
    - Offset 0x0B11 - Sa Graphics Pei Test Unit Level ClockGating Test Unit Level ClockGating.*
  - UINT8 [SaTestAutoTearDown](#)
    - Offset 0x0B12 - Sa Graphics Pei Test Auto TearDown Test Auto TearDown.*
  - UINT8 [SaTestGraphicsVideoFreq](#)
    - Offset 0x0B13 - Sa Graphics Pei Test Graphics Video Freq Test Graphics Video Freq.*
  - UINT8 [SaTestWOPCMSize](#)
    - Offset 0x0B14 - Sa Graphics Pei Test WOPCM Size Test WOPCM Size.*
  - UINT8 [SaTestGraphicsFreqReq](#)
    - Offset 0x0B15 - Sa Graphics Pei Test Graphics Freq Req Test Graphics Freq Req.*
  - UINT8 [GtProchotEnable](#)
    - Offset 0x0B16 - Gt Prochot Enable Enable/Disable Gt Prochot Setting \$EN\_DIS.*
  - UINT8 [SaTestSpcLock](#)
    - Offset 0x0B17 - Sa Graphics Pei Test SPC Lock Test Spc Lock \$EN\_DIS.*
  - UINT8 [TestGnaErrorCheckDis](#)
    - Offset 0x0B18 - Enable or disable GNA Error Check Disable Bit 0=Disable, 1(Default)=Enable \$EN\_DIS.*
  - UINT8 [SaTestSrlLock](#)
    - Offset 0x0B19 - Sa ITBT PCIe Test SRL Lock Test SRL Lock \$EN\_DIS.*
  - UINT8 [PchHdaTestPowerClockGating](#)
    - Offset 0x0B1A - HDA Power/Clock Gating (PGD/CGD) Enable/Disable HD Audio Power and Clock Gating(POR↔: Enable).*
  - UINT8 [PchHdaTestConfigLockdown](#)
-

- Offset 0x0B1B - Configuration Lockdown (BCLD) 0: POR (Enable), 1: Enable, 2: Disable.*
- UINT8 [PchHdaTestLowFreqLinkClkSrc](#)

*Offset 0x0B1C - Low Frequency Link Clock Source (LFLCS) 0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL).*
- UINT8 [PchDmiTestMemCloseStateEn](#)

*Offset 0x0B1D - MEM CLOSED State on PCH side Enable/Disable MEM CLOSED State on PCH side.*
- UINT8 [PchDmiTestInternalObffEn](#)

*Offset 0x0B1E - Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side enable/disable Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side.*
- UINT8 [PchDmiTestDmiExtSync](#)

*Offset 0x0B1F - Determines if force extended transmission of FTS ordered sets Determines if force extended transmission of FTS ordered sets when exiting L0s prior to entering L0.*
- UINT8 [PchDmiTestExternalObffEn](#)

*Offset 0x0B20 - Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side Enable/Disable Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side.*
- UINT8 [PchDmiTestClientObffEn](#)

*Offset 0x0B21 - Client Obff Enable Client Obff Enable.*
- UINT8 [PchDmiTestCxObffEntryDelay](#)

*Offset 0x0B22 - CxObff Entry Delay CxObff Entry Delay.*
- UINT8 [PchDmiTestPchTcLockDown](#)

*Offset 0x0B23 - Pch Tc Lock Down Pch Tc Lock Down.*
- UINT8 [PchDmiTestDmiSecureRegLock](#)

*Offset 0x0B24 - DMI Secure Reg Lock DMI Secure Reg Lock.*
- UINT8 [PchDmiTestOpiPllPowerGating](#)

*Offset 0x0B25 - OPI PLL Power Gating OPI PLL Power Gating.*
- UINT8 [PchLanTestPchWOLFastSupport](#)

*Offset 0x0B26 - PCH Lan Test WOL Fast Support Enables bit B\_PCH\_ACPI\_GPE0\_EN\_127\_96\_PME\_B0 during PchLanSxCallback in PchLanSxSmm.*
- UINT8 [PchLockDownTestSmiUnlock](#)

*Offset 0x0B27 - Smi Unlock bit for SV policy 0: Lock; 1: Unlock.*
- UINT8 [PchTestFlashLockDown](#)

*Offset 0x0B28 - Restricted Flash Lock Down Restricted Flash Lock Down.*
- UINT8 [TestPcieRpSriEnable](#)

*Offset 0x0B29 - Secure Register Lock Enable/Disable Secure Register Lock, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.*
- UINT8 [TestPchPcieClockGating](#)

*Offset 0x0B2A - PCIE RootPort Clock Gating Enable/Disable PCI Express Clock Gating (Power Management) for each root port, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.*
- UINT8 [TestUsbXhciAccessControlLock](#)

*Offset 0x0B2B - XHCI Access Control Lock Enable/Disable Access Control Lock To Xhci Registers, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.*
- UINT8 [PcieRpTestEqPh2Override](#) [24]

*Offset 0x0B2C - Gen3 EQ Phase2 Tx override Coefficient requested by the remote device is ignored.*
- UINT8 [PcieRpTestEqPh2Preset](#) [24]

*Offset 0x0B44 - Tx preset to use when TestEqPh2Override is set Tx preset to use when TestEqPh2Override is set.*
- UINT8 [PcieRpTestForceLtrOverride](#) [24]

*Offset 0x0B5C - Force LTR Override Force LTR Override.*
- UINT8 [PchPmTestPchPmRegisterLock](#)

*Offset 0x0B74 - PCH Pm Register Lock PCH Pm Register Lock.*
- UINT8 [PchPmTestSlpS0CsMePgQDis](#)

*Offset 0x0B75 - PCH Pm Test SlpS0 CsMe PgQDis CPPM VRIC CSME Power Gated Qualification Disable.*
- UINT8 [PchPmTestSlpS0GbeDiscQDis](#)

- Offset 0x0B76 - PCH Pm Test Slp S0 Gbe Disc QDis CPPM VRIC GbE Disconnected Qualification Disable.*

    - UINT8 [PchPmTestSlpS0ADspD3QDis](#)
  - Offset 0x0B77 - PCH Pm Test Slp S0A Dsp D3 QDis CPPM VRIC Audio DSP is in D3 Qualification Disable.*

    - UINT8 [PchPmTestSlpS0XhciD3QDis](#)
  - Offset 0x0B78 - PCH Pm Test Slp S0 Xhci D3QDis CPPM VRIC XHCI is in D3 Qualification Disable.*

    - UINT8 [PchPmTestSlpS0LpioD3QDis](#)
  - Offset 0x0B79 - PCH Pm Test Slp S0 Lpio D3QDis CPPM VRIC LPIO is in D3 Qualification Disable.*

    - UINT8 [PchPmTestSlpS0IccPIIWBEn](#)
  - Offset 0x0B7A - PCH Pm Test Slp S0 Icc PII W BEn CPPM VRIC ICC PLL Wake Block Enable.*

    - UINT8 [PchPmTestSlpS0PUGBEn](#)
  - Offset 0x0B7B - PCH Pm Test Slp S0 PUGB En PCH Pm CPPM VRIC Power Ungate Block Enable.*

    - UINT8 [PchPmTestPchClearPowerSts](#)
  - Offset 0x0B7C - PCH Pm Test Clear Power Sts.*

    - UINT8 [TestUsbTsLdoShutdown](#)
  - Offset 0x0B7D - USB2/TS LDO Dynamic Shutdown Enable/Disable USB2/TS LDO Dynamic Shutdown 0: POR, 1: force enable, 2: force disable.*

    - UINT8 [TestPchPmErDebugMode](#)
  - Offset 0x0B7E - PCH PMC ER Debug mode Disable/Enable Energy Reporting Debug Mode.*

    - UINT8 [TestPchPmLatchEventsC10Exit](#)
  - Offset 0x0B7F - PCH Pm Latch events C10 exit PCH Pm Latch events C10 exit Enable.*

    - UINT8 [TestPmcDbgModeLock](#)
  - Offset 0x0B80 - PMC Debug Mode Lock This option is used to enable or disable debug mode lock.*

    - UINT8 [TestPmcSlpsxStrPolLock](#)
  - Offset 0x0B81 - Sleep Sx Strech Policy Lock This option is used to enable or disable Sleep Sx Strech Policy Lock.*

    - UINT8 [TestCnviBtInterface](#)
  - Offset 0x0B82 - CNVi BT Interface This option configures BT device interface to either USB or UART 0:UART, 1:USB.*

    - UINT8 [TestCnviBtUartType](#)
  - Offset 0x0B83 - CNVi BT Uart Type This is a test option which allows configuration of UART type for BT communication 0:Serial IO Uart0, 1:ISH Uart0, 2:Uart over external pads.*

    - UINT8 [TestCnviBtWirelessCharging](#)
  - Offset 0x0B84 - CNVi BT Wireless Charging Enable/Disable CNVi BT Wireless Charging.*

    - UINT8 [TestCnviWifiLtrEn](#)
  - Offset 0x0B85 - CNVi WiFi LTR Enable/Disable CNVi WiFi LTR.*

    - UINT8 [TestCnviLteCoex](#)
  - Offset 0x0B86 - CNVi LTE Coexistence Enable/Disable MFUART2 connection for coexistence between LTE and Wi-Fi/BT.*

    - UINT8 [TestCnviSharedXtalClocking](#)
  - Offset 0x0B87 - CNVi Shared XTAL Clocking This option is used to tell CNVi that XTAL is being shared.*

    - UINT8 [SataTestRstPcieStorageTestMode](#) [3]
  - Offset 0x0B88 - PCH Sata Test Rst Pcie Storage Test Mode PCIe Storage remapping Test Mode to override existing PCIe Storage remapping POR setting for development purpose.*

    - UINT8 [SataTestRstPcieStoragePortConfigCheck](#) [3]
  - Offset 0x0B8B - PCH Sata Test Rst Pcie Storage Port Config Check Enable/Disable Port Configuration Check for RST PCIe Storage Remapping.*

    - UINT8 [SataTestRstPcieStorageDeviceInterface](#) [3]
  - Offset 0x0B8E - PCH Sata Test Rst Pcie Storage Device Interface Select the device interface (AHCI/NVME) for remapped device.*

    - UINT8 [SataTestRstPcieStorageDeviceBarSizeCheck](#) [3]
  - Offset 0x0B91 - PCH Sata Test Rst Pcie Storage Device Bar Size Check Enable/Disable Device BAR Size Check for remapped device.*

    - UINT8 [SataTestRstPcieStorageDeviceBarSelect](#) [3]
-

- Offset 0x0B94 - PCH Sata Test Rst Pcie Storage Device Bar Select Select the device BAR (BAR0-BAR5) that will be used for Remapping.*
- UINT8 [SataTestRstPcieStorageDeviceInterrupt](#) [3]  
*Offset 0x0B97 - PCH Sata Test Rst Pcie Storage Device Interrupt Select the device interrupt (Legacy/MSIX) for remapped device.*
  - UINT8 [SataTestRstPcieStorageAspmProgramming](#) [3]  
*Offset 0x0B9A - PCH Sata Test Rst Pcie Storage Aspm Programming Enable/Disable ASPM Programming for remapped device.*
  - UINT8 [SataTestRstPcieStorageSaveRestore](#) [3]  
*Offset 0x0B9D - PCH Sata Test Rst Pcie Storage Save Restore Enable/Disable ASPM Programming for remapped device.*
  - UINT8 [SataTestLtrEnable](#)  
*Offset 0x0BA0 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT8 [SataTestLtrConfigLock](#)  
*Offset 0x0BA1 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT8 [SataTestLtrOverride](#)  
*Offset 0x0BA2 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT8 [SataTestSnoopLatencyOverrideMultiplier](#)  
*Offset 0x0BA3 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT16 [SataTestSnoopLatencyOverrideValue](#)  
*Offset 0x0BA4 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT8 [SataTestSataAssel](#)  
*Offset 0x0BA6 - Latency Tolerance Reporting Mechanism Latency Tolerance Reporting Mechanism.*
  - UINT8 [PchTestTselLock](#)  
*Offset 0x0BA7 - This locks down Enables the thermal sensor Deprecated in ICL.*
  - UINT8 [PchTestTscLock](#)  
*Offset 0x0BA8 - This locks down Catastrophic Power-Down Enable and Catastrophic Trip Point Register 0: Disabled, 1: Enabled.*
  - UINT8 [PchTestPhlcLock](#)  
*Offset 0x0BA9 - This locks down PHL and PHLC 0: Disabled, 1: Enabled.*
  - UINT8 [UnusedUpdSpace24](#) [2]  
*Offset 0x0BAA.*
  - UINT32 [PchTestEPTypeLockPolicy](#)  
*Offset 0x0BAC - USB EP Type Lock Policy USB EP Type Lock Policy.*
  - UINT32 [PchTestEPTypeLockPolicyPortControl1](#)  
*Offset 0x0BB0 - USB EP Type Lock Policy Control 1 USB EP Type Lock Policy Control 1.*
  - UINT32 [PchTestEPTypeLockPolicyPortControl2](#)  
*Offset 0x0BB4 - USB EP Type Lock Policy Control 2 USB EP Type Lock Policy Control 2.*
  - UINT8 [PchTestControllerEnabled](#)  
*Offset 0x0BB8 - Xhci Controller Enable 0: Disable; 1: Enable.*
  - UINT8 [PchTestUnlockUsbForSvNoa](#)  
*Offset 0x0BB9 - Unlock to enable NOA for SV usage 1: Unlock to enable NOA usage.*
  - UINT8 [PchTestClkGatingXhci](#)  
*Offset 0x0BBA - Enable XHCI Clock Gating for SV usage 1: Enable XHCI Clock Gating.*
  - UINT8 [PcieTestSaPcieRpdbcgen](#)  
*Offset 0x0BBB - SA Test PcieRp dbc gen SA Test PcieRp dbc gen.*
  - UINT8 [PcieTestSaPcieRpdlcgen](#)  
*Offset 0x0BBC - SA Test PcieRp dlc gen SA Test PcieRp dlc gen.*
  - UINT8 [PcieTestSaPcieDcgeisma](#)  
*Offset 0x0BBD - SA Test Pcie Dcgeisma SA Test Pcie Dcgeisma.*
  - UINT8 [PcieTestSaPcieRpscgen](#)  
*Offset 0x0BBE - SA Test PcieRp scgen SA Test PcieRp scgen.*
-

- UINT8 [PcieTestSaPcieSrdbcgen](#)  
*Offset 0x0BBF - SA Test Pcie Srdbcgen SA Test Pcie Srdbcgen.*
- UINT8 [PcieTestSaPcieScptcge](#)  
*Offset 0x0BC0 - SA Test Pcie Scptcge SA Test Pcie Scptcge.*
- UINT8 [PcieTestSaPcieFdppge](#)  
*Offset 0x0BC1 - SA Test Pcie Fdppge SA Test Pcie Fdppge.*
- UINT8 [PcieTestSaPciePhyclpge](#)  
*Offset 0x0BC2 - SA Test Pcie Phyclpge SA Test Pcie Phyclpge.*
- UINT8 [PcieTestSaPcieFdcpgge](#)  
*Offset 0x0BC3 - SA Test Pcie Fdcpgge SA Test Pcie Fdcpgge.*
- UINT8 [PcieTestSaPcieDetscpge](#)  
*Offset 0x0BC4 - SA Test Pcie Detscpge PCH Test Pcie Detscpge.*
- UINT8 [PcieTestSaPcieL23rdyscpge](#)  
*Offset 0x0BC5 - SA Test Pcie L23 rdyscpge SA Test Pcie L23 rdyscpge.*
- UINT8 [PcieTestSaPcieDisscpge](#)  
*Offset 0x0BC6 - SA Test Pcie Disscpge SA Test Pcie Disscpge.*
- UINT8 [SaPcieAllowL0sWithGen3](#)  
*Offset 0x0BC7 - PCIE Allow L0s with Gen3 Allows SA rootports to have both L0s and Gen3 speed enabled at the same time.*
- UINT8 [SaPcieRpTestEqPh2Override](#) [4]  
*Offset 0x0BC8 - Gen3 EQ Phase2 Tx override Coefficient requested by the remote device is ignored.*
- UINT8 [SaPcieRpTestEqPh2Preset](#) [4]  
*Offset 0x0BCC - Tx preset to use when TestEqPh2Override is set Tx preset to use when TestEqPh2Override is set.*
- UINT8 [SaPcieRpTestAspmOc](#) [4]  
*Offset 0x0BD0 - Enable/Disable ASPM Optionality Compliance Enable/Disable ASPM Optionality Compliance.*
- UINT8 [SaPcieRpTestForceLtrOverride](#) [4]  
*Offset 0x0BD4 - Force LTR Override Force LTR Override.*
- UINT8 [UnusedUpdSpace25](#) [4]  
*Offset 0x0BD8.*
- UINT8 [ReservedFspSRestrictedUpd](#) [4]  
*Offset 0x0BDC.*

### 12.10.1 Detailed Description

Fsp S Restricted Configuration.

Definition at line 3632 of file FspSUpd.h.

### 12.10.2 Member Data Documentation

#### 12.10.2.1 PchDmiTestClientObffEn

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestClientObffEn

Offset 0x0B21 - Client Obff Enable Client Obff Enable.

\$EN\_DIS

Definition at line 3925 of file FspSUpd.h.

### 12.10.2.2 PchDmiTestDmiSecureRegLock

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestDmiSecureRegLock

Offset 0x0B24 - DMI Secure Reg Lock DMI Secure Reg Lock.

0: POR (Enable), 1: Enable, 2: Disable

Definition at line 3942 of file FspUpd.h.

### 12.10.2.3 PchDmiTestExternalObffEn

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestExternalObffEn

Offset 0x0B20 - Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side Enable/Disable Optimized Buffer Flush/Fill (OBFF) protocol for external on PCH side.

\$EN\_DIS

Definition at line 3919 of file FspUpd.h.

### 12.10.2.4 PchDmiTestInternalObffEn

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestInternalObffEn

Offset 0x0B1E - Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side enable/disable Optimized Buffer Flush/Fill (OBFF) protocol for internal on PCH side.

\$EN\_DIS

Definition at line 3907 of file FspUpd.h.

### 12.10.2.5 PchDmiTestMemCloseStateEn

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestMemCloseStateEn

Offset 0x0B1D - MEM CLOSED State on PCH side Enable/Disable MEM CLOSED State on PCH side.

\$EN\_DIS

Definition at line 3901 of file FspUpd.h.

### 12.10.2.6 PchDmiTestOpiPllPowerGating

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestOpiPllPowerGating

Offset 0x0B25 - OPI PLL Power Gating OPI PLL Power Gating.

0: POR, 1: force enable, 2: force disable

Definition at line 3948 of file FspUpd.h.

### 12.10.2.7 PchDmiTestPchTcLockDown

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchDmiTestPchTcLockDown

---

Offset 0x0B23 - Pch Tc Lock Down Pch Tc Lock Down.

\$EN\_DIS

Definition at line 3936 of file FspUpd.h.

#### 12.10.2.8 PchHdaTestConfigLockdown

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchHdaTestConfigLockdown

Offset 0x0B1B - Configuration Lockdown (BCLD) 0: POR (Enable), 1: Enable, 2: Disable.

0: POR (Enable), 1: Enable, 2: Disable

Definition at line 3889 of file FspUpd.h.

#### 12.10.2.9 PchHdaTestLowFreqLinkClkSrc

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchHdaTestLowFreqLinkClkSrc

Offset 0x0B1C - Low Frequency Link Clock Source (LFLCS) 0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL).

0: POR (Enable), 1: Enable (XTAL), 2: Disable (Audio PLL)

Definition at line 3895 of file FspUpd.h.

#### 12.10.2.10 PchHdaTestPowerClockGating

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchHdaTestPowerClockGating

Offset 0x0B1A - HDA Power/Clock Gating (PGD/CGD) Enable/Disable HD Audio Power and Clock Gating(POR: Enable).

0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 3883 of file FspUpd.h.

#### 12.10.2.11 PchLanTestPchWOLFastSupport

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchLanTestPchWOLFastSupport

Offset 0x0B26 - PCH Lan Test WOL Fast Support Enables bit B\_PCH\_ACPI\_GPE0\_EN\_127\_96\_PME\_B0 during PchLanSxCallback in PchLanSxSmm.

\$EN\_DIS

Definition at line 3954 of file FspUpd.h.

#### 12.10.2.12 PchLockDownTestSmiUnlock

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchLockDownTestSmiUnlock

Offset 0x0B27 - Smi Unlock bit for SV policy 0: Lock; 1: Unlock.

---

\$EN\_DIS

Definition at line 3960 of file FspUpd.h.

#### 12.10.2.13 PchPmTestPchClearPowerSts

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchPmTestPchClearPowerSts

Offset 0x0B7C - PCH Pm Test Clear Power Sts.

**Todo** ADD DESCRIPTION.

Policy for SV usage. NO USE..

Definition at line 4045 of file FspUpd.h.

#### 12.10.2.14 PchTestClkGatingXhci

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchTestClkGatingXhci

Offset 0x0BBA - Enable XHCI Clock Gating for SV usage 1: Enable XHCI Clock Gating.

0: Disable XHCI Clock Gating. Policy for SV usage. \$EN\_DIS

Definition at line 4241 of file FspUpd.h.

#### 12.10.2.15 PchTestPhlcLock

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchTestPhlcLock

Offset 0x0BA9 - This locks down PHL and PHLC 0: Disabled, 1: Enabled.

\$EN\_DIS

Definition at line 4204 of file FspUpd.h.

#### 12.10.2.16 PchTestTscLock

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchTestTscLock

Offset 0x0BA8 - This locks down Catastrophic Power-Down Enable and Catastrophic Trip Point Register 0: Disabled, 1: Enabled.

\$EN\_DIS

Definition at line 4198 of file FspUpd.h.

#### 12.10.2.17 PchTestTselLock

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchTestTselLock

Offset 0x0BA7 - This locks down Enables the thermal sensor Deprecated in ICL.

0: Disabled, 1: Enabled. \$EN\_DIS

---

Definition at line 4192 of file FspUpd.h.

#### 12.10.2.18 PchTestUnlockUsbForSvNoa

UINT8 FSP\_S\_RESTRICTED\_CONFIG::PchTestUnlockUsbForSvNoa

Offset 0x0BB9 - Unlock to enable NOA for SV usage 1: Unlock to enable NOA usage.

0: Set Xhci OC registers, Set Xhci OCCDone bit, XHCI Access Control Bit. \$EN\_DIS

Definition at line 4235 of file FspUpd.h.

#### 12.10.2.19 SaPcieAllowL0sWithGen3

UINT8 FSP\_S\_RESTRICTED\_CONFIG::SaPcieAllowL0sWithGen3

Offset 0x0BC7 - PCIE Allow L0s with Gen3 Allows SA rootports to have both L0s and Gen3 speed enabled at the same time.

\$EN\_DIS

Definition at line 4307 of file FspUpd.h.

#### 12.10.2.20 SataTestRstPcieStorageDeviceInterface

UINT8 FSP\_S\_RESTRICTED\_CONFIG::SataTestRstPcieStorageDeviceInterface[3]

Offset 0x0B8E - PCH Sata Test Rst Pcie Storage Device Interface Select the device interface (AHCI/NVME) for remapped device.

NO USE.

Definition at line 4131 of file FspUpd.h.

#### 12.10.2.21 SiSvPolicyEnable

UINT8 FSP\_S\_RESTRICTED\_CONFIG::SiSvPolicyEnable

Offset 0x0AA4 - Si Config SvPolicyEnable.

Platform specific common policies that used by several silicon components. SvPolicyEnable. \$EN\_DIS

Definition at line 3642 of file FspUpd.h.

#### 12.10.2.22 TestCnviBtWirelessCharging

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestCnviBtWirelessCharging

Offset 0x0B84 - CNVi BT Wireless Charging Enable/Disable CNVi BT Wireless Charging.

0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4095 of file FspUpd.h.

---

### 12.10.2.23 TestCnviLteCoex

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestCnviLteCoex

Offset 0x0B86 - CNVi LTE Coexistence Enable/Disable MFUART2 connection for coexistence between LTE and Wi-Fi/BT.

0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4108 of file FspUpd.h.

### 12.10.2.24 TestCnviSharedXtalClocking

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestCnviSharedXtalClocking

Offset 0x0B87 - CNVi Shared XTAL Clocking This option is used to tell CNVi that XTAL is being shared.

0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4115 of file FspUpd.h.

### 12.10.2.25 TestCnviWifiLtrEn

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestCnviWifiLtrEn

Offset 0x0B85 - CNVi WiFi LTR Enable/Disable CNVi WiFi LTR.

0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4101 of file FspUpd.h.

### 12.10.2.26 TestPchPcieClockGating

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestPchPcieClockGating

Offset 0x0B2A - PCIE RootPort Clock Gating Enable/Disable PCI Express Clock Gating (Power Management) for each root port, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.

0: POR, 1: Force Enable, 2: Force Disable

Definition at line 3978 of file FspUpd.h.

### 12.10.2.27 TestPchPmErDebugMode

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestPchPmErDebugMode

Offset 0x0B7E - PCH PMC ER Debug mode Disable/Enable Energy Reporting Debug Mode.

\$EN\_DIS

Definition at line 4057 of file FspUpd.h.

### 12.10.2.28 TestPchPmLatchEventsC10Exit

UINT8 FSP\_S\_RESTRICTED\_CONFIG::TestPchPmLatchEventsC10Exit

---

Offset 0x0B7F - PCH Pm Latch events C10 exit PCH Pm Latch events C10 exit Enable.

0: POR, 1: force enable, 2: force disable

Definition at line 4063 of file FspUpd.h.

#### 12.10.2.29 TestPcieRpSrlEnable

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPcieRpSrlEnable
```

Offset 0x0B29 - Secure Register Lock Enable/Disable Secure Register Lock, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.

0: POR, 1: Force Enable, 2: Force Disable

Definition at line 3971 of file FspUpd.h.

#### 12.10.2.30 TestPmcDbgModeLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPmcDbgModeLock
```

Offset 0x0B80 - PMC Debug Mode Lock This option is used to enable or disable debug mode lock.

Set to disable to prevent locking. 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4070 of file FspUpd.h.

#### 12.10.2.31 TestPmcSlpsxStrPolLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestPmcSlpsxStrPolLock
```

Offset 0x0B81 - Sleep Sx Stretch Policy Lock This option is used to enable or disable Sleep Sx Stretch Policy Lock.

Set to disable to prevent locking. 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE. 0: POR, 1: Force Enable, 2: Force Disable

Definition at line 4077 of file FspUpd.h.

#### 12.10.2.32 TestUsbXhciAccessControlLock

```
UINT8 FSP_S_RESTRICTED_CONFIG::TestUsbXhciAccessControlLock
```

Offset 0x0B2B - XHCI Access Control Lock Enable/Disable Access Control Lock To Xhci Registers, 0: PLATFORM\_POR, 1: FORCE\_ENABLE, 2: FORCE\_DISABLE.

0: POR, 1: Force Enable, 2: Force Disable

Definition at line 3985 of file FspUpd.h.

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

- [FspUpd.h](#)

## 12.11 FSP\_T\_CONFIG Struct Reference

Fsp T Configuration.

```
#include <FsptUpd.h>
```

### Public Attributes

- UINT64 [PcdPciExpressBaseAddress](#)  
*Offset 0x0040 - Pci Express Base Address Base address to be programmed for Pci Express.*
- UINT32 [PcdPciExpressRegionLength](#)  
*Offset 0x0048 - Pci Express Region Length Region Length to be programmed for Pci Express.*
- UINT8 [SaFsptRsvd](#) [16]  
*Offset 0x004C.*
- UINT8 [PcdSerialloUartDebugEnabled](#)  
*Offset 0x005C - PcdSerialloUartDebugEnabled Enable Seriallo Uart debug library with/without initializing Seriallo Uart device in FSP.*
- UINT8 [PcdSerialloUartNumber](#)  
*Offset 0x005D - PcdSerialloUartNumber - FSPT Select Seriallo Uart Controller for debug.*
- UINT8 [PcdSerialloUartMode](#)  
*Offset 0x005E - PcdSerialloUartMode - FSPT Select Seriallo Uart Controller mode 0:SerialloUartDisabled, 1:SerialloUartPci, 2:SerialloUartHidden, 3:SerialloUartCom, 4:SerialloUartSkipInit.*
- UINT8 [UnusedUpdSpace0](#)  
*Offset 0x005F.*
- UINT32 [PcdSerialloUartBaudRate](#)  
*Offset 0x0060 - PcdSerialloUartBaudRate - FSPT Set default BaudRate Supported from 0 - default to 6000000.*
- UINT8 [PcdSerialloUartParity](#)  
*Offset 0x0064 - PcdSerialloUartParity - FSPT Set default Parity.*
- UINT8 [PcdSerialloUartDataBits](#)  
*Offset 0x0065 - PcdSerialloUartDataBits - FSPT Set default word length.*
- UINT8 [PcdSerialloUartStopBits](#)  
*Offset 0x0066 - PcdSerialloUartStopBits - FSPT Set default stop bits.*
- UINT8 [PcdSerialloUartAutoFlow](#)  
*Offset 0x0067 - PcdSerialloUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.*
- UINT32 [PcdSerialloUartRxPinMux](#)  
*Offset 0x0068 - PcdSerialloUartRxPinMux - FSPT Select RX pin muxing for Seriallo UART used for debug.*
- UINT32 [PcdSerialloUartTxPinMux](#)  
*Offset 0x006C - PcdSerialloUartTxPinMux - FSPT Select TX pin muxing for Seriallo UART used for debug.*
- UINT32 [PcdSerialloUartRtsPinMux](#)  
*Offset 0x0070 - PcdSerialloUartRtsPinMux - FSPT Select Seriallo Uart used for debug Rts pin muxing.*
- UINT32 [PcdSerialloUartCtsPinMux](#)  
*Offset 0x0074 - PcdSerialloUartCtsPinMux - FSPT Select Seriallo Uart used for debug Cts pin muxing.*
- UINT8 [ReservedFsptUpd1](#) [8]  
*Offset 0x0078.*

### 12.11.1 Detailed Description

Fsp T Configuration.

Definition at line 68 of file FsptUpd.h.

---

## 12.11.2 Member Data Documentation

### 12.11.2.1 PcdSerialIoUartAutoFlow

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartAutoFlow

Offset 0x0067 - PcdSerialIoUartAutoFlow - FSPT Enables UART hardware flow control, CTS and RTS lines.

0: Disable, 1:Enable

Definition at line 134 of file FsptUpd.h.

### 12.11.2.2 PcdSerialIoUartCtsPinMux

UINT32 FSP\_T\_CONFIG::PcdSerialIoUartCtsPinMux

Offset 0x0074 - PcdSerialIoUartCtsPinMux - FSPT Select SerialIo Uart used for debug Cts pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_CTS\* for possible values.

Definition at line 156 of file FsptUpd.h.

### 12.11.2.3 PcdSerialIoUartDataBits

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartDataBits

Offset 0x0065 - PcdSerialIoUartDataBits - FSPT Set default word length.

0: Default, 5,6,7,8

Definition at line 122 of file FsptUpd.h.

### 12.11.2.4 PcdSerialIoUartDebugEnabled

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartDebugEnabled

Offset 0x005C - 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 88 of file FsptUpd.h.

### 12.11.2.5 PcdSerialIoUartNumber

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartNumber

Offset 0x005D - PcdSerialIoUartNumber - FSPT Select SerialIo Uart Controller for debug.

Note: If UART0 is selected as CNVi BT Core interface, it cannot be used for debug purpose. 0:SerialIoUart0, 1:SerialIoUart1, 2:SerialIoUart2

Definition at line 95 of file FsptUpd.h.

---

### 12.11.2.6 PcdSerialIoUartParity

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartParity

Offset 0x0064 - PcdSerialIoUartParity - FSPT Set default Parity.

0: DefaultParity, 1: NoParity, 2: EvenParity, 3: OddParity

Definition at line 117 of file FsptUpd.h.

### 12.11.2.7 PcdSerialIoUartRtsPinMux

UINT32 FSP\_T\_CONFIG::PcdSerialIoUartRtsPinMux

Offset 0x0070 - PcdSerialIoUartRtsPinMux - FSPT Select SerialIo Uart used for debug Rts pin muxing.

Refer to GPIO\_\*\_MUXING\_SERIALIO\_UARTx\_RTS\* for possible values.

Definition at line 150 of file FsptUpd.h.

### 12.11.2.8 PcdSerialIoUartStopBits

UINT8 FSP\_T\_CONFIG::PcdSerialIoUartStopBits

Offset 0x0066 - PcdSerialIoUartStopBits - FSPT Set default stop bits.

0: DefaultStopBits, 1: OneStopBit, 2: OneFiveStopBits, 3: TwoStopBits

Definition at line 128 of file FsptUpd.h.

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

- [FsptUpd.h](#)

## 12.12 FSP\_T\_RESTRICTED\_CONFIG Struct Reference

Fsp T Restricted Configuration.

```
#include <FsptUpd.h>
```

### Public Attributes

- [UINT32 Signature](#)  
*Offset 0x0080.*
- [UINT8 ReservedFsptRestrictedUpd \[12\]](#)  
*Offset 0x0084.*

### 12.12.1 Detailed Description

Fsp T Restricted Configuration.

Definition at line 165 of file FsptUpd.h.

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

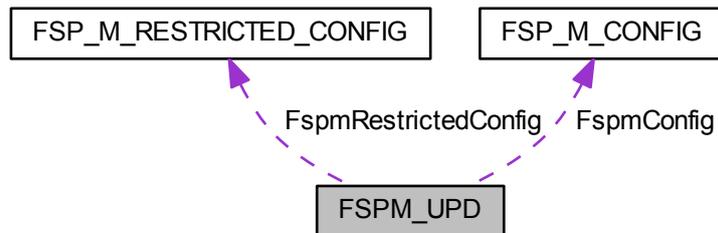
- [FsptUpd.h](#)
-

## 12.13 FSPM\_UPD Struct Reference

Fsp M UPD Configuration.

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

Collaboration diagram for FSPM\_UPD:



### Public Attributes

- FSPM\_UPD\_HEADER [FspUpdHeader](#)  
*Offset 0x0000.*
- FSPM\_ARCH\_UPD [FspmArchUpd](#)  
*Offset 0x0020.*
- FSP\_M\_CONFIG [FspmConfig](#)  
*Offset 0x0040.*
- FSP\_M\_RESTRICTED\_CONFIG [FspmRestrictedConfig](#)  
*Offset 0x0798.*
- UINT8 [UnusedUpdSpace31](#) [6]  
*Offset 0x0860.*
- UINT16 [UpdTerminator](#)  
*Offset 0x0866.*

### 12.13.1 Detailed Description

Fsp M UPD Configuration.

Definition at line 3853 of file [FspmUpd.h](#).

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

- [FspmUpd.h](#)

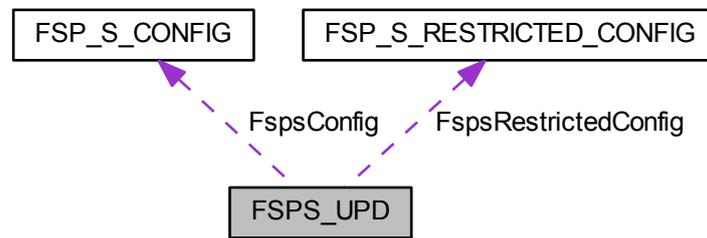
## 12.14 FSPS\_UPD Struct Reference

Fsp S UPD Configuration.

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

---

Collaboration diagram for FSPS\_UPD:



### Public Attributes

- `FSP_UPD_HEADER` [FspUpdHeader](#)  
*Offset 0x0000.*
- `FSP_S_CONFIG` [FspConfig](#)  
*Offset 0x0020.*
- `FSP_S_RESTRICTED_CONFIG` [FspRestrictedConfig](#)  
*Offset 0x0AA0.*
- `UINT8` [UnusedUpdSpace26](#) [2]  
*Offset 0x0BE0.*
- `UINT16` [UpdTerminator](#)  
*Offset 0x0BE2.*

#### 12.14.1 Detailed Description

Fsp S UPD Configuration.

Definition at line 4340 of file `FspUpd.h`.

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

- [FspUpd.h](#)

## 12.15 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.*

### 12.15.1 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:

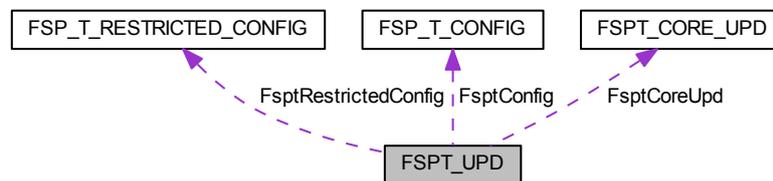
- [FsptUpd.h](#)

## 12.16 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 [FspCoreUpd](#)  
*Offset 0x0020.*
- FSP\_T\_CONFIG [FspConfig](#)  
*Offset 0x0040.*
- FSP\_T\_RESTRICTED\_CONFIG [FspRestrictedConfig](#)  
*Offset 0x0080.*
- UINT8 [UnusedUpdSpace1](#) [2]  
*Offset 0x0090.*
- UINT16 [UpdTerminator](#)  
*Offset 0x0092.*

### 12.16.1 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](#)

## 12.17 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.*

### 12.17.1 Detailed Description

GPIO configuration structure used for pin programming.

Structure contains fields that can be used to configure pad.

Definition at line 55 of file GpioConfig.h.

### 12.17.2 Member Data Documentation

---

### 12.17.2.1 Direction

UINT32 GPIO\_CONFIG::Direction

GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.

Refer to definition of GPIO\_DIRECTION for supported settings.

Definition at line 76 of file GpioConfig.h.

### 12.17.2.2 ElectricalConfig

UINT32 GPIO\_CONFIG::ElectricalConfig

GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.

Refer to definition of GPIO\_ELECTRICAL\_CONFIG for supported settings.

Definition at line 102 of file GpioConfig.h.

### 12.17.2.3 HostSoftPadOwn

UINT32 GPIO\_CONFIG::HostSoftPadOwn

Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.

Refer to definition of GPIO\_HOSTSW\_OWN.

Definition at line 70 of file GpioConfig.h.

### 12.17.2.4 InterruptConfig

UINT32 GPIO\_CONFIG::InterruptConfig

GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).

This setting is applicable only if GPIO is in GpioMode with input enabled. Refer to definition of GPIO\_INT\_CONFIG for supported settings.

Definition at line 90 of file GpioConfig.h.

### 12.17.2.5 LockConfig

UINT32 GPIO\_CONFIG::LockConfig

GPIO Lock Configuration This setting controls pads lock.

Refer to definition of GPIO\_LOCK\_CONFIG for supported settings.

Definition at line 108 of file GpioConfig.h.

### 12.17.2.6 OutputState

UINT32 GPIO\_CONFIG::OutputState

---

Output State Set Pad output value.

Refer to definition of GPIO\_OUTPUT\_STATE for supported settings. This setting takes place when output is enabled.

Definition at line 83 of file GpioConfig.h.

#### 12.17.2.7 PadMode

```
UINT32 GPIO_CONFIG::PadMode
```

Pad Mode Pad can be set as GPIO or one of its native functions.

When in native mode setting Direction (except Inversion), OutputState, InterruptConfig, Host Software Pad Ownership and OutputStateLock are unnecessary. Refer to definition of GPIO\_PAD\_MODE. Refer to EDS for each native mode according to the pad.

Definition at line 64 of file GpioConfig.h.

#### 12.17.2.8 PowerConfig

```
UINT32 GPIO_CONFIG::PowerConfig
```

GPIO Power Configuration.

This setting controls Pad Reset Configuration. Refer to definition of GPIO\_RESET\_CONFIG for supported settings.

Definition at line 96 of file GpioConfig.h.

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

- [GpioConfig.h](#)

## 12.18 SI\_PCH\_DEVICE\_INTERRUPT\_CONFIG Struct Reference

The PCH\_DEVICE\_INTERRUPT\_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

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

### Public Attributes

- [UINT8 Device](#)  
*Device number.*
- [UINT8 Function](#)  
*Device function.*
- [UINT8 IntX](#)  
*Interrupt pin: INTA-INTD (see SI\_PCH\_INT\_PIN)*
- [UINT8 Irq](#)  
*IRQ to be set for device.*

#### 12.18.1 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:

- [FspUpd.h](#)

## 12.19 SMBIOS\_STRUCTURE Struct Reference

The Smbios structure header.

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

### 12.19.1 Detailed Description

The Smbios structure header.

Definition at line 47 of file FirmwareVersionInfoHob.h.

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

- [FirmwareVersionInfoHob.h](#)
-

# Chapter 13

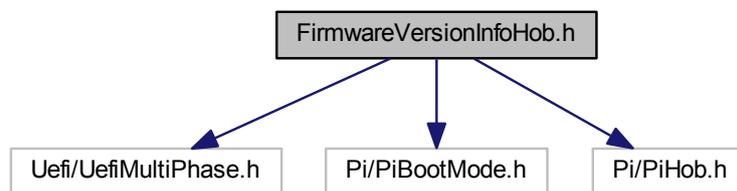
## File Documentation

### 13.1 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.*

#### 13.1.1 Detailed Description

Header file for Firmware Version Information.

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.

## 13.2 FspFixedPcds.h File Reference

This file lists all FixedAtBuild PCDs referenced in FSP integration guide.

### Macros

- #define `PcdFspAreaBaseAddress` 0xFFE30000  
*FspAreaBaseAddress.*
- #define `PcdFspImageIdString` \$ICLFSP\$  
*FspImageIdString.*
- #define `PcdSiliconInitVersionMajor` 0x08  
*SiliconInitVersionMajor.*
- #define `PcdSiliconInitVersionMinor` 0x00  
*SiliconInitVersionMinor.*
- #define `PcdSiliconInitVersionRevision` 0x52  
*SiliconInitVersionRevision.*
- #define `PcdSiliconInitVersionBuild` 0x40  
*SiliconInitVersionBuild.*
- #define `PcdGlobalDataPointerAddress` 0xFED00148  
*GlobalDataPointerAddress.*
- #define `PcdTemporaryRamBase` 0xFE000000  
*TemporaryRamBase.*
- #define `PcdTemporaryRamSize` 0x00040000  
*TemporaryRamSize.*
- #define `PcdFspReservedBufferSize` 0x100  
*FspReservedBufferSize.*

### 13.2.1 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.

## 13.3 FspInfoHob.h File Reference

Header file for FSP Information HOB.

### 13.3.1 Detailed Description

Header file for FSP Information HOB.

---

### Copyright

Copyright (c) 2017 - 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.

### Specification Reference:

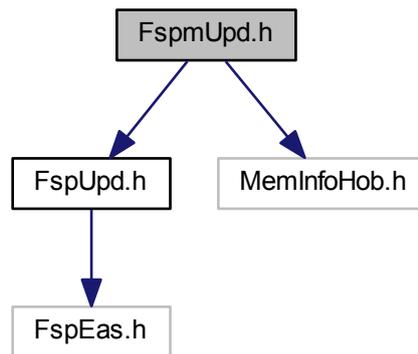
## 13.4 FspmUpd.h File Reference

Copyright (c) 2019, Intel Corporation.

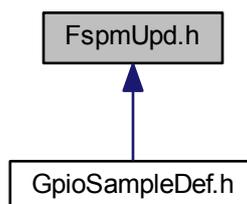
```
#include <FspUpd.h>
```

```
#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\\_RESTRICTED\\_CONFIG](#)

*Fsp M Restricted Configuration.*

- struct [FSPM\\_UPD](#)

*Fsp M UPD Configuration.*

### 13.4.1 Detailed Description

Copyright (c) 2019, 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 !!!

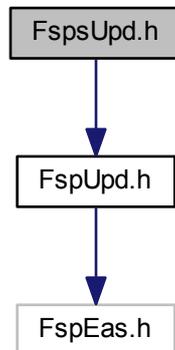
## 13.5 FspUpd.h File Reference

Copyright (c) 2018, Intel Corporation.

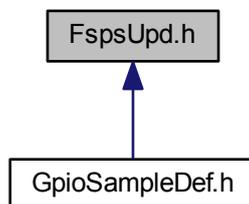
---

```
#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\\_RESTRICTED\\_CONFIG](#)  
*Fsp S Restricted Configuration.*
  - struct [FSPS\\_UPD](#)  
*Fsp S UPD Configuration.*
-

## Macros

- `#define SI_PCH_MAX_DEVICE_INTERRUPT_CONFIG 64`  
*Number of all PCH devices.*

## Enumerations

- enum `SI_PCH_INT_PIN`  
*Refer to the definition of PCH\_INT\_PIN.*

### 13.5.1 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 !!!

### 13.5.2 Enumeration Type Documentation

#### 13.5.2.1 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.

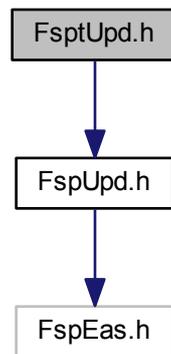
---

## 13.6 FsptUpd.h File Reference

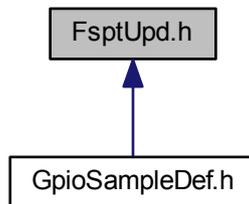
Copyright (c) 2018, Intel Corporation.

```
#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\\_RESTRICTED\\_CONFIG](#)  
*Fsp T Restricted Configuration.*
  - struct [FSPT\\_UPD](#)  
*Fsp T UPD Configuration.*
-

### 13.6.1 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.

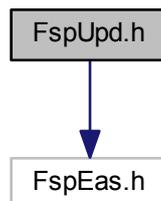
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE 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 !!!

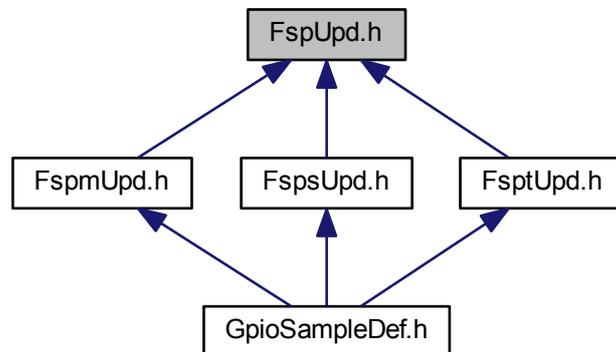
### 13.7 FspUpd.h File Reference

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:



### 13.7.1 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 !!!

## 13.8 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:*

### 13.8.1 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:

### 13.8.2 Enumeration Type Documentation

#### 13.8.2.1 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 167 of file GpioConfig.h.

#### 13.8.2.2 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 296 of file GpioConfig.h.

#### 13.8.2.3 GPIO\_HARDWARE\_DEFAULT

enum [GPIO\\_HARDWARE\\_DEFAULT](#)

#### Enumerator

GpioHardwareDefault	Leave setting unmodified.
---------------------	---------------------------

Definition at line 118 of file GpioConfig.h.

#### 13.8.2.4 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 146 of file GpioConfig.h.

### 13.8.2.5 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 207 of file GpioConfig.h.

### 13.8.2.6 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 329 of file GpioConfig.h.

### 13.8.2.7 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 346 of file `GpioConfig.h`.

### 13.8.2.8 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 181 of file `GpioConfig.h`.

### 13.8.2.9 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 132 of file `GpioConfig.h`.

---

## 13.8.2.10 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"> <li>• DeepSx transition</li> <li>• G3 Pad settings will not reset on:</li> <li>• S3/S4/S5 transition</li> <li>• Warm/Cold/Global reset</li> </ul>
<code>GpioHostDeepReset</code>	Host Deep Reset <code>PadRstCfg = 01b = "Deep GPIO Reset"</code> Pad settings will reset on: <ul style="list-style-type: none"> <li>• Warm/Cold/Global reset</li> <li>• DeepSx transition</li> <li>• G3 Pad settings will not reset on:</li> <li>• S3/S4/S5 transition</li> </ul>
<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"> <li>• S3/S4/S5 transition</li> <li>• Warm/Cold/Global reset</li> <li>• DeepSx transition</li> <li>• G3</li> </ul>
<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"> <li>• G3 Pad settings will not reset on:</li> <li>• S3/S4/S5 transition</li> <li>• Warm/Cold/Global reset</li> <li>• DeepSx transition</li> </ul>

Definition at line 229 of file `GpioConfig.h`.

## 13.9 GpioSampleDef.h File Reference

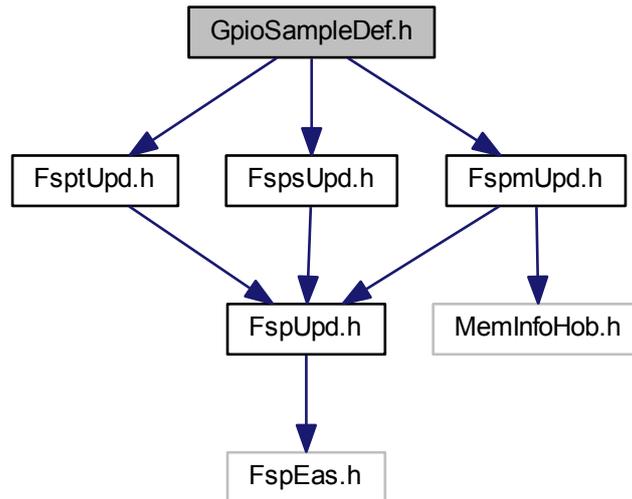
Sample enum definitions for GPIO table.

```
#include <FsptUpd.h>
```

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

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

Include dependency graph for GpioSampleDef.h:



### 13.9.1 Detailed Description

Sample enum definitions for GPIO table.

#### 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.

#### Specification Reference:

# Index

- AUDIO\_AZALIA\_VERB\_TABLE, [35](#)
- AZALIA\_HEADER, [36](#)
- AcLoadline
  - FSP\_S\_CONFIG, [145](#)
- AcousticNoiseMitigation
  - FSP\_S\_CONFIG, [145](#)
- ActiveCoreCount
  - FSP\_M\_CONFIG, [63](#)
- AmtEnabled
  - FSP\_S\_CONFIG, [145](#)
- AmtKvmEnabled
  - FSP\_S\_CONFIG, [146](#)
- AmtSolEnabled
  - FSP\_S\_CONFIG, [146](#)
- ApIdleManner
  - FSP\_S\_CONFIG, [146](#)
- ApStartupBase
  - FSP\_M\_CONFIG, [63](#)
- ApertureSize
  - FSP\_M\_CONFIG, [63](#)
- AsfEnabled
  - FSP\_S\_CONFIG, [146](#)
- AutoThermalReporting
  - FSP\_S\_CONFIG, [146](#)
- Avx2RatioOffset
  - FSP\_M\_CONFIG, [63](#)
- Avx2VoltageScaleFactor
  - FSP\_M\_CONFIG, [64](#)
- Avx3RatioOffset
  - FSP\_M\_CONFIG, [64](#)
- Avx512VoltageScaleFactor
  - FSP\_M\_CONFIG, [64](#)
  
- BclkAdaptiveVoltage
  - FSP\_M\_CONFIG, [64](#)
- BdatEnable
  - FSP\_M\_CONFIG, [64](#)
- BdatTestType
  - FSP\_M\_CONFIG, [64](#)
- BiosAcmBase
  - FSP\_M\_CONFIG, [65](#)
- BiosAcmSize
  - FSP\_M\_CONFIG, [65](#)
- BiosGuard
  - FSP\_M\_CONFIG, [65](#)
- BiosSize
  - FSP\_M\_CONFIG, [65](#)
- BistOnReset
  - FSP\_M\_CONFIG, [65](#)
- BootFrequency
  - FSP\_M\_CONFIG, [66](#)
- BypassPhySyncReset
  - FSP\_M\_CONFIG, [66](#)
  
- C1StateAutoDemotion
  - FSP\_S\_CONFIG, [147](#)
- C1StateUnDemotion
  - FSP\_S\_CONFIG, [147](#)
- C1e
  - FSP\_S\_CONFIG, [146](#)
- CHIPSET\_INIT\_INFO, [36](#)
- CStatePreWake
  - FSP\_S\_CONFIG, [148](#)
- ChHashEnable
  - FSP\_M\_CONFIG, [66](#)
- ChHashInterleaveBit
  - FSP\_M\_CONFIG, [66](#)
- ChHashMask
  - FSP\_M\_CONFIG, [66](#)
- CkeRankMapping
  - FSP\_M\_CONFIG, [67](#)
- CleanMemory
  - FSP\_M\_CONFIG, [67](#)
- CmdRanksTerminated
  - FSP\_M\_CONFIG, [67](#)
- CnviBtAudioOffload
  - FSP\_S\_CONFIG, [147](#)
- CnviBtCore
  - FSP\_S\_CONFIG, [147](#)
- CnviClkreqPinMux
  - FSP\_S\_CONFIG, [147](#)
- CnviMode
  - FSP\_S\_CONFIG, [148](#)
- CnviRfResetPinMux
  - FSP\_S\_CONFIG, [148](#)
- ConfigTdpBios
  - FSP\_S\_CONFIG, [148](#)
- CoreHighVoltageMode
  - FSP\_M\_CONFIG, [67](#)
- CoreMaxOcRatio
  - FSP\_M\_CONFIG, [67](#)
- CorePIIVoltageOffset
  - FSP\_M\_CONFIG, [68](#)
- CoreVoltageAdaptive
  - FSP\_M\_CONFIG, [68](#)
- CoreVoltageMode
  - FSP\_M\_CONFIG, [68](#)
- CoreVoltageOverride
  - FSP\_M\_CONFIG, [68](#)
- Count

- FIRMWARE\_VERSION\_INFO\_HOB, 38
- CpuCrashLogEnable
  - FSP\_M\_CONFIG, 68
- CpuMpHob
  - FSP\_S\_CONFIG, 148
- CpuRatio
  - FSP\_M\_CONFIG, 68
- CpuTraceHubMemReg0Size
  - FSP\_M\_CONFIG, 69
- CpuTraceHubMemReg1Size
  - FSP\_M\_CONFIG, 69
- CpuTraceHubMode
  - FSP\_M\_CONFIG, 69
- CstCfgCtrlIoMwaitRedirection
  - FSP\_S\_CONFIG, 149
- Custom1PowerLimit1
  - FSP\_S\_CONFIG, 149
- Custom1PowerLimit1Time
  - FSP\_S\_CONFIG, 149
- Custom1PowerLimit2
  - FSP\_S\_CONFIG, 149
- Custom1TurboActivationRatio
  - FSP\_S\_CONFIG, 149
- Custom2PowerLimit1
  - FSP\_S\_CONFIG, 150
- Custom2PowerLimit1Time
  - FSP\_S\_CONFIG, 150
- Custom2PowerLimit2
  - FSP\_S\_CONFIG, 150
- Custom2TurboActivationRatio
  - FSP\_S\_CONFIG, 150
- Custom3PowerLimit1
  - FSP\_S\_CONFIG, 150
- Custom3PowerLimit1Time
  - FSP\_S\_CONFIG, 150
- Custom3PowerLimit2
  - FSP\_S\_CONFIG, 151
- Custom3TurboActivationRatio
  - FSP\_S\_CONFIG, 151
- Cx
  - FSP\_S\_CONFIG, 151
- DcLoadline
  - FSP\_S\_CONFIG, 151
- DciUsb3TypecUfpDbg
  - FSP\_M\_CONFIG, 69
- Ddr4OneDpc
  - FSP\_M\_CONFIG, 69
- DdrFreqLimit
  - FSP\_M\_CONFIG, 70
- DdrSpeedControl
  - FSP\_M\_CONFIG, 70
- DebugInterfaceLockEnable
  - FSP\_M\_CONFIG, 70
- DevIntConfigPtr
  - FSP\_S\_CONFIG, 151
- Direction
  - GPIO\_CONFIG, 231
- DisableDimmChannel0
  - FSP\_M\_CONFIG, 70
- DisableDimmChannel1
  - FSP\_M\_CONFIG, 70
- DisableMessageCheck
  - FSP\_M\_CONFIG, 71
- DisableProcHotOut
  - FSP\_S\_CONFIG, 152
- DisableResets
  - FSP\_M\_RESTRICTED\_CONFIG, 112
- DisableVrThermalAlert
  - FSP\_S\_CONFIG, 152
- DmiDeEmphasis
  - FSP\_M\_CONFIG, 71
- DmiGen3EndPointHint
  - FSP\_M\_CONFIG, 71
- DmiGen3EndPointPreset
  - FSP\_M\_CONFIG, 71
- DmiGen3EqPh2Enable
  - FSP\_M\_CONFIG, 71
- DmiGen3EqPh3Method
  - FSP\_M\_CONFIG, 72
- DmiGen3ProgramStaticEq
  - FSP\_M\_CONFIG, 72
- DmiGen3RootPortPreset
  - FSP\_M\_CONFIG, 72
- DmiSuggestedSetting
  - FSP\_S\_CONFIG, 152
- DmiTS0TW
  - FSP\_S\_CONFIG, 152
- DmiTS1TW
  - FSP\_S\_CONFIG, 152
- DmiTS2TW
  - FSP\_S\_CONFIG, 153
- DmiTS3TW
  - FSP\_S\_CONFIG, 153
- EcCmdLock
  - FSP\_S\_CONFIG, 153
- EcCmdProvisionEav
  - FSP\_S\_CONFIG, 153
- Eist
  - FSP\_S\_CONFIG, 153
- ElectricalConfig
  - GPIO\_CONFIG, 232
- EnCmdRate
  - FSP\_M\_CONFIG, 73
- Enable8254ClockGating
  - FSP\_S\_CONFIG, 153
- Enable8254ClockGatingOnS3
  - FSP\_S\_CONFIG, 154
- EnableC6Dram
  - FSP\_M\_CONFIG, 72
- EnableEpbPeciOverride
  - FSP\_S\_CONFIG, 154
- EnableFastMsrHwpReq
  - FSP\_S\_CONFIG, 154
- EnableHwpAutoEppGrouping
  - FSP\_S\_CONFIG, 154
- EnableHwpAutoPerCorePstate

- FSP\_S\_CONFIG, 154
- EnableIbM
  - FSP\_S\_CONFIG, 155
- EnableMinVoltageOverride
  - FSP\_S\_CONFIG, 155
- EnablePerCorePState
  - FSP\_S\_CONFIG, 155
- EnableSgx
  - FSP\_M\_CONFIG, 72
- EnableTcoTimer
  - FSP\_S\_CONFIG, 155
- EndOfPostMessage
  - FSP\_S\_CONFIG, 155
- EnergyEfficientPState
  - FSP\_S\_CONFIG, 156
- EnergyEfficientTurbo
  - FSP\_S\_CONFIG, 156
- EpgEnable
  - FSP\_M\_CONFIG, 73
- EsataSpeedLimit
  - FSP\_S\_CONFIG, 156
- FClkFrequency
  - FSP\_M\_CONFIG, 73
- FIRMWARE\_VERSION\_INFO\_HOB, 38
  - Count, 38
- FIRMWARE\_VERSION\_INFO, 37
- FIRMWARE\_VERSION, 37
- FSP\_M\_CONFIG, 39
  - ActiveCoreCount, 63
  - ApStartupBase, 63
  - ApertureSize, 63
  - Avx2RatioOffset, 63
  - Avx2VoltageScaleFactor, 64
  - Avx3RatioOffset, 64
  - Avx512VoltageScaleFactor, 64
  - BclkAdaptiveVoltage, 64
  - BdatEnable, 64
  - BdatTestType, 64
  - BiosAcmBase, 65
  - BiosAcmSize, 65
  - BiosGuard, 65
  - BiosSize, 65
  - BistOnReset, 65
  - BootFrequency, 66
  - BypassPhySyncReset, 66
  - ChHashEnable, 66
  - ChHashInterleaveBit, 66
  - ChHashMask, 66
  - CkeRankMapping, 67
  - CleanMemory, 67
  - CmdRanksTerminated, 67
  - CoreHighVoltageMode, 67
  - CoreMaxOcRatio, 67
  - CorePIIVoltageOffset, 68
  - CoreVoltageAdaptive, 68
  - CoreVoltageMode, 68
  - CoreVoltageOverride, 68
  - CpuCrashLogEnable, 68
  - CpuRatio, 68
  - CpuTraceHubMemReg0Size, 69
  - CpuTraceHubMemReg1Size, 69
  - CpuTraceHubMode, 69
  - DciUsb3TypecUfpDbg, 69
  - Ddr4OneDpc, 69
  - DdrFreqLimit, 70
  - DdrSpeedControl, 70
  - DebugInterfaceLockEnable, 70
  - DisableDimmChannel0, 70
  - DisableDimmChannel1, 70
  - DisableMessageCheck, 71
  - DmiDeEmphasis, 71
  - DmiGen3EndPointHint, 71
  - DmiGen3EndPointPreset, 71
  - DmiGen3EqPh2Enable, 71
  - DmiGen3EqPh3Method, 72
  - DmiGen3ProgramStaticEq, 72
  - DmiGen3RootPortPreset, 72
  - EnCmdRate, 73
  - EnableC6Dram, 72
  - EnableSgx, 72
  - EpgEnable, 73
  - FClkFrequency, 73
  - FivrEfficiency, 73
  - FivrFaults, 73
  - FivrProtection, 74
  - FivrPs, 74
  - FivrTdc, 74
  - ForceOltmOrRefresh2x, 74
  - FreqSaGvLow, 74
  - FreqSaGvMid, 75
  - FullRangeMultiplierUnlockEn, 75
  - Gen3SwEqAlwaysAttempt, 75
  - Gen3SwEqEnableVocTest, 75
  - Gen3SwEqJitterDwellTime, 75
  - Gen3SwEqJitterErrorTarget, 76
  - Gen3SwEqNumberOfPresets, 76
  - Gen3SwEqVocDwellTime, 76
  - Gen3SwEqVocErrorTarget, 76
  - GmAdr, 76
  - GtPIIVoltageOffset, 77
  - GtPsmiSupport, 77
  - GttMmAdr, 77
  - HeciCommunication2, 77
  - HobBufferSize, 78
  - HotThresholdCh0Dimm0, 78
  - HotThresholdCh0Dimm1, 78
  - HotThresholdCh1Dimm0, 78
  - HotThresholdCh1Dimm1, 78
  - Idd3n, 78
  - Idd3p, 79
  - IgdDvmt50PreAlloc, 79
  - ImguCikOutEn, 79
  - ImrRpSelection, 79
  - InitPcieAspmAfterOprom, 79
  - InternalGfx, 80
  - IsvtloPort, 80

- JtagC10PowerGateDisable, 80
- KtDeviceEnable, 80
- LockPTMregs, 80
- MarginLimitCheck, 81
- McPllVoltageOffset, 81
- MemoryTrace, 81
- MmioSize, 81
- NonCoreHighVoltageMode, 81
- OcLock, 81
- PanelPowerEnable, 82
- PcdDebugInterfaceFlags, 82
- PcdIlsaSerialUartBase, 82
- PcdSerialDebugBaudRate, 82
- PcdSerialDebugLevel, 82
- PchLpcEnhancePort8xhDecoding, 83
- PchNumRsvdSmbusAddresses, 83
- PchPort80Route, 83
- PchSmbAlertEnable, 83
- PchTraceHubMemReg0Size, 83
- PchTraceHubMemReg1Size, 84
- PchTraceHubMode, 84
- PcieImrSize, 84
- PcieMultipleSegmentEnabled, 84
- PcieRpEnableMask, 84
- Peg0Gen3EqPh2Enable, 85
- Peg0Gen3EqPh3Method, 85
- Peg1Gen3EqPh2Enable, 85
- Peg1Gen3EqPh3Method, 85
- Peg2Gen3EqPh2Enable, 85
- Peg2Gen3EqPh3Method, 86
- Peg3Gen3EqPh2Enable, 86
- Peg3Gen3EqPh3Method, 86
- PegDataPtr, 86
- PegDisableSpreadSpectrumClocking, 87
- PegGen3EndPointHint, 87
- PegGen3EndPointPreset, 87
- PegGen3ProgramStaticEq, 87
- PegGen3RootPortPreset, 87
- PegGenerateBdatMarginTable, 88
- PegImrEnable, 88
- PegImrRpSelection, 88
- PegRxCemLoopbackLane, 88
- PegRxCemNonProtocolAwareness, 88
- PerCoreRatioLimit, 89
- PlatformDebugConsent, 89
- PrmrrSize, 89
- ProbelessTrace, 89
- PvdRatioThreshold, 89
- PwdnIdleCounter, 90
- RMTBIT, 92
- RMTLoopCount, 93
- RMT, 92
- RankInterleave, 90
- Ratio, 90
- RealtimeMemoryTiming, 90
- RefClk, 90
- RetrainOnFastFail, 90
- RhSolution, 91
- RingDownBin, 91
- RingMaxOcRatio, 91
- RingPllVoltageOffset, 91
- RingVoltageAdaptive, 91
- RingVoltageMode, 92
- RingVoltageOffset, 92
- RingVoltageOverride, 92
- RmtPerTask, 93
- SaGv, 93
- SaPcieRpEnableMask, 93
- SaPcieRpLinkDownGpios, 93
- SaPllFreqOverride, 94
- SaPllVoltageOffset, 94
- SafeMode, 93
- ScanExtGfxForLegacyOpRom, 94
- ScramblerSupport, 94
- SerialUartDebugAutoFlow, 94
- SerialUartDebugBaudRate, 95
- SerialUartDebugControllerNumber, 95
- SerialUartDebugDataBits, 95
- SerialUartDebugParity, 95
- SerialUartDebugStopBits, 95
- SinitMemorySize, 96
- SkipMbpHob, 96
- SkipMplInitPreMem, 96
- SmbusArpEnable, 96
- SmbusDynamicPowerGating, 96
- SmbusEnable, 97
- SmbusSpdWriteDisable, 97
- SpdAddressTable, 97
- SpdProfileSelected, 97
- tRTP, 100
- TcssDma0En, 97
- TcssDma1En, 97
- TcssIltbtPcie0En, 98
- TcssIltbtPcie1En, 98
- TcssIltbtPcie2En, 98
- TcssIltbtPcie3En, 98
- TcssXdcIEn, 98
- TcssXhciEn, 99
- TgaSize, 99
- ThrtCkeMinTmr, 99
- ThrtCkeMinTmrLpddr, 99
- TjMaxOffset, 99
- TmeEnable, 99
- TrainTrace, 100
- TschWFixup, 100
- TsegSize, 100
- TsodAlarmwindowLockBit, 100
- TsodCriticalEventOnly, 101
- TsodCriticaltripLockBit, 101
- TsodEventMode, 101
- TsodEventOutputControl, 101
- TsodEventPolarity, 101
- TsodManualEnable, 102
- TsodShutdownMode, 102
- TsodTcritMax, 102
- Txt, 102

- TxtAcheckRequest, [102](#)
- TxtDprMemoryBase, [103](#)
- TxtDprMemorySize, [103](#)
- TxtHeapMemorySize, [103](#)
- TxtImplemented, [103](#)
- TxtLcpPdBase, [103](#)
- TxtLcpPdSize, [104](#)
- UserBudgetEnable, [104](#)
- UserThresholdEnable, [104](#)
- VccInVoltageOverride, [104](#)
- VccinVrMaxVoltage, [104](#)
- VddVoltage, [104](#)
- VmxEnable, [105](#)
- WarmThresholdCh0Dimm0, [105](#)
- WarmThresholdCh0Dimm1, [105](#)
- WarmThresholdCh1Dimm0, [105](#)
- WarmThresholdCh1Dimm1, [105](#)
- WdtDisableAndLock, [106](#)
- XhciPIIOVERRIDE, [106](#)
- FSP\_M\_RESTRICTED\_CONFIG, [106](#)
  - DisableResets, [112](#)
  - HeciCommunication, [112](#)
  - HeciCommunication3, [112](#)
  - LowMemChannel, [113](#)
  - MsegSize, [113](#)
  - PchTestDmiMeUmaRootSpaceCheck, [113](#)
  - PcuDdrVoltage, [113](#)
  - tRRDD, [114](#)
  - tRRDG, [114](#)
  - tRRDR, [114](#)
  - tRRSG, [114](#)
  - tRWDD, [114](#)
  - tRWDG, [115](#)
  - tRWDR, [115](#)
  - tRWSG, [115](#)
  - tWRDD, [115](#)
  - tWRDG, [115](#)
  - tWRDR, [116](#)
  - tWRSG, [116](#)
  - tWWDD, [116](#)
  - tWWDG, [116](#)
  - tWWDR, [116](#)
  - tWWSG, [117](#)
  - TestMenuDprLock, [113](#)
- FSP\_S\_CONFIG, [117](#)
  - AcLoadline, [145](#)
  - AcousticNoiseMitigation, [145](#)
  - AmtEnabled, [145](#)
  - AmtKvmEnabled, [146](#)
  - AmtSolEnabled, [146](#)
  - ApIdleManner, [146](#)
  - AsfEnabled, [146](#)
  - AutoThermalReporting, [146](#)
  - C1StateAutoDemotion, [147](#)
  - C1StateUnDemotion, [147](#)
  - C1e, [146](#)
  - CStatePreWake, [148](#)
  - CnviBtAudioOffload, [147](#)
  - CnviBtCore, [147](#)
  - CnviClkreqPinMux, [147](#)
  - CnviMode, [148](#)
  - CnviRfResetPinMux, [148](#)
  - ConfigTdpBios, [148](#)
  - CpuMpHob, [148](#)
  - CstCfgCtrlMwaitRedirection, [149](#)
  - Custom1PowerLimit1, [149](#)
  - Custom1PowerLimit1Time, [149](#)
  - Custom1PowerLimit2, [149](#)
  - Custom1TurboActivationRatio, [149](#)
  - Custom2PowerLimit1, [150](#)
  - Custom2PowerLimit1Time, [150](#)
  - Custom2PowerLimit2, [150](#)
  - Custom2TurboActivationRatio, [150](#)
  - Custom3PowerLimit1, [150](#)
  - Custom3PowerLimit1Time, [150](#)
  - Custom3PowerLimit2, [151](#)
  - Custom3TurboActivationRatio, [151](#)
  - Cx, [151](#)
  - DcLoadline, [151](#)
  - DevIntConfigPtr, [151](#)
  - DisableProcHotOut, [152](#)
  - DisableVrThermalAlert, [152](#)
  - DmiSuggestedSetting, [152](#)
  - DmiTS0TW, [152](#)
  - DmiTS1TW, [152](#)
  - DmiTS2TW, [153](#)
  - DmiTS3TW, [153](#)
  - EcCmdLock, [153](#)
  - EcCmdProvisionEav, [153](#)
  - Eist, [153](#)
  - Enable8254ClockGating, [153](#)
  - Enable8254ClockGatingOnS3, [154](#)
  - EnableEpbPeciOverride, [154](#)
  - EnableFastMsrHwpReq, [154](#)
  - EnableHwpAutoEppGrouping, [154](#)
  - EnableHwpAutoPerCorePstate, [154](#)
  - EnableIltbm, [155](#)
  - EnableMinVoltageOverride, [155](#)
  - EnablePerCorePState, [155](#)
  - EnableTcoTimer, [155](#)
  - EndOfPostMessage, [155](#)
  - EnergyEfficientPState, [156](#)
  - EnergyEfficientTurbo, [156](#)
  - EsataSpeedLimit, [156](#)
  - FastPkgCRampDisableFivr, [156](#)
  - FivrRfiFrequency, [156](#)
  - FivrSpreadSpectrum, [157](#)
  - ForcMebxSyncUp, [157](#)
  - FwProgress, [157](#)
  - GpioIrqRoute, [157](#)
  - HdcControl, [157](#)
  - Heci3Enabled, [158](#)
  - Hwp, [158](#)
  - HwpInterruptControl, [158](#)
  - ITbtConnectTopologyTimeoutInMs, [159](#)
  - ITbtForcePowerOnTimeoutInMs, [159](#)

- IccMax, 158
- ImonOffset, 158
- ImonSlope, 159
- IomTypeCPortPadCfg, 159
- MachineCheckEnable, 159
- ManageabilityMode, 160
- MaxRingRatioLimit, 160
- MctpBroadcastCycle, 160
- MeUnconfigOnRtcClear, 160
- MinRingRatioLimit, 160
- MinVoltageC8, 160
- MinVoltageRuntime, 161
- MlcStreamerPrefetcher, 161
- MonitorMwaitEnable, 161
- NumOfDevIntConfig, 161
- NumberOfEntries, 161
- OneCoreRatioLimit, 162
- PchCrid, 162
- PchDmiAspmCtrl, 162
- PchDmiTsawEn, 162
- PchEnableComplianceMode, 162
- PchEnableDbcObs, 163
- PchEspHostC10ReportEnable, 163
- PchFivrDynPm, 163
- PchFivrExtVnnRailSxEnabledStates, 163
- PchFivrExtVnnRailSxIccMax, 163
- PchFivrExtVnnRailSxVoltage, 164
- PchFivrVccinAuxLowToHighCurModeVolTranTime, 164
- PchFivrVccinAuxOffToHighCurModeVolTranTime, 164
- PchFivrVccinAuxRetToHighCurModeVolTranTime, 164
- PchFivrVccinAuxRetToLowCurModeVolTranTime, 164
- PchHdaAudioLinkDmic0, 165
- PchHdaAudioLinkDmic1, 165
- PchHdaAudioLinkHda, 165
- PchHdaAudioLinkSndw1, 165
- PchHdaAudioLinkSndw2, 165
- PchHdaAudioLinkSndw3, 166
- PchHdaAudioLinkSndw4, 166
- PchHdaAudioLinkSsp0, 166
- PchHdaAudioLinkSsp1, 166
- PchHdaAudioLinkSsp2, 166
- PchHdaAudioLinkSsp3, 166
- PchHdaAudioLinkSsp4, 167
- PchHdaAudioLinkSsp5, 167
- PchHdaDspEnable, 167
- PchHdaDspUaaCompliance, 167
- PchHdaDispCodecDisconnect, 167
- PchHdaDispLinkFrequency, 168
- PchHdaLinkFrequency, 168
- PchHdaPme, 168
- PchHdaResetWaitTimer, 168
- PchHdaVcType, 168
- PchHotEnable, 169
- PchIoApicEntry24\_119, 169
- PchIoApicId, 169
- PchIshGp0GpioAssign, 169
- PchIshGp1GpioAssign, 169
- PchIshGp2GpioAssign, 169
- PchIshGp3GpioAssign, 170
- PchIshGp4GpioAssign, 170
- PchIshGp5GpioAssign, 170
- PchIshGp6GpioAssign, 170
- PchIshGp7GpioAssign, 170
- PchIshI2c0GpioAssign, 171
- PchIshI2c1GpioAssign, 171
- PchIshI2c2GpioAssign, 171
- PchIshPdtUnlock, 171
- PchIshSpiGpioAssign, 171
- PchIshUart0GpioAssign, 171
- PchIshUart1GpioAssign, 172
- PchLanEnable, 172
- PchLanLtrEnable, 172
- PchLockDownBiosInterface, 172
- PchLockDownBiosLock, 172
- PchLockDownGlobalSmi, 173
- PchLockDownRtcMemoryLock, 173
- PchMemoryThrottlingEnable, 173
- PchPmDeepSxPol, 173
- PchPmDisableDsxAcPresentPulldown, 173
- PchPmDisableEnergyReport, 174
- PchPmDisableNativePowerButton, 174
- PchPmLanWakeFromDeepSx, 174
- PchPmMeWakeSts, 174
- PchPmPciePllSsc, 174
- PchPmPcieWakeFromDeepSx, 174
- PchPmPmeB0S5Dis, 175
- PchPmPwrBtnOverridePeriod, 175
- PchPmPwrCycDur, 175
- PchPmS0i3Support, 175
- PchPmSlpAMinAssert, 175
- PchPmSlpLanLowDc, 176
- PchPmSlpS0Enable, 176
- PchPmSlpS3MinAssert, 176
- PchPmSlpS4MinAssert, 176
- PchPmSlpStrchSusUp, 176
- PchPmSlpSusMinAssert, 177
- PchPmVrAlert, 177
- PchPmWoWlanDeepSxEnable, 177
- PchPmWoWlanEnable, 177
- PchPmWoLEnableOverride, 177
- PchPmWoLOverWkSts, 177
- PchPwrOptEnable, 178
- PchSbAccessUnlock, 178
- PchScsEmmcHs400DIIIDataValid, 178
- PchSerialIoI2cPadsTermination, 178
- PchTTEnable, 178
- PchTTLock, 179
- PchTTState13Enable, 179
- PchUnlockGpioPads, 179
- PchXhciOclLock, 179
- PcieComplianceTestMode, 179
- PcieEnablePeerMemoryWrite, 180

- PcieEnablePort8xhDecode, 180
- PcieEqPh3LaneParamCm, 180
- PcieEqPh3LaneParamCp, 180
- PcieRpAspm, 180
- PcieRpCompletionTimeout, 181
- PcieRpDpcExtensionsMask, 181
- PcieRpDpcMask, 181
- PcieRpDptp, 181
- PcieRpFunctionSwap, 181
- PcieRpGen3EqPh3Method, 182
- PcieRpL1Substates, 182
- PcieRpPcieSpeed, 182
- PcieRpPhysicalSlotNumber, 182
- PcieRpPtmMask, 182
- PcieRpSlotPowerLimitScale, 183
- PcieRpSlotPowerLimitValue, 183
- PcieRpUptp, 183
- PcieSwEqCoeffListCm, 183
- PcieSwEqCoeffListCp, 183
- PkgCStateDemotion, 183
- PkgCStateLimit, 184
- PkgCStateUnDemotion, 184
- PmcCpuC10GatePinEnable, 184
- PmcCrashLogEnable, 184
- PmcDbgMsgEn, 184
- PmcModPhySusPgEnable, 185
- PmcPowerButtonDebounce, 185
- PmgCstCfgCtrlLock, 185
- PortUsb20Enable, 185
- PortUsb30Enable, 185
- PowerLimit1, 186
- PowerLimit1Time, 186
- PowerLimit2, 186
- PowerLimit2Power, 186
- PowerLimit3, 186
- PowerLimit4, 186
- PpinSupport, 187
- PreWake, 187
- ProcHotResponse, 188
- ProcessorTraceEnable, 187
- ProcessorTraceMemBase, 187
- ProcessorTraceMemLength, 187
- ProcessorTraceOutputScheme, 188
- PsOnEnable, 189
- Psi1Threshold, 188
- Psi2Threshold, 188
- Psi3Enable, 188
- Psi3Threshold, 189
- PsysOffset, 189
- PsysPmax, 189
- PsysPowerLimit1, 189
- PsysPowerLimit1Power, 190
- PsysPowerLimit2, 190
- PsysPowerLimit2Power, 190
- PsysSlope, 190
- PxRcConfig, 190
- RaceToHalt, 191
- RemoteAssistance, 191
- SaPcieComplianceTestMode, 191
- SaPcieDeviceOverrideTablePtr, 191
- SaPcieDisableRootPortClockGating, 191
- SaPcieEnablePeerMemoryWrite, 192
- SaPcieEqPh3LaneParamCm, 192
- SaPcieEqPh3LaneParamCp, 192
- SaPcieRpAspm, 192
- SaPcieRpDpcExtensionsMask, 192
- SaPcieRpDpcMask, 192
- SaPcieRpDptp, 193
- SaPcieRpFunctionSwap, 193
- SaPcieRpGen3EqPh3Method, 193
- SaPcieRpL1Substates, 193
- SaPcieRpPcieSpeed, 193
- SaPcieRpPhysicalSlotNumber, 194
- SaPcieRpPtmMask, 194
- SaPcieRpUptp, 194
- SataEnable, 194
- SataLedEnable, 194
- SataMode, 195
- SataP0TDispFinit, 195
- SataP1TDispFinit, 195
- SataPortsDevSlp, 195
- SataPortsDmVal, 195
- SataPortsEnable, 195
- SataPwrOptEnable, 196
- SataRstHddUnlock, 196
- SataRstInterrupt, 196
- SataRstLrrt, 196
- SataRstLrrtOnly, 196
- SataRstLedLocate, 197
- SataRstOromUiBanner, 197
- SataRstPcieDeviceResetDelay, 197
- SataRstRaid0, 197
- SataRstRaid1, 197
- SataRstRaid10, 198
- SataRstRaid5, 198
- SataRstRaidDeviceId, 198
- SataRstSmartStorage, 198
- SataSalpSupport, 198
- SataTestMode, 198
- SataThermalSuggestedSetting, 199
- ScilrqSelect, 199
- ScsEmmcEnabled, 199
- ScsEmmcHs400Enabled, 199
- ScsSdCardEnabled, 199
- SendEcCmd, 200
- SendVrMbxCmd, 200
- SerialIoDebugUartNumber, 200
- SerialIoI2cMode, 200
- SerialIoSpi0CsEnable, 200
- SerialIoSpi0CsPolarity, 201
- SerialIoSpi1CsEnable, 201
- SerialIoSpi1CsPolarity, 201
- SerialIoSpi2CsEnable, 201
- SerialIoSpi2CsPolarity, 201
- SerialIoSpiDefaultCsOutput, 201
- SerialIoSpiMode, 202

- SerialloUartCtsPinMux, 202
- SerialloUartDataBits, 202
- SerialloUartDmaEnable, 202
- SerialloUartMode, 202
- SerialloUartParity, 203
- SerialloUartPowerGating, 203
- SerialloUartRtsPinMux, 203
- SerialloUartRxPinMux, 203
- SerialloUartStopBits, 203
- SerialloUartTxPinMux, 204
- SiCsmFlag, 204
- SkipMplnit, 204
- SlowSlewRateForFivr, 204
- SlpS0DisQForDebug, 204
- SlpS0Override, 204
- StateRatio, 205
- StateRatioMax16, 205
- TStates, 208
- TTsuggestedSetting, 208
- TccActivationOffset, 205
- TccOffsetClamp, 205
- TccOffsetLock, 206
- TccOffsetTimeWindowForRatl, 206
- TcolrqSelect, 206
- TcssAuxOri, 206
- TcssHslOri, 206
- TcssLoopbackModeBitMap, 206
- TcssXhciEnableComplianceMode, 207
- TdcPowerLimit, 207
- TdcTimeWindow, 207
- ThreeStrikeCounterDisable, 207
- TimedMwait, 207
- TurboMode, 208
- TxtEnable, 208
- UfsEnable, 208
- Usb2PhyPehalfbit, 208
- Usb2PhyPetxiset, 209
- Usb2PhyPredeemp, 209
- Usb2PhyTxiset, 209
- Usb3HsioTxDeEmph, 209
- Usb3HsioTxDeEmphEnable, 209
- Usb3HsioTxDownscaleAmp, 210
- Usb3HsioTxDownscaleAmpEnable, 210
- UsbPdoProgramming, 210
- UsbTcPortEn, 210
- VmdEnable, 210
- VmdPortA, 211
- VmdPortB, 211
- VmdPortC, 211
- VmdPortD, 211
- VrVoltageLimit, 211
- WatchDog, 212
- WatchDogTimerBios, 212
- WatchDogTimerOs, 212
- XdciEnable, 212
- FSP\_S\_RESTRICTED\_CONFIG, 212
  - PchDmiTestClientObffEn, 218
  - PchDmiTestDmiSecureRegLock, 218
  - PchDmiTestExternalObffEn, 219
  - PchDmiTestInternalObffEn, 219
  - PchDmiTestMemCloseStateEn, 219
  - PchDmiTestOpiPIIPowerGating, 219
  - PchDmiTestPchTcLockDown, 219
  - PchHdaTestConfigLockdown, 220
  - PchHdaTestLowFreqLinkClkSrc, 220
  - PchHdaTestPowerClockGating, 220
  - PchLanTestPchWOLFastSupport, 220
  - PchLockDownTestSmiUnlock, 220
  - PchPmTestPchClearPowerSts, 221
  - PchTestClkGatingXhci, 221
  - PchTestPhlcLock, 221
  - PchTestTscLock, 221
  - PchTestTselLock, 221
  - PchTestUnlockUsbForSvNoa, 222
  - SaPcieAllowL0sWithGen3, 222
  - SataTestRstPcieStorageDeviceInterface, 222
  - SiSvPolicyEnable, 222
  - TestCnviBtWirelessCharging, 222
  - TestCnviLteCoex, 222
  - TestCnviSharedXtalClocking, 223
  - TestCnviWifiLtrEn, 223
  - TestPchPcieClockGating, 223
  - TestPchPmErDebugMode, 223
  - TestPchPmLatchEventsC10Exit, 223
  - TestPcieRpSrlEnable, 224
  - TestPmcDbgModeLock, 224
  - TestPmcSlpsxStrPolLock, 224
  - TestUsbXhciAccessControlLock, 224
- FSP\_T\_CONFIG, 225
  - PcdSerialloUartAutoFlow, 226
  - PcdSerialloUartCtsPinMux, 226
  - PcdSerialloUartDataBits, 226
  - PcdSerialloUartDebugEnabled, 226
  - PcdSerialloUartNumber, 226
  - PcdSerialloUartParity, 226
  - PcdSerialloUartRtsPinMux, 227
  - PcdSerialloUartStopBits, 227
- FSP\_T\_RESTRICTED\_CONFIG, 227
- FSPM\_UPD, 228
- FSPS\_UPD, 228
- FSPT\_CORE\_UPD, 229
- FSPT\_UPD, 230
- FastPkgCRampDisableFivr
  - FSP\_S\_CONFIG, 156
- FirmwareVersionInfoHob.h, 235
- FivrEfficiency
  - FSP\_M\_CONFIG, 73
- FivrFaults
  - FSP\_M\_CONFIG, 73
- FivrProtection
  - FSP\_M\_CONFIG, 74
- FivrPs
  - FSP\_M\_CONFIG, 74
- FivrRfiFrequency
  - FSP\_S\_CONFIG, 156
- FivrSpreadSpectrum

- FSP\_S\_CONFIG, 157
- FivrTdc
  - FSP\_M\_CONFIG, 74
- ForcMebxSyncUp
  - FSP\_S\_CONFIG, 157
- ForceOltmOrRefresh2x
  - FSP\_M\_CONFIG, 74
- FreqSaGvLow
  - FSP\_M\_CONFIG, 74
- FreqSaGvMid
  - FSP\_M\_CONFIG, 75
- FspFixedPcds.h, 236
- FspInfoHob.h, 236
- FspUpd.h, 242
- FspmUpd.h, 237
- FspsUpd.h, 238
  - SI\_PCH\_INT\_PIN, 240
- FsptUpd.h, 241
- FullRangeMultiplierUnlockEn
  - FSP\_M\_CONFIG, 75
- FwProgress
  - FSP\_S\_CONFIG, 157
- GPIO\_CONFIG, 231
  - Direction, 231
  - ElectricalConfig, 232
  - HostSoftPadOwn, 232
  - InterruptConfig, 232
  - LockConfig, 232
  - OutputState, 232
  - PadMode, 233
  - PowerConfig, 233
- GPIO\_DIRECTION
  - GpioConfig.h, 245
- GPIO\_ELECTRICAL\_CONFIG
  - GpioConfig.h, 245
- GPIO\_HARDWARE\_DEFAULT
  - GpioConfig.h, 246
- GPIO\_HOSTSW\_OWN
  - GpioConfig.h, 246
- GPIO\_INT\_CONFIG
  - GpioConfig.h, 247
- GPIO\_LOCK\_CONFIG
  - GpioConfig.h, 247
- GPIO\_OTHER\_CONFIG
  - GpioConfig.h, 248
- GPIO\_OUTPUT\_STATE
  - GpioConfig.h, 248
- GPIO\_PAD\_MODE
  - GpioConfig.h, 248
- GPIO\_RESET\_CONFIG
  - GpioConfig.h, 248
- Gen3SwEqAlwaysAttempt
  - FSP\_M\_CONFIG, 75
- Gen3SwEqEnableVocTest
  - FSP\_M\_CONFIG, 75
- Gen3SwEqJitterDwellTime
  - FSP\_M\_CONFIG, 75
- Gen3SwEqJitterErrorTarget
  - FSP\_M\_CONFIG, 76
- Gen3SwEqNumberOfPresets
  - FSP\_M\_CONFIG, 76
- Gen3SwEqVocDwellTime
  - FSP\_M\_CONFIG, 76
- Gen3SwEqVocErrorTarget
  - FSP\_M\_CONFIG, 76
- GmAdr
  - FSP\_M\_CONFIG, 76
- GpioConfig.h, 243
  - GPIO\_DIRECTION, 245
  - GPIO\_ELECTRICAL\_CONFIG, 245
  - GPIO\_HARDWARE\_DEFAULT, 246
  - GPIO\_HOSTSW\_OWN, 246
  - GPIO\_INT\_CONFIG, 247
  - GPIO\_LOCK\_CONFIG, 247
  - GPIO\_OTHER\_CONFIG, 248
  - GPIO\_OUTPUT\_STATE, 248
  - GPIO\_PAD\_MODE, 248
  - GPIO\_RESET\_CONFIG, 248
- GpioIrqRoute
  - FSP\_S\_CONFIG, 157
- GpioSampleDef.h, 250
- GtPllVoltageOffset
  - FSP\_M\_CONFIG, 77
- GtPsmiSupport
  - FSP\_M\_CONFIG, 77
- GttMmAdr
  - FSP\_M\_CONFIG, 77
- HdcControl
  - FSP\_S\_CONFIG, 157
- Heci3Enabled
  - FSP\_S\_CONFIG, 158
- HeciCommunication
  - FSP\_M\_RESTRICTED\_CONFIG, 112
- HeciCommunication2
  - FSP\_M\_CONFIG, 77
- HeciCommunication3
  - FSP\_M\_RESTRICTED\_CONFIG, 112
- HobBufferSize
  - FSP\_M\_CONFIG, 78
- HostSoftPadOwn
  - GPIO\_CONFIG, 232
- HotThresholdCh0Dimm0
  - FSP\_M\_CONFIG, 78
- HotThresholdCh0Dimm1
  - FSP\_M\_CONFIG, 78
- HotThresholdCh1Dimm0
  - FSP\_M\_CONFIG, 78
- HotThresholdCh1Dimm1
  - FSP\_M\_CONFIG, 78
- Hwp
  - FSP\_S\_CONFIG, 158
- HwpInterruptControl
  - FSP\_S\_CONFIG, 158
- ITbtConnectTopologyTimeoutInMs
  - FSP\_S\_CONFIG, 159

- ITbtForcePowerOnTimeoutInMs
  - FSP\_S\_CONFIG, 159
- IccMax
  - FSP\_S\_CONFIG, 158
- Idd3n
  - FSP\_M\_CONFIG, 78
- Idd3p
  - FSP\_M\_CONFIG, 79
- IgdDvmt50PreAlloc
  - FSP\_M\_CONFIG, 79
- ImguClkOutEn
  - FSP\_M\_CONFIG, 79
- ImonOffset
  - FSP\_S\_CONFIG, 158
- ImonSlope
  - FSP\_S\_CONFIG, 159
- ImrRpSelection
  - FSP\_M\_CONFIG, 79
- InitPcieAspmAfterOprom
  - FSP\_M\_CONFIG, 79
- InternalGfx
  - FSP\_M\_CONFIG, 80
- InterruptConfig
  - GPIO\_CONFIG, 232
- IomTypeCPortPadCfg
  - FSP\_S\_CONFIG, 159
- IsvtIoPort
  - FSP\_M\_CONFIG, 80
- JtagC10PowerGateDisable
  - FSP\_M\_CONFIG, 80
- KtDeviceEnable
  - FSP\_M\_CONFIG, 80
- LockConfig
  - GPIO\_CONFIG, 232
- LockPTMregs
  - FSP\_M\_CONFIG, 80
- LowMemChannel
  - FSP\_M\_RESTRICTED\_CONFIG, 113
- MachineCheckEnable
  - FSP\_S\_CONFIG, 159
- ManageabilityMode
  - FSP\_S\_CONFIG, 160
- MarginLimitCheck
  - FSP\_M\_CONFIG, 81
- MaxRingRatioLimit
  - FSP\_S\_CONFIG, 160
- McPllVoltageOffset
  - FSP\_M\_CONFIG, 81
- MctpBroadcastCycle
  - FSP\_S\_CONFIG, 160
- MeUnconfigOnRtcClear
  - FSP\_S\_CONFIG, 160
- MemoryTrace
  - FSP\_M\_CONFIG, 81
- MinRingRatioLimit
  - FSP\_S\_CONFIG, 160
- MinVoltageC8
  - FSP\_S\_CONFIG, 160
- MinVoltageRuntime
  - FSP\_S\_CONFIG, 161
- MlcStreamerPrefetcher
  - FSP\_S\_CONFIG, 161
- MmioSize
  - FSP\_M\_CONFIG, 81
- MonitorMwaitEnable
  - FSP\_S\_CONFIG, 161
- MsegSize
  - FSP\_M\_RESTRICTED\_CONFIG, 113
- NonCoreHighVoltageMode
  - FSP\_M\_CONFIG, 81
- NumOfDevIntConfig
  - FSP\_S\_CONFIG, 161
- NumberOfEntries
  - FSP\_S\_CONFIG, 161
- OcLock
  - FSP\_M\_CONFIG, 81
- OneCoreRatioLimit
  - FSP\_S\_CONFIG, 162
- OutputState
  - GPIO\_CONFIG, 232
- PadMode
  - GPIO\_CONFIG, 233
- PanelPowerEnable
  - FSP\_M\_CONFIG, 82
- PcdDebugInterfaceFlags
  - FSP\_M\_CONFIG, 82
- PcdIsaSerialUartBase
  - FSP\_M\_CONFIG, 82
- PcdSerialDebugBaudRate
  - FSP\_M\_CONFIG, 82
- PcdSerialDebugLevel
  - FSP\_M\_CONFIG, 82
- PcdSerialIoUartAutoFlow
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartCtsPinMux
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartDataBits
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartDebugEnable
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartNumber
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartParity
  - FSP\_T\_CONFIG, 226
- PcdSerialIoUartRtsPinMux
  - FSP\_T\_CONFIG, 227
- PcdSerialIoUartStopBits
  - FSP\_T\_CONFIG, 227
- PchCrid
  - FSP\_S\_CONFIG, 162
- PchDmiAspmCtrl

- FSP\_S\_CONFIG, 162
- PchDmiTestClientObffEn
  - FSP\_S\_RESTRICTED\_CONFIG, 218
- PchDmiTestDmiSecureRegLock
  - FSP\_S\_RESTRICTED\_CONFIG, 218
- PchDmiTestExternalObffEn
  - FSP\_S\_RESTRICTED\_CONFIG, 219
- PchDmiTestInternalObffEn
  - FSP\_S\_RESTRICTED\_CONFIG, 219
- PchDmiTestMemCloseStateEn
  - FSP\_S\_RESTRICTED\_CONFIG, 219
- PchDmiTestOpiPllPowerGating
  - FSP\_S\_RESTRICTED\_CONFIG, 219
- PchDmiTestPchTcLockDown
  - FSP\_S\_RESTRICTED\_CONFIG, 219
- PchDmiTsawEn
  - FSP\_S\_CONFIG, 162
- PchEnableComplianceMode
  - FSP\_S\_CONFIG, 162
- PchEnableDbcObs
  - FSP\_S\_CONFIG, 163
- PchEspHostC10ReportEnable
  - FSP\_S\_CONFIG, 163
- PchFivrDynPm
  - FSP\_S\_CONFIG, 163
- PchFivrExtVnnRailSxEnabledStates
  - FSP\_S\_CONFIG, 163
- PchFivrExtVnnRailSxLccMax
  - FSP\_S\_CONFIG, 163
- PchFivrExtVnnRailSxVoltage
  - FSP\_S\_CONFIG, 164
- PchFivrVccinAuxLowToHighCurModeVolTranTime
  - FSP\_S\_CONFIG, 164
- PchFivrVccinAuxOffToHighCurModeVolTranTime
  - FSP\_S\_CONFIG, 164
- PchFivrVccinAuxRetToHighCurModeVolTranTime
  - FSP\_S\_CONFIG, 164
- PchFivrVccinAuxRetToLowCurModeVolTranTime
  - FSP\_S\_CONFIG, 164
- PchHdaAudioLinkDmic0
  - FSP\_S\_CONFIG, 165
- PchHdaAudioLinkDmic1
  - FSP\_S\_CONFIG, 165
- PchHdaAudioLinkHda
  - FSP\_S\_CONFIG, 165
- PchHdaAudioLinkSndw1
  - FSP\_S\_CONFIG, 165
- PchHdaAudioLinkSndw2
  - FSP\_S\_CONFIG, 165
- PchHdaAudioLinkSndw3
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSndw4
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSsp0
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSsp1
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSsp2
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSsp3
  - FSP\_S\_CONFIG, 166
- PchHdaAudioLinkSsp4
  - FSP\_S\_CONFIG, 167
- PchHdaAudioLinkSsp5
  - FSP\_S\_CONFIG, 167
- PchHdaDspEnable
  - FSP\_S\_CONFIG, 167
- PchHdaDspUaaCompliance
  - FSP\_S\_CONFIG, 167
- PchHdaDispCodecDisconnect
  - FSP\_S\_CONFIG, 167
- PchHdaDispLinkFrequency
  - FSP\_S\_CONFIG, 168
- PchHdaLinkFrequency
  - FSP\_S\_CONFIG, 168
- PchHdaPme
  - FSP\_S\_CONFIG, 168
- PchHdaResetWaitTimer
  - FSP\_S\_CONFIG, 168
- PchHdaTestConfigLockdown
  - FSP\_S\_RESTRICTED\_CONFIG, 220
- PchHdaTestLowFreqLinkClkSrc
  - FSP\_S\_RESTRICTED\_CONFIG, 220
- PchHdaTestPowerClockGating
  - FSP\_S\_RESTRICTED\_CONFIG, 220
- PchHdaVcType
  - FSP\_S\_CONFIG, 168
- PchHotEnable
  - FSP\_S\_CONFIG, 169
- PchIoApicEntry24\_119
  - FSP\_S\_CONFIG, 169
- PchIoApicId
  - FSP\_S\_CONFIG, 169
- PchIshGp0GpioAssign
  - FSP\_S\_CONFIG, 169
- PchIshGp1GpioAssign
  - FSP\_S\_CONFIG, 169
- PchIshGp2GpioAssign
  - FSP\_S\_CONFIG, 169
- PchIshGp3GpioAssign
  - FSP\_S\_CONFIG, 170
- PchIshGp4GpioAssign
  - FSP\_S\_CONFIG, 170
- PchIshGp5GpioAssign
  - FSP\_S\_CONFIG, 170
- PchIshGp6GpioAssign
  - FSP\_S\_CONFIG, 170
- PchIshGp7GpioAssign
  - FSP\_S\_CONFIG, 170
- PchIshI2c0GpioAssign
  - FSP\_S\_CONFIG, 171
- PchIshI2c1GpioAssign
  - FSP\_S\_CONFIG, 171
- PchIshI2c2GpioAssign
  - FSP\_S\_CONFIG, 171
- PchIshPdtUnlock

- FSP\_S\_CONFIG, 171
- PchIshSpiGpioAssign
  - FSP\_S\_CONFIG, 171
- PchIshUart0GpioAssign
  - FSP\_S\_CONFIG, 171
- PchIshUart1GpioAssign
  - FSP\_S\_CONFIG, 172
- PchLanEnable
  - FSP\_S\_CONFIG, 172
- PchLanLtrEnable
  - FSP\_S\_CONFIG, 172
- PchLanTestPchWOLFastSupport
  - FSP\_S\_RESTRICTED\_CONFIG, 220
- PchLockDownBiosInterface
  - FSP\_S\_CONFIG, 172
- PchLockDownBiosLock
  - FSP\_S\_CONFIG, 172
- PchLockDownGlobalSmi
  - FSP\_S\_CONFIG, 173
- PchLockDownRtcMemoryLock
  - FSP\_S\_CONFIG, 173
- PchLockDownTestSmiUnlock
  - FSP\_S\_RESTRICTED\_CONFIG, 220
- PchLpcEnhancePort8xhDecoding
  - FSP\_M\_CONFIG, 83
- PchMemoryThrottlingEnable
  - FSP\_S\_CONFIG, 173
- PchNumRsvdSmbusAddresses
  - FSP\_M\_CONFIG, 83
- PchPmDeepSxPol
  - FSP\_S\_CONFIG, 173
- PchPmDisableDsxAcPresentPulldown
  - FSP\_S\_CONFIG, 173
- PchPmDisableEnergyReport
  - FSP\_S\_CONFIG, 174
- PchPmDisableNativePowerButton
  - FSP\_S\_CONFIG, 174
- PchPmLanWakeFromDeepSx
  - FSP\_S\_CONFIG, 174
- PchPmMeWakeSts
  - FSP\_S\_CONFIG, 174
- PchPmPciePIISsc
  - FSP\_S\_CONFIG, 174
- PchPmPcieWakeFromDeepSx
  - FSP\_S\_CONFIG, 174
- PchPmPmeB0S5Dis
  - FSP\_S\_CONFIG, 175
- PchPmPwrBtnOverridePeriod
  - FSP\_S\_CONFIG, 175
- PchPmPwrCycDur
  - FSP\_S\_CONFIG, 175
- PchPmS0i3Support
  - FSP\_S\_CONFIG, 175
- PchPmSlpAMinAssert
  - FSP\_S\_CONFIG, 175
- PchPmSlpLanLowDc
  - FSP\_S\_CONFIG, 176
- PchPmSlpS0Enable
  - FSP\_S\_CONFIG, 176
- PchPmSlpS3MinAssert
  - FSP\_S\_CONFIG, 176
- PchPmSlpS4MinAssert
  - FSP\_S\_CONFIG, 176
- PchPmSlpStrchSusUp
  - FSP\_S\_CONFIG, 176
- PchPmSlpSusMinAssert
  - FSP\_S\_CONFIG, 177
- PchPmTestPchClearPowerSts
  - FSP\_S\_RESTRICTED\_CONFIG, 221
- PchPmVrAlert
  - FSP\_S\_CONFIG, 177
- PchPmWoWlanDeepSxEnable
  - FSP\_S\_CONFIG, 177
- PchPmWoWlanEnable
  - FSP\_S\_CONFIG, 177
- PchPmWolEnableOverride
  - FSP\_S\_CONFIG, 177
- PchPmWolOvrWkSts
  - FSP\_S\_CONFIG, 177
- PchPort80Route
  - FSP\_M\_CONFIG, 83
- PchPwrOptEnable
  - FSP\_S\_CONFIG, 178
- PchSbAccessUnlock
  - FSP\_S\_CONFIG, 178
- PchScsEmmcHs400DIIDataValid
  - FSP\_S\_CONFIG, 178
- PchSerialIoI2cPadsTermination
  - FSP\_S\_CONFIG, 178
- PchSmbAlertEnable
  - FSP\_M\_CONFIG, 83
- PchTTEnable
  - FSP\_S\_CONFIG, 178
- PchTTLock
  - FSP\_S\_CONFIG, 179
- PchTTState13Enable
  - FSP\_S\_CONFIG, 179
- PchTestClkGatingXhci
  - FSP\_S\_RESTRICTED\_CONFIG, 221
- PchTestDmiMeUmaRootSpaceCheck
  - FSP\_M\_RESTRICTED\_CONFIG, 113
- PchTestPhlcLock
  - FSP\_S\_RESTRICTED\_CONFIG, 221
- PchTestTscLock
  - FSP\_S\_RESTRICTED\_CONFIG, 221
- PchTestTselLock
  - FSP\_S\_RESTRICTED\_CONFIG, 221
- PchTestUnlockUsbForSvNoa
  - FSP\_S\_RESTRICTED\_CONFIG, 222
- PchTraceHubMemReg0Size
  - FSP\_M\_CONFIG, 83
- PchTraceHubMemReg1Size
  - FSP\_M\_CONFIG, 84
- PchTraceHubMode
  - FSP\_M\_CONFIG, 84
- PchUnlockGpioPads

- FSP\_S\_CONFIG, 179
- PchXhciOcLock
  - FSP\_S\_CONFIG, 179
- PcieComplianceTestMode
  - FSP\_S\_CONFIG, 179
- PcieEnablePeerMemoryWrite
  - FSP\_S\_CONFIG, 180
- PcieEnablePort8xhDecode
  - FSP\_S\_CONFIG, 180
- PcieEqPh3LaneParamCm
  - FSP\_S\_CONFIG, 180
- PcieEqPh3LaneParamCp
  - FSP\_S\_CONFIG, 180
- PcieImrSize
  - FSP\_M\_CONFIG, 84
- PcieMultipleSegmentEnabled
  - FSP\_M\_CONFIG, 84
- PcieRpAspm
  - FSP\_S\_CONFIG, 180
- PcieRpCompletionTimeout
  - FSP\_S\_CONFIG, 181
- PcieRpDpcExtensionsMask
  - FSP\_S\_CONFIG, 181
- PcieRpDpcMask
  - FSP\_S\_CONFIG, 181
- PcieRpDptp
  - FSP\_S\_CONFIG, 181
- PcieRpEnableMask
  - FSP\_M\_CONFIG, 84
- PcieRpFunctionSwap
  - FSP\_S\_CONFIG, 181
- PcieRpGen3EqPh3Method
  - FSP\_S\_CONFIG, 182
- PcieRpL1Substates
  - FSP\_S\_CONFIG, 182
- PcieRpPcieSpeed
  - FSP\_S\_CONFIG, 182
- PcieRpPhysicalSlotNumber
  - FSP\_S\_CONFIG, 182
- PcieRpPtmMask
  - FSP\_S\_CONFIG, 182
- PcieRpSlotPowerLimitScale
  - FSP\_S\_CONFIG, 183
- PcieRpSlotPowerLimitValue
  - FSP\_S\_CONFIG, 183
- PcieRpUptp
  - FSP\_S\_CONFIG, 183
- PcieSwEqCoeffListCm
  - FSP\_S\_CONFIG, 183
- PcieSwEqCoeffListCp
  - FSP\_S\_CONFIG, 183
- PcuDdrVoltage
  - FSP\_M\_RESTRICTED\_CONFIG, 113
- Peg0Gen3EqPh2Enable
  - FSP\_M\_CONFIG, 85
- Peg0Gen3EqPh3Method
  - FSP\_M\_CONFIG, 85
- Peg1Gen3EqPh2Enable
  - FSP\_M\_CONFIG, 85
- Peg1Gen3EqPh3Method
  - FSP\_M\_CONFIG, 85
- Peg2Gen3EqPh2Enable
  - FSP\_M\_CONFIG, 85
- Peg2Gen3EqPh3Method
  - FSP\_M\_CONFIG, 86
- Peg3Gen3EqPh2Enable
  - FSP\_M\_CONFIG, 86
- Peg3Gen3EqPh3Method
  - FSP\_M\_CONFIG, 86
- PegDataPtr
  - FSP\_M\_CONFIG, 86
- PegDisableSpreadSpectrumClocking
  - FSP\_M\_CONFIG, 87
- PegGen3EndPointHint
  - FSP\_M\_CONFIG, 87
- PegGen3EndPointPreset
  - FSP\_M\_CONFIG, 87
- PegGen3ProgramStaticEq
  - FSP\_M\_CONFIG, 87
- PegGen3RootPortPreset
  - FSP\_M\_CONFIG, 87
- PegGenerateBdatMarginTable
  - FSP\_M\_CONFIG, 88
- PegImrEnable
  - FSP\_M\_CONFIG, 88
- PegImrRpSelection
  - FSP\_M\_CONFIG, 88
- PegRxCemLoopbackLane
  - FSP\_M\_CONFIG, 88
- PegRxCemNonProtocolAwareness
  - FSP\_M\_CONFIG, 88
- PerCoreRatioLimit
  - FSP\_M\_CONFIG, 89
- PkgCStateDemotion
  - FSP\_S\_CONFIG, 183
- PkgCStateLimit
  - FSP\_S\_CONFIG, 184
- PkgCStateUnDemotion
  - FSP\_S\_CONFIG, 184
- PlatformDebugConsent
  - FSP\_M\_CONFIG, 89
- PmcCpuC10GatePinEnable
  - FSP\_S\_CONFIG, 184
- PmcCrashLogEnable
  - FSP\_S\_CONFIG, 184
- PmcDbgMsgEn
  - FSP\_S\_CONFIG, 184
- PmcModPhySusPgEnable
  - FSP\_S\_CONFIG, 185
- PmcPowerButtonDebounce
  - FSP\_S\_CONFIG, 185
- PmgCstCfgCtrlLock
  - FSP\_S\_CONFIG, 185
- PortUsb20Enable
  - FSP\_S\_CONFIG, 185
- PortUsb30Enable

- FSP\_S\_CONFIG, 185
- PowerConfig
  - GPIO\_CONFIG, 233
- PowerLimit1
  - FSP\_S\_CONFIG, 186
- PowerLimit1Time
  - FSP\_S\_CONFIG, 186
- PowerLimit2
  - FSP\_S\_CONFIG, 186
- PowerLimit2Power
  - FSP\_S\_CONFIG, 186
- PowerLimit3
  - FSP\_S\_CONFIG, 186
- PowerLimit4
  - FSP\_S\_CONFIG, 186
- PpinSupport
  - FSP\_S\_CONFIG, 187
- PreWake
  - FSP\_S\_CONFIG, 187
- PrmrrSize
  - FSP\_M\_CONFIG, 89
- ProbelessTrace
  - FSP\_M\_CONFIG, 89
- ProcHotResponse
  - FSP\_S\_CONFIG, 188
- ProcessorTraceEnable
  - FSP\_S\_CONFIG, 187
- ProcessorTraceMemBase
  - FSP\_S\_CONFIG, 187
- ProcessorTraceMemLength
  - FSP\_S\_CONFIG, 187
- ProcessorTraceOutputScheme
  - FSP\_S\_CONFIG, 188
- PsOnEnable
  - FSP\_S\_CONFIG, 189
- Psi1Threshold
  - FSP\_S\_CONFIG, 188
- Psi2Threshold
  - FSP\_S\_CONFIG, 188
- Psi3Enable
  - FSP\_S\_CONFIG, 188
- Psi3Threshold
  - FSP\_S\_CONFIG, 189
- PsysOffset
  - FSP\_S\_CONFIG, 189
- PsysPmax
  - FSP\_S\_CONFIG, 189
- PsysPowerLimit1
  - FSP\_S\_CONFIG, 189
- PsysPowerLimit1Power
  - FSP\_S\_CONFIG, 190
- PsysPowerLimit2
  - FSP\_S\_CONFIG, 190
- PsysPowerLimit2Power
  - FSP\_S\_CONFIG, 190
- PsysSlope
  - FSP\_S\_CONFIG, 190
- PvdRatioThreshold
  - FSP\_M\_CONFIG, 89
- PwdnIdleCounter
  - FSP\_M\_CONFIG, 90
- PxRcConfig
  - FSP\_S\_CONFIG, 190
- RMTBIT
  - FSP\_M\_CONFIG, 92
- RMTLoopCount
  - FSP\_M\_CONFIG, 93
- RMT
  - FSP\_M\_CONFIG, 92
- RaceToHalt
  - FSP\_S\_CONFIG, 191
- RankInterleave
  - FSP\_M\_CONFIG, 90
- Ratio
  - FSP\_M\_CONFIG, 90
- RealtimeMemoryTiming
  - FSP\_M\_CONFIG, 90
- RefClk
  - FSP\_M\_CONFIG, 90
- RemoteAssistance
  - FSP\_S\_CONFIG, 191
- RetrainOnFastFail
  - FSP\_M\_CONFIG, 90
- RhSolution
  - FSP\_M\_CONFIG, 91
- RingDownBin
  - FSP\_M\_CONFIG, 91
- RingMaxOcRatio
  - FSP\_M\_CONFIG, 91
- RingPIIVoltageOffset
  - FSP\_M\_CONFIG, 91
- RingVoltageAdaptive
  - FSP\_M\_CONFIG, 91
- RingVoltageMode
  - FSP\_M\_CONFIG, 92
- RingVoltageOffset
  - FSP\_M\_CONFIG, 92
- RingVoltageOverride
  - FSP\_M\_CONFIG, 92
- RmtPerTask
  - FSP\_M\_CONFIG, 93
- SI\_PCH\_DEVICE\_INTERRUPT\_CONFIG, 233
- SI\_PCH\_INT\_PIN
  - FspsUpd.h, 240
- SMBIOS\_STRUCTURE, 234
- SaGv
  - FSP\_M\_CONFIG, 93
- SaPcieAllowL0sWithGen3
  - FSP\_S\_RESTRICTED\_CONFIG, 222
- SaPcieComplianceTestMode
  - FSP\_S\_CONFIG, 191
- SaPcieDeviceOverrideTablePtr
  - FSP\_S\_CONFIG, 191
- SaPcieDisableRootPortClockGating
  - FSP\_S\_CONFIG, 191

- SaPcieEnablePeerMemoryWrite
    - FSP\_S\_CONFIG, 192
  - SaPcieEqPh3LaneParamCm
    - FSP\_S\_CONFIG, 192
  - SaPcieEqPh3LaneParamCp
    - FSP\_S\_CONFIG, 192
  - SaPcieRpAspm
    - FSP\_S\_CONFIG, 192
  - SaPcieRpDpcExtensionsMask
    - FSP\_S\_CONFIG, 192
  - SaPcieRpDpcMask
    - FSP\_S\_CONFIG, 192
  - SaPcieRpDptp
    - FSP\_S\_CONFIG, 193
  - SaPcieRpEnableMask
    - FSP\_M\_CONFIG, 93
  - SaPcieRpFunctionSwap
    - FSP\_S\_CONFIG, 193
  - SaPcieRpGen3EqPh3Method
    - FSP\_S\_CONFIG, 193
  - SaPcieRpL1Substates
    - FSP\_S\_CONFIG, 193
  - SaPcieRpLinkDownGpios
    - FSP\_M\_CONFIG, 93
  - SaPcieRpPcieSpeed
    - FSP\_S\_CONFIG, 193
  - SaPcieRpPhysicalSlotNumber
    - FSP\_S\_CONFIG, 194
  - SaPcieRpPtmMask
    - FSP\_S\_CONFIG, 194
  - SaPcieRpUptp
    - FSP\_S\_CONFIG, 194
  - SaPllFreqOverride
    - FSP\_M\_CONFIG, 94
  - SaPllVoltageOffset
    - FSP\_M\_CONFIG, 94
  - SafeMode
    - FSP\_M\_CONFIG, 93
  - SataEnable
    - FSP\_S\_CONFIG, 194
  - SataLedEnable
    - FSP\_S\_CONFIG, 194
  - SataMode
    - FSP\_S\_CONFIG, 195
  - SataP0TDispFinit
    - FSP\_S\_CONFIG, 195
  - SataP1TDispFinit
    - FSP\_S\_CONFIG, 195
  - SataPortsDevSlp
    - FSP\_S\_CONFIG, 195
  - SataPortsDmVal
    - FSP\_S\_CONFIG, 195
  - SataPortsEnable
    - FSP\_S\_CONFIG, 195
  - SataPwrOptEnable
    - FSP\_S\_CONFIG, 196
  - SataRstHddUnlock
    - FSP\_S\_CONFIG, 196
  - SataRstInterrupt
    - FSP\_S\_CONFIG, 196
  - SataRstIrrt
    - FSP\_S\_CONFIG, 196
  - SataRstIrrtOnly
    - FSP\_S\_CONFIG, 196
  - SataRstLedLocate
    - FSP\_S\_CONFIG, 197
  - SataRstOromUiBanner
    - FSP\_S\_CONFIG, 197
  - SataRstPcieDeviceResetDelay
    - FSP\_S\_CONFIG, 197
  - SataRstRaid0
    - FSP\_S\_CONFIG, 197
  - SataRstRaid1
    - FSP\_S\_CONFIG, 197
  - SataRstRaid10
    - FSP\_S\_CONFIG, 198
  - SataRstRaid5
    - FSP\_S\_CONFIG, 198
  - SataRstRaidDeviceId
    - FSP\_S\_CONFIG, 198
  - SataRstSmartStorage
    - FSP\_S\_CONFIG, 198
  - SataSalpSupport
    - FSP\_S\_CONFIG, 198
  - SataTestMode
    - FSP\_S\_CONFIG, 198
  - SataTestRstPcieStorageDeviceInterface
    - FSP\_S\_RESTRICTED\_CONFIG, 222
  - SataThermalSuggestedSetting
    - FSP\_S\_CONFIG, 199
  - ScanExtGfxForLegacyOpRom
    - FSP\_M\_CONFIG, 94
  - ScilrqSelect
    - FSP\_S\_CONFIG, 199
  - ScramblerSupport
    - FSP\_M\_CONFIG, 94
  - ScsEmmcEnabled
    - FSP\_S\_CONFIG, 199
  - ScsEmmcHs400Enabled
    - FSP\_S\_CONFIG, 199
  - ScsSdCardEnabled
    - FSP\_S\_CONFIG, 199
  - SendEcCmd
    - FSP\_S\_CONFIG, 200
  - SendVrMbxCmd
    - FSP\_S\_CONFIG, 200
  - SerialloDebugUartNumber
    - FSP\_S\_CONFIG, 200
  - SerialloI2cMode
    - FSP\_S\_CONFIG, 200
  - SerialloSpi0CsEnable
    - FSP\_S\_CONFIG, 200
  - SerialloSpi0CsPolarity
    - FSP\_S\_CONFIG, 201
  - SerialloSpi1CsEnable
    - FSP\_S\_CONFIG, 201
-

- SerialloSpi1CsPolarity
  - FSP\_S\_CONFIG, 201
- SerialloSpi2CsEnable
  - FSP\_S\_CONFIG, 201
- SerialloSpi2CsPolarity
  - FSP\_S\_CONFIG, 201
- SerialloSpiDefaultCsOutput
  - FSP\_S\_CONFIG, 201
- SerialloSpiMode
  - FSP\_S\_CONFIG, 202
- SerialloUartCtsPinMux
  - FSP\_S\_CONFIG, 202
- SerialloUartDataBits
  - FSP\_S\_CONFIG, 202
- SerialloUartDebugAutoFlow
  - FSP\_M\_CONFIG, 94
- SerialloUartDebugBaudRate
  - FSP\_M\_CONFIG, 95
- SerialloUartDebugControllerNumber
  - FSP\_M\_CONFIG, 95
- SerialloUartDebugDataBits
  - FSP\_M\_CONFIG, 95
- SerialloUartDebugParity
  - FSP\_M\_CONFIG, 95
- SerialloUartDebugStopBits
  - FSP\_M\_CONFIG, 95
- SerialloUartDmaEnable
  - FSP\_S\_CONFIG, 202
- SerialloUartMode
  - FSP\_S\_CONFIG, 202
- SerialloUartParity
  - FSP\_S\_CONFIG, 203
- SerialloUartPowerGating
  - FSP\_S\_CONFIG, 203
- SerialloUartRtsPinMux
  - FSP\_S\_CONFIG, 203
- SerialloUartRxPinMux
  - FSP\_S\_CONFIG, 203
- SerialloUartStopBits
  - FSP\_S\_CONFIG, 203
- SerialloUartTxPinMux
  - FSP\_S\_CONFIG, 204
- SiCsmFlag
  - FSP\_S\_CONFIG, 204
- SiSvPolicyEnable
  - FSP\_S\_RESTRICTED\_CONFIG, 222
- SinitMemorySize
  - FSP\_M\_CONFIG, 96
- SkipMbpHob
  - FSP\_M\_CONFIG, 96
- SkipMpInit
  - FSP\_S\_CONFIG, 204
- SkipMpInitPreMem
  - FSP\_M\_CONFIG, 96
- SlowSlewRateForFivr
  - FSP\_S\_CONFIG, 204
- SlpS0DisQForDebug
  - FSP\_S\_CONFIG, 204
- SlpS0Override
  - FSP\_S\_CONFIG, 204
- SmbusArpEnable
  - FSP\_M\_CONFIG, 96
- SmbusDynamicPowerGating
  - FSP\_M\_CONFIG, 96
- SmbusEnable
  - FSP\_M\_CONFIG, 97
- SmbusSpdWriteDisable
  - FSP\_M\_CONFIG, 97
- SpdAddressTable
  - FSP\_M\_CONFIG, 97
- SpdProfileSelected
  - FSP\_M\_CONFIG, 97
- StateRatio
  - FSP\_S\_CONFIG, 205
- StateRatioMax16
  - FSP\_S\_CONFIG, 205
- tRRDD
  - FSP\_M\_RESTRICTED\_CONFIG, 114
- tRRDG
  - FSP\_M\_RESTRICTED\_CONFIG, 114
- tRRDR
  - FSP\_M\_RESTRICTED\_CONFIG, 114
- tRRSG
  - FSP\_M\_RESTRICTED\_CONFIG, 114
- tRTP
  - FSP\_M\_CONFIG, 100
- tRWDD
  - FSP\_M\_RESTRICTED\_CONFIG, 114
- tRWDG
  - FSP\_M\_RESTRICTED\_CONFIG, 115
- tRWDR
  - FSP\_M\_RESTRICTED\_CONFIG, 115
- tRWSG
  - FSP\_M\_RESTRICTED\_CONFIG, 115
- TStates
  - FSP\_S\_CONFIG, 208
- TTSuggestedSetting
  - FSP\_S\_CONFIG, 208
- tWRDD
  - FSP\_M\_RESTRICTED\_CONFIG, 115
- tWRDG
  - FSP\_M\_RESTRICTED\_CONFIG, 115
- tWRDR
  - FSP\_M\_RESTRICTED\_CONFIG, 116
- tWRSG
  - FSP\_M\_RESTRICTED\_CONFIG, 116
- tWWDD
  - FSP\_M\_RESTRICTED\_CONFIG, 116
- tWWDG
  - FSP\_M\_RESTRICTED\_CONFIG, 116
- tWWDR
  - FSP\_M\_RESTRICTED\_CONFIG, 116
- tWWSG
  - FSP\_M\_RESTRICTED\_CONFIG, 117
- TccActivationOffset
  - FSP\_S\_CONFIG, 205

- TccOffsetClamp
  - FSP\_S\_CONFIG, 205
- TccOffsetLock
  - FSP\_S\_CONFIG, 206
- TccOffsetTimeWindowForRatl
  - FSP\_S\_CONFIG, 206
- TcolrqSelect
  - FSP\_S\_CONFIG, 206
- TcssAuxOri
  - FSP\_S\_CONFIG, 206
- TcssDma0En
  - FSP\_M\_CONFIG, 97
- TcssDma1En
  - FSP\_M\_CONFIG, 97
- TcssHslOri
  - FSP\_S\_CONFIG, 206
- TcsslbtPcie0En
  - FSP\_M\_CONFIG, 98
- TcsslbtPcie1En
  - FSP\_M\_CONFIG, 98
- TcsslbtPcie2En
  - FSP\_M\_CONFIG, 98
- TcsslbtPcie3En
  - FSP\_M\_CONFIG, 98
- TcssLoopbackModeBitMap
  - FSP\_S\_CONFIG, 206
- TcssXdcIEn
  - FSP\_M\_CONFIG, 98
- TcssXhciEn
  - FSP\_M\_CONFIG, 99
- TcssXhciEnableComplianceMode
  - FSP\_S\_CONFIG, 207
- TdcPowerLimit
  - FSP\_S\_CONFIG, 207
- TdcTimeWindow
  - FSP\_S\_CONFIG, 207
- TestCnviBtWirelessCharging
  - FSP\_S\_RESTRICTED\_CONFIG, 222
- TestCnviLteCoex
  - FSP\_S\_RESTRICTED\_CONFIG, 222
- TestCnviSharedXtalClocking
  - FSP\_S\_RESTRICTED\_CONFIG, 223
- TestCnviWifiLtrEn
  - FSP\_S\_RESTRICTED\_CONFIG, 223
- TestMenuDprLock
  - FSP\_M\_RESTRICTED\_CONFIG, 113
- TestPchPcieClockGating
  - FSP\_S\_RESTRICTED\_CONFIG, 223
- TestPchPmErDebugMode
  - FSP\_S\_RESTRICTED\_CONFIG, 223
- TestPchPmLatchEventsC10Exit
  - FSP\_S\_RESTRICTED\_CONFIG, 223
- TestPcieRpSriEnable
  - FSP\_S\_RESTRICTED\_CONFIG, 224
- TestPmcDbgModeLock
  - FSP\_S\_RESTRICTED\_CONFIG, 224
- TestPmcSlpsxStrPolLock
  - FSP\_S\_RESTRICTED\_CONFIG, 224
- TestUsbXhciAccessControlLock
  - FSP\_S\_RESTRICTED\_CONFIG, 224
- TgaSize
  - FSP\_M\_CONFIG, 99
- ThreeStrikeCounterDisable
  - FSP\_S\_CONFIG, 207
- ThrtCkeMinTmr
  - FSP\_M\_CONFIG, 99
- ThrtCkeMinTmrLpddr
  - FSP\_M\_CONFIG, 99
- TimedMwait
  - FSP\_S\_CONFIG, 207
- TjMaxOffset
  - FSP\_M\_CONFIG, 99
- TmeEnable
  - FSP\_M\_CONFIG, 99
- TrainTrace
  - FSP\_M\_CONFIG, 100
- TscHwFixup
  - FSP\_M\_CONFIG, 100
- TsegSize
  - FSP\_M\_CONFIG, 100
- TsodAlarmwindowLockBit
  - FSP\_M\_CONFIG, 100
- TsodCriticalEventOnly
  - FSP\_M\_CONFIG, 101
- TsodCriticaltripLockBit
  - FSP\_M\_CONFIG, 101
- TsodEventMode
  - FSP\_M\_CONFIG, 101
- TsodEventOutputControl
  - FSP\_M\_CONFIG, 101
- TsodEventPolarity
  - FSP\_M\_CONFIG, 101
- TsodManualEnable
  - FSP\_M\_CONFIG, 102
- TsodShutdownMode
  - FSP\_M\_CONFIG, 102
- TsodTcritMax
  - FSP\_M\_CONFIG, 102
- TurboMode
  - FSP\_S\_CONFIG, 208
- Txt
  - FSP\_M\_CONFIG, 102
- TxtAcheckRequest
  - FSP\_M\_CONFIG, 102
- TxtDprMemoryBase
  - FSP\_M\_CONFIG, 103
- TxtDprMemorySize
  - FSP\_M\_CONFIG, 103
- TxtEnable
  - FSP\_S\_CONFIG, 208
- TxtHeapMemorySize
  - FSP\_M\_CONFIG, 103
- TxtImplemented
  - FSP\_M\_CONFIG, 103
- TxtLcpPdBase
  - FSP\_M\_CONFIG, 103

- TxtLcpPdSize
    - FSP\_M\_CONFIG, 104
  - UfsEnable
    - FSP\_S\_CONFIG, 208
  - Usb2PhyPehalfbit
    - FSP\_S\_CONFIG, 208
  - Usb2PhyPetxiset
    - FSP\_S\_CONFIG, 209
  - Usb2PhyPredeemp
    - FSP\_S\_CONFIG, 209
  - Usb2PhyTxiset
    - FSP\_S\_CONFIG, 209
  - Usb3HsioTxDeEmph
    - FSP\_S\_CONFIG, 209
  - Usb3HsioTxDeEmphEnable
    - FSP\_S\_CONFIG, 209
  - Usb3HsioTxDownscaleAmp
    - FSP\_S\_CONFIG, 210
  - Usb3HsioTxDownscaleAmpEnable
    - FSP\_S\_CONFIG, 210
  - UsbPdoProgramming
    - FSP\_S\_CONFIG, 210
  - UsbTcPortEn
    - FSP\_S\_CONFIG, 210
  - UserBudgetEnable
    - FSP\_M\_CONFIG, 104
  - UserThresholdEnable
    - FSP\_M\_CONFIG, 104
  - VccInVoltageOverride
    - FSP\_M\_CONFIG, 104
  - VccinVrMaxVoltage
    - FSP\_M\_CONFIG, 104
  - VddVoltage
    - FSP\_M\_CONFIG, 104
  - VmdEnable
    - FSP\_S\_CONFIG, 210
  - VmdPortA
    - FSP\_S\_CONFIG, 211
  - VmdPortB
    - FSP\_S\_CONFIG, 211
  - VmdPortC
    - FSP\_S\_CONFIG, 211
  - VmdPortD
    - FSP\_S\_CONFIG, 211
  - VmxEnable
    - FSP\_M\_CONFIG, 105
  - VrVoltageLimit
    - FSP\_S\_CONFIG, 211
  - WarmThresholdCh0Dimm0
    - FSP\_M\_CONFIG, 105
  - WarmThresholdCh0Dimm1
    - FSP\_M\_CONFIG, 105
  - WarmThresholdCh1Dimm0
    - FSP\_M\_CONFIG, 105
  - WarmThresholdCh1Dimm1
    - FSP\_M\_CONFIG, 105
  - WatchDog
    - FSP\_S\_CONFIG, 212
  - WatchDogTimerBios
    - FSP\_S\_CONFIG, 212
  - WatchDogTimerOs
    - FSP\_S\_CONFIG, 212
  - WdtDisableAndLock
    - FSP\_M\_CONFIG, 106
  - XdciEnable
    - FSP\_S\_CONFIG, 212
  - XhciPIIOVERRIDE
    - FSP\_M\_CONFIG, 106
-