

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

Fri Apr 7 2017 00:41:32

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

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

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

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

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

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

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

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

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

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

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

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

Copyright ©Intel Corporation. All rights reserved.

Contents

1	INTF	RODUC	ΓΙΟΝ		1						
2	FSP	OVERV	IEW		3						
3	FSP INTEGRATION										
4	FSP OUTPUT										
5	FSP POSTCODE										
6	Clas	s Index			19						
	6.1	Class I	_ist		19						
7	File	Index			21						
	7.1	File Lis	st		21						
8	Clas	s Docu	mentation	n	23						
	8.1	AUDIC	_AZALIA_	_VERB_TABLE Struct Reference	23						
		8.1.1	Detailed	Description	23						
	8.2	AZALI	A_HEADE	ER Struct Reference	24						
		8.2.1	Detailed	Description	24						
	8.3	DIMM_	_INFO Stru	uct Reference	24						
		8.3.1	Detailed	Description	25						
	8.4	FSP_N	_CONFIG	G Struct Reference	25						
		8.4.1	Detailed	Description	35						
		8.4.2	Member	Data Documentation	35						
			8.4.2.1	ActiveCoreCount	35						
			8.4.2.2	ApertureSize	35						
			8.4.2.3	Avx2RatioOffset	35						
			8.4.2.4	BclkAdaptiveVoltage	35						
			8.4.2.5	BiosGuard	35						
			8.4.2.6	BistOnReset	35						
			8.4.2.7	BootFrequency	36						
			8.4.2.8	CmdTriStateDis	36						

iv CONTENTS

8.4.2.9	CoreMaxOcRatio	36
8.4.2.10	CorePIIVoltageOffset	36
8.4.2.11	CoreVoltageAdaptive	36
8.4.2.12	CoreVoltageMode	36
8.4.2.13	CoreVoltageOverride	36
8.4.2.14	CpuRatio	37
8.4.2.15	CpuRatioOverride	37
8.4.2.16	DdrFreqLimit	37
8.4.2.17	DmiDeEmphasis	37
8.4.2.18	DmiGen3EndPointHint	37
8.4.2.19	DmiGen3EndPointPreset	37
8.4.2.20	DmiGen3ProgramStaticEq	37
8.4.2.21	DmiGen3RootPortPreset	38
8.4.2.22	EnableC6Dram	38
8.4.2.23	EnableSgx	38
8.4.2.24	EnableTraceHub	38
8.4.2.25	EvLoader	38
8.4.2.26	FCIkFrequency	38
8.4.2.27	FlashWearOutProtection	38
8.4.2.28	HeciTimeouts	39
8.4.2.29	IgdDvmt50PreAlloc	39
8.4.2.30	InitPcieAspmAfterOprom	39
8.4.2.31	InternalGfx	39
8.4.2.32	JtagC10PowerGateDisable	39
8.4.2.33	MmioSize	39
8.4.2.34	OcLock	39
8.4.2.35	PcdDebugInterfaceFlags	40
8.4.2.36	PcdlsaSerialUartBase	40
8.4.2.37	PcdSerialDebugBaudRate	40
8.4.2.38	PcdSerialDebugLevel	40
8.4.2.39	PcdSerialloUartNumber	40
8.4.2.40	PchAcpiBase	40
8.4.2.41	PchHpetBase	40
8.4.2.42	PchHpetBdfValid	41
8.4.2.43	PchHpetBusNumber	41
8.4.2.44	PchHpetDeviceNumber	41
8.4.2.45	PchHpetEnable	41
8.4.2.46	PchHpetFunctionNumber	41
8.4.2.47	PchLpcEnhancePort8xhDecoding	41
8.4.2.48	PchNumRsvdSmbusAddresses	41

CONTENTS

		8.4.2.49	PchPmPciePIISsc	41
		8.4.2.50	PchPort80Route	42
		8.4.2.51	PcieRpEnableMask	42
		8.4.2.52	PeciC10Reset	42
		8.4.2.53	PeciSxReset	42
		8.4.2.54	PegDataPtr	42
		8.4.2.55	PegDisableSpreadSpectrumClocking	42
		8.4.2.56	PrmrrSize	42
		8.4.2.57	ProbelessTrace	43
		8.4.2.58	Ratio	43
		8.4.2.59	RefClk	43
		8.4.2.60	RingMaxOcRatio	43
		8.4.2.61	RingMinOcRatio	43
		8.4.2.62	RMT	43
		8.4.2.63	SaGv	43
		8.4.2.64	SinitMemorySize	44
		8.4.2.65	SmbusArpEnable	44
		8.4.2.66	SmbusEnable	44
		8.4.2.67	SpdProfileSelected	44
		8.4.2.68	trtp	44
		8.4.2.69	TsegSize	44
		8.4.2.70	Txt	44
		8.4.2.71	TxtDprMemoryBase	45
		8.4.2.72	TxtDprMemorySize	45
		8.4.2.73	TxtHeapMemorySize	45
		8.4.2.74	TxtImplemented	45
		8.4.2.75	VddVoltage	45
		8.4.2.76	VmxEnable	45
8.5	FSP_N	/_TEST_C	CONFIG Struct Reference	45
	8.5.1	Detailed	Description	48
	8.5.2	Member	Data Documentation	49
		8.5.2.1	BdatEnable	49
		8.5.2.2	BiosAcmBase	49
		8.5.2.3	BiosAcmSize	49
		8.5.2.4	BiosSize	49
		8.5.2.5	BypassPhySyncReset	49
		8.5.2.6	ChipsetInitMessage	49
		8.5.2.7	DisableHeciRetry	49
		8.5.2.8	DisableMessageCheck	50
		8.5.2.9	DmiGen3EqPh2Enable	50

vi

	8.5.2.10	DmiGen3EqPh3Method	50
	8.5.2.11	DmiVc1	50
	8.5.2.12	DmiVcm	50
	8.5.2.13	Gen3SwEqAlwaysAttempt	50
	8.5.2.14	Gen3SwEqEnableVocTest	50
	8.5.2.15	Gen3SwEqJitterDwellTime	51
	8.5.2.16	Gen3SwEqJitterErrorTarget	51
	8.5.2.17	Gen3SwEqNumberOfPresets	51
	8.5.2.18	Gen3SwEqVocDwellTime	51
	8.5.2.19	Gen3SwEqVocErrorTarget	51
	8.5.2.20	HeciCommunication2	52
	8.5.2.21	IderDeviceEnable	52
	8.5.2.22	KtDeviceEnable	52
	8.5.2.23	LockPTMregs	52
	8.5.2.24	PanelPowerEnable	52
	8.5.2.25	PchDciEn	52
	8.5.2.26	Peg0Gen3EqPh2Enable	52
	8.5.2.27	Peg0Gen3EqPh3Method	53
	8.5.2.28	Peg1Gen3EqPh2Enable	53
	8.5.2.29	Peg1Gen3EqPh3Method	53
	8.5.2.30	Peg2Gen3EqPh2Enable	53
	8.5.2.31	Peg2Gen3EqPh3Method	53
	8.5.2.32	PegGen3EndPointHint	53
	8.5.2.33	PegGen3EndPointPreset	54
	8.5.2.34	PegGen3ProgramStaticEq	54
	8.5.2.35	PegGen3RootPortPreset	54
	8.5.2.36	PegGenerateBdatMarginTable	54
	8.5.2.37	PegRxCemLoopbackLane	54
	8.5.2.38	PegRxCemNonProtocolAwareness	54
	8.5.2.39	ScanExtGfxForLegacyOpRom	55
	8.5.2.40	SkipMbpHob	55
	8.5.2.41	SmbusDynamicPowerGating	55
	8.5.2.42	SmbusSpdWriteDisable	55
	8.5.2.43	TgaSize	55
	8.5.2.44	TotalFlashSize	55
	8.5.2.45	TxtLcpPdBase	55
	8.5.2.46	TxtLcpPdSize	56
	8.5.2.47	WdtDisableAndLock	56
8.6	FSP_S_CONFIG	Struct Reference	56
	8.6.1 Detailed	Description	71

CONTENTS vii

8.6.2	Member I	Data Documentation	71
	8.6.2.1	AcLoadline	71
	8.6.2.2	AcousticNoiseMitigation	72
	8.6.2.3	AmtEnabled	72
	8.6.2.4	AmtSolEnabled	72
	8.6.2.5	AsfEnabled	72
	8.6.2.6	DcLoadline	72
	8.6.2.7	DelayUsbPdoProgramming	72
	8.6.2.8	DevIntConfigPtr	72
	8.6.2.9	DmiSuggestedSetting	72
	8.6.2.10	Early8254ClockGatingEnable	73
	8.6.2.11	EcCmdLock	73
	8.6.2.12	EcCmdProvisionEav	73
	8.6.2.13	EnableTcoTimer	73
	8.6.2.14	EsataSpeedLimit	73
	8.6.2.15	FastPkgCRampDisableGt	73
	8.6.2.16	FastPkgCRampDisablela	74
	8.6.2.17	FastPkgCRampDisableSa	74
	8.6.2.18	FwProgress	74
	8.6.2.19	GpioIrqRoute	74
	8.6.2.20	Heci3Enabled	74
	8.6.2.21	lccMax	74
	8.6.2.22	ImonOffset	74
	8.6.2.23	ImonSlope	75
	8.6.2.24	ManageabilityMode	75
	8.6.2.25	MeUnconfigIsValid	75
	8.6.2.26	MicrocodePatchAddress	75
	8.6.2.27	NumOfDevIntConfig	75
	8.6.2.28	PchCio2Enable	75
	8.6.2.29	PchCrid	75
	8.6.2.30	PchDisableComplianceMode	76
	8.6.2.31	PchDmiAspm	76
	8.6.2.32	PchDmiTsawEn	76
	8.6.2.33	PchHdaDspEnable	76
	8.6.2.34	PchHdaDspEndpointBluetooth	76
	8.6.2.35	PchHdaDspEndpointl2s	76
	8.6.2.36	PchHdaDspFeatureMask	76
	8.6.2.37	PchHdaDspUaaCompliance	77
	8.6.2.38	PchHdaEnable	77
	8.6.2.39	PchHdalDispCodecDisconnect	77

viii CONTENTS

8.6.2.40	PchHdaloBufferOwnership	77
8.6.2.41	PchHdaPme	77
8.6.2.42	PchloApicBdfValid	77
8.6.2.43	PchloApicBusNumber	77
8.6.2.44	PchloApicDeviceNumber	78
8.6.2.45	PchloApicEntry24_119	78
8.6.2.46	PchloApicFunctionNumber	78
8.6.2.47	PchloApicId	78
8.6.2.48	PchloApicRangeSelect	78
8.6.2.49	PchlshEnable	78
8.6.2.50	PchlshGp0GpioAssign	78
8.6.2.51	PchlshGp1GpioAssign	78
8.6.2.52	PchlshGp2GpioAssign	79
8.6.2.53	PchlshGp3GpioAssign	79
8.6.2.54	PchlshGp4GpioAssign	79
8.6.2.55	PchlshGp5GpioAssign	79
8.6.2.56	PchlshGp6GpioAssign	79
8.6.2.57	PchlshGp7GpioAssign	79
8.6.2.58	Pchlshl2c0GpioAssign	79
8.6.2.59	Pchlshl2c1GpioAssign	80
8.6.2.60	Pchlshl2c2GpioAssign	80
8.6.2.61	PchlshPdtUnlock	80
8.6.2.62	PchlshSpiGpioAssign	80
8.6.2.63	PchlshUart0GpioAssign	80
8.6.2.64	PchlshUart1GpioAssign	80
8.6.2.65	PchLanClkReqSupported	80
8.6.2.66	PchLanEnable	80
8.6.2.67	PchLanK1OffEnable	81
8.6.2.68	PchLanLtrEnable	81
8.6.2.69	PchLockDownBiosLock	81
8.6.2.70	PchLockDownSpiEiss	81
8.6.2.71	PchMemoryThrottlingEnable	81
8.6.2.72	PchPcieDeviceOverrideTablePtr	81
8.6.2.73	PchPmCapsuleResetType	81
8.6.2.74	PchPmDeepSxPol	82
8.6.2.75	PchPmDisableDsxAcPresentPulldown	82
8.6.2.76	PchPmDisableNativePowerButton	82
8.6.2.77	PchPmLanWakeFromDeepSx	82
8.6.2.78	PchPmLpcClockRun	82
8.6.2.79	PchPmMeWakeSts	82

CONTENTS

8.6.2.80 PchPmPcieWakeFromDeepSx
8.6.2.81 PchPmPmeB0S5Dis
8.6.2.82 PchPmPwrBtnOverridePeriod
8.6.2.83 PchPmPwrCycDur
8.6.2.84 PchPmSlpAMinAssert
8.6.2.85 PchPmSlpLanLowDc
8.6.2.86 PchPmSlpS0Enable
8.6.2.87 PchPmSlpS0VmEnable
8.6.2.88 PchPmSlpS3MinAssert
8.6.2.89 PchPmSlpS4MinAssert
8.6.2.90 PchPmSlpStrchSusUp
8.6.2.91 PchPmSlpSusMinAssert
8.6.2.92 PchPmWolEnableOverride
8.6.2.93 PchPmWolOvrWkSts
8.6.2.94 PchPmWoWlanDeepSxEnable
8.6.2.95 PchPmWoWlanEnable
8.6.2.96 PchPort61hEnable
8.6.2.97 PchPwrOptEnable
8.6.2.98 PchScsEmmcHs400DllDataValid
8.6.2.99 PchScsEmmcHs400TuningRequired
8.6.2.100 PchSirqEnable
8.6.2.101 PchSirqMode
8.6.2.102 PchSkyCamPortACtleEnable
8.6.2.103 PchSkyCamPortATermOvrEnable
8.6.2.104 PchSkyCamPortATrimEnable
8.6.2.105 PchSkyCamPortBCtleEnable
8.6.2.106 PchSkyCamPortBTermOvrEnable
8.6.2.107 PchSkyCamPortBTrimEnable
8.6.2.108 PchSkyCamPortCDCtleEnable
8.6.2.109 PchSkyCamPortCTermOvrEnable
8.6.2.110 PchSkyCamPortCTrimEnable
8.6.2.111 PchSkyCamPortDTermOvrEnable
8.6.2.112 PchSkyCamPortDTrimEnable
8.6.2.113 PchSubSystemId
8.6.2.114 PchSubSystemVendorld
8.6.2.115 PchThermalDeviceEnable
8.6.2.116 PchTsmicLock
8.6.2.117 PchTTEnable
8.6.2.118 PchTTLock
8.6.2.119 PchTTState13Enable

X CONTENTS

8.6.2.120 PcieAllowNoLtrlccPllShutdown
8.6.2.121 PcieComplianceTestMode
8.6.2.122 PcieDisableRootPortClockGating
8.6.2.123 PcieEnablePeerMemoryWrite
8.6.2.124 PcieEqPh3LaneParamCm
8.6.2.125 PcieEqPh3LaneParamCp
8.6.2.126 PcieRpAspm
8.6.2.127 PcieRpClkReqNumber
8.6.2.128 PcieRpClkReqSupport
8.6.2.129 PcieRpCompletionTimeout
8.6.2.130 PcieRpDeviceResetPad
8.6.2.131 PcieRpFunctionSwap
8.6.2.132 PcieRpGen3EqPh3Method
8.6.2.133 PcieRpL1Substates
8.6.2.134 PcieRpPcieSpeed
8.6.2.135 PcieRpPhysicalSlotNumber
8.6.2.136 PcieSwEqCoeffListCm
8.6.2.137 PcieSwEqCoeffListCp
8.6.2.138 PortUsb20Enable
8.6.2.139 PortUsb30Enable
8.6.2.140 Psi1Threshold
8.6.2.141 Psi2Threshold
8.6.2.142 Psi3Enable
8.6.2.143 Psi3Threshold
8.6.2.144 PsysOffset
8.6.2.145 PsysSlope
8.6.2.146 PxRcConfig
8.6.2.147 SataEnable
8.6.2.148 SataMode
8.6.2.149 SataP0TDispFinit
8.6.2.150 SataP1TDispFinit
8.6.2.151 SataPortsDevSlp
8.6.2.152 SataPortsDmVal
8.6.2.153 SataPortsEnable
8.6.2.154 SataPwrOptEnable
8.6.2.155 SataRstHddUnlock
8.6.2.156 SataRstIrrt
8.6.2.157 SataRstIrrtOnly
8.6.2.158 SataRstLedLocate
8.6.2.159 SataRstOromUiBanner

CONTENTS xi

8.6.2.160 SataRstPcieDeviceResetDelay
8.6.2.161 SataRstRaid0
8.6.2.162 SataRstRaid1
8.6.2.163 SataRstRaid10
8.6.2.164 SataRstRaid5
8.6.2.165 SataRstRaidAlternateId
8.6.2.166 SataRstSmartStorage
8.6.2.167 SataSalpSupport
8.6.2.168 SataThermalSuggestedSetting
8.6.2.169 ScilrqSelect
8.6.2.170 ScsEmmcEnabled
8.6.2.171 ScsEmmcHs400Enabled
8.6.2.172 ScsSdCardEnabled
8.6.2.173 SendEcCmd
8.6.2.174 SendVrMbxCmd
8.6.2.175 SendVrMbxCmd1
8.6.2.176 SerialloDebugUartNumber
8.6.2.177 SerialloDevMode
8.6.2.178 SerialloGpio
8.6.2.179 ShowSpiController
8.6.2.180 SlowSlewRateForGt
8.6.2.181 SlowSlewRateForla
8.6.2.182 SlowSlewRateForSa
8.6.2.183 SsicPortEnable
8.6.2.184 TcolrqSelect
8.6.2.185 TdcPowerLimit
8.6.2.186 TdcTimeWindow
8.6.2.187 TTSuggestedSetting
8.6.2.188 TurboMode
8.6.2.189 Usb2AfePehalfbit
8.6.2.190 Usb2AfePetxiset
8.6.2.191 Usb2AfePredeemp
8.6.2.192 Usb2AfeTxiset
8.6.2.193 Usb3HsioTxDeEmph
8.6.2.194 Usb3HsioTxDeEmphEnable
8.6.2.195 Usb3HsioTxDownscaleAmp
8.6.2.196 Usb3HsioTxDownscaleAmpEnable
8.6.2.197 VrVoltageLimit
8.6.2.198 WatchDog
8.6.2.199 WatchDogTimerBios

xii CONTENTS

		8.6.2.200	WatchDogTimerOs
		8.6.2.201	I XdciEnable 99
8.7	FSP_S	S_TEST_C	ONFIG Struct Reference
	8.7.1	Detailed	Description
	8.7.2	Member	Data Documentation
		8.7.2.1	ApHandoffManner
		8.7.2.2	ApIdleManner
		8.7.2.3	AutoThermalReporting
		8.7.2.4	C1e
		8.7.2.5	ConfigTdpBios
		8.7.2.6	CstateLatencyControl0Irtl
		8.7.2.7	CStatePreWake
		8.7.2.8	CstCfgCtrloMwaitRedirection
		8.7.2.9	Custom1ConfigTdpControl
		8.7.2.10	Custom1PowerLimit1
		8.7.2.11	Custom1PowerLimit1Time
		8.7.2.12	Custom1PowerLimit2
		8.7.2.13	Custom1TurboActivationRatio
		8.7.2.14	Custom2ConfigTdpControl
		8.7.2.15	Custom2PowerLimit1
		8.7.2.16	Custom2PowerLimit1Time
		8.7.2.17	Custom2PowerLimit2
		8.7.2.18	Custom2TurboActivationRatio
		8.7.2.19	Custom3ConfigTdpControl
		8.7.2.20	Custom3PowerLimit1
		8.7.2.21	Custom3PowerLimit1Time
		8.7.2.22	Custom3PowerLimit2
		8.7.2.23	Custom3TurboActivationRatio
		8.7.2.24	Cx
		8.7.2.25	DebugInterfaceEnable
		8.7.2.26	DebugInterfaceLockEnable
		8.7.2.27	DisableProcHotOut
		8.7.2.28	Disable VrThermal Alert
		8.7.2.29	Eist
		8.7.2.30	EndOfPostMessage
		8.7.2.31	EnergyEfficientPState
		8.7.2.32	EnergyEfficientTurbo
		8.7.2.33	HdcControl
			Hwp
		8.7.2.35	MachineCheckEnable

CONTENTS xiii

8.7.2.36	MlcStreamerPrefetcher
8.7.2.37	MonitorMwaitEnable
8.7.2.38	NumberOfEntries
8.7.2.39	OneCoreRatioLimit
8.7.2.40	PchHdaResetWaitTimer
8.7.2.41	PchLockDownBiosInterface
8.7.2.42	PchLockDownGlobalSmi
8.7.2.43	PchLockDownRtcLock
8.7.2.44	PchPmDisableEnergyReport
8.7.2.45	PchPmPmcReadDisable
8.7.2.46	PchSbAccessUnlock
8.7.2.47	PchSbiUnlock
8.7.2.48	PcieEnablePort8xhDecode
8.7.2.49	PcieRpDptp
8.7.2.50	PcieRpSlotPowerLimitScale
8.7.2.51	PcieRpSlotPowerLimitValue
8.7.2.52	PcieRpUptp
8.7.2.53	PkgCStateDemotion
8.7.2.54	PkgCStateLimit
8.7.2.55	PkgCStateUnDemotion
8.7.2.56	PmgCstCfgCtrlLock
8.7.2.57	PowerLimit1
8.7.2.58	PowerLimit1Time
8.7.2.59	PowerLimit2
8.7.2.60	PowerLimit2Power
8.7.2.61	PowerLimit3
8.7.2.62	PowerLimit3Time
8.7.2.63	PowerLimit4
8.7.2.64	ProcHotResponse
8.7.2.65	ProcTraceEnable
8.7.2.66	ProcTraceOutputScheme
8.7.2.67	PsysPmax
8.7.2.68	PsysPowerLimit1
8.7.2.69	PsysPowerLimit1Power
8.7.2.70	PsysPowerLimit2
8.7.2.71	PsysPowerLimit2Power
8.7.2.72	RaceToHalt
8.7.2.73	SataTestMode
8.7.2.74	StateRatio
8.7.2.75	TccActivationOffset

XIV

		8.7.2.76	TccOffsetC	lamp				 	 	 	117
		8.7.2.77	TccOffsetL	ock				 	 	 	117
		8.7.2.78	TccOffsetT	imeWindo	wForRatl			 	 	 	118
		8.7.2.79	TimedMwa	it				 	 	 	118
		8.7.2.80	TStates					 	 	 	118
8.8	FSP_T	_CONFIG	Struct Refer	ence				 	 	 	118
	8.8.1	Detailed I	Description					 	 	 	119
	8.8.2	Member I	Data Docum	entation .				 	 	 	119
		8.8.2.1	PcdSeriallo	UartDebu	ıgEnable			 	 	 	119
		8.8.2.2	PcdSeriallo	UartNumb	ber			 	 	 	119
8.9	FSPM_	_UPD Stru	ct Reference)				 	 	 	119
	8.9.1	Detailed I	Description					 	 	 	120
8.10	FSPS_	UPD Struc	ct Reference					 	 	 	120
	8.10.1	Detailed I	Description					 	 	 	121
8.11	FSPT_	CORE_UF	PD Struct Re	ference .				 	 	 	121
	8.11.1	Detailed I	Description					 	 	 	121
8.12	FSPT_	UPD Struc	ct Reference					 	 	 	121
	8.12.1	Detailed I	Description					 	 	 	122
8.13	GPIO_	CONFIG S	Struct Refere	nce				 	 	 	122
	8.13.1	Detailed I	Description					 	 	 	123
	8.13.2	Member I	Data Docum	entation .				 	 	 	123
		8.13.2.1	Direction .					 	 	 	123
		8.13.2.2	ElectricalCo	onfig				 	 	 	123
		8.13.2.3	HostSoftPa	ıdOwn				 	 	 	123
		8.13.2.4	InterruptCo	nfig				 	 	 	124
		8.13.2.5	LockConfig					 	 	 	124
		8.13.2.6	OutputState	e				 	 	 	124
		8.13.2.7	PadMode .					 	 	 	124
		8.13.2.8	PowerConf	ig				 	 	 	124
8.14	MEMO	RY_PLAT	FORM_DAT	A Struct R	Reference			 	 	 	124
	8.14.1	Detailed I	Description					 	 	 	124
8.15	SI_CHI	PSET_INI	IT_INFO Stru	uct Refere	nce			 	 	 	125
	8.15.1	Detailed I	Description					 	 	 	125
8.16	SI_PCI	H_DEVICE	_INTERRUI	PT_CONF	IG Struct	Referer	ice	 	 	 	125
	8.16.1	Detailed I	Description					 	 	 	125
8.17	SMBIO	S_CACHE	E_INFO Stru	ct Referen	ice			 	 	 	126
	8.17.1	Detailed I	Description					 	 	 	126
8.18	SMBIO	S_PROCE	ESSOR_INF	O Struct F	Reference			 	 	 	126
	8.18.1	Detailed I	Description					 	 	 	127

CONTENTS

9	File I	Docume	entation	129
	9.1	CpuCo	onfigFspData.h File Reference	129
		9.1.1	Detailed Description	129
	9.2	Doxyge	enFspIntegrationGuide.h File Reference	130
		9.2.1	Detailed Description	130
	9.3	FspmL	Jpd.h File Reference	130
		9.3.1	Detailed Description	131
	9.4	FspsU	pd.h File Reference	132
		9.4.1	Detailed Description	133
		9.4.2	Enumeration Type Documentation	134
			9.4.2.1 SI_PCH_INT_PIN	134
	9.5	FsptUp	od.h File Reference	134
		9.5.1	Detailed Description	135
	9.6	FspUp	d.h File Reference	135
		9.6.1	Detailed Description	136
	9.7	GpioCo	onfig.h File Reference	137
		9.7.1	Detailed Description	138
		9.7.2	Enumeration Type Documentation	138
			9.7.2.1 GPIO_DIRECTION	138
			9.7.2.2 GPIO_ELECTRICAL_CONFIG	139
			9.7.2.3 GPIO_HARDWARE_DEFAULT	139
			9.7.2.4 GPIO_HOSTSW_OWN	139
			9.7.2.5 GPIO_INT_CONFIG	140
			9.7.2.6 GPIO_LOCK_CONFIG	140
			9.7.2.7 GPIO_OTHER_CONFIG	140
			9.7.2.8 GPIO_OUTPUT_STATE	141
			9.7.2.9 GPIO_PAD_MODE	141
			9.7.2.10 GPIO_RESET_CONFIG	141
	9.8	GpioSa	ampleDef.h File Reference	142
		9.8.1	Detailed Description	143
	9.9	MemIn	nfoHob.h File Reference	143
		9.9.1	Detailed Description	144
	9.10	Smbios	sCacheInfoHob.h File Reference	144
		9.10.1	Detailed Description	145
	9.11	Smbios	sProcessorInfoHob.h File Reference	145
		9.11.1	Detailed Description	146
Inc	dex			147

Chapter 1

INTRODUCTION

1 Introduction

1.1 Purpose

The purpose of this document is to describe the steps required to integrate the Intel® Firmware Support Package (FSP) into a boot loader solution. It supports Kabylake platforms with Kabylake/Skylake processor and Sunrise point Platform Controller Hub (PCH).

1.2 Intended Audience

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

1.3 Related Documents

- Platform Initialization (PI) Specification v1.4 located at http://www.uefi.org/specifications
- UEFI Specification v2.5 located at http://www.uefi.org/specifications
- Intel® Firmware Support Package: External Architecture Specification (EAS) v2.0 located at http←
 ://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp
 pdf
- Boot Setting File Specification (BSF) v1.0 https://firmware.intel.com/sites/default/files/ \leftarrow 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

2 INTRODUCTION

BWG	BIOS Writer's Guide
CAR	Cache As Ram
CRB	Customer Reference Board
FIT	Firmware Interface Table
FSP	Firmware Support Package
FSP API	Firmware Support Package Interface
FW	Firmware
PCH	Platform Controller Hub
PMC	Power Management Controller
SBSP	System BSP
SMI	System Management Interrupt
SMM	System Management Mode
SPI	Serial Peripheral Interface
TSEG	Memory Reserved at the Top of Memory to be used
	as SMRAM
UPD	Updatable Product Data

Chapter 2

FSP OVERVIEW

FSP Overview

2.1 Technical Overview

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

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

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

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

Below are some required steps for the integration:

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

2.2 FSP Distribution Package

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

4 FSP OVERVIEW

2.2.1 Package Layout

- Docs (Auto generated)
 - Kabylake_FSP_Integration_Guide.pdf (this doc)
 - Kabylake_FSP_Integration_Guide.chm

Include

- FsptUpd.h, FspmUpd.h and FspsUpd.h (FSP UPD structure and related definitions)
- GpioSampleDef.h (Sample enum definitions for Gpio table)
- KabylakeFspBinPkg.dec (EDKII declaration file for package)
- Fsp.bsf (BSF file for configuring the data using BCT tool)
- Fsp.fd (FSP Binary)

Chapter 3

FSP INTEGRATION

3 FSP Integration

3.1 Assumptions Used in this Document

The FSP for the Kabylake platform is built with a preferred base address of 0xFFEC0000 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 AP ← I parameters could change over different FSP IDs and revisions. The FSP API parameters documented in this integration guide are applicable for the Image ID and Revision specified as below.

The current FSP ImageId string in the FSP information header is **\$KBLFSP\$** and the ImageRevision field is **0x02010000.(2.1.0.0)**.

3.5 FSP APIs

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

6 FSP INTEGRATION

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

3.5.1 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 temporary ram currently available is from 0xFEF0 0000 (ECX) to 0xFEF4 0000 (EDX).

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

Note

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

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

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

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

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

3.5.2 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 156KB, stack base is 0xFEF18F00 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.

3.5.3 TempRamExit API

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

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

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

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

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

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

3.5.4 FspSiliconInit API

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

The FspsUpdPtr is pointer to FSPS UPD structure which is described in header file FspsUpd.h.

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

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

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

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

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

PCH required initialization is done for the following HECI, USB, HSIO, Integrated Sensor Hub, Display, Sky Cam, Camera, PCI Express, Vt-d, straps (cores, hyper-threading, BIST, ..)

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

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

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

On normal boot CPU S3 Resume Data HOB is produced in this phase. This CPU S3 Resume Data HOB is described in section 4.4. Unless UPD SkipMpInit is enabled, on S3 resume, this data (not the entire HOB) must be passed through UPD CpuS3ResumeData, and optionally final S3 boot MTRRs is passed through UPD CpuS3 \leftarrow ResumeMtrrData. During S3 resume unless SkipMpInit is enabled, GDT base and length and IDT base and length on APs are programmed to that of the BSP.

3.5.5 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.

3.5.5.1 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.

8 FSP INTEGRATION

3.5.5.2 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).

3.5.5.3 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

3.6 Memory Map

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

3.7 Porting recommendation

Here listed some notes or recommendation when porting with FSP.

3.7.1 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_PO LICY_STRUCT -> SA_MISC_PEI_CONFIG -> SkipPamLock, and platform or wrapper code should do the PAM locking right before booting OS (so do it outside FSP instead) by programming one PCI config space register as below

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

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

3.7.2 Locking SMRAM register

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

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

3.7.3 Locking SMI register

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

3.7.4 Verify below settings are correct for your platforms

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

Note

:

- It is recommended that you do not change these settings as it may require significant changes to the System Agent reference code.
- Those memory regions should be reserved from any memory service functions in platform code so it will not cause any conflict when other modules or drivers allocating memory resource.
- Boot Loader can use different value for PCIEXBAR_BASE_ADDRESS either by modifying the UPD (under FSP-T) or by overriding the PCIEXBAR (B0:D0:F0:R60h) before calling FspMemoryInit Api.
- Boot Loader should avoid using conflicting address when reprogramming PCIEXBAR_BASE_ADDR ← ESS than the recommended one.

3.7.5 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

10 FSP INTEGRATION

Chapter 4

FSP OUTPUT

4 FSP Output

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

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

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

4.1 SMRAM Resource Descriptor HOB

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

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

4.2 SMBIOS INFO HOB

The FSP will report the SMBIOS through a HOB with below GUID. This information can be consumed by the bootloader to produce the SMBIOS tables. These structures are included as part of MemInfoHob.h , Smbios← CacheInfoHob.h & SmbiosProcessorInfoHob.h. Note: The Smbios Cache Info Hob & Smbios Processor Info Hob won't be published on S3 boot.

```
#define SI_MEMORY_INFO_DATA_HOB_GUID \
{ 0x9b2071d4, 0xb054, 0x4e0c, { 0x8d, 0x09, 0x11, 0xcf, 0x8b, 0x9f, 0x03, 0x23 } };
typedef struct {
  MrcDimmStatus Status;
                                               \protect\ensuremath{\text{///\text{<}}} See MrcDimmStatus for the definition of this field.
            DimmId;
DimmCapacity;
 UTNT8
                                               ///< DIMM size in MBvtes.
 UINT32
 UINT16
               MfgId;
ModulePartNum[20];
                                               ///< Module part number for DDR3 is 18 bytes however for DRR4
 UINT8
       20 bytes as per JEDEC Spec, so reserving 20 bytes
 UINT8 RankInDimm; ///< The number of ranks in this DIMM.
UINT8 SpdDramDeviceType; ///< Save SPD DramDeviceType informati
                                               ///< Save SPD DramDeviceType information needed for SMBIOS
       structure creation.
 UINT8
                                               ///< Save SPD ModuleType information needed for SMBIOS
                SpdModuleType;
       structure creation.
                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 {
```

12 FSP OUTPUT

```
UINT8
                                               ///< Indicates whether this channel should be used.
                 Status;
  UINT8
                 ChannelId;
 HITNT8
                 DimmCount;
                                               ///< Number of valid DIMMs that exist in the channel.
 MRC_CH_TIMING Timing[MAX_PROFILE];
                                               \ensuremath{///\!<} The channel timing values.
 DIMM INFO
                Dimm[MAX_DIMM];
                                               ///< Save the DIMM output characteristics.
} CHANNEL_INFO;
typedef struct {
  STNTII
                    Status;
                                               ///< Indicates whether this controller should be used.
  UINT16
                    DeviceId;
                                               \ensuremath{///\!<} The PCI device id of this memory controller.
                                               ///< The PCI revision id of this memory controller.
///< Number of valid channels that exist on the controller.
                    RevisionId:
 UINT8
 UINT8
                    ChannelCount:
 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
  HITNT8
                    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
                    ErrorCorrectionType;
                     Version;
  SiMrcVersion
 UINT32
                     FreqMax;
  BOOLEAN
                     EccSupport:
  UINT8
                     MemoryProfile;
  UINT32
                     TotalPhysicalMemorySize;
  BOOLEAN
                     XmpProfileEnable;
 UTNT8
                     Ratio;
 HITNT8
                     RefClk;
                     VddVoltage[MAX_PROFILE];
 UINT32
  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];
  IIINT32
                     BootMode;
 UINT32
                     TsegSize;
 UINT32
                     TseqBase;
 UINT32
                     PrmrrSize:
 UINT32
                     PrmrrBase:
  UINT32
                     GttBase;
                     MmioSize;
 UINT32
 UINT32
                     PciEBaseAddress;
} MEMORY PLATFORM DATA;
typedef struct {
  EFI_HOB_GUID_TYPE
                        EfiHobGuidType;
  MEMORY_PLATFORM_DATA Data;
  UTNT8
                        *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
111
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
             InstalledSize:
                                             ///< Format defined in SMBIOS Spec v3.0 Section7.8.1
 UINT16
             SupportedSramType;
                                             ///< Format defined in SMBIOS Spec v3.0 Section7.8.2
  UINT16
                                             ///< Format defined in SMBIOS Spec v3.0 Section7.8.2
  UINT16
             CurrentSramType;
 UINT8
                                             ///< Cache Speed in nanoseconds. O if speed is unknown.
             CacheSpeed;
 UINT8
             ErrorCorrectionType;
                                             ///< ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.3
 HITNT8
             SystemCacheType;
                                             ///< ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.4 \,
 VINT8 Associativity; /// ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.5 ///String Buffer - each string terminated by NULL "0x000" ///String buffer terminated by double NULL "0x0000"
             Associativity;
} SMBIOS_CACHE_INFO;
#define SMBIOS_PROCESSOR_INFO_HOB_GUID \
  { 0xe6d73d92, 0xff56, 0x4146, {0xaf, 0xac, 0xlc, 0xl8, 0x81, 0x7d, 0x68, 0x7l} }
```

```
/// SMBIOS Processor Info HOB Structure
typedef struct {
 UINT16
             TotalNumberOfSockets;
 UINT16
             CurrentSocketNumber;
                                              ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.1
 UINT8
             ProcessorType:
  ///This info is used for both ProcessorFamily and ProcessorFamily2 fields
  ///See ENUM defined in SMBIOS Spec v3.0 Section 7.5.2
  UINT16
             ProcessorFamily;
  UTNT8
             ProcessorManufacturerStrIndex; ///< Index of the String in the String Buffer
 UINT64
                                              ///< ENUM defined in SMBIOS Spec v3.0 Section 7.5.3
             ProcessorId:
                                              ///< Index of the String in the String Buffer
 UINT8
             ProcessorVersionStrIndex:
                                              ///< Format defined in SMBIOS Spec v3.0 Section 7.5.4
  UINT8
             Voltage;
             ExternalClockInMHz;
  UINT16
                                              ///< External Clock Frequency. Set to 0 if unknown.
  UINT16
             CurrentSpeedInMHz;
                                              ///< Snapshot of current processor speed during boot
  UTNT8
             Status;
                                              ///< Format defined in the SMBIOS Spec v3.0 Table 21
                                              ///< \tt ENUM defined in SMBIOS Spec v3.0 Section 7.5.5
 IITNT8
             ProcessorUpgrade;
  ///This info is used for both CoreCount & CoreCount2 fields
  /// See detailed description in SMBIOS Spec v3.0 Section 7.5.6
             CoreCount;
  UINT16
  ///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
             ThreadCount;
             ProcessorCharacteristics;
                                              ///< Format defined in SMBIOS Spec v3.0 Section 7.5.9
 UINT16
  /// String Buffer - each string terminated by NULL "0x00" /// String buffer terminated by double NULL "0x0000"
} SMBIOS_PROCESSOR_INFO;
```

4.3 CHIPSETINIT INFO HOB

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

4.4 CPU S3 Resume Data HOB

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

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

14 FSP OUTPUT

Chapter 5

FSP POSTCODE

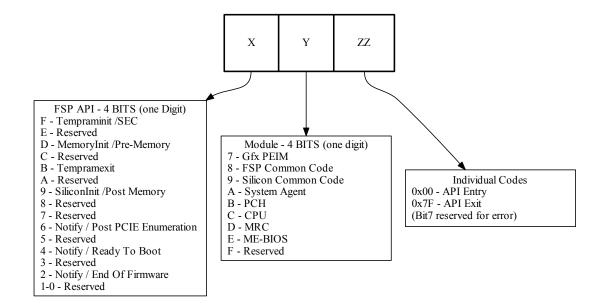
5 FSP PostCode

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

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

5.1 PostCode Info

Below diagram represents the 16 bit PostCode usage in FSP.



5.1.1 TempRamInit API Status Codes (0xFxxx)

16 FSP POSTCODE

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

5.1.2 FspMemoryInit API Status Codes (0xDxxx)

PostCode	Module	Description
0xD800	FSP	FspMemoryInit API Entry
0xD87F	FSP	FSpMemoryInit API Exit
0xDA00	SA	Pre-Mem Salnit Entry
0xDA01	SA	DeviceConfigurePreMem Start
0xDA02	SA	OverrideDev0Did Start
0xDA04	SA	OverrideDev2Did Start
0xDA06	SA	Programming SA Bars
0xDA08	SA	Install SA HOBs
0xDA0A	SA	Reporting SA PCIe code version
0xDA0C	SA	SaSvInit Start
0xDA10	SA	Initializing DMI
0xDA1F	SA	Initializing DMI/OPI Max PayLoad
		Size
0xDA20	SA	Initializing SwitchableGraphics
0xDA30	SA	Initializing SA PCIe
0xDA3F	SA	Programming PEG credit values
		Start
0xDA40	SA	Initializing DMI Tc/Vc mapping
0xDA42	SA	CheckOffboardPcieVga
0xDA44	SA	CheckAndInitializePegVga
0xDA50	SA	Initializing Graphics
0xDA7F	SA	Pre-Mem Salnit Exit
0xDB00	PCH	PCH API Entry
0xDC00	CPU	Pre-Mem Entry
0xDC7F	CPU	Pre-Mem Exit

5.1.3 TempRamExit API Status Codes (0xBxxx)

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

5.1.3 FspSiliconInit API Status Codes (0x9xxx)

PostCode	Module	Description
0x9800	FSP	FspSiliconInit API Entry
0x987F	FSP	FspSiliconInit API Exit
0x9A00	SA	Post-Mem Salnit Entry
0x9A01	SA	DeviceConfigure Start
0x9A02	SA	UpdateSaHobPostMem Start
0x9A03	SA	Initializing Pei Display
0x9A04	SA	PeiGraphicsNotifyCallback Entry

0x9A05	SA	CallPpiAndFillFrameBuffer
0x9A06	SA	GraphicsPpilnit
0x9A07	SA	GraphicsPpiGetMode
0x9A08	SA	FillFrameBufferAndShowLogo
0x9A0F	SA	PeiGraphicsNotifyCallback Exit
0x9A10	SA	Initializing SA Overclocking
0x9A14	SA	Initializing SA SkyCam device
0x9A16	SA	Initializing SA GMM device
0x9A18	SA	Internal Device and Misc
0,0,7110		Configurations
0x9A1A	SA	SaProgramLlcWays Start
0x9A20	SA	Initializing PciExpressInitPostMem
0x9A30	SA	Initializing Vtd
0x9A32	SA	Initializing Pavp
0x9A34	SA	PeilnstallSmmAccessPpi 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
ONO/ NO 1	0,1	all configurations complete
0x9A62	SA	SaSvInit2 Start
0x9A63	SA	GraphicsPmInit Start
0x9A64	SA	SaPeiPolicyDump Start
0x9A6F	SA	SaSResetComplete Exit
0x9A70	SA	SaS3ResumeAtEndOfPei Callback
UX3A7U	JA.	Entry Entry
0x9A7F	SA	SaS3ResumeAtEndOfPei Callback
OXOTTI	O/ C	Exit
0x9B7F	PCH	Post-Mem ScInit Entry
0x9B01	PCH	Post-Mem Program HSIO
0x9601	1 011	ModPHY settings
0x9B02	PCH	Post-Mem SMBus configuration
0x9B03	PCH	Post-Mem LPC configuration
0x9B04	PCH	Post-Mem SATA initizalization
0x9B05	PCH	Post-Mem PCIe initizalization
0x9B06	PCH	Post-Mem xHCl initizalization
0x9B07	PCH	Post-Mem xDCI initizalization
0x9B08	PCH	Post-Mem HD Audio initizalization
	PCH	Post-Mem GMM configuration
0x9B09	PCH	Post-Mem LPSS initizalization
0x9B0A		
0x9B0B	PCH	Post-Mem SCS initizalization
0x9B0C	PCH	Post-Mem ISH initizalization
0x9B0D	PCH	Post-Mem ITSS configuration
0x9B40	PCH	Post-Mem OnEndOfPEI Entry
0x9B4F	PCH	Post-Mem OnEndOfPEI Exit
0x9B7F	PCH	Post-Mem ScInit Exit

18 FSP POSTCODE

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

5.1.4 NotifyPhase API Status Codes (0x6xxx)

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

Chapter 6

Class Index

6.1 Class List

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

AUDIO_AZALIA_VERB_TABLE	
Audio Azalia Verb Table structure	23
AZALIA_HEADER	
Azalia Header structure	24
DIMM_INFO	
Memory SMBIOS & OC Memory Data Hob	24
FSP_M_CONFIG	
Fsp M Configuration	25
FSP_M_TEST_CONFIG	
,	45
FSP_S_CONFIG	
· · · · · · · · · · · · · · · · · · ·	56
FSP_S_TEST_CONFIG	
1 9	99
FSP_T_CONFIG	
1 6	18
FSPM_UPD	
-1 9	19
FSPS_UPD	
i v	20
FSPT_CORE_UPD	
Fsp T Core UPD	21
FSPT_UPD	
Fsp T UPD Configuration	21
GPIO_CONFIG	
	22
MEMORY_PLATFORM_DATA	
Memory Platform Data Hob	24
SI_CHIPSET_INIT_INFO	
The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIO ChipsetInit CRC	0.5
S ChipsetInit CRC	25
SI_PCH_DEVICE_INTERRUPT_CONFIG	
The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt	O.E.
mode for PCH device	25
SMBIOS_CACHE_INFO SMBIOS Cache Info HOB Structure	20
SMBIOS PROCESSOR INFO	20
-	26

20 Class Index

Chapter 7

File Index

7.1 File List

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

CpuConfigFspData.h	
FSP CPU Data Config Block	29
DoxygenFspIntegrationGuide.h	
This file contains doxygen KabylakeFspIntegration Guide	30
FspmUpd.h	
Copyright (c) 2017, Intel Corporation	30
FspsUpd.h	
Copyright (c) 2017, Intel Corporation	32
FsptUpd.h	
Copyright (c) 2017, Intel Corporation	34
FspUpd.h	
Copyright (c) 2017, Intel Corporation	35
GpioConfig.h	
Header file for GpioConfig structure used by GPIO library	37
GpioSampleDef.h	
Copyright (c) 2015, Intel Corporation	42
MemInfoHob.h	
This file contains definitions required for creation of Memory S3 Save data, Memory Info data	
and Memory Platform data hobs	43
SmbiosCacheInfoHob.h	
Header file for SMBIOS Cache Info HOB	44
SmbiosProcessorInfoHob.h	
Header file for SMBIOS Processor Info HOB	45

22 File Index

Chapter 8

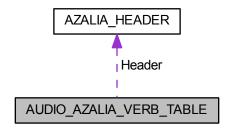
Class Documentation

8.1 AUDIO_AZALIA_VERB_TABLE Struct Reference

Audio Azalia Verb Table structure.

#include <FspsUpd.h>

Collaboration diagram for AUDIO_AZALIA_VERB_TABLE:



Public Attributes

• AZALIA_HEADER Header

AZALIA PCH header.

UINT32 * Data

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

8.1.1 Detailed Description

Audio Azalia Verb Table structure.

Definition at line 57 of file FspsUpd.h.

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

• FspsUpd.h

8.2 AZALIA HEADER Struct Reference

Azalia Header structure.

#include <FspsUpd.h>

Public Attributes

UINT16 Vendorld

Codec Vendor ID.

UINT16 DeviceId

Codec Device ID.

UINT8 RevisionId

Revision ID of the codec. 0xFF matches any revision.

UINT8 SdiNum

SDI number, 0xFF matches any SDI.

UINT16 DataDwords

Number of data DWORDs pointed by the codec data buffer.

UINT32 Reserved

Reserved for future use. Must be set to 0.

8.2.1 Detailed Description

Azalia Header structure.

Definition at line 45 of file FspsUpd.h.

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

• FspsUpd.h

8.3 DIMM_INFO Struct Reference

Memory SMBIOS & OC Memory Data Hob.

#include <MemInfoHob.h>

Public Attributes

UINT8 Status

See MrcDimmStatus for the definition of this field.

UINT32 DimmCapacity

DIMM size in MBytes.

UINT8 ModulePartNum [20]

Module part number for DDR3 is 18 bytes however for DRR4 20 bytes as per JEDEC Spec, so reserving 20 bytes.

UINT8 RankInDimm

The number of ranks in this DIMM.

UINT8 SpdDramDeviceType

Save SPD DramDeviceType information needed for SMBIOS structure creation.

UINT8 SpdModuleType

Save SPD ModuleType information needed for SMBIOS structure creation.

UINT8 SpdModuleMemoryBusWidth

Save SPD ModuleMemoryBusWidth information needed for SMBIOS structure creation.

UINT8 SpdSave [MAX_SPD_SAVE]

Save SPD Manufacturing information needed for SMBIOS structure creation.

8.3.1 Detailed Description

Memory SMBIOS & OC Memory Data Hob.

Definition at line 181 of file MemInfoHob.h.

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

MemInfoHob.h

8.4 FSP_M_CONFIG Struct Reference

Fsp M Configuration.

#include <FspmUpd.h>

Public Attributes

UINT64 PlatformMemorySize

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

UINT32 MemorySpdPtr00

Offset 0x0048 - Memory SPD Pointer Channel 0 Dimm 0 Pointer to SPD data in Memory.

UINT32 MemorySpdPtr01

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

UINT32 MemorySpdPtr10

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

UINT32 MemorySpdPtr11

Offset 0x0054 - Memory SPD Pointer Channel 1 Dimm 1 Pointer to SPD data in Memory.

UINT16 MemorySpdDataLen

Offset 0x0058 - SPD Data Length Length of SPD Data 0x100:256 Bytes, 0x200:512 Bytes.

UINT8 DqByteMapCh0 [12]

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

UINT8 DqByteMapCh1 [12]

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

UINT8 DqsMapCpu2DramCh0 [8]

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

UINT8 DqsMapCpu2DramCh1 [8]

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

UINT16 RcompResistor [3]

Offset 0x0082 - RcompResister settings Indicates RcompReister settings: Board-dependent.

• UINT16 RcompTarget [5]

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

UINT8 DqPinsInterleaved

Offset 0x0092 - Dgs Pins Interleaved Setting Indicates DqPinsInterleaved setting: board-dependent \$EN_DIS.

UINT8 CaVrefConfig

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

UINT8 SmramMask

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

UINT8 MrcFastBoot

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

UINT8 UnusedUpdSpace0 [2]

Offset 0x0096.

UINT32 ledSize

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

UINT32 TsegSize

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

UINT16 MmioSize

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

UINT8 ProbelessTrace

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

UINT8 UnusedUpdSpace1 [2]

Offset 0x00A3.

UINT8 SmbusEnable

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

UINT8 EnableTraceHub

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

UINT8 UnusedUpdSpace2 [60]

Offset 0x00A7.

UINT8 lgdDvmt50PreAlloc

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

UINT8 InternalGfx

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

UINT8 ApertureSize

Offset 0x00E5 - Aperture Size Select the Aperture Size.

UINT8 SaGv

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

UINT8 RMT

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

UINT16 DdrFreqLimit

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

UINT8 UserBd

Offset 0x00EA - Board Type MrcBoardType, Options are 0=Mobile/Mobile Halo, 1=Desktop/DT Halo, 5=ULT/ULX/\circ Mobile Halo, 7=UP Server 0:Mobile/Mobile Halo, 1:Desktop/DT Halo, 5:ULT/ULX/Mobile Halo, 7:UP Server.

• UINT8 UnusedUpdSpace3 [105]

Offset 0x00EB.

• UINT32 MmaTestContentPtr

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

UINT32 MmaTestContentSize

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

UINT32 MmaTestConfigPtr

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

UINT32 MmaTestConfigSize

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

UINT8 UnusedUpdSpace4 [19]

Offset 0x0164.

UINT8 SpdProfileSelected

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

UINT16 VddVoltage

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

UINT8 RefClk

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

UINT8 Ratio

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

UINT8 OddRatioMode

Offset 0x017C - QCLK Odd Ratio Adds 133 or 100 MHz to QCLK frequency, depending on RefClk \$EN DIS.

UINT8 tCL

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

UINT16 tFAW

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

UINT16 tRAS

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

UINT8 tCWL

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

UINT8 tRCDtRP

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

UINT16 tREFI

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

UINT16 tRFC

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

UINT8 tRRD

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

UINT8 tRTP

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

UINT8 tWR

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

UINT8 tWTR

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

UINT8 NModeSupport

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

UINT8 DIIBwEn0

Offset 0x018D - DIIBwEn[0] DIIBwEn[0], for 1067 (0..7)

UINT8 DIIBwEn1

Offset 0x018E - DIIBwEn[1] DIIBwEn[1], for 1333 (0..7)

• UINT8 DIIBwEn2

Offset 0x018F - DIIBwEn[2] DIIBwEn[2], for 1600 (0..7)

UINT8 DIIBwEn3

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

UINT8 CmdTriStateDis

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

UINT8 UnusedUpdSpace5 [14]

Offset 0x0192.

UINT32 Heci1BarAddress

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

• UINT32 Heci2BarAddress

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

UINT32 Heci3BarAddress

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

UINT8 HeciTimeouts

Offset 0x01AC - HECI Timeouts Enable/Disable.

UINT8 UnusedUpdSpace6 [115]

Offset 0x01AD.

UINT16 SgDelayAfterPwrEn

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

UINT16 SgDelayAfterHoldReset

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

UINT16 MmioSizeAdjustment

Offset 0x0224 - MMIO size adjustment for AUTO mode Positive number means increasing MMIO size, Negative value means decreasing MMIO size: 0 (Default)=no change to AUTO mode MMIO size.

UINT8 DmiGen3ProgramStaticEq

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

UINT8 Peg0Enable

Offset 0x0227 - Enable/Disable PEG 0 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.

UINT8 Peg1Enable

Offset 0x0228 - Enable/Disable PEG 1 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.

UINT8 Peg2Enable

Offset 0x0229 - Enable/Disable PEG 2 Disabled(0x0): Disable PEG Port, Enabled(0x1): Enable PEG Port (If Silicon SKU permits it), Auto(0x2)(Default): If an endpoint is present, enable the PEG Port, Disable otherwise 0:Disable, 1:Enable, 2:AUTO.

UINT8 Peg0MaxLinkSpeed

Offset 0x022A - PEG 0 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.

• UINT8 Peg1MaxLinkSpeed

Offset 0x022B - PEG 1 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.

UINT8 Peg2MaxLinkSpeed

Offset 0x022C - PEG 2 Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.

UINT8 Peg0MaxLinkWidth

Offset 0x022D - PEG 0 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4, (0x4): Limit Link to x8 0:Auto, 1:x1, 2:x2, 3:x4, 4:x8.

UINT8 Peg1MaxLinkWidth

Offset 0x022E - PEG 1 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2, (0x3):Limit Link to x4 0:Auto, 1:x1, 2:x2, 3:x4.

• UINT8 Peg2MaxLinkWidth

Offset 0x022F - PEG 2 Max Link Width Auto (Default)(0x0): Maximum possible link width, (0x1): Limit Link to x1, (0x2): Limit Link to x2 0:Auto, 1:x1, 2:x2.

• UINT8 Peg0PowerDownUnusedLanes

Offset 0x0230 - Power down unused lanes on PEG 0 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

UINT8 Peg1PowerDownUnusedLanes

Offset 0x0231 - Power down unused lanes on PEG 1 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

UINT8 Peg2PowerDownUnusedLanes

Offset 0x0232 - Power down unused lanes on PEG 2 (0x0): Do not power down any lane, (0x1): Bios will power down unused lanes based on the max possible link width 0:No power saving, 1:Auto.

UINT8 InitPcieAspmAfterOprom

Offset 0x0233 - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.

UINT8 PegDisableSpreadSpectrumClocking

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

UINT8 DmiGen3RootPortPreset [4]

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

• UINT8 DmiGen3EndPointPreset [4]

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

UINT8 DmiGen3EndPointHint [4]

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

UINT8 DmiGen3RxCtlePeaking [2]

Offset 0x0241 - DMI Gen3 RxCTLEp per-Bundle control Range: 0-15, 12 is default for each bundle, must be specified based upon platform design.

UINT8 DmiDeEmphasis

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

• UINT8 PegGen3RxCtlePeaking [8]

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

UINT32 PegDataPtr

Offset 0x024C - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA_PEG_DATA) and platform code can save/restore this data to skip preset search in the following boots.

• UINT8 PegGpioData [16]

Offset 0x0250 - PEG PERST# GPIO information The reference code will use the information in this structure in order to reset PCIe Gen3 devices during equalization, if necessary.

• UINT8 UnusedUpdSpace7 [1]

Offset 0x0260.

UINT8 PegRootPortHPE [3]

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

• UINT32 GttMmAdr

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

UINT16 GttSize

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

UINT8 PrimaryDisplay

Offset 0x026A - Selection of the primary display device 0=iGFX, 1=PEG, 2=PCle Graphics on PCH, 3(Default)=A←UTO, 4=Switchable Graphics 0:iGFX, 1:PEG, 2:PCle Graphics on PCH, 3:AUTO, 4:Switchable Graphics.

UINT8 SaRtd3Pcie0Gpio [24]

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

UINT8 SaRtd3Pcie1Gpio [24]

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

• UINT8 SaRtd3Pcie2Gpio [24]

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

UINT8 RootPortDev

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

UINT8 RootPortFun

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

UINT8 TxtImplemented

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

UINT8 SaOcSupport

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

UINT8 GtsVoltageMode

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

UINT8 GtusVoltageMode

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

UINT8 GtsMaxOcRatio

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

UINT16 GtsVoltageOffset

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

UINT16 GtsVoltageOverride

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

• UINT16 GtsExtraTurboVoltage

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

• UINT16 GtusVoltageOffset

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

• UINT16 GtusVoltageOverride

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

UINT16 GtusExtraTurboVoltage

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

UINT16 SaVoltageOffset

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

UINT8 EdramRatio

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

• UINT8 GtusMaxOcRatio

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

UINT8 BistOnReset

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

UINT8 SkipStopPbet

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

• UINT8 EnableC6Dram

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

UINT8 OcSupport

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

UINT8 OcLock

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

• UINT8 CoreMaxOcRatio

Offset 0x02CF - Maximum Core Turbo Ratio Override Maximum core turbo ratio override allows to increase CPU core frequency beyond the fused max turbo ratio limit.

UINT8 CoreVoltageMode

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

UINT8 RingMinOcRatio

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

• UINT8 RingMaxOcRatio

Offset 0x02D2 - Maximum clr turbo ratio override Maximum clr turbo ratio override allows to increase CPU clr frequency beyond the fused max turbo ratio limit.

UINT8 HyperThreading

Offset 0x02D3 - Hyper Threading Enable/Disable Enable or Disable Hyper Threading; 0: Disable; **1: Enable** \$EN←_DIS.

UINT8 CpuRatioOverride

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

UINT8 CpuRatio

Offset 0x02D5 - CPU ratio value CPU ratio value.

UINT8 BootFrequency

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

UINT8 ActiveCoreCount

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

UINT8 FClkFrequency

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

• UINT8 JtagC10PowerGateDisable

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

UINT8 VmxEnable

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

UINT8 Avx2RatioOffset

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

• UINT16 CoreVoltageOverride

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

UINT16 CoreVoltageAdaptive

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

UINT16 CoreVoltageOffset

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

UINT16 CorePllVoltageOffset

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

UINT8 BclkAdaptiveVoltage

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

UINT8 BiosGuard

Offset 0x02E5 - BiosGuard Enable/Disable.

UINT8 EnableSgx

Offset 0x02E6 - EnableSgx Enable/Disable.

UINT8 Txt

Offset 0x02E7 - Txt Enable/Disable.

UINT32 PrmrrSize

Offset 0x02E8 - PrmrrSize Enable/Disable.

UINT32 SinitMemorySize

Offset 0x02EC - SinitMemorySize Enable/Disable.

UINT64 TxtDprMemoryBase

Offset 0x02F0 - TxtDprMemoryBase Enable/Disable.

UINT32 TxtDprMemorySize

Offset 0x02F8 - TxtDprMemorySize Enable/Disable.

UINT32 TxtHeapMemorySize

Offset 0x02FC - TxtHeapMemorySize Enable/Disable.

• UINT8 FlashWearOutProtection

Offset 0x0300 - FlashWearOutProtection Enable/Disable.

• UINT8 ReservedSecurityPreMem [9]

Offset 0x0301 - ReservedSecurityPreMem Reserved for Security Pre-Mem \$EN_DIS.

UINT8 PchHpetEnable

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

UINT8 PchHpetBdfValid

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

UINT32 PchHpetBase

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

UINT8 PchHpetBusNumber

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

UINT8 PchHpetDeviceNumber

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

UINT8 PchHpetFunctionNumber

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

UINT8 PchPcieHsioRxSetCtleEnable [24]

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

UINT8 PchPcieHsioRxSetCtle [24]

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

UINT8 PchPcieHsioTxGen1DownscaleAmpEnable [24]

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

UINT8 PchPcieHsioTxGen1DownscaleAmp [24]

Offset 0x035B - PCH HSIO PCIE Gen 2 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 2 TX Output Downscale Amplitude Adjustment value.

• UINT8 PchPcieHsioTxGen2DownscaleAmpEnable [24]

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

UINT8 PchPcieHsioTxGen2DownscaleAmp [24]

Offset 0x038B - PCH HSIO PCIE Gen 2 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 2 TX Output Downscale Amplitude Adjustment value.

UINT8 PchPcieHsioTxGen3DownscaleAmpEnable [24]

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

UINT8 PchPcieHsioTxGen3DownscaleAmp [24]

Offset 0x03BB - PCH HSIO PCIE Gen 3 TX Output Downscale Amplitude Adjustment value PCH PCIe Gen 3 TX Output Downscale Amplitude Adjustment value.

UINT8 PchPcieHsioTxGen1DeEmphEnable [24]

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

• UINT8 PchPcieHsioTxGen1DeEmph [24]

Offset 0x03EB - PCH HSIO PCIE Gen 1 TX Output De-Emphasis Adjustment value PCH PCIe Gen 1 TX Output De-Emphasis Adjustment Setting.

• UINT8 PchPcieHsioTxGen2DeEmph3p5Enable [24]

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

• UINT8 PchPcieHsioTxGen2DeEmph3p5 [24]

Offset 0x041B - PCH HSIO PCIE Gen 2 TX Output -3.5dB De-Emphasis Adjustment value PCH PCIe Gen 2 TX Output -3.5dB De-Emphasis Adjustment Setting.

UINT8 PchPcieHsioTxGen2DeEmph6p0Enable [24]

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

• UINT8 PchPcieHsioTxGen2DeEmph6p0 [24]

Offset 0x044B - PCH HSIO PCIE Gen 2 TX Output -6.0dB De-Emphasis Adjustment value PCH PCIe Gen 2 TX Output -6.0dB De-Emphasis Adjustment Setting.

UINT8 PchSataHsioRxGen1EqBoostMagEnable [8]

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

UINT8 PchSataHsioRxGen1EgBoostMag [8]

Offset 0x046B - PCH HSIO SATA 1.5 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 1.5 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

UINT8 PchSataHsioRxGen2EqBoostMagEnable [8]

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

UINT8 PchSataHsioRxGen2EqBoostMag [8]

Offset 0x047B - PCH HSIO SATA 3.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 3.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

UINT8 PchSataHsioRxGen3EqBoostMagEnable [8]

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

UINT8 PchSataHsioRxGen3EqBoostMag [8]

Offset 0x048B - PCH HSIO SATA 6.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value PCH HSIO SATA 6.0 Gb/s Receiver Equalization Boost Magnitude Adjustment value.

UINT8 PchSataHsioTxGen1DownscaleAmpEnable [8]

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

UINT8 PchSataHsioTxGen1DownscaleAmp [8]

Offset 0x049B - PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 1.5 Gb/s TX Output Downscale Amplitude Adjustment value.

UINT8 PchSataHsioTxGen2DownscaleAmpEnable [8]

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

UINT8 PchSataHsioTxGen2DownscaleAmp [8]

Offset 0x04AB - PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 3.0 Gb/s TX Output Downscale Amplitude Adjustment value.

UINT8 PchSataHsioTxGen3DownscaleAmpEnable [8]

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

UINT8 PchSataHsioTxGen3DownscaleAmp [8]

Offset 0x04BB - PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value PCH HSIO SATA 6.0 Gb/s TX Output Downscale Amplitude Adjustment value.

UINT8 PchSataHsioTxGen1DeEmphEnable [8]

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

UINT8 PchSataHsioTxGen1DeEmph [8]

Offset 0x04CB - PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 1.5 Gb/s TX Output De-Emphasis Adjustment Setting.

UINT8 PchSataHsioTxGen2DeEmphEnable [8]

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

UINT8 PchSataHsioTxGen2DeEmph [8]

Offset 0x04DB - PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 3.0 Gb/s TX Output De-Emphasis Adjustment Setting.

UINT8 PchSataHsioTxGen3DeEmphEnable [8]

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

UINT8 PchSataHsioTxGen3DeEmph [8]

Offset 0x04EB - PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting PCH HSIO SATA 6.0 Gb/s TX Output De-Emphasis Adjustment Setting.

UINT8 PchLpcEnhancePort8xhDecoding

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

UINT16 PchAcpiBase

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

UINT8 PchPort80Route

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

UINT8 SmbusArpEnable

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

UINT16 PchSmbusloBase

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

UINT8 PchNumRsvdSmbusAddresses

Offset 0x04FA - Number of RsvdSmbusAddressTable.

UINT8 UnusedUpdSpace8

Offset 0x04FB.

UINT32 RsvdSmbusAddressTablePtr

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

UINT32 TraceHubMemReg0Size

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

• UINT32 TraceHubMemReg1Size

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

UINT32 PcieRpEnableMask

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

• UINT8 PcdDebugInterfaceFlags

Offset 0x050C - Debug Interfaces Debug Interfaces.

UINT8 PcdSerialloUartNumber

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

UINT8 PcdlsaSerialUartBase

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

• UINT8 PchPmPciePllSsc

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

UINT8 PeciC10Reset

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

UINT8 PeciSxReset

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

• UINT8 PcdSerialDebugBaudRate

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

UINT8 PcdSerialDebugLevel

Offset 0x0513 - PcdSerialDebugLevel Serial Debug Message Level.

UINT8 EvLoader

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

• UINT8 ReservedFspmUpd [11]

Offset 0x0515.

8.4.1 Detailed Description

Fsp M Configuration.

Definition at line 56 of file FspmUpd.h.

8.4.2 Member Data Documentation

8.4.2.1 UINT8 FSP_M_CONFIG::ActiveCoreCount

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

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

Definition at line 796 of file FspmUpd.h.

8.4.2.2 UINT8 FSP_M_CONFIG::ApertureSize

Offset 0x00E5 - Aperture Size Select the Aperture Size.

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

Definition at line 208 of file FspmUpd.h.

8.4.2.3 UINT8 FSP_M_CONFIG::Avx2RatioOffset

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

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

Definition at line 821 of file FspmUpd.h.

8.4.2.4 UINT8 FSP_M_CONFIG::BclkAdaptiveVoltage

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

0: Disable;1: Enable \$EN_DIS

Definition at line 850 of file FspmUpd.h.

8.4.2.5 UINT8 FSP_M_CONFIG::BiosGuard

Offset 0x02E5 - BiosGuard Enable/Disable.

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

Definition at line 856 of file FspmUpd.h.

8.4.2.6 UINT8 FSP_M_CONFIG::BistOnReset

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

\$EN_DIS

Definition at line 716 of file FspmUpd.h.

8.4.2.7 UINT8 FSP_M_CONFIG::BootFrequency

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

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

Note

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

Definition at line 789 of file FspmUpd.h.

8.4.2.8 UINT8 FSP_M_CONFIG::CmdTriStateDis

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

\$EN_DIS

Definition at line 386 of file FspmUpd.h.

8.4.2.9 UINT8 FSP_M_CONFIG::CoreMaxOcRatio

Offset 0x02CF - Maximum Core Turbo Ratio Override Maximum core turbo ratio override allows to increase CPU core frequency beyond the fused max turbo ratio limit.

0: Hardware defaults. Range: 0-83

Definition at line 746 of file FspmUpd.h.

8.4.2.10 UINT16 FSP_M_CONFIG::CorePIIVoltageOffset

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

0: No offset. Range 0-63

Definition at line 843 of file FspmUpd.h.

8.4.2.11 UINT16 FSP_M_CONFIG::CoreVoltageAdaptive

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

Valid Range 0 to 2000

Definition at line 833 of file FspmUpd.h.

8.4.2.12 UINT8 FSP_M_CONFIG::CoreVoltageMode

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

\$EN_DIS

Definition at line 752 of file FspmUpd.h.

8.4.2.13 UINT16 FSP_M_CONFIG::CoreVoltageOverride

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

Valid Range 0 to 2000

Definition at line 827 of file FspmUpd.h.

8.4.2.14 UINT8 FSP_M_CONFIG::CpuRatio

Offset 0x02D5 - CPU ratio value CPU ratio value.

Valid Range 0 to 63

Definition at line 781 of file FspmUpd.h.

8.4.2.15 UINT8 FSP_M_CONFIG::CpuRatioOverride

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

Note

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

Definition at line 776 of file FspmUpd.h.

8.4.2.16 UINT16 FSP_M_CONFIG::DdrFreqLimit

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

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

Definition at line 229 of file FspmUpd.h.

8.4.2.17 UINT8 FSP_M_CONFIG::DmiDeEmphasis

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

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

Definition at line 565 of file FspmUpd.h.

8.4.2.18 UINT8 FSP_M_CONFIG::DmiGen3EndPointHint[4]

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

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

Definition at line 554 of file FspmUpd.h.

8.4.2.19 UINT8 FSP_M_CONFIG::DmiGen3EndPointPreset[4]

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

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

Definition at line 549 of file FspmUpd.h.

8.4.2.20 UINT8 FSP_M_CONFIG::DmiGen3ProgramStaticEq

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

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

Definition at line 440 of file FspmUpd.h.

8.4.2.21 UINT8 FSP_M_CONFIG::DmiGen3RootPortPreset[4]

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

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

Definition at line 544 of file FspmUpd.h.

8.4.2.22 UINT8 FSP_M_CONFIG::EnableC6Dram

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

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

Definition at line 728 of file FspmUpd.h.

8.4.2.23 UINT8 FSP_M_CONFIG::EnableSgx

Offset 0x02E6 - EnableSgx Enable/Disable.

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

Definition at line 862 of file FspmUpd.h.

8.4.2.24 UINT8 FSP_M_CONFIG::EnableTraceHub

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

\$EN_DIS

Definition at line 186 of file FspmUpd.h.

8.4.2.25 UINT8 FSP_M_CONFIG::EvLoader

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

\$EN DIS

Definition at line 1212 of file FspmUpd.h.

8.4.2.26 UINT8 FSP_M_CONFIG::FClkFrequency

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

1: 1 GHz (DT/Halo). Not supported on ULT/ULX.- 2: 400 MHz. - 3: Reserved 0:800 MHz, 1: 1 GHz, 2: 400 MHz, 3: Reserved

Definition at line 803 of file FspmUpd.h.

8.4.2.27 UINT8 FSP_M_CONFIG::FlashWearOutProtection

Offset 0x0300 - FlashWearOutProtection Enable/Disable.

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

Definition at line 899 of file FspmUpd.h.

8.4.2.28 UINT8 FSP_M_CONFIG::HeciTimeouts

Offset 0x01AC - HECI Timeouts Enable/Disable.

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

Definition at line 411 of file FspmUpd.h.

8.4.2.29 UINT8 FSP_M_CONFIG::lgdDvmt50PreAlloc

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

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

Definition at line 196 of file FspmUpd.h.

8.4.2.30 UINT8 FSP_M_CONFIG::InitPcieAspmAfterOprom

Offset 0x0233 - PCIe ASPM programming will happen in relation to the Oprom Select when PCIe ASPM programming will happen in relation to the Oprom.

Before(0x0)(Default): Do PCle ASPM programming before Oprom, After(0x1): Do PCle ASPM programming after Oprom, requires an SMI handler to save/restore ASPM settings during S3 resume 0:Before, 1:After

Definition at line 532 of file FspmUpd.h.

8.4.2.31 UINT8 FSP_M_CONFIG::InternalGfx

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

\$EN DIS

Definition at line 202 of file FspmUpd.h.

8.4.2.32 UINT8 FSP_M_CONFIG::JtagC10PowerGateDisable

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

\$EN_DIS

Definition at line 809 of file FspmUpd.h.

8.4.2.33 UINT16 FSP_M_CONFIG::MmioSize

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

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

Definition at line 163 of file FspmUpd.h.

8.4.2.34 UINT8 FSP_M_CONFIG::OcLock

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

\$EN DIS

Definition at line 740 of file FspmUpd.h.

8.4.2.35 UINT8 FSP_M_CONFIG::PcdDebugInterfaceFlags

Offset 0x050C - Debug Interfaces Debug Interfaces.

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

Definition at line 1161 of file FspmUpd.h.

8.4.2.36 UINT8 FSP_M_CONFIG::PcdlsaSerialUartBase

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

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

Definition at line 1173 of file FspmUpd.h.

8.4.2.37 UINT8 FSP_M_CONFIG::PcdSerialDebugBaudRate

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

3:9600, 4:19200, 6:56700, 7:115200. 3:9600, 4:19200, 6:56700, 7:115200

Definition at line 1197 of file FspmUpd.h.

8.4.2.38 UINT8 FSP_M_CONFIG::PcdSerialDebugLevel

Offset 0x0513 - PcdSerialDebugLevel Serial Debug Message Level.

0:Disable, 1:Error Only, 2:Error & Warnings, 3:Load, Error, Warnings & Info, 4:Load, Error, Warnings, Info & Event, 5:Load, Error, Warnings, Info & Verbose 0:Disable, 1:Error Only, 2:Error and Warnings, 3:Load Error Warnings and Info, 4:Load Error Warnings and Info, 5:Load Error Warnings Info and Verbose

Definition at line 1206 of file FspmUpd.h.

8.4.2.39 UINT8 FSP_M_CONFIG::PcdSerialIoUartNumber

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

0:SerialloUart0, 1:SerialloUart1, 2:SerialloUart2

Definition at line 1167 of file FspmUpd.h.

8.4.2.40 UINT16 FSP_M_CONFIG::PchAcpiBase

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

Default is 0x1800.

Definition at line 1108 of file FspmUpd.h.

8.4.2.41 UINT32 FSP_M_CONFIG::PchHpetBase

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

Default is 0xFED00000.

Definition at line 922 of file FspmUpd.h.

8.4.2.42 UINT8 FSP_M_CONFIG::PchHpetBdfValid

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

0: Disable; 1: Enable. \$EN_DIS

Definition at line 917 of file FspmUpd.h.

8.4.2.43 UINT8 FSP_M_CONFIG::PchHpetBusNumber

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

Default is 0xF0.

Definition at line 927 of file FspmUpd.h.

8.4.2.44 UINT8 FSP_M_CONFIG::PchHpetDeviceNumber

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

Default is 0x1F.

Definition at line 932 of file FspmUpd.h.

8.4.2.45 UINT8 FSP_M_CONFIG::PchHpetEnable

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

\$EN DIS

Definition at line 911 of file FspmUpd.h.

8.4.2.46 UINT8 FSP_M_CONFIG::PchHpetFunctionNumber

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

Default is 0x00.

Definition at line 937 of file FspmUpd.h.

8.4.2.47 UINT8 FSP_M_CONFIG::PchLpcEnhancePort8xhDecoding

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

\$EN_DIS

Definition at line 1103 of file FspmUpd.h.

8.4.2.48 UINT8 FSP_M_CONFIG::PchNumRsvdSmbusAddresses

Offset 0x04FA - Number of RsvdSmbusAddressTable.

The number of elements in the RsvdSmbusAddressTable.

Definition at line 1130 of file FspmUpd.h.

8.4.2.49 UINT8 FSP_M_CONFIG::PchPmPciePIISsc

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

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

Definition at line 1179 of file FspmUpd.h.

8.4.2.50 UINT8 FSP_M_CONFIG::PchPort80Route

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

\$EN DIS

Definition at line 1114 of file FspmUpd.h.

8.4.2.51 UINT32 FSP_M_CONFIG::PcieRpEnableMask

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

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

Definition at line 1155 of file FspmUpd.h.

8.4.2.52 UINT8 FSP_M_CONFIG::PeciC10Reset

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

\$EN DIS

Definition at line 1185 of file FspmUpd.h.

8.4.2.53 UINT8 FSP_M_CONFIG::PeciSxReset

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

\$EN_DIS

Definition at line 1191 of file FspmUpd.h.

8.4.2.54 UINT32 FSP_M_CONFIG::PegDataPtr

Offset 0x024C - Memory data pointer for saved preset search results The reference code will store the Gen3 Preset Search results in the SaDataHob's PegData structure (SA_PEG_DATA) and platform code can save/restore this data to skip preset search in the following boots.

Range: 0-0xFFFFFFF, default is 0

Definition at line 577 of file FspmUpd.h.

8.4.2.55 UINT8 FSP_M_CONFIG::PegDisableSpreadSpectrumClocking

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

 $Normal\ Operation (0x0) (Default)\ -\ SSC\ enabled,\ Disable\ SSC (0X1)\ -\ Disable\ SSC\ per\ platform\ design\ or\ for\ compliance\ testing\ 0: Normal\ Operation,\ 1: Disable\ SSC$

Definition at line 539 of file FspmUpd.h.

8.4.2.56 UINT32 FSP_M_CONFIG::PrmrrSize

Offset 0x02E8 - PrmrrSize Enable/Disable.

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

Definition at line 873 of file FspmUpd.h.

8.4.2.57 UINT8 FSP_M_CONFIG::ProbelessTrace

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

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

Definition at line 170 of file FspmUpd.h.

8.4.2.58 UINT8 FSP_M_CONFIG::Ratio

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

Set to Auto to recalculate memory timings listed below. 0:Auto, 4:4, 5:5, 6:6, 7:7, 8:8, 9:9, 10:10, 11:11, 12:12, 13:13, 14:14, 15:15

Definition at line 292 of file FspmUpd.h.

8.4.2.59 UINT8 FSP_M_CONFIG::RefClk

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

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

Definition at line 285 of file FspmUpd.h.

8.4.2.60 UINT8 FSP_M_CONFIG::RingMaxOcRatio

Offset 0x02D2 - Maximum clr turbo ratio override Maximum clr turbo ratio override allows to increase CPU clr frequency beyond the fused max turbo ratio limit.

0: Hardware defaults. Range: 0-83

Definition at line 763 of file FspmUpd.h.

8.4.2.61 UINT8 FSP_M_CONFIG::RingMinOcRatio

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

0: Hardware defaults. Range: 0-83

Definition at line 757 of file FspmUpd.h.

8.4.2.62 UINT8 FSP_M_CONFIG::RMT

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

\$EN_DIS

Definition at line 222 of file FspmUpd.h.

8.4.2.63 UINT8 FSP_M_CONFIG::SaGv

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

Only effects ULX/ULT CPUs. 0=Disabled, 1=FixedLow, 2=FixedHigh, and 3=Enabled. 0:Disabled, 1:FixedLow, 2:FixedHigh, 3:Enabled

Definition at line 216 of file FspmUpd.h.

8.4.2.64 UINT32 FSP_M_CONFIG::SinitMemorySize

Offset 0x02EC - SinitMemorySize Enable/Disable.

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

Definition at line 878 of file FspmUpd.h.

8.4.2.65 UINT8 FSP_M_CONFIG::SmbusArpEnable

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

\$EN_DIS

Definition at line 1120 of file FspmUpd.h.

8.4.2.66 UINT8 FSP_M_CONFIG::SmbusEnable

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

\$EN DIS

Definition at line 180 of file FspmUpd.h.

8.4.2.67 UINT8 FSP_M_CONFIG::SpdProfileSelected

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

Options are 0=Default profile, 1=Custom profile, 2=XMP Profile 1, 3=XMP Profile 2 0:Default profile, 1:Custom profile, 2:XMP profile 1, 3:XMP profile 2

Definition at line 271 of file FspmUpd.h.

8.4.2.68 UINT8 FSP_M_CONFIG::tRTP

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

DDR4 legal values: 5, 6, 7, 8, 9, 10, 12

Definition at line 344 of file FspmUpd.h.

8.4.2.69 UINT32 FSP_M_CONFIG::TsegSize

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

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

Definition at line 158 of file FspmUpd.h.

8.4.2.70 UINT8 FSP_M_CONFIG::Txt

Offset 0x02E7 - Txt Enable/Disable.

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

Definition at line 868 of file FspmUpd.h.

8.4.2.71 UINT64 FSP_M_CONFIG::TxtDprMemoryBase

Offset 0x02F0 - TxtDprMemoryBase Enable/Disable.

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

Definition at line 883 of file FspmUpd.h.

8.4.2.72 UINT32 FSP_M_CONFIG::TxtDprMemorySize

Offset 0x02F8 - TxtDprMemorySize Enable/Disable.

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

Definition at line 888 of file FspmUpd.h.

8.4.2.73 UINT32 FSP_M_CONFIG::TxtHeapMemorySize

Offset 0x02FC - TxtHeapMemorySize Enable/Disable.

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

Definition at line 893 of file FspmUpd.h.

8.4.2.74 UINT8 FSP_M_CONFIG::TxtImplemented

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

Disabled(0x0)(Default): MRC will not wait for TXT initialization, Enabled(0x1): MRC will wait for TXT initialization \mathbb{E} DIS

Definition at line 642 of file FspmUpd.h.

8.4.2.75 UINT16 FSP_M_CONFIG::VddVoltage

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

Default = no override 0:Default, 1100:1.10 Volts, 1150:1.15 Volts, 1200:1.20 Volts, 1250:1.25 Volts, 1300:1.30 Volts, 1350:1.35 Volts, 1400:1.40 Volts, 1450:1.45 Volts, 1500:1.50 Volts, 1550:1.55 Volts, 1600:1.60 Volts, 1650:1.65 Volts

Definition at line 279 of file FspmUpd.h.

8.4.2.76 UINT8 FSP_M_CONFIG::VmxEnable

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

\$EN_DIS

Definition at line 815 of file FspmUpd.h.

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

FspmUpd.h

8.5 FSP_M_TEST_CONFIG Struct Reference

Fsp M Test Configuration.

#include <FspmUpd.h>

Public Attributes

UINT32 Signature

Offset 0x0520.

UINT8 SkipExtGfxScan

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

UINT8 BdatEnable

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

UINT8 ScanExtGfxForLegacyOpRom

Offset 0x0526 - Detect External Graphics device for LegacyOpROM Detect and report if external graphics device only support LegacyOpROM or not (to support CSM auto-enable).

UINT8 LockPTMregs

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

UINT8 DmiVc1

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

UINT8 DmiVcm

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

UINT8 DmiMaxLinkSpeed

Offset 0x052A - DMI Max Link Speed Auto (Default)(0x0): Maximum possible link speed, Gen1(0x1): Limit Link to Gen1 Speed, Gen2(0x2): Limit Link to Gen2 Speed, Gen3(0x3):Limit Link to Gen3 Speed 0:Auto, 1:Gen1, 2:Gen2, 3:Gen3.

UINT8 DmiGen3EqPh2Enable

Offset 0x052B - DMI Equalization Phase 2 DMI Equalization Phase 2.

UINT8 DmiGen3EqPh3Method

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

UINT8 Peg0Gen3EqPh2Enable

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

• UINT8 Peg1Gen3EqPh2Enable

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

UINT8 Peg2Gen3EqPh2Enable

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

• UINT8 Peg0Gen3EqPh3Method

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

UINT8 Peg1Gen3EqPh3Method

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

• UINT8 Peg2Gen3EqPh3Method

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

UINT8 PegGen3ProgramStaticEq

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

UINT8 Gen3SwEqAlwaysAttempt

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

UINT8 Gen3SwEqNumberOfPresets

Offset 0x0535 - Select number of TxEq presets to test in the PCIe/DMI SwEq Select number of TxEq presets to test in the PCIe/DMI SwEq.

UINT8 Gen3SwEqEnableVocTest

Offset 0x0536 - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.

UINT8 PegRxCemTestingMode

Offset 0x0537 - PPCIe Rx Compliance Testing Mode Disabled(0x0)(Default): Normal Operation - Disable PCIe Rx Compliance testing, Enabled(0x1): PCIe Rx Compliance Test Mode - PEG controller is in Rx Compliance Testing Mode; it should only be set when doing PCIe compliance testing \$EN_DIS.

UINT8 PegRxCemLoopbackLane

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

UINT8 PegGenerateBdatMarginTable

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

• UINT8 UnusedUpdSpace9 [6]

Offset 0x053A.

UINT8 PegRxCemNonProtocolAwareness

Offset 0x0540 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

• UINT8 PegGen3RxCtleOverride

Offset 0x0541 - PCIe Override RxCTLE Disable(0x0)(Default): Normal Operation - RxCTLE adaptive behavior enabled, Enable(0x1): Override RxCTLE - Disable RxCTLE adaptive behavior to keep the configured RxCTLE peak values unmodified \$EN_DIS.

UINT8 PegGen3Rsvd

Offset 0x0542 - Rsvd Disable(0x0)(Default): Normal Operation - RxCTLE adaptive behavior enabled, Enable(0x1)←: Override RxCTLE - Disable RxCTLE adaptive behavior to keep the configured RxCTLE peak values unmodified \$EN_DIS.

• UINT8 PanelPowerEnable

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

UINT8 PegGen3RootPortPreset [16]

Offset 0x0544 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.

UINT8 PegGen3EndPointPreset [16]

Offset 0x0554 - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.

UINT8 PegGen3EndPointHint [16]

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

UINT16 Gen3SwEqJitterDwellTime

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

UINT16 Gen3SwEqJitterErrorTarget

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

UINT16 Gen3SwEqVocDwellTime

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

UINT16 Gen3SwEqVocErrorTarget

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

UINT8 SaPreMemTestRsvd [4]

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

UINT64 BiosAcmBase

Offset 0x0580 - BiosAcmBase Enable/Disable.

UINT32 BiosAcmSize

Offset 0x0588 - BiosAcmSize Enable/Disable.

UINT32 TgaSize

Offset 0x058C - TgaSize Enable/Disable.

UINT64 TxtLcpPdBase

Offset 0x0590 - TxtLcpPdBase Enable/Disable.

UINT64 TxtLcpPdSize

Offset 0x0598 - TxtLcpPdSize Enable/Disable.

• UINT16 TotalFlashSize

Offset 0x05A0 - TotalFlashSize Enable/Disable.

• UINT16 BiosSize

Offset 0x05A2 - BiosSize Enable/Disable.

UINT8 PchDciEn

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

UINT8 PchDciAutoDetect

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

UINT8 SmbusDynamicPowerGating

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

• UINT8 WdtDisableAndLock

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

UINT8 SmbusSpdWriteDisable

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

• UINT8 ChipsetInitMessage

Offset 0x05A9 - ChipsetInit HECI message Enable/Disable.

UINT8 BypassPhySyncReset

Offset 0x05AA - Bypass ChipsetInit sync reset.

UINT8 DidInitStat

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

UINT8 DisableCpuReplacedPolling

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

UINT8 SendDidMsg

Offset 0x05AD - ME DID Message Test, 0: disable, 1: enable, Enable/Disable ME DID Message (disable will prevent the DID message from being sent) \$EN_DIS.

UINT8 DisableHeciRetry

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

• UINT8 DisableMessageCheck

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

UINT8 SkipMbpHob

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

• UINT8 HeciCommunication2

Offset 0x05B1 - HECl2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECl2 Device from PCl space.

• UINT8 KtDeviceEnable

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

UINT8 IderDeviceEnable

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

• UINT8 ReservedFspmTestUpd [12]

Offset 0x05B4

8.5.1 Detailed Description

Fsp M Test Configuration.

Definition at line 1221 of file FspmUpd.h.

8.5.2 Member Data Documentation

8.5.2.1 UINT8 FSP_M_TEST_CONFIG::BdatEnable

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

Disable (Default): Do not generate it \$EN_DIS

Definition at line 1238 of file FspmUpd.h.

8.5.2.2 UINT64 FSP_M_TEST_CONFIG::BiosAcmBase

Offset 0x0580 - BiosAcmBase Enable/Disable.

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

Definition at line 1474 of file FspmUpd.h.

8.5.2.3 UINT32 FSP_M_TEST_CONFIG::BiosAcmSize

Offset 0x0588 - BiosAcmSize Enable/Disable.

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

Definition at line 1479 of file FspmUpd.h.

8.5.2.4 UINT16 FSP_M_TEST_CONFIG::BiosSize

Offset 0x05A2 - BiosSize Enable/Disable.

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

Definition at line 1504 of file FspmUpd.h.

8.5.2.5 UINT8 FSP_M_TEST_CONFIG::BypassPhySyncReset

Offset 0x05AA - Bypass ChipsetInit sync reset.

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

Definition at line 1548 of file FspmUpd.h.

8.5.2.6 UINT8 FSP_M_TEST_CONFIG::ChipsetInitMessage

Offset 0x05A9 - ChipsetInit HECI message Enable/Disable.

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

Definition at line 1542 of file FspmUpd.h.

8.5.2.7 UINT8 FSP_M_TEST_CONFIG::DisableHeciRetry

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

\$EN_DIS

Definition at line 1574 of file FspmUpd.h.

8.5.2.8 UINT8 FSP_M_TEST_CONFIG::DisableMessageCheck

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

\$EN DIS

Definition at line 1580 of file FspmUpd.h.

8.5.2.9 UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh2Enable

Offset 0x052B - DMI Equalization Phase 2 DMI Equalization Phase 2.

(0x0): Disable phase 2, (0x1): Enable phase 2, (0x2)(Default): AUTO - Use the current default method 0:Disable phase2, 1:Enable phase2, 2:Auto

Definition at line 1277 of file FspmUpd.h.

8.5.2.10 UINT8 FSP_M_TEST_CONFIG::DmiGen3EqPh3Method

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

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

Definition at line 1287 of file FspmUpd.h.

8.5.2.11 UINT8 FSP_M_TEST_CONFIG::DmiVc1

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

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

Definition at line 1257 of file FspmUpd.h.

8.5.2.12 UINT8 FSP_M_TEST_CONFIG::DmiVcm

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

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

Definition at line 1263 of file FspmUpd.h.

8.5.2.13 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqAlwaysAttempt

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

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

Definition at line 1353 of file FspmUpd.h.

8.5.2.14 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqEnableVocTest

Offset 0x0536 - Enable use of the Voltage Offset and Centering Test in the PCIe SwEq Enable use of the Voltage Offset and Centering Test in the PCIe Software Equalization Algorithm.

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

Definition at line 1371 of file FspmUpd.h.

8.5.2.15 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterDwellTime

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

Warning

Do not change from the default

Definition at line 1448 of file FspmUpd.h.

8.5.2.16 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqJitterErrorTarget

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

Warning

Do not change from the default

Definition at line 1453 of file FspmUpd.h.

8.5.2.17 UINT8 FSP_M_TEST_CONFIG::Gen3SwEqNumberOfPresets

Offset 0x0535 - Select number of TxEq presets to test in the PCle/DMI SwEq Select number of TxEq presets to test in the PCle/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 1363 of file FspmUpd.h.

8.5.2.18 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocDwellTime

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

Warning

Do not change from the default

Definition at line 1458 of file FspmUpd.h.

8.5.2.19 UINT16 FSP_M_TEST_CONFIG::Gen3SwEqVocErrorTarget

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

Warning

Do not change from the default

Definition at line 1463 of file FspmUpd.h.

8.5.2.20 UINT8 FSP_M_TEST_CONFIG::HeciCommunication2

Offset 0x05B1 - HECl2 Interface Communication Test, 0: disable, 1: enable, Adds or Removes HECl2 Device from PCl space.

\$EN_DIS

Definition at line 1592 of file FspmUpd.h.

8.5.2.21 UINT8 FSP_M_TEST_CONFIG::IderDeviceEnable

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

\$EN DIS

Definition at line 1604 of file FspmUpd.h.

8.5.2.22 UINT8 FSP_M_TEST_CONFIG::KtDeviceEnable

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

\$EN DIS

Definition at line 1598 of file FspmUpd.h.

8.5.2.23 UINT8 FSP_M_TEST_CONFIG::LockPTMregs

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

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

Definition at line 1251 of file FspmUpd.h.

8.5.2.24 UINT8 FSP_M_TEST_CONFIG::PanelPowerEnable

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

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

Definition at line 1428 of file FspmUpd.h.

8.5.2.25 UINT8 FSP_M_TEST_CONFIG::PchDciEn

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

\$EN_DIS

Definition at line 1510 of file FspmUpd.h.

8.5.2.26 UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh2Enable

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

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

Definition at line 1294 of file FspmUpd.h.

8.5.2.27 UINT8 FSP_M_TEST_CONFIG::Peg0Gen3EqPh3Method

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

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

Definition at line 1318 of file FspmUpd.h.

8.5.2.28 UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh2Enable

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

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

Definition at line 1301 of file FspmUpd.h.

8.5.2.29 UINT8 FSP_M_TEST_CONFIG::Peg1Gen3EqPh3Method

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

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

Definition at line 1328 of file FspmUpd.h.

8.5.2.30 UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh2Enable

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

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

Definition at line 1308 of file FspmUpd.h.

8.5.2.31 UINT8 FSP_M_TEST_CONFIG::Peg2Gen3EqPh3Method

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

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

Definition at line 1338 of file FspmUpd.h.

8.5.2.32 UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointHint[16]

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

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

Definition at line 1443 of file FspmUpd.h.

8.5.2.33 UINT8 FSP_M_TEST_CONFIG::PegGen3EndPointPreset[16]

Offset 0x0554 - PEG Gen3 End port preset values per lane Used for programming PEG Gen3 preset values per lane.

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

Definition at line 1438 of file FspmUpd.h.

8.5.2.34 UINT8 FSP_M_TEST_CONFIG::PegGen3ProgramStaticEq

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

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

Definition at line 1345 of file FspmUpd.h.

8.5.2.35 UINT8 FSP_M_TEST_CONFIG::PegGen3RootPortPreset[16]

Offset 0x0544 - PEG Gen3 Root port preset values per lane Used for programming PEG Gen3 preset values per lane.

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

Definition at line 1433 of file FspmUpd.h.

8.5.2.36 UINT8 FSP_M_TEST_CONFIG::PegGenerateBdatMarginTable

Offset 0x0539 - Generate PCle BDAT Margin Table Set this policy to enable the generation and addition of PCle 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 1392 of file FspmUpd.h.

8.5.2.37 UINT8 FSP_M_TEST_CONFIG::PegRxCemLoopbackLane

Offset 0x0538 - PCle Rx Compliance Loopback Lane When PegRxCemTestingMode is Enabled the specificied Lane (0 - 15) will be used for RxCEMLoopback.

Default is Lane 0

Definition at line 1384 of file FspmUpd.h.

8.5.2.38 UINT8 FSP_M_TEST_CONFIG::PegRxCemNonProtocolAwareness

Offset 0x0540 - PCIe Non-Protocol Awareness for Rx Compliance Testing Set this policy to enable the generation and addition of PCIe margin data to the BDAT table.

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

Definition at line 1405 of file FspmUpd.h.

8.5.2.39 UINT8 FSP_M_TEST_CONFIG::ScanExtGfxForLegacyOpRom

Offset 0x0526 - Detect External Graphics device for LegacyOpROM Detect and report if external graphics device only support LegacyOpROM or not (to support CSM auto-enable).

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

Definition at line 1245 of file FspmUpd.h.

8.5.2.40 UINT8 FSP_M_TEST_CONFIG::SkipMbpHob

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

\$EN_DIS

Definition at line 1586 of file FspmUpd.h.

8.5.2.41 UINT8 FSP_M_TEST_CONFIG::SmbusDynamicPowerGating

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

\$EN_DIS

Definition at line 1522 of file FspmUpd.h.

8.5.2.42 UINT8 FSP_M_TEST_CONFIG::SmbusSpdWriteDisable

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

0: leave SPD Write Disable bit; 1: set SPD Write Disable bit. For security recommendations, SPD write disable bit must be set. \$EN_DIS

Definition at line 1535 of file FspmUpd.h.

8.5.2.43 UINT32 FSP_M_TEST_CONFIG::TgaSize

Offset 0x058C - TgaSize Enable/Disable.

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

Definition at line 1484 of file FspmUpd.h.

8.5.2.44 UINT16 FSP_M_TEST_CONFIG::TotalFlashSize

Offset 0x05A0 - TotalFlashSize Enable/Disable.

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

Definition at line 1499 of file FspmUpd.h.

8.5.2.45 UINT64 FSP_M_TEST_CONFIG::TxtLcpPdBase

Offset 0x0590 - TxtLcpPdBase Enable/Disable.

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

Definition at line 1489 of file FspmUpd.h.

8.5.2.46 UINT64 FSP_M_TEST_CONFIG::TxtLcpPdSize

Offset 0x0598 - TxtLcpPdSize Enable/Disable.

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

Definition at line 1494 of file FspmUpd.h.

8.5.2.47 UINT8 FSP_M_TEST_CONFIG::WdtDisableAndLock

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

\$EN DIS

Definition at line 1528 of file FspmUpd.h.

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

• FspmUpd.h

8.6 FSP_S_CONFIG Struct Reference

Fsp S Configuration.

#include <FspsUpd.h>

Public Attributes

UINT32 LogoPtr

Offset 0x0020 - Logo Pointer Points to PEI Display Logo Image.

UINT32 LogoSize

Offset 0x0024 - Logo Size Size of PEI Display Logo Image.

· UINT32 GraphicsConfigPtr

Offset 0x0028 - Graphics Configuration Ptr Points to VBT.

UINT8 Device4Enable

Offset 0x002C - Enable Device 4 Enable/disable Device 4 \$EN_DIS.

• UINT8 PchHdaEnable

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

UINT8 PchHdaDspEnable

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

UINT8 PchHdaloBufferOwnership

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

• UINT8 PchCio2Enable

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

UINT8 ScsEmmcEnabled

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

UINT8 ScsEmmcHs400Enabled

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

UINT8 ScsSdCardEnabled

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

UINT8 PchlshEnable

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

• UINT8 ShowSpiController

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

UINT8 UnusedUpdSpace0 [2]

Offset 0x0036.

UINT32 MicrocodeRegionBase

Offset 0x0038 - MicrocodeRegionBase Memory Base of Microcode Updates.

UINT32 MicrocodeRegionSize

Offset 0x003C - MicrocodeRegionSize Size of Microcode Updates.

UINT8 TurboMode

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

UINT8 SataSalpSupport

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

• UINT8 SataPortsEnable [8]

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

UINT8 SataPortsDevSlp [8]

Offset 0x004A - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.

• UINT8 PortUsb20Enable [16]

Offset 0x0052 - Enable USB2 ports Enable/disable per USB2 ports.

• UINT8 PortUsb30Enable [10]

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

UINT8 XdciEnable

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

UINT8 SsicPortEnable

Offset 0x006D - Enable XHCI SSIC Eanble Enable/disable XHCI SSIC port.

UINT8 UnusedUpdSpace1

Offset 0x006E.

UINT8 NumOfDevIntConfig

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

UINT32 DevIntConfigPtr

Offset 0x0070 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.

UINT8 SerialloDevMode [11]

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

• UINT8 PxRcConfig [8]

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

• UINT8 GpiolrqRoute

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

UINT8 ScilrqSelect

Offset 0x0088 - Select ScilrqSelect SCI IRQ Select.

UINT8 TcolrqSelect

Offset 0x0089 - Select TcolrqSelect TCO IRQ Select.

UINT8 TcolrqEnable

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

UINT8 PchHdaVerbTableEntryNum

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

• UINT32 PchHdaVerbTablePtr

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

UINT8 UnusedUpdSpace2

Offset 0x0090.

• UINT8 SataEnable

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

UINT8 SataMode

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

UINT8 Usb2AfePetxiset [16]

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

UINT8 Usb2AfeTxiset [16]

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

UINT8 Usb2AfePredeemp [16]

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

UINT8 Usb2AfePehalfbit [16]

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

• UINT8 Usb3HsioTxDeEmphEnable [10]

Offset 0x00D3 - Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment.

• UINT8 Usb3HsioTxDeEmph [10]

Offset 0x00DD - USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting USB 3.0 TX Output -3.5dB De-← Emphasis Adjustment Setting, HSIO_TX_DWORD5[21:16], **Default = 29h** (approximately -3.5dB De-Emphasis).

UINT8 Usb3HsioTxDownscaleAmpEnable [10]

Offset 0x00E7 - Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment, Each value in arrary can be between 0-1.

UINT8 Usb3HsioTxDownscaleAmp [10]

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

• UINT8 PchLanEnable

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

UINT8 DelayUsbPdoProgramming

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

UINT8 UnusedUpdSpace3 [23]

Offset 0x00FD.

UINT8 PcieRpClkReqSupport [24]

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

• UINT8 PcieRpClkReqNumber [24]

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

UINT8 UnusedUpdSpace4 [5]

Offset 0x0144.

• UINT8 Heci3Enabled

Offset 0x0149 - HECl3 state The HECl3 state from Mbp for reference in S3 path or when MbpHob is not installed.

• UINT8 UnusedUpdSpace5 [9]

Offset 0x014A.

UINT8 AmtEnabled

Offset 0x0153 - AMT Switch Enable/Disable.

UINT8 WatchDog

Offset 0x0154 - WatchDog Timer Switch Enable/Disable.

UINT8 AsfEnabled

Offset 0x0155 - ASF Switch Enable/Disable.

UINT8 ManageabilityMode

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

UINT8 FwProgress

Offset 0x0157 - PET Progress Enable/Disable.

UINT16 WatchDogTimerOs

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

UINT16 WatchDogTimerBios

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

UINT8 AmtSolEnabled

Offset 0x015C - SOL Switch Enable/Disable.

UINT8 UnusedUpdSpace6 [163]

Offset 0x015D.

UINT16 DefaultSvid

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

UINT16 DefaultSid

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

UINT8 CridEnable

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

UINT8 DmiAspm

Offset 0x0205 - DMI ASPM 0=Disable, 2(Default)=L1 0:Disable, 2:L1.

UINT16 PegPhysicalSlotNumber [3]

Offset 0x0206 - PCIe Physical Slot Number per root port Physical Slot Number per root port.

UINT8 PegDeEmphasis [3]

Offset 0x020C - PCIe DeEmphasis control per root port 0: -6dB, 1(Default): -3.5dB 0:Disable, 2:L1.

UINT8 PegSlotPowerLimitValue [3]

Offset 0x020F - PCle Slot Power Limit value per root port Slot power limit value per root port.

UINT8 PegSlotPowerLimitScale [3]

Offset 0x0212 - PCle Slot Power Limit scale per root port Slot power limit scale per root port 0:1.0x, 1:0.1x, 2:0.01x, 3:0x001x.

UINT8 PavpEnable

Offset 0x0215 - Enable/Disable PavpEnable Enable(Default): Enable PavpEnable, Disable: Disable PavpEnable \$← EN DIS.

UINT8 CdClock

Offset 0x0216 - CdClock Frequency selection 0=308.57 Mhz, 1=337.5 Mhz, 2=432 Mhz, 3=450 Mhz, 4=540 Mhz, 5=617.14 Mhz, 6(Default)= 675 Mhz 0: 308.57 Mhz, 1: 337.5 Mhz, 2: 432 Mhz, 3: 450 Mhz, 4: 540 Mhz, 5: 617.14 Mhz, 6: 675 Mhz.

· UINT8 PeiGraphicsPeimInit

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

UINT8 SalmguEnable

Offset 0x0218 - Enable/Disable SA IMGU(SKYCAM) Enable(Default): Enable SA IMGU(SKYCAM), Disable: Disable SA IMGU(SKYCAM) \$EN DIS.

UINT8 GmmEnable

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

• UINT8 X2ApicOptOut

Offset 0x021A - State of X2APIC_OPT_OUT bit in the DMAR table 0=Disable/Clear, 1(Default)=Enable/Set \$EN_DIS.

UINT8 UnusedUpdSpace7 [1]

Offset 0x021B.

• UINT32 VtdBaseAddress [2]

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

UINT8 UnusedUpdSpace8 [19]

Offset 0x0224.

UINT8 SaPostMemProductionRsvd [16]

Offset 0x0237 - SaPostMemProductionRsvd Reserved for SA Post-Mem Production \$EN_DIS.

UINT8 UnusedUpdSpace9 [7]

Offset 0x0247.

• UINT8 Psi3Enable [5]

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

• UINT8 Psi4Enable [5]

Offset 0x0253 - Power State 4 enable/disable PCODE MMIO Mailbox: Power State 4 enable/disable; 0: Disable; 1: Enable.For all VR Indexes.

• UINT8 ImonSlope [5]

Offset 0x0258 - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.

UINT8 ImonOffset [5]

Offset 0x025D - Imon offset correction PCODE MMIO Mailbox: Imon offset correction.

UINT8 VrConfigEnable [5]

Offset 0x0262 - Enable/Disable BIOS configuration of VR Enable/Disable BIOS configuration of VR; **0: Disable**; 1: Enable.For all VR Indexes.

• UINT8 TdcEnable [5]

Offset 0x0267 - Thermal Design Current enable/disable PCODE MMIO Mailbox: Thermal Design Current enable/disable; 0: Disable; 1: Enable.For all VR Indexes.

• UINT8 TdcTimeWindow [5]

Offset 0x026C - HECl3 state PCODE MMIO Mailbox: Thermal Design Current time window.

UINT8 TdcLock [5]

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

UINT8 PsysSlope

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

UINT8 PsysOffset

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

UINT8 AcousticNoiseMitigation

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

UINT8 FastPkgCRampDisablela

Offset 0x0279 - Disable Fast Slew Rate for Deep Package C States for VR IA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

• UINT8 SlowSlewRateForla

Offset 0x027A - Slew Rate configuration for Deep Package C States for VR IA domain Slew Rate configuration for Deep Package C States for VR IA domain based on Acoustic Noise Mitigation feature enabled.

UINT8 SlowSlewRateForGt

Offset 0x027B - Slew Rate configuration for Deep Package C States for VR GT domain Slew Rate configuration for Deep Package C States for VR GT domain based on Acoustic Noise Mitigation feature enabled.

• UINT8 SlowSlewRateForSa

Offset 0x027C - Slew Rate configuration for Deep Package C States for VR SA domain Slew Rate configuration for Deep Package C States for VR SA domain based on Acoustic Noise Mitigation feature enabled.

UINT8 UnusedUpdSpace10 [9]

Offset 0x027D.

UINT16 TdcPowerLimit [5]

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

UINT8 UnusedUpdSpace11 [8]

Offset 0x0290.

UINT16 AcLoadline [5]

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

• UINT16 DcLoadline [5]

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

• UINT16 Psi1Threshold [5]

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

UINT16 Psi2Threshold [5]

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

UINT16 Psi3Threshold [5]

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

• UINT16 IccMax [5]

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

UINT16 VrVoltageLimit [5]

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

• UINT8 UnusedUpdSpace12

Offset 0x02DE.

UINT8 FastPkgCRampDisableGt

Offset 0x02DF - Disable Fast Slew Rate for Deep Package C States for VR GT domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

• UINT8 FastPkgCRampDisableSa

Offset 0x02E0 - Disable Fast Slew Rate for Deep Package C States for VR SA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

UINT8 UnusedUpdSpace13

Offset 0x02E1.

UINT8 SendVrMbxCmd

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

UINT8 SendVrMbxCmd1

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

UINT32 CpuS3ResumeMtrrData

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

CPU_CONFIG_FSP_DATA CpuConfig

Offset 0x02E8 - Cpu Configuration Cpu Configuration data.

• UINT64 MicrocodePatchAddress

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

UINT16 CpuS3ResumeMtrrDataSize

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

UINT8 UnusedUpdSpace14

Offset 0x02FA.

UINT8 PchSkyCamPortATermOvrEnable

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

• UINT8 PchSkyCamPortBTermOvrEnable

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

UINT8 PchSkyCamPortCTermOvrEnable

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

UINT8 PchSkyCamPortDTermOvrEnable

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

UINT8 PchSkyCamPortATrimEnable

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

UINT8 PchSkyCamPortBTrimEnable

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

UINT8 PchSkyCamPortCTrimEnable

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

UINT8 PchSkyCamPortDTrimEnable

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

UINT8 PchSkyCamPortACtleEnable

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

UINT8 PchSkyCamPortBCtleEnable

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

UINT8 PchSkyCamPortCDCtleEnable

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

UINT8 PchSkyCamPortACtleCapValue

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

UINT8 PchSkyCamPortBCtleCapValue

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

UINT8 PchSkyCamPortCDCtleCapValue

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

UINT8 PchSkyCamPortACtleResValue

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

UINT8 PchSkyCamPortBCtleResValue

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

UINT8 PchSkyCamPortCDCtleResValue

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

UINT8 PchSkyCamPortAClkTrimValue

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

UINT8 PchSkyCamPortBClkTrimValue

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

UINT8 PchSkyCamPortCClkTrimValue

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

UINT8 PchSkyCamPortDClkTrimValue

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

UINT16 PchSkyCamPortADataTrimValue

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

• UINT16 PchSkyCamPortBDataTrimValue

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

UINT16 PchSkyCamPortCDDataTrimValue

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

UINT8 PchDmiAspm

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

UINT8 PchPwrOptEnable

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

UINT8 PchWriteProtectionEnable [5]

Offset 0x0318 - PCH Flash Protection Ranges Write Enble Write or erase is blocked by hardware.

• UINT8 PchReadProtectionEnable [5]

Offset 0x031D - PCH Flash Protection Ranges Read Enble Read is blocked by hardware.

• UINT16 PchProtectedRangeLimit [5]

Offset 0x0322 - PCH Protect Range Limit Left shifted address by 12 bits with address bits 11:0 are assumed to be FFFh for limit comparison.

UINT16 PchProtectedRangeBase [5]

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

UINT8 PchHdaPme

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

• UINT8 PchHdaloBufferVoltage

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

UINT8 PchHdaVcType

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

• UINT8 PchHdaLinkFrequency

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

UINT8 PchHdalDispLinkFrequency

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

UINT8 PchHdalDispLinkTmode

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

UINT8 PchHdaDspUaaCompliance

Offset 0x033C - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).

UINT8 PchHdalDispCodecDisconnect

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

UINT8 PchHdaDspEndpointDmic

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

UINT8 PchHdaDspEndpointBluetooth

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

UINT32 PchHdaDspFeatureMask

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

UINT32 PchHdaDspPpModuleMask

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

UINT8 PchHdaDspEndpointl2s

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

UINT8 PchloApicBdfValid

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

UINT8 PchloApicBusNumber

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

UINT8 PchloApicDeviceNumber

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

UINT8 PchloApicFunctionNumber

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

• UINT8 PchloApicEntry24 119

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

UINT8 PchloApicId

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

• UINT8 PchloApicRangeSelect

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

UINT8 PchlshSpiGpioAssign

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

· UINT8 PchlshUart0GpioAssign

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

UINT8 PchlshUart1GpioAssign

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

• UINT8 Pchlshl2c0GpioAssign

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

UINT8 Pchlshl2c1GpioAssign

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

UINT8 Pchlshl2c2GpioAssign

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

UINT8 PchlshGp0GpioAssign

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

UINT8 PchlshGp1GpioAssign

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

UINT8 PchlshGp2GpioAssign

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

UINT8 PchlshGp3GpioAssign

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

• UINT8 PchlshGp4GpioAssign

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

UINT8 PchlshGp5GpioAssign

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

UINT8 PchlshGp6GpioAssign

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

UINT8 PchlshGp7GpioAssign

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

UINT8 PchlshPdtUnlock

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

• UINT8 PchLanLtrEnable

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

• UINT8 PchLanK1OffEnable

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

UINT8 PchLanClkReqSupported

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

UINT8 PchLanClkReqNumber

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

UINT8 PchLockDownBiosLock

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

UINT8 PchLockDownSpiEiss

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

UINT8 PchCrid

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

• UINT16 PchSubSystemVendorId

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

UINT16 PchSubSystemId

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

UINT8 PchLegacyloLowLatency

Offset 0x036A - PCH Legacy IO Low Latency Enable todo \$EN_DIS.

UINT8 UnusedUpdSpace15 [5]

Offset 0x036B.

• UINT8 PcieRpHotPlug [24]

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

• UINT8 PcieRpPmSci [24]

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

UINT8 PcieRpExtSync [24]

Offset 0x03A0 - Enable PCIE RP Ext Sync Indicate whether the extended synch is enabled.

UINT8 PcieRpTransmitterHalfSwing [24]

Offset 0x03B8 - Enable PCIE RP Transmitter Half Swing Indicate whether the Transmitter Half Swing is enabled.

UINT8 PcieRpClkReqDetect [24]

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

UINT8 PcieRpAdvancedErrorReporting [24]

Offset 0x03E8 - PCIE RP Advanced Error Report Indicate whether the Advanced Error Reporting is enabled.

UINT8 PcieRpUnsupportedRequestReport [24]

Offset 0x0400 - PCIE RP Unsupported Request Report Indicate whether the Unsupported Request Report is enabled.

UINT8 PcieRpFatalErrorReport [24]

Offset 0x0418 - PCIE RP Fatal Error Report Indicate whether the Fatal Error Report is enabled.

UINT8 PcieRpNoFatalErrorReport [24]

Offset 0x0430 - PCIE RP No Fatal Error Report Indicate whether the No Fatal Error Report is enabled.

UINT8 PcieRpCorrectableErrorReport [24]

Offset 0x0448 - PCIE RP Correctable Error Report Indicate whether the Correctable Error Report is enabled.

UINT8 PcieRpSystemErrorOnFatalError [24]

Offset 0x0460 - PCIE RP System Error On Fatal Error Indicate whether the System Error on Fatal Error is enabled.

UINT8 PcieRpSystemErrorOnNonFatalError [24]

Offset 0x0478 - PCIE RP System Error On Non Fatal Error Indicate whether the System Error on Non Fatal Error is enabled.

UINT8 PcieRpSystemErrorOnCorrectableError [24]

Offset 0x0490 - PCIE RP System Error On Correctable Error Indicate whether the System Error on Correctable Error is enabled.

UINT8 PcieRpMaxPayload [24]

Offset 0x04A8 - PCIE RP Max Payload Max Payload Size supported, Default 128B, see enum PCH_PCIE_MAX_← PAYLOAD.

UINT8 PcieRpDeviceResetPadActiveHigh [24]

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

• UINT8 PcieRpPcieSpeed [24]

Offset 0x04D8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.

UINT8 PcieRpGen3EqPh3Method [24]

Offset 0x04F0 - PCIE RP Gen3 Equalization Phase Method PCIe Gen3 Eq Ph3 Method (see PCH_PCIE_EQ_ME← THOD).

UINT8 PcieRpPhysicalSlotNumber [24]

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

UINT8 PcieRpCompletionTimeout [24]

Offset 0x0520 - PCIE RP Completion Timeout The root port completion timeout(see: PCH_PCIE_COMPLETION_ \leftarrow TIMEOUT).

UINT32 PcieRpDeviceResetPad [24]

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

• UINT8 PcieRpAspm [24]

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

UINT8 PcieRpL1Substates [24]

Offset 0x05B0 - PCIE RP L1 Substates The L1 Substates configuration of the root port (see: PCH_PCIE_L1SUB← STATES_CONTROL).

UINT8 PcieRpLtrEnable [24]

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

• UINT8 PcieRpLtrConfigLock [24]

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

UINT8 PcieEqPh3LaneParamCm [24]

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

UINT8 PcieEqPh3LaneParamCp [24]

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

UINT8 PcieSwEqCoeffListCm [5]

Offset 0x0628 - PCIE Sw Eq CoeffList Cm PCH PCIE EQ PARAM.

UINT8 PcieSwEqCoeffListCp [5]

Offset 0x062D - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

UINT8 PcieDisableRootPortClockGating

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

UINT8 PcieEnablePeerMemoryWrite

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

UINT8 PcieAllowNoLtrlccPllShutdown

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

UINT8 PcieComplianceTestMode

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

• UINT16 PcieDetectTimeoutMs

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

UINT8 PcieRpFunctionSwap

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

UINT8 PchPmPmeB0S5Dis

Offset 0x0639 - PCH Pm PME_B0_S5_DIS When cleared (default), wake events from PME_B0_STS are allowed in S5 if PME_B0_EN = 1.

UINT8 PchPmSlpS0VmEnable

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

UINT8 UnusedUpdSpace16 [5]

Offset 0x063B.

• UINT8 PchPmWolEnableOverride

Offset 0x0640 - PCH Pm Wol Enable Override Corresponds to the WOL Enable Override bit in the General PM Configuration B (GEN_PMCON_B) register.

UINT8 PchPmPcieWakeFromDeepSx

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

• UINT8 PchPmWoWlanEnable

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

UINT8 PchPmWoWlanDeepSxEnable

Offset 0x0643 - PCH Pm WoW Ian DeepSx Enable Determine if WLAN wake from DeepSx, corresponds to the DSX_WLAN_PP_EN bit in the PWRM_CFG3 register.

UINT8 PchPmLanWakeFromDeepSx

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

UINT8 PchPmDeepSxPol

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

UINT8 PchPmSlpS3MinAssert

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

• UINT8 PchPmSlpS4MinAssert

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

UINT8 PchPmSlpSusMinAssert

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

UINT8 PchPmSlpAMinAssert

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

UINT8 UnusedUpdSpace17 [6]

Offset 0x064A.

UINT8 PchPmLpcClockRun

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

UINT8 PchPmSlpStrchSusUp

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

UINT8 PchPmSlpLanLowDc

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

UINT8 PchPmPwrBtnOverridePeriod

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

UINT8 PchPmDisableDsxAcPresentPulldown

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

UINT8 PchPmCapsuleResetType

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

UINT8 PchPmDisableNativePowerButton

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

UINT8 PchPmSlpS0Enable

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

UINT8 PchPmMeWakeSts

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

UINT8 PchPmWolOvrWkSts

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

UINT8 PchPmPwrCycDur

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

• UINT8 UnusedUpdSpace18

Offset 0x065B.

UINT8 PchPort61hEnable

Offset 0x065C - PCH Pm WOL_OVR_WK_STS Clear the WOL_OVR_WK_STS bit in the Power and Reset Status (PRSTS) register.

UINT8 SataPwrOptEnable

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

UINT8 EsataSpeedLimit

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

UINT8 SataSpeedLimit

Offset 0x065F - PCH Sata Speed Limit Indicates the maximum speed the SATA controller can support 0h: Pch⇔ SataSpeedDefault.

• UINT8 SataPortsHotPlug [8]

Offset 0x0660 - Enable SATA Port HotPlug Enable SATA Port HotPlug.

• UINT8 SataPortsInterlockSw [8]

Offset 0x0668 - Enable SATA Port Interlock Sw Enable SATA Port Interlock Sw.

UINT8 SataPortsExternal [8]

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

UINT8 SataPortsSpinUp [8]

Offset 0x0678 - Enable SATA Port SpinUp Enable the COMRESET initialization Sequence to the device.

• UINT8 SataPortsSolidStateDrive [8]

Offset 0x0680 - Enable SATA Port Solid State Drive 0: HDD; 1: SSD.

UINT8 SataPortsEnableDitoConfig [8]

Offset 0x0688 - Enable SATA Port Enable Dito Config Enable DEVSLP Idle Timeout settings (DmVal, DitoVal).

UINT8 SataPortsDmVal [8]

Offset 0x0690 - Enable SATA Port DmVal DITO multiplier.

UINT16 SataPortsDitoVal [8]

Offset 0x0698 - Enable SATA Port DmVal DEVSLP Idle Timeout (DITO), Default is 625.

UINT8 SataPortsZpOdd [8]

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

UINT8 SataRstRaidAlternateId

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

UINT8 SataRstRaid0

Offset 0x06B1 - PCH Sata Rst Raid0 RAID0.

UINT8 SataRstRaid1

Offset 0x06B2 - PCH Sata Rst Raid1 RAID1.

UINT8 SataRstRaid10

Offset 0x06B3 - PCH Sata Rst Raid10 RAID10.

UINT8 SataRstRaid5

Offset 0x06B4 - PCH Sata Rst Raid5 RAID5.

UINT8 SataRstIrrt

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

UINT8 SataRstOromUiBanner

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

UINT8 SataRstOromUiDelay

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

UINT8 SataRstHddUnlock

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

• UINT8 SataRstLedLocate

Offset 0x06B9 - PCH Sata Rst Led Locate Indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

UINT8 SataRstIrrtOnly

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

• UINT8 SataRstSmartStorage

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

UINT8 SataRstPcieEnable [3]

Offset 0x06BC - PCH Sata Rst Pcie Storage Remap enable Enable Intel RST for PCIe Storage remapping.

UINT8 SataRstPcieStoragePort [3]

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

UINT8 SataRstPcieDeviceResetDelay [3]

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

• UINT8 PchScsEmmcHs400TuningRequired

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

UINT8 PchScsEmmcHs400DllDataValid

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

UINT8 PchScsEmmcHs400RxStrobeDll1

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

UINT8 PchScsEmmcHs400TxDataDII

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

• UINT8 PchScsEmmcHs400DriverStrength

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

UINT8 SerialloGpio

Offset 0x06CA - Enable Pch Serial IO GPIO Determines if enable Serial IO GPIO.

UINT8 Seriallol2cVoltage [6]

Offset 0x06CB - IO voltage for I2C controllers Selects the IO voltage for I2C controllers, 0: PchSeriallols33V, 1: PchSeriallols18V.

UINT8 SerialloSpiCsPolarity [2]

Offset 0x06D1 - SPI ChipSelect signal polarity Selects SPI ChipSelect signal polarity.

UINT8 SerialloUartHwFlowCtrl [3]

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

• UINT8 SerialIoDebugUartNumber

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

UINT8 SerialloEnableDebugUartAfterPost

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

UINT8 PchSirqEnable

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

UINT8 PchSirqMode

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

UINT8 PchStartFramePulse

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

• UINT8 PchThermalDeviceEnable

Offset 0x06DB - Enable Thermal Device Enable Thermal Device.

UINT16 PchT0Level

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

UINT16 PchT1Level

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

UINT16 PchT2Level

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

UINT8 PchTsmicLock

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

UINT8 PchTTEnable

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

UINT8 PchTTState13Enable

Offset 0x06E4 - PMSync State 13 When set to 1 and the programmed GPIO pin is a 1, then PMSync state 13 will force at least T2 state.

UINT8 PchTTLock

Offset 0x06E5 - Thermal Throttle Lock Thermal Throttle Lock.

UINT8 TTSuggestedSetting

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

UINT8 TTCrossThrottling

Offset 0x06E7 - Enable PCH Cross Throttling Enable/Disable PCH Cross Throttling \$EN DIS.

UINT8 PchDmiTsawEn

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

UINT8 DmiSuggestedSetting

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

UINT8 DmiTS0TW

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

UINT8 DmiTS1TW

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

UINT8 DmiTS2TW

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

UINT8 DmiTS3TW

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

UINT8 SataP0T1M

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

UINT8 SataP0T2M

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

UINT8 SataP0T3M

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

UINT8 SataP0TDisp

Offset 0x06F1 - Port 0 Tdispatch Port 0 Tdispatch.

UINT8 SataP1T1M

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

UINT8 SataP1T2M

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

UINT8 SataP1T3M

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

UINT8 SataP1TDisp

Offset 0x06F5 - Port 1 Tdispatch Port 1 Tdispatch.

UINT8 SataP0Tinact

Offset 0x06F6 - Port 0 Tinactive Port 0 Tinactive.

• UINT8 SataP0TDispFinit

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

UINT8 SataP1Tinact

Offset 0x06F8 - Port 1 Tinactive Port 1 Tinactive.

UINT8 SataP1TDispFinit

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

UINT8 SataThermalSuggestedSetting

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

UINT8 PchMemoryThrottlingEnable

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

• UINT8 PchMemoryPmsyncEnable [2]

Offset 0x06FC - Memory Thermal Throttling Enable Memory Thermal Throttling.

UINT8 PchMemoryC0TransmitEnable [2]

Offset 0x06FE - Enable Memory Thermal Throttling Enable Memory Thermal Throttling.

• UINT8 PchMemoryPinSelection [2]

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

• UINT16 PchTemperatureHotLevel

Offset 0x0702 - Thermal Device Temperature Decides the temperature.

UINT8 PchDisableComplianceMode

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

• UINT8 Usb2OverCurrentPin [16]

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

UINT8 Usb3OverCurrentPin [10]

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

• UINT8 Early8254ClockGatingEnable

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

UINT8 SataRstOptaneMemory

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

UINT8 UnusedUpdSpace19 [3]

Offset 0x0721.

UINT32 PchPcieDeviceOverrideTablePtr

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

UINT8 EnableTcoTimer

Offset 0x0728 - Enable TCO timer.

UINT8 EcCmdProvisionEav

Offset 0x0729 - EcCmdProvisionEav Ephemeral Authorization Value default values.

UINT8 EcCmdLock

Offset 0x072A - EcCmdLock EcCmdLock default values.

UINT8 UnusedUpdSpace20 [5]

Offset 0x072B.

UINT64 SendEcCmd

Offset 0x0730 - SendEcCmd SendEcCmd function pointer.

UINT64 BgpdtHash [4]

Offset 0x0738 - BgpdtHash[4] BgpdtHash values.

UINT64 BiosGuardModulePtr

Offset 0x0758 - BiosGuardModulePtr BiosGuardModulePtr default values.

• UINT32 BiosGuardAttr

Offset 0x0760 - BiosGuardAttr BiosGuardAttr default values.

UINT8 SgxSinitNvsData

Offset 0x0764 - SgxSinitNvsData SgxSinitNvsData default values.

• UINT8 UnusedUpdSpace21 [3]

Offset 0x0765.

UINT64 SgxEpoch0

Offset 0x0768 - SgxEpoch0 SgxEpoch0 default values.

UINT64 SgxEpoch1

Offset 0x0770 - SgxEpoch1 SgxEpoch1 default values.

UINT8 MeUnconfigOnRtcClear

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

· UINT8 MeUnconfigIsValid

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

• UINT8 ReservedFspsUpd [6]

Offset 0x077A.

8.6.1 Detailed Description

Fsp S Configuration.

Definition at line 87 of file FspsUpd.h.

8.6.2 Member Data Documentation

8.6.2.1 UINT16 FSP_S_CONFIG::AcLoadline[5]

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

1250 = 12.50 mOhm); Range is 0-6249. Intel Recommended Defaults vary by domain and SKU.

Definition at line 667 of file FspsUpd.h.

8.6.2.2 UINT8 FSP_S_CONFIG::AcousticNoiseMitigation

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

0: Disabled; 1: Enabled \$EN_DIS

Definition at line 619 of file FspsUpd.h.

8.6.2.3 UINT8 FSP_S_CONFIG::AmtEnabled

Offset 0x0153 - AMT Switch Enable/Disable.

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

Definition at line 402 of file FspsUpd.h.

8.6.2.4 UINT8 FSP_S_CONFIG::AmtSolEnabled

Offset 0x015C - SOL Switch Enable/Disable.

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

Definition at line 445 of file FspsUpd.h.

8.6.2.5 UINT8 FSP_S_CONFIG::AsfEnabled

Offset 0x0155 - ASF Switch Enable/Disable.

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

Definition at line 414 of file FspsUpd.h.

8.6.2.6 UINT16 FSP_S_CONFIG::DcLoadline[5]

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

1250 = 12.50 mOhm); Range is 0-6249. Intel Recommended Defaults vary by domain and SKU.

Definition at line 673 of file FspsUpd.h.

8.6.2.7 UINT8 FSP_S_CONFIG::DelayUsbPdoProgramming

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

0: disable, 1: enable \$EN_DIS

Definition at line 365 of file FspsUpd.h.

8.6.2.8 UINT32 FSP_S_CONFIG::DevIntConfigPtr

Offset 0x0070 - Address of PCH_DEVICE_INTERRUPT_CONFIG table.

The address of the table of PCH_DEVICE_INTERRUPT_CONFIG.

Definition at line 243 of file FspsUpd.h.

8.6.2.9 UINT8 FSP_S_CONFIG::DmiSuggestedSetting

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

\$EN_DIS

Definition at line 1821 of file FspsUpd.h.

8.6.2.10 UINT8 FSP_S_CONFIG::Early8254ClockGatingEnable

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

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

Definition at line 1960 of file FspsUpd.h.

8.6.2.11 UINT8 FSP_S_CONFIG::EcCmdLock

Offset 0x072A - EcCmdLock EcCmdLock default values.

Locks Ephemeral Authorization Value sent previously

Definition at line 1996 of file FspsUpd.h.

8.6.2.12 UINT8 FSP_S_CONFIG::EcCmdProvisionEav

Offset 0x0729 - EcCmdProvisionEav Ephemeral Authorization Value default values.

Provisions an ephemeral shared secret to the EC

Definition at line 1991 of file FspsUpd.h.

8.6.2.13 UINT8 FSP_S_CONFIG::EnableTcoTimer

Offset 0x0728 - Enable TCO timer.

When FALSE, it disables PCH ACPI timer, and stops TCO timer. NOTE: This will have huge power impact when it's enabled. If TCO timer is disabled, uCode ACPI timer emulation must be enabled, and WDAT table must not be exposed to the OS. \$EN_DIS

Definition at line 1986 of file FspsUpd.h.

8.6.2.14 UINT8 FSP_S_CONFIG::EsataSpeedLimit

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

\$EN_DIS

Definition at line 1539 of file FspsUpd.h.

8.6.2.15 UINT8 FSP_S_CONFIG::FastPkgCRampDisableGt

Offset 0x02DF - Disable Fast Slew Rate for Deep Package C States for VR GT domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True \$EN DIS

Definition at line 712 of file FspsUpd.h.

8.6.2.16 UINT8 FSP_S_CONFIG::FastPkgCRampDisablela

Offset 0x0279 - Disable Fast Slew Rate for Deep Package C States for VR IA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True \$EN_DIS

Definition at line 626 of file FspsUpd.h.

8.6.2.17 UINT8 FSP_S_CONFIG::FastPkgCRampDisableSa

Offset 0x02E0 - Disable Fast Slew Rate for Deep Package C States for VR SA domain Disable Fast Slew Rate for Deep Package C States based on Acoustic Noise Mitigation feature enabled.

0: False; 1: True \$EN DIS

Definition at line 719 of file FspsUpd.h.

8.6.2.18 UINT8 FSP_S_CONFIG::FwProgress

Offset 0x0157 - PET Progress Enable/Disable.

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

Definition at line 427 of file FspsUpd.h.

8.6.2.19 UINT8 FSP_S_CONFIG::GpiolrqRoute

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

The valid value is 14 or 15.

Definition at line 262 of file FspsUpd.h.

8.6.2.20 UINT8 FSP_S_CONFIG::Heci3Enabled

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

0: disable, 1: enable \$EN_DIS

Definition at line 392 of file FspsUpd.h.

8.6.2.21 UINT16 FSP_S_CONFIG::lccMax[5]

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

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

Definition at line 696 of file FspsUpd.h.

8.6.2.22 UINT8 FSP_S_CONFIG::ImonOffset[5]

Offset 0x025D - Imon offset correction PCODE MMIO Mailbox: Imon offset correction.

Value is a 2's complement signed integer. Units 1/1000, Range 0-63999. For an offset = 12.580, use 12580. **0: Auto**

Definition at line 577 of file FspsUpd.h.

8.6.2.23 UINT8 FSP_S_CONFIG::ImonSlope[5]

Offset 0x0258 - Imon slope correction PCODE MMIO Mailbox: Imon slope correction.

Specified in 1/100 increment values. Range is 0-200. 125 = 1.25. 0: Auto. For all VR Indexes

Definition at line 571 of file FspsUpd.h.

8.6.2.24 UINT8 FSP_S_CONFIG::ManageabilityMode

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

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

Definition at line 420 of file FspsUpd.h.

8.6.2.25 UINT8 FSP_S_CONFIG::MeUnconfiglsValid

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

\$EN_DIS

Definition at line 2053 of file FspsUpd.h.

8.6.2.26 UINT64 FSP_S_CONFIG::MicrocodePatchAddress

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

0:Disable, 1:Enable

Definition at line 754 of file FspsUpd.h.

8.6.2.27 UINT8 FSP_S_CONFIG::NumOfDevIntConfig

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

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

Definition at line 238 of file FspsUpd.h.

8.6.2.28 UINT8 FSP_S_CONFIG::PchCio2Enable

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

\$EN_DIS

Definition at line 136 of file FspsUpd.h.

8.6.2.29 UINT8 FSP_S_CONFIG::PchCrid

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

\$EN_DIS

Definition at line 1171 of file FspsUpd.h.

8.6.2.30 UINT8 FSP_S_CONFIG::PchDisableComplianceMode

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

Complicance Mode should be default enabled. \$EN_DIS

Definition at line 1942 of file FspsUpd.h.

8.6.2.31 UINT8 FSP_S_CONFIG::PchDmiAspm

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

\$EN DIS

Definition at line 900 of file FspsUpd.h.

8.6.2.32 UINT8 FSP_S_CONFIG::PchDmiTsawEn

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

\$EN DIS

Definition at line 1815 of file FspsUpd.h.

8.6.2.33 UINT8 FSP_S_CONFIG::PchHdaDspEnable

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

\$EN DIS

Definition at line 120 of file FspsUpd.h.

8.6.2.34 UINT8 FSP_S_CONFIG::PchHdaDspEndpointBluetooth

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

\$EN DIS

Definition at line 982 of file FspsUpd.h.

8.6.2.35 UINT8 FSP_S_CONFIG::PchHdaDspEndpointl2s

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

\$EN_DIS

Definition at line 1002 of file FspsUpd.h.

8.6.2.36 UINT32 FSP_S_CONFIG::PchHdaDspFeatureMask

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

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

Definition at line 989 of file FspsUpd.h.

8.6.2.37 UINT8 FSP_S_CONFIG::PchHdaDspUaaCompliance

Offset 0x033C - Universal Audio Architecture compliance for DSP enabled system 0: Not-UAA Compliant (Intel SST driver supported only), 1: UAA Compliant (HDA Inbox driver or SST driver supported).

\$EN DIS

Definition at line 965 of file FspsUpd.h.

8.6.2.38 UINT8 FSP_S_CONFIG::PchHdaEnable

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

\$EN DIS

Definition at line 114 of file FspsUpd.h.

8.6.2.39 UINT8 FSP_S_CONFIG::PchHdalDispCodecDisconnect

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

\$EN DIS

Definition at line 971 of file FspsUpd.h.

8.6.2.40 UINT8 FSP_S_CONFIG::PchHdaloBufferOwnership

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

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

Definition at line 130 of file FspsUpd.h.

8.6.2.41 UINT8 FSP_S_CONFIG::PchHdaPme

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

\$EN DIS

Definition at line 933 of file FspsUpd.h.

8.6.2.42 UINT8 FSP_S_CONFIG::PchloApicBdfValid

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

\$EN_DIS

Definition at line 1008 of file FspsUpd.h.

8.6.2.43 UINT8 FSP_S_CONFIG::PchloApicBusNumber

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

Default is 0xF0.

Definition at line 1013 of file FspsUpd.h.

8.6.2.44 UINT8 FSP_S_CONFIG::PchloApicDeviceNumber

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

Default is 0x1F.

Definition at line 1018 of file FspsUpd.h.

8.6.2.45 UINT8 FSP_S_CONFIG::PchloApicEntry24_119

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

\$EN_DIS

Definition at line 1029 of file FspsUpd.h.

8.6.2.46 UINT8 FSP_S_CONFIG::PchloApicFunctionNumber

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

Default is 0x00.

Definition at line 1023 of file FspsUpd.h.

8.6.2.47 UINT8 FSP_S_CONFIG::PchloApicId

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

Default is 0x02.

Definition at line 1034 of file FspsUpd.h.

8.6.2.48 UINT8 FSP_S_CONFIG::PchloApicRangeSelect

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

Default is 0.

Definition at line 1039 of file FspsUpd.h.

8.6.2.49 UINT8 FSP_S_CONFIG::PchlshEnable

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

\$EN_DIS

Definition at line 160 of file FspsUpd.h.

8.6.2.50 UINT8 FSP_S_CONFIG::PchlshGp0GpioAssign

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

\$EN_DIS

Definition at line 1081 of file FspsUpd.h.

8.6.2.51 UINT8 FSP_S_CONFIG::PchlshGp1GpioAssign

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

\$EN_DIS

Definition at line 1087 of file FspsUpd.h.

8.6.2.52 UINT8 FSP_S_CONFIG::PchlshGp2GpioAssign

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

\$EN_DIS

Definition at line 1093 of file FspsUpd.h.

8.6.2.53 UINT8 FSP_S_CONFIG::PchlshGp3GpioAssign

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

\$EN_DIS

Definition at line 1099 of file FspsUpd.h.

8.6.2.54 UINT8 FSP_S_CONFIG::PchlshGp4GpioAssign

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

\$EN_DIS

Definition at line 1105 of file FspsUpd.h.

8.6.2.55 UINT8 FSP_S_CONFIG::PchlshGp5GpioAssign

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

\$EN DIS

Definition at line 1111 of file FspsUpd.h.

8.6.2.56 UINT8 FSP_S_CONFIG::PchlshGp6GpioAssign

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

\$EN DIS

Definition at line 1117 of file FspsUpd.h.

8.6.2.57 UINT8 FSP_S_CONFIG::PchlshGp7GpioAssign

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

\$EN DIS

Definition at line 1123 of file FspsUpd.h.

8.6.2.58 UINT8 FSP_S_CONFIG::Pchlshl2c0GpioAssign

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

\$EN_DIS

Definition at line 1063 of file FspsUpd.h.

8.6.2.59 UINT8 FSP_S_CONFIG::Pchlshl2c1GpioAssign

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

\$EN_DIS

Definition at line 1069 of file FspsUpd.h.

8.6.2.60 UINT8 FSP_S_CONFIG::Pchlshl2c2GpioAssign

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

\$EN_DIS

Definition at line 1075 of file FspsUpd.h.

8.6.2.61 UINT8 FSP_S_CONFIG::PchlshPdtUnlock

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

\$EN DIS

Definition at line 1129 of file FspsUpd.h.

8.6.2.62 UINT8 FSP_S_CONFIG::PchlshSpiGpioAssign

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

\$EN_DIS

Definition at line 1045 of file FspsUpd.h.

8.6.2.63 UINT8 FSP_S_CONFIG::PchlshUart0GpioAssign

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

\$EN_DIS

Definition at line 1051 of file FspsUpd.h.

8.6.2.64 UINT8 FSP_S_CONFIG::PchlshUart1GpioAssign

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

\$EN_DIS

Definition at line 1057 of file FspsUpd.h.

8.6.2.65 UINT8 FSP_S_CONFIG::PchLanClkReqSupported

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

\$EN_DIS

Definition at line 1147 of file FspsUpd.h.

8.6.2.66 UINT8 FSP_S_CONFIG::PchLanEnable

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

\$EN_DIS

Definition at line 358 of file FspsUpd.h.

8.6.2.67 UINT8 FSP_S_CONFIG::PchLanK1OffEnable

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

\$EN DIS

Definition at line 1141 of file FspsUpd.h.

8.6.2.68 UINT8 FSP_S_CONFIG::PchLanLtrEnable

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

\$EN DIS

Definition at line 1135 of file FspsUpd.h.

8.6.2.69 UINT8 FSP_S_CONFIG::PchLockDownBiosLock

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

\$EN_DIS

Definition at line 1159 of file FspsUpd.h.

8.6.2.70 UINT8 FSP_S_CONFIG::PchLockDownSpiEiss

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

\$EN_DIS

Definition at line 1165 of file FspsUpd.h.

8.6.2.71 UINT8 FSP_S_CONFIG::PchMemoryThrottlingEnable

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

\$EN DIS

Definition at line 1915 of file FspsUpd.h.

8.6.2.72 UINT32 FSP_S_CONFIG::PchPcieDeviceOverrideTablePtr

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

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

Definition at line 1978 of file FspsUpd.h.

8.6.2.73 UINT8 FSP_S_CONFIG::PchPmCapsuleResetType

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

Always Warm reset. \$EN_DIS

Definition at line 1487 of file FspsUpd.h.

8.6.2.74 UINT8 FSP_S_CONFIG::PchPmDeepSxPol

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

\$EN DIS

Definition at line 1428 of file FspsUpd.h.

8.6.2.75 UINT8 FSP_S_CONFIG::PchPmDisableDsxAcPresentPulldown

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

\$EN DIS

Definition at line 1481 of file FspsUpd.h.

8.6.2.76 UINT8 FSP_S_CONFIG::PchPmDisableNativePowerButton

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

\$EN DIS

Definition at line 1493 of file FspsUpd.h.

8.6.2.77 UINT8 FSP_S_CONFIG::PchPmLanWakeFromDeepSx

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

\$EN DIS

Definition at line 1422 of file FspsUpd.h.

8.6.2.78 UINT8 FSP_S_CONFIG::PchPmLpcClockRun

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

\$EN DIS

Definition at line 1458 of file FspsUpd.h.

8.6.2.79 UINT8 FSP_S_CONFIG::PchPmMeWakeSts

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

\$EN_DIS

Definition at line 1505 of file FspsUpd.h.

8.6.2.80 UINT8 FSP_S_CONFIG::PchPmPcieWakeFromDeepSx

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

\$EN DIS

Definition at line 1403 of file FspsUpd.h.

8.6.2.81 UINT8 FSP_S_CONFIG::PchPmPmeB0S5Dis

Offset 0x0639 - PCH Pm PME_B0_S5_DIS When cleared (default), wake events from PME_B0_STS are allowed in S5 if PME_B0_EN = 1.

\$EN_DIS

Definition at line 1381 of file FspsUpd.h.

8.6.2.82 UINT8 FSP_S_CONFIG::PchPmPwrBtnOverridePeriod

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

000b-4s, 001b-6s, 010b-8s, 011b-10s, 100b-12s, 101b-14s.

Definition at line 1475 of file FspsUpd.h.

8.6.2.83 UINT8 FSP_S_CONFIG::PchPmPwrCycDur

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

Please refer to EDS for all support settings. 0 is default, 1 is 1 second, 2 is 2 seconds, ...

Definition at line 1517 of file FspsUpd.h.

8.6.2.84 UINT8 FSP_S_CONFIG::PchPmSlpAMinAssert

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

Default is PchSlpA2s.

Definition at line 1448 of file FspsUpd.h.

8.6.2.85 UINT8 FSP_S_CONFIG::PchPmSlpLanLowDc

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

\$EN_DIS

Definition at line 1470 of file FspsUpd.h.

8.6.2.86 UINT8 FSP_S_CONFIG::PchPmSlpS0Enable

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

\$EN DIS

Definition at line 1499 of file FspsUpd.h.

8.6.2.87 UINT8 FSP_S_CONFIG::PchPmSlpS0VmEnable

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

\$EN_DIS

Definition at line 1387 of file FspsUpd.h.

8.6.2.88 UINT8 FSP_S_CONFIG::PchPmSlpS3MinAssert

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

Default is PchSlpS350ms.

Definition at line 1433 of file FspsUpd.h.

8.6.2.89 UINT8 FSP_S_CONFIG::PchPmSlpS4MinAssert

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

Default is PchSlpS44s.

Definition at line 1438 of file FspsUpd.h.

8.6.2.90 UINT8 FSP_S_CONFIG::PchPmSlpStrchSusUp

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

\$EN_DIS

Definition at line 1464 of file FspsUpd.h.

8.6.2.91 UINT8 FSP_S_CONFIG::PchPmSlpSusMinAssert

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

Default is PchSlpSus4s.

Definition at line 1443 of file FspsUpd.h.

8.6.2.92 UINT8 FSP_S_CONFIG::PchPmWolEnableOverride

Offset 0x0640 - PCH Pm Wol Enable Override Corresponds to the WOL Enable Override bit in the General PM Configuration B (GEN PMCON B) register.

\$EN_DIS

Definition at line 1397 of file FspsUpd.h.

8.6.2.93 UINT8 FSP_S_CONFIG::PchPmWolOvrWkSts

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

\$EN_DIS

Definition at line 1511 of file FspsUpd.h.

8.6.2.94 UINT8 FSP_S_CONFIG::PchPmWoWlanDeepSxEnable

Offset 0x0643 - PCH Pm WoW lan DeepSx Enable Determine if WLAN wake from DeepSx, corresponds to the DSX_WLAN_PP_EN bit in the PWRM_CFG3 register.

\$EN DIS

Definition at line 1416 of file FspsUpd.h.

8.6.2.95 UINT8 FSP_S_CONFIG::PchPmWoWlanEnable

Offset 0x0642 - PCH Pm WoW Ian 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 1409 of file FspsUpd.h.

8.6.2.96 UINT8 FSP_S_CONFIG::PchPort61hEnable

Offset 0x065C - 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 1527 of file FspsUpd.h.

8.6.2.97 UINT8 FSP_S_CONFIG::PchPwrOptEnable

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

\$EN DIS

Definition at line 906 of file FspsUpd.h.

8.6.2.98 UINT8 FSP_S_CONFIG::PchScsEmmcHs400DIIDataValid

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

\$EN DIS

Definition at line 1688 of file FspsUpd.h.

8.6.2.99 UINT8 FSP_S_CONFIG::PchScsEmmcHs400TuningRequired

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

\$EN_DIS

Definition at line 1682 of file FspsUpd.h.

8.6.2.100 UINT8 FSP_S_CONFIG::PchSirqEnable

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

\$EN_DIS

Definition at line 1740 of file FspsUpd.h.

8.6.2.101 UINT8 FSP_S_CONFIG::PchSirqMode

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

\$EN_DIS

Definition at line 1746 of file FspsUpd.h.

8.6.2.102 UINT8 FSP_S_CONFIG::PchSkyCamPortACtleEnable

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

\$EN_DIS

Definition at line 817 of file FspsUpd.h.

8.6.2.103 UINT8 FSP_S_CONFIG::PchSkyCamPortATermOvrEnable

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

\$EN_DIS

Definition at line 769 of file FspsUpd.h.

8.6.2.104 UINT8 FSP_S_CONFIG::PchSkyCamPortATrimEnable

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

\$EN DIS

Definition at line 793 of file FspsUpd.h.

8.6.2.105 UINT8 FSP_S_CONFIG::PchSkyCamPortBCtleEnable

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

\$EN_DIS

Definition at line 823 of file FspsUpd.h.

8.6.2.106 UINT8 FSP_S_CONFIG::PchSkyCamPortBTermOvrEnable

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

\$EN DIS

Definition at line 775 of file FspsUpd.h.

8.6.2.107 UINT8 FSP_S_CONFIG::PchSkyCamPortBTrimEnable

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

\$EN_DIS

Definition at line 799 of file FspsUpd.h.

8.6.2.108 UINT8 FSP_S_CONFIG::PchSkyCamPortCDCtleEnable

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

\$EN_DIS

Definition at line 829 of file FspsUpd.h.

8.6.2.109 UINT8 FSP_S_CONFIG::PchSkyCamPortCTermOvrEnable

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

\$EN_DIS

Definition at line 781 of file FspsUpd.h.

8.6.2.110 UINT8 FSP_S_CONFIG::PchSkyCamPortCTrimEnable

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

\$EN_DIS

Definition at line 805 of file FspsUpd.h.

8.6.2.111 UINT8 FSP_S_CONFIG::PchSkyCamPortDTermOvrEnable

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

\$EN_DIS

Definition at line 787 of file FspsUpd.h.

8.6.2.112 UINT8 FSP_S_CONFIG::PchSkyCamPortDTrimEnable

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

\$EN_DIS

Definition at line 811 of file FspsUpd.h.

8.6.2.113 UINT16 FSP_S_CONFIG::PchSubSystemId

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

Default is 0x7270.

Definition at line 1181 of file FspsUpd.h.

8.6.2.114 UINT16 FSP_S_CONFIG::PchSubSystemVendorld

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

Default is 0x8086.

Definition at line 1176 of file FspsUpd.h.

8.6.2.115 UINT8 FSP_S_CONFIG::PchThermalDeviceEnable

Offset 0x06DB - Enable Thermal Device Enable Thermal Device.

\$EN_DIS

Definition at line 1757 of file FspsUpd.h.

8.6.2.116 UINT8 FSP_S_CONFIG::PchTsmicLock

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

\$EN_DIS

Definition at line 1778 of file FspsUpd.h.

8.6.2.117 UINT8 FSP_S_CONFIG::PchTTEnable

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

\$EN DIS

Definition at line 1784 of file FspsUpd.h.

8.6.2.118 UINT8 FSP_S_CONFIG::PchTTLock

Offset 0x06E5 - Thermal Throttle Lock Thermal Throttle Lock.

\$EN DIS

Definition at line 1797 of file FspsUpd.h.

8.6.2.119 UINT8 FSP_S_CONFIG::PchTTState13Enable

Offset 0x06E4 - PMSync State 13 When set to 1 and the programmed GPIO pin is a 1, then PMSync state 13 will force at least T2 state.

\$EN_DIS

Definition at line 1791 of file FspsUpd.h.

8.6.2.120 UINT8 FSP_S_CONFIG::PcieAllowNoLtrlccPllShutdown

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

\$EN_DIS

Definition at line 1356 of file FspsUpd.h.

8.6.2.121 UINT8 FSP_S_CONFIG::PcieComplianceTestMode

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

\$EN DIS

Definition at line 1362 of file FspsUpd.h.

8.6.2.122 UINT8 FSP_S_CONFIG::PcieDisableRootPortClockGating

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

0: Disable; 1: Enable. \$EN DIS

Definition at line 1343 of file FspsUpd.h.

8.6.2.123 UINT8 FSP_S_CONFIG::PcieEnablePeerMemoryWrite

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

\$EN DIS

Definition at line 1349 of file FspsUpd.h.

8.6.2.124 UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCm[24]

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

Coefficient C-1.

Definition at line 1321 of file FspsUpd.h.

8.6.2.125 UINT8 FSP_S_CONFIG::PcieEqPh3LaneParamCp[24]

Offset 0x0610 - PCIE Eq Ph3 Lane Param Cp PCH PCIE EQ LANE PARAM.

Coefficient C+1.

Definition at line 1326 of file FspsUpd.h.

8.6.2.126 UINT8 FSP_S_CONFIG::PcieRpAspm[24]

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

Default is PchPcieAspmAutoConfig.

Definition at line 1300 of file FspsUpd.h.

8.6.2.127 UINT8 FSP_S_CONFIG::PcieRpClkReqNumber[24]

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

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

Definition at line 381 of file FspsUpd.h.

8.6.2.128 UINT8 FSP_S_CONFIG::PcieRpClkReqSupport[24]

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

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

Definition at line 375 of file FspsUpd.h.

8.6.2.129 UINT8 FSP_S_CONFIG::PcieRpCompletionTimeout[24]

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

Default is PchPcieCompletionTO_Default.

Definition at line 1288 of file FspsUpd.h.

8.6.2.130 UINT32 FSP_S_CONFIG::PcieRpDeviceResetPad[24]

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

See also DeviceResetPadActiveHigh.

Definition at line 1294 of file FspsUpd.h.

8.6.2.131 UINT8 FSP_S_CONFIG::PcieRpFunctionSwap

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

\$EN DIS

Definition at line 1375 of file FspsUpd.h.

8.6.2.132 UINT8 FSP_S_CONFIG::PcieRpGen3EqPh3Method[24]

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

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

Definition at line 1278 of file FspsUpd.h.

8.6.2.133 UINT8 FSP_S_CONFIG::PcieRpL1Substates[24]

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

Default is PchPcieL1SubstatesL1_1_2.

Definition at line 1306 of file FspsUpd.h.

8.6.2.134 UINT8 FSP_S_CONFIG::PcieRpPcieSpeed[24]

Offset 0x04D8 - PCIE RP Pcie Speed Determines each PCIE Port speed capability.

0: Auto; 1: Gen1; 2: Gen2; 3: Gen3 (see: PCH_PCIE_SPEED).

Definition at line 1272 of file FspsUpd.h.

8.6.2.135 UINT8 FSP_S_CONFIG::PcieRpPhysicalSlotNumber[24]

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

Default is the value as root port index.

Definition at line 1283 of file FspsUpd.h.

8.6.2.136 UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCm[5]

Offset 0x0628 - PCIE Sw Eq CoeffList Cm PCH_PCIE_EQ_PARAM.

Coefficient C-1.

Definition at line 1331 of file FspsUpd.h.

8.6.2.137 UINT8 FSP_S_CONFIG::PcieSwEqCoeffListCp[5]

Offset 0x062D - PCIE Sw Eq CoeffList Cp PCH_PCIE_EQ_PARAM.

Coefficient C+1.

Definition at line 1336 of file FspsUpd.h.

8.6.2.138 UINT8 FSP_S_CONFIG::PortUsb20Enable[16]

Offset 0x0052 - Enable USB2 ports Enable/disable per USB2 ports.

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

Definition at line 210 of file FspsUpd.h.

8.6.2.139 UINT8 FSP_S_CONFIG::PortUsb30Enable[10]

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

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

Definition at line 216 of file FspsUpd.h.

8.6.2.140 UINT16 FSP_S_CONFIG::Psi1Threshold[5]

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

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

Definition at line 679 of file FspsUpd.h.

8.6.2.141 UINT16 FSP_S_CONFIG::Psi2Threshold[5]

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

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

Definition at line 685 of file FspsUpd.h.

8.6.2.142 UINT8 FSP_S_CONFIG::Psi3Enable[5]

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

For all VR Indexes

Definition at line 559 of file FspsUpd.h.

8.6.2.143 UINT16 FSP_S_CONFIG::Psi3Threshold[5]

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

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

Definition at line 691 of file FspsUpd.h.

8.6.2.144 UINT8 FSP_S_CONFIG::PsysOffset

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

0 - Auto Units 1/4, Range 0-255. Value of 100 = 100/4 = 25 offset

Definition at line 613 of file FspsUpd.h.

8.6.2.145 UINT8 FSP_S_CONFIG::PsysSlope

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

0 - Auto Specified in 1/100 increment values. Range is 0-200. 125 = 1.25

Definition at line 607 of file FspsUpd.h.

8.6.2.146 UINT8 FSP_S_CONFIG::PxRcConfig[8]

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

The valid value is 0x00 to 0x0F for each. First byte is for PIRQA, second byte is for PIRQB, and so on. The setting is only available in Legacy 8259 PCI mode.

Definition at line 257 of file FspsUpd.h.

8.6.2.147 UINT8 FSP_S_CONFIG::SataEnable

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

\$EN_DIS

Definition at line 298 of file FspsUpd.h.

8.6.2.148 UINT8 FSP_S_CONFIG::SataMode

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

0:AHCI, 1:RAID

Definition at line 304 of file FspsUpd.h.

8.6.2.149 UINT8 FSP_S_CONFIG::SataP0TDispFinit

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

\$EN_DIS

Definition at line 1892 of file FspsUpd.h.

8.6.2.150 UINT8 FSP_S_CONFIG::SataP1TDispFinit

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

\$EN_DIS

Definition at line 1903 of file FspsUpd.h.

8.6.2.151 UINT8 FSP_S_CONFIG::SataPortsDevSlp[8]

Offset 0x004A - Enable SATA DEVSLP Feature Enable/disable SATA DEVSLP per port.

0 is disable, 1 is enable. One byte for each port, byte0 for port0, byte1 for port1, and so on.

Definition at line 204 of file FspsUpd.h.

8.6.2.152 UINT8 FSP_S_CONFIG::SataPortsDmVal[8]

Offset 0x0690 - Enable SATA Port DmVal DITO multiplier.

Default is 15.

Definition at line 1579 of file FspsUpd.h.

8.6.2.153 UINT8 FSP_S_CONFIG::SataPortsEnable[8]

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

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

Definition at line 198 of file FspsUpd.h.

8.6.2.154 UINT8 FSP_S_CONFIG::SataPwrOptEnable

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

\$EN DIS

Definition at line 1533 of file FspsUpd.h.

8.6.2.155 UINT8 FSP_S_CONFIG::SataRstHddUnlock

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

\$EN DIS

Definition at line 1642 of file FspsUpd.h.

8.6.2.156 UINT8 FSP_S_CONFIG::SataRstIrrt

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

\$EN DIS

Definition at line 1625 of file FspsUpd.h.

8.6.2.157 UINT8 FSP_S_CONFIG::SataRstIrrtOnly

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

\$EN_DIS

Definition at line 1655 of file FspsUpd.h.

8.6.2.158 UINT8 FSP_S_CONFIG::SataRstLedLocate

Offset 0x06B9 - PCH Sata Rst Led Locate Indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

\$EN_DIS

Definition at line 1649 of file FspsUpd.h.

8.6.2.159 UINT8 FSP_S_CONFIG::SataRstOromUiBanner

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

\$EN_DIS

Definition at line 1631 of file FspsUpd.h.

8.6.2.160 UINT8 FSP_S_CONFIG::SataRstPcieDeviceResetDelay[3]

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

Default value is 100ms

Definition at line 1676 of file FspsUpd.h.

8.6.2.161 UINT8 FSP_S_CONFIG::SataRstRaid0

Offset 0x06B1 - PCH Sata Rst Raid0 RAID0.

\$EN_DIS

Definition at line 1601 of file FspsUpd.h.

8.6.2.162 UINT8 FSP_S_CONFIG::SataRstRaid1

Offset 0x06B2 - PCH Sata Rst Raid1 RAID1.

\$EN DIS

Definition at line 1607 of file FspsUpd.h.

8.6.2.163 UINT8 FSP_S_CONFIG::SataRstRaid10

Offset 0x06B3 - PCH Sata Rst Raid10 RAID10.

\$EN_DIS

Definition at line 1613 of file FspsUpd.h.

8.6.2.164 UINT8 FSP_S_CONFIG::SataRstRaid5

Offset 0x06B4 - PCH Sata Rst Raid5 RAID5.

\$EN_DIS

Definition at line 1619 of file FspsUpd.h.

8.6.2.165 UINT8 FSP_S_CONFIG::SataRstRaidAlternateId

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

0:Client, 1:Alternate, 2:Server

Definition at line 1595 of file FspsUpd.h.

8.6.2.166 UINT8 FSP_S_CONFIG::SataRstSmartStorage

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

\$EN_DIS

Definition at line 1661 of file FspsUpd.h.

8.6.2.167 UINT8 FSP_S_CONFIG::SataSalpSupport

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

\$EN_DIS

Definition at line 192 of file FspsUpd.h.

8.6.2.168 UINT8 FSP_S_CONFIG::SataThermalSuggestedSetting

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

\$EN DIS

Definition at line 1909 of file FspsUpd.h.

8.6.2.169 UINT8 FSP_S_CONFIG::ScilrqSelect

Offset 0x0088 - Select ScilrgSelect SCI IRQ Select.

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

Definition at line 267 of file FspsUpd.h.

8.6.2.170 UINT8 FSP_S_CONFIG::ScsEmmcEnabled

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

\$EN DIS

Definition at line 142 of file FspsUpd.h.

8.6.2.171 UINT8 FSP_S_CONFIG::ScsEmmcHs400Enabled

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

\$EN_DIS

Definition at line 148 of file FspsUpd.h.

8.6.2.172 UINT8 FSP_S_CONFIG::ScsSdCardEnabled

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

\$EN_DIS

Definition at line 154 of file FspsUpd.h.

8.6.2.173 UINT64 FSP_S_CONFIG::SendEcCmd

Offset 0x0730 - SendEcCmd SendEcCmd function pointer.

Definition at line 2007 of file FspsUpd.h.

8.6.2.174 UINT8 FSP_S_CONFIG::SendVrMbxCmd

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

00b - no VR specific command sent. 01b - A VR mailbox command specifically for the MPS IMPV8 VR will be sent. 10b - VR specific command sent for PS4 exit issue. 11b - Reserved. \$EN_DIS

Definition at line 731 of file FspsUpd.h.

8.6.2.175 UINT8 FSP_S_CONFIG::SendVrMbxCmd1

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

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

Definition at line 738 of file FspsUpd.h.

8.6.2.176 UINT8 FSP_S_CONFIG::SerialIoDebugUartNumber

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

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

Definition at line 1729 of file FspsUpd.h.

8.6.2.177 UINT8 FSP_S_CONFIG::SerialloDevMode[11]

Offset 0x0074 - Enable Seriallo Device Mode 0:Disabled, 1:ACPI Mode, 2:PCI Mode, 3:Hidden mode, 4:Legacy UART mode - Enable/disable Seriallo I2C0,I2C1,I2C2,I2C3,I2C4,I2C5,SPI0,SPI1,UART0,UART1,UART2 device mode respectively.

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

Definition at line 250 of file FspsUpd.h.

8.6.2.178 UINT8 FSP_S_CONFIG::SerialloGpio

Offset 0x06CA - Enable Pch Serial IO GPIO Determines if enable Serial IO GPIO.

\$EN DIS

Definition at line 1709 of file FspsUpd.h.

8.6.2.179 UINT8 FSP_S_CONFIG::ShowSpiController

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

\$EN_DIS

Definition at line 166 of file FspsUpd.h.

8.6.2.180 UINT8 FSP_S_CONFIG::SlowSlewRateForGt

Offset 0x027B - Slew Rate configuration for Deep Package C States for VR GT domain Slew Rate configuration for Deep Package C States for VR GT domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 640 of file FspsUpd.h.

8.6.2.181 UINT8 FSP_S_CONFIG::SlowSlewRateForla

Offset 0x027A - Slew Rate configuration for Deep Package C States for VR IA domain Slew Rate configuration for Deep Package C States for VR IA domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 633 of file FspsUpd.h.

8.6.2.182 UINT8 FSP_S_CONFIG::SlowSlewRateForSa

Offset 0x027C - Slew Rate configuration for Deep Package C States for VR SA domain Slew Rate configuration for Deep Package C States for VR SA domain based on Acoustic Noise Mitigation feature enabled.

0: Fast/2; 1: Fast/4; 2: Fast/8; 3: Fast/16 0: Fast/2, 1: Fast/4, 2: Fast/8, 3: Fast/16

Definition at line 647 of file FspsUpd.h.

8.6.2.183 UINT8 FSP_S_CONFIG::SsicPortEnable

Offset 0x006D - Enable XHCI SSIC Eanble Enable/disable XHCI SSIC port.

\$EN DIS

Definition at line 228 of file FspsUpd.h.

8.6.2.184 UINT8 FSP_S_CONFIG::TcolrqSelect

Offset 0x0089 - Select TcolrqSelect TCO IRQ Select.

The valid value is 9, 10, 11, 20, 21, 22, 23.

Definition at line 272 of file FspsUpd.h.

8.6.2.185 UINT16 FSP_S_CONFIG::TdcPowerLimit[5]

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

Specified in 1/8A units. Range is 0-4095. 1000 = 125A. 0: Auto. For all VR Indexes

Definition at line 657 of file FspsUpd.h.

8.6.2.186 UINT8 FSP_S_CONFIG::TdcTimeWindow[5]

Offset 0x026C - HECI3 state PCODE MMIO Mailbox: Thermal Design Current time window.

Defined in milli seconds. Valid Values 1 - 1ms, 2 - 2ms, 3 - 3ms, 4 - 4ms, 5 - 5ms, 6 - 6ms, 7 - 7ms, 8 - 8ms, 10 - 10ms. For all VR Indexe

Definition at line 595 of file FspsUpd.h.

8.6.2.187 UINT8 FSP_S_CONFIG::TTSuggestedSetting

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

\$EN DIS

Definition at line 1803 of file FspsUpd.h.

8.6.2.188 UINT8 FSP_S_CONFIG::TurboMode

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

0: disable, 1: enable \$EN_DIS

Definition at line 186 of file FspsUpd.h.

8.6.2.189 UINT8 FSP_S_CONFIG::Usb2AfePehalfbit[16]

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

1b - half-bit pre-emphasis, 0b - full-bit pre-emphasis. One byte for each port.

Definition at line 328 of file FspsUpd.h.

8.6.2.190 UINT8 FSP_S_CONFIG::Usb2AfePetxiset[16]

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

000b-0mV, 001b-11.25mV, 010b-16.9mV, 011b-28.15mV, 100b-28.15mV, 101b-39.35mV, 110b-45mV, 111b-56. \hookleftarrow 3mV. One byte for each port.

Definition at line 310 of file FspsUpd.h.

8.6.2.191 UINT8 FSP_S_CONFIG::Usb2AfePredeemp[16]

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

00b - Emphasis OFF, 01b - De-emphasis ON, 10b - Pre-emphasis ON, 11b - Pre-emphasis & De-emphasis ON. One byte for each port.

Definition at line 322 of file FspsUpd.h.

8.6.2.192 UINT8 FSP_S_CONFIG::Usb2AfeTxiset[16]

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

000b-0mV, 001b-11.25mV, 010b-16.9mV, 011b-28.15mV, 100b-28.15mV, 101b-39.35mV, 110b-45mV, 111b-56. \hookleftarrow 3mV, One byte for each port.

Definition at line 316 of file FspsUpd.h.

8.6.2.193 UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmph[10]

Offset 0x00DD - USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Setting USB 3.0 TX Output -3.5dB De-← Emphasis Adjustment Setting, HSIO_TX_DWORD5[21:16], **Default = 29h** (approximately -3.5dB De-Emphasis).

One byte for each port.

Definition at line 340 of file FspsUpd.h.

8.6.2.194 UINT8 FSP_S_CONFIG::Usb3HsioTxDeEmphEnable[10]

Offset 0x00D3 - Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment Enable the write to USB 3.0 TX Output -3.5dB De-Emphasis Adjustment.

Each value in arrary can be between 0-1. One byte for each port.

Definition at line 334 of file FspsUpd.h.

8.6.2.195 UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmp[10]

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

One byte for each port.

Definition at line 352 of file FspsUpd.h.

8.6.2.196 UINT8 FSP_S_CONFIG::Usb3HsioTxDownscaleAmpEnable[10]

Offset 0x00E7 - Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment Enable the write to USB 3.0 TX Output Downscale Amplitude Adjustment, Each value in arrary can be between 0-1.

One byte for each port.

Definition at line 346 of file FspsUpd.h.

8.6.2.197 UINT16 FSP_S_CONFIG::VrVoltageLimit[5]

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

Range is 0-7999mV.

Definition at line 701 of file FspsUpd.h.

8.6.2.198 UINT8 FSP_S_CONFIG::WatchDog

Offset 0x0154 - WatchDog Timer Switch Enable/Disable.

0: Disable, 1: enable, Enable or disable WatchDog timer. \$EN_DIS

Definition at line 408 of file FspsUpd.h.

8.6.2.199 UINT16 FSP_S_CONFIG::WatchDogTimerBios

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

\$EN DIS

Definition at line 439 of file FspsUpd.h.

8.6.2.200 UINT16 FSP_S_CONFIG::WatchDogTimerOs

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

\$EN_DIS

Definition at line 433 of file FspsUpd.h.

8.6.2.201 UINT8 FSP_S_CONFIG::XdciEnable

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

\$EN_DIS

Definition at line 222 of file FspsUpd.h.

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

• FspsUpd.h

8.7 FSP_S_TEST_CONFIG Struct Reference

Fsp S Test Configuration.

#include <FspsUpd.h>

Public Attributes

UINT32 Signature

Offset 0x0780.

UINT8 ChapDeviceEnable

Offset 0x0784 - Enable/Disable Device 7 Enable: Device 7 enabled, Disable (Default): Device 7 disabled \$EN_DIS.

UINT8 SkipPamLock

Offset 0x0785 - Skip PAM register lock Enable: PAM register will not be locked by RC, platform code should lock it, Disable(Default): PAM registers will be locked by RC \$EN_DIS.

UINT8 EdramTestMode

Offset 0x0786 - EDRAM Test Mode Enable: PAM register will not be locked by RC, platform code should lock it, Disable(Default): PAM registers will be locked by RC 0: EDRAM SW disable, 1: EDRAM SW Enable, 2: EDRAM HW mode.

UINT8 DmiExtSync

Offset 0x0787 - DMI Extended Sync Control Enable: Enable DMI Extended Sync Control, Disable(Default): Disable DMI Extended Sync Control \$EN DIS.

UINT8 Dmilot

Offset 0x0788 - DMI IOT Control Enable: Enable DMI IOT Control, Disable(Default): Disable DMI IOT Control \$EN⊷_DIS.

UINT8 PegMaxPayload [3]

Offset 0x0789 - PEG Max Payload size per root port 0xFF(Default):Auto, 0x1: Force 128B, 0X2: Force 256B 0xFF: Auto, 0x1: Force 128B, 0x2: Force 256B.

· UINT8 RenderStandby

Offset 0x078C - Enable/Disable IGFX RenderStandby Enable(Default): Enable IGFX RenderStandby, Disable: Disable IGFX RenderStandby \$EN_DIS.

UINT8 PmSupport

Offset 0x078D - Enable/Disable IGFX PmSupport Enable(Default): Enable IGFX PmSupport, Disable: Disable IGFX PmSupport \$EN_DIS.

UINT8 CdynmaxClampEnable

Offset 0x078E - Enable/Disable CdynmaxClamp Enable(Default): Enable CdynmaxClamp, Disable: Disable CdynmaxClamp \$EN DIS.

UINT8 VtdDisable

Offset 0x078F - Disable VT-d 0=Enable/FALSE(VT-d disabled), 1=Disable/TRUE (VT-d enabled) \$EN_DIS.

UINT8 GtFreqMax

Offset 0x0790 - GT Frequency Limit 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz 0xFF: Auto(Default), 2: 100 Mhz, 3: 150 Mhz, 4: 200 Mhz, 5: 250 Mhz, 6: 300 Mhz, 7: 350 Mhz, 8: 400 Mhz, 9: 450 Mhz, 0xA: 500 Mhz, 0xB: 550 Mhz, 0xC: 600 Mhz, 0xD: 650 Mhz, 0xE: 700 Mhz, 0xF: 750 Mhz, 0x10: 800 Mhz, 0x11: 850 Mhz, 0x12:900 Mhz, 0x13: 950 Mhz, 0x14: 1000 Mhz, 0x15: 1050 Mhz, 0x16: 1100 Mhz, 0x17: 1150 Mhz, 0x18: 1200 Mhz.

UINT8 SaPostMemTestRsvd [11]

Offset 0x0791 - SaPostMemTestRsvd Reserved for SA Post-Mem Test \$EN_DIS.

• UINT8 OneCoreRatioLimit

Offset 0x079C - 1-Core Ratio Limit 1-Core Ratio Limit: 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 0x079D - 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 0x079E - 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 0x079F - 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 UnusedUpdSpace22

Offset 0x07A0.

UINT8 Hwp

Offset 0x07A1 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

UINT8 HdcControl

Offset 0x07A2 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

UINT8 PowerLimit1Time

Offset 0x07A3 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds.

UINT8 PowerLimit2

Offset 0x07A4 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

UINT8 TurboPowerLimitLock

Offset 0x07A5 - Turbo settings Lock Lock all Turbo settings Enable/Disable; 0: Disable , 1: Enable \$EN_DIS.

UINT8 PowerLimit3Time

Offset 0x07A6 - Package PL3 time window Package PL3 time window range for this policy in milliseconds.

UINT8 PowerLimit3DutyCycle

Offset 0x07A7 - Package PL3 Duty Cycle Package PL3 Duty Cycle; Valid Range is 0 to 100.

UINT8 PowerLimit3Lock

Offset 0x07A8 - Package PL3 Lock Package PL3 Lock Enable/Disable; 0: Disable; 1: Enable \$EN_DIS.

UINT8 PowerLimit4Lock

Offset 0x07A9 - Package PL4 Lock Package PL4 Lock Enable/Disable; 0: Disable; 1: Enable \$EN_DIS.

UINT8 TccActivationOffset

Offset 0x07AA - TCC Activation Offset TCC Activation Offset.

UINT8 TccOffsetClamp

Offset 0x07AB - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For SKL Y SKU, the recommended default for this policy is 1: Enabled, For all other SKUs the recommended default are 0: Disabled.

UINT8 TccOffsetLock

Offset 0x07AC - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0:** Disabled; 1: Enabled.

UINT8 NumberOfEntries

Offset 0x07AD - Custom Ratio State Entries The number of custom ratio state entries, ranges from 0 to 40 for a valid custom ratio table. Sets the number of custom P-states.

UINT8 Custom1PowerLimit1Time

Offset 0x07AE - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.

• UINT8 Custom1TurboActivationRatio

Offset 0x07AF - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

UINT8 Custom1ConfigTdpControl

Offset 0x07B0 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

UINT8 Custom2PowerLimit1Time

Offset 0x07B1 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.

UINT8 Custom2TurboActivationRatio

Offset 0x07B2 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

UINT8 Custom2ConfigTdpControl

Offset 0x07B3 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

UINT8 Custom3PowerLimit1Time

Offset 0x07B4 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.

UINT8 Custom3TurboActivationRatio

Offset 0x07B5 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

UINT8 Custom3ConfigTdpControl

Offset 0x07B6 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

UINT8 ConfigTdpLock

Offset 0x07B7 - ConfigTdp mode settings Lock Lock the ConfigTdp mode settings from runtime changes; **0: Disable**; 1: Enable \$EN_DIS.

UINT8 ConfigTdpBios

Offset 0x07B8 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.

UINT8 PsysPowerLimit1

Offset 0x07B9 - PL1 Enable value PL1 Enable value to limit average platform power.

UINT8 PsysPowerLimit1Time

Offset 0x07BA - PL1 timewindow PL1 timewindow in seconds. Valid values(Unit in seconds) 0 to 8, 10, 12,14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128.

• UINT8 PsysPowerLimit2

Offset 0x07BB - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

UINT8 UnusedUpdSpace23 [2]

Offset 0x07BC.

UINT8 MlcStreamerPrefetcher

Offset 0x07BE - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0: Disable; 1: Enable.

UINT8 MlcSpatialPrefetcher

Offset 0x07BF - Enable or Disable MLC Spatial Prefetcher Enable or Disable MLC Spatial Prefetcher; 0: Disable; 1: Enable \$EN_DIS.

UINT8 MonitorMwaitEnable

Offset 0x07C0 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; 1: Enable.

UINT8 MachineCheckEnable

Offset 0x07C1 - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; 1: Enable.

• UINT8 DebugInterfaceEnable

Offset 0x07C2 - Enable or Disable processor debug features Enable or Disable processor debug features; **0: Disable**; 1: Enable.

UINT8 DebugInterfaceLockEnable

Offset 0x07C3 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; 1: Enable.

UINT8 ApIdleManner

Offset 0x07C4 - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; 2: MWAIT loop; 3: RUN loop.

UINT8 ApHandoffManner

Offset 0x07C5 - Settings for AP Handoff to OS Settings for AP Handoff to OS; 1: HALT loop; 2: MWAIT loop.

UINT8 UnusedUpdSpace24 [2]

Offset 0x07C6.

UINT8 ProcTraceOutputScheme

Offset 0x07C8 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.

• UINT8 ProcTraceEnable

Offset 0x07C9 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

• UINT8 ProcTraceMemSize

Offset 0x07CA - Memory region allocation for Processor Trace Memory region allocation for Processor Trace, Total Memory required is up to requested value * 2 (for memory alignment) * 8 active threads, to enable Processor Trace, PcdFspReservedMemoryLength must be increased by the total memory required, and PlatformMemorySize policy must also be increased by the total memory required over 32MB, Valid Values are 0 - 4KB, 0x1 - 8KB, 0x2 - 16KB, 0x3 - 32KB, 0x4 - 64KB, 0x5 - 128KB, 0x6 - 256KB, 0x7 - 512KB, 0x8 - 1MB, 0x9 - 2MB, 0xA - 4MB, 0xB - 8MB, 0xC - 16MB, 0xD - 32MB, 0xE - 64MB, 0xF - 128MB, 0xFF: Disable.

UINT8 UnusedUpdSpace25

Offset 0x07CB.

UINT8 VoltageOptimization

Offset 0x07CC - Enable or Disable Voltage Optimization feature Enable or Disable Voltage Optimization feature 0: Disable; 1: Enable \$EN_DIS.

UINT8 Eist

Offset 0x07CD - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

UINT8 EnergyEfficientPState

Offset 0x07CE - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.

UINT8 EnergyEfficientTurbo

Offset 0x07CF - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.

UINT8 TStates

Offset 0x07D0 - Enable or Disable T states Enable or Disable T states; 0: Disable; 1: Enable.

UINT8 BiProcHot

Offset 0x07D1 - Enable or Disable Bi-Directional PROCHOT# Enable or Disable Bi-Directional PROCHOT#; 0←: Disable; 1: Enable \$EN_DIS.

UINT8 DisableProcHotOut

Offset 0x07D2 - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; 1: Enable.

UINT8 ProcHotResponse

Offset 0x07D3 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0:** Disable; 1: Enable.

• UINT8 DisableVrThermalAlert

Offset 0x07D4 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; 0: Disable; 1: Enable.

UINT8 AutoThermalReporting

Offset 0x07D5 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; 1: Enable.

• UINT8 ThermalMonitor

Offset 0x07D6 - Enable or Disable Thermal Monitor Enable or Disable Thermal Monitor; 0: Disable; 1: Enable \$EN_DIS.

• UINT8 Cx

Offset 0x07D7 - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).

UINT8 PmgCstCfgCtrlLock

Offset 0x07D8 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; 1: Enable.

• UINT8 C1e

Offset 0x07D9 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

· UINT8 PkgCStateDemotion

Offset 0x07DA - Enable or Disable Package C-State Demotion Enable or Disable Package C-State Demotion.

UINT8 PkgCStateUnDemotion

Offset 0x07DB - Enable or Disable Package C-State UnDemotion Enable or Disable Package C-State UnDemotion.

• UINT8 CStatePreWake

Offset 0x07DC - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

UINT8 TimedMwait

Offset 0x07DD - Enable or Disable TimedMwait Support.

UINT8 CstCfgCtrloMwaitRedirection

Offset 0x07DE - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.

UINT8 PkgCStateLimit

Offset 0x07DF - Set the Max Pkg Cstate Set the Max Pkg Cstate.

UINT8 CstateLatencyControl0TimeUnit

Offset 0x07E0 - TimeUnit for C-State Latency Control0 TimeUnit for C-State Latency Control0; Valid values 0 - 1ns, 1 - 32ns, 2 - 1024ns, 3 - 32768ns, 4 - 1048576ns, 5 - 33554432ns.

UINT8 CstateLatencyControl1TimeUnit

Offset 0x07E1 - TimeUnit for C-State Latency Control1 TimeUnit for C-State Latency Control1; Valid values 0 - 1ns, 1 - 32ns, 2 - 1024ns, 3 - 32768ns, 4 - 1048576ns, 5 - 33554432ns.

UINT8 CstateLatencyControl2TimeUnit

Offset 0x07E2 - TimeUnit for C-State Latency Control2 TimeUnit for C-State Latency Control2; Valid values 0 - 1ns, 1 - 32ns, 2 - 1024ns, 3 - 32768ns, 4 - 1048576ns, 5 - 33554432ns.

UINT8 CstateLatencyControl3TimeUnit

 $Offset\ 0x07E3\ -\ TimeUnit\ for\ C-State\ Latency\ Control3\ TimeUnit\ for\ C-State\ Latency\ Control3\ ; Valid\ values\ 0\ -\ 1ns\ ,\ 1\ -\ 32ns\ ,\ 2\ -\ 1024ns\ ,\ 3\ -\ 32768ns\ ,\ 4\ -\ 1048576ns\ ,\ 5\ -\ 33554432ns.$

UINT8 CstateLatencyControl4TimeUnit

Offset 0x07E4 - TimeUnit for C-State Latency Control4 TimeUnit for C-State Latency Control4; Valid values 0 - 1ns, 1 - 32ns, 2 - 1024ns, 3 - 32768ns, 4 - 1048576ns, 5 - 33554432ns.

UINT8 CstateLatencyControl5TimeUnit

Offset 0x07E5 - TimeUnit for C-State Latency Control5 TimeUnit for C-State Latency Control5; Valid values 0 - 1ns, 1 - 32ns, 2 - 1024ns, 3 - 32768ns, 4 - 1048576ns, 5 - 33554432ns.

UINT8 PpmIrmSetting

Offset 0x07E6 - Interrupt Redirection Mode Select Interrupt Redirection Mode Select.0: Fixed priority; 1: Round robin;2: Hash vector;4: PAIR with fixed priority;5: PAIR with round robin;6: PAIR with hash vector;7: No change.

UINT8 ProcHotLock

Offset 0x07E7 - Lock prochot configuration Lock prochot configuration Enable/Disable; **0: Disable**; 1: Enable \$EN←_DIS.

UINT8 ConfigTdpLevel

Offset 0x07E8 - Configuration for boot TDP selection Configuration for boot TDP selection; **0: TDP Nominal**; 1: TDP Down; 2: TDP Up;0xFF: Deactivate 0:TDP Nominal, 1:TDP Down, 2:TDP Up, 0xFF:Deactivate.

UINT8 RaceToHalt

Offset 0x07E9 - Race To Halt Enable/Disable Race To Halt feature.

UINT16 MaxRatio

Offset 0x07EA - Max P-State Ratio Max P-State Ratio , Valid Range 0 to 0x7F.

UINT16 StateRatio [40]

Offset 0x07EC - Maximum P-state ratio to use in the custom P-state table Maximum P-state ratio to use in the custom P-state table.

UINT16 CstateLatencyControl0Irtl

Offset 0x083C - Interrupt Response Time Limit of C-State LatencyContol0 Interrupt Response Time Limit of C-State LatencyContol0.

UINT16 CstateLatencyControl1Irtl

Offset 0x083E - Interrupt Response Time Limit of C-State LatencyContol1 Interrupt Response Time Limit of C-State LatencyContol1.Range of value 0 to 0x3FF.

UINT16 CstateLatencyControl2Irtl

Offset 0x0840 - Interrupt Response Time Limit of C-State LatencyContol2 Interrupt Response Time Limit of C-State LatencyContol2.Range of value 0 to 0x3FF.

UINT16 CstateLatencyControl3Irtl

Offset 0x0842 - Interrupt Response Time Limit of C-State LatencyContol3 Interrupt Response Time Limit of C-State LatencyContol3.Range of value 0 to 0x3FF.

UINT16 CstateLatencyControl4Irtl

Offset 0x0844 - Interrupt Response Time Limit of C-State LatencyContol4 Interrupt Response Time Limit of C-State LatencyContol4.Range of value 0 to 0x3FF.

UINT16 CstateLatencyControl5Irtl

Offset 0x0846 - Interrupt Response Time Limit of C-State LatencyContol5 Interrupt Response Time Limit of C-State LatencyContol5.Range of value 0 to 0x3FF.

UINT32 PowerLimit1

Offset 0x0848 - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.

UINT32 PowerLimit2Power

Offset 0x084C - Package Short duration turbo mode power limit Package Short duration turbo mode power limit.

UINT32 PowerLimit3

Offset 0x0850 - Package PL3 power limit Package PL3 power limit.

UINT32 PowerLimit4

Offset 0x0854 - Package PL4 power limit Package PL4 power limit.

UINT32 TccOffsetTimeWindowForRatl

Offset 0x0858 - Tcc Offset Time Window for RATL Package PL4 power limit.

UINT32 Custom1PowerLimit1

Offset 0x085C - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.

UINT32 Custom1PowerLimit2

Offset 0x0860 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.

UINT32 Custom2PowerLimit1

Offset 0x0864 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.

UINT32 Custom2PowerLimit2

Offset 0x0868 - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2

UINT32 Custom3PowerLimit1

Offset 0x086C - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3

UINT32 Custom3PowerLimit2

Offset 0x0870 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.

UINT32 PsysPowerLimit1Power

Offset 0x0874 - Platform PL1 power Platform PL1 power.

• UINT32 PsysPowerLimit2Power

Offset 0x0878 - Platform PL2 power Platform PL2 power.

UINT16 PsysPmax

Offset 0x087C - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.

UINT16 CpuS3ResumeDataSize

Offset 0x087E - CpuS3ResumeDataSize Size of CPU S3 Resume Data.

UINT32 CpuS3ResumeData

Offset 0x0880 - CpuS3ResumeData Pointer to CPU S3 Resume Data.

UINT8 ReservedCpuPostMemTest [6]

Offset 0x0884 - ReservedCpuPostMemTest Reserved for CPU Post-Mem Test \$EN_DIS.

UINT8 SgxSinitDataFromTpm

Offset 0x088A - SgxSinitDataFromTpm SgxSinitDataFromTpm default values.

UINT8 EndOfPostMessage

Offset 0x088B - End of Post message Test, Send End of Post message.

UINT8 DisableD0l3SettingForHeci

Offset 0x088C - D0l3 Setting for HECI Disable Test, 0: disable, 1: enable, Setting this option disables setting D0l3 bit for all HECI devices \$EN_DIS.

UINT8 PchLockDownGlobalSmi

Offset 0x088D - Enable LOCKDOWN SMI Enable SMI LOCK bit to prevent writes to the Global SMI Enable bit.

UINT16 PchHdaResetWaitTimer

Offset 0x088E - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds.

UINT8 PchLockDownBiosInterface

Offset 0x0890 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

UINT8 PchLockDownRtcLock

Offset 0x0891 - RTC CMOS RAM LOCK Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.

UINT8 PchSbiUnlock

Offset 0x0892 - PCH Sbi lock bit This unlock the SBI lock bit to allow SBI after post time.

UINT8 PchSbAccessUnlock

Offset 0x0893 - PCH Psf lock bit The PSF registers will be locked before 3rd party code execution.

UINT16 PcieRpLtrMaxSnoopLatency [24]

Offset 0x0894 - PCIE RP Ltr Max Snoop Latency Latency Tolerance Reporting, Max Snoop Latency.

UINT16 PcieRpLtrMaxNoSnoopLatency [24]

Offset 0x08C4 - PCIE RP Ltr Max No Snoop Latency Latency Tolerance Reporting, Max Non-Snoop Latency.

UINT8 PcieRpSnoopLatencyOverrideMode [24]

Offset 0x08F4 - PCIE RP Snoop Latency Override Mode Latency Tolerance Reporting, Snoop Latency Override Mode.

UINT8 PcieRpSnoopLatencyOverrideMultiplier [24]

Offset 0x090C - PCIE RP Snoop Latency Override Multiplier Latency Tolerance Reporting, Snoop Latency Override Multiplier.

UINT16 PcieRpSnoopLatencyOverrideValue [24]

Offset 0x0924 - PCIE RP Snoop Latency Override Value Latency Tolerance Reporting, Snoop Latency Override Value.

UINT8 PcieRpNonSnoopLatencyOverrideMode [24]

Offset 0x0954 - PCIE RP Non Snoop Latency Override Mode Latency Tolerance Reporting, Non-Snoop Latency Override Mode.

UINT8 PcieRpNonSnoopLatencyOverrideMultiplier [24]

Offset 0x096C - PCIE RP Non Snoop Latency Override Multiplier Latency Tolerance Reporting, Non-Snoop Latency Override Multiplier.

UINT16 PcieRpNonSnoopLatencyOverrideValue [24]

Offset 0x0984 - PCIE RP Non Snoop Latency Override Value Latency Tolerance Reporting, Non-Snoop Latency Override Value.

• UINT8 PcieRpSlotPowerLimitScale [24]

Offset 0x09B4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

UINT16 PcieRpSlotPowerLimitValue [24]

Offset 0x09CC - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.

• UINT8 PcieRpUptp [24]

Offset 0x09FC - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.

• UINT8 PcieRpDptp [24]

Offset 0x0A14 - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.

• UINT8 PcieEnablePort8xhDecode

Offset 0x0A2C - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.

• UINT8 PchPciePort8xhDecodePortIndex

Offset 0x0A2D - PCIE Port8xh Decode Port Index The Index of PCIe Port that is selected for Port8xh Decode (0 Rased)

UINT8 PchPmDisableEnergyReport

Offset 0x0A2E - PCH Pm Disable Energy Report Disable/Enable PCH to CPU enery report feature.

UINT8 PchPmPmcReadDisable

Offset 0x0A2F - PCH Pm Pmc Read Disable When set to true, this bit disallows host reads to PMC XRAM.

UINT8 SataTestMode

Offset 0x0A30 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

UINT8 ReservedFspsTestUpd [15]

Offset 0x0A31.

8.7.1 Detailed Description

Fsp S Test Configuration.

Definition at line 2062 of file FspsUpd.h.

8.7.2 Member Data Documentation

8.7.2.1 UINT8 FSP_S_TEST_CONFIG::ApHandoffManner

Offset 0x07C5 - Settings for AP Handoff to OS Settings for AP Handoff to OS; 1: HALT loop; 2: MWAIT loop.

1:HALT loop, 2:MWAIT loop

Definition at line 2392 of file FspsUpd.h.

8.7.2.2 UINT8 FSP_S_TEST_CONFIG::ApIdleManner

Offset 0x07C4 - AP Idle Manner of waiting for SIPI AP Idle Manner of waiting for SIPI; 1: HALT loop; **2: MWAIT loop**; 3: RUN loop.

1:HALT loop, 2:MWAIT loop, 3:RUN loop

Definition at line 2386 of file FspsUpd.h.

8.7.2.3 UINT8 FSP_S_TEST_CONFIG::AutoThermalReporting

Offset 0x07D5 - Enable or Disable Thermal Reporting Enable or Disable Thermal Reporting through ACPI tables; 0: Disable; **1: Enable**.

\$EN_DIS

Definition at line 2485 of file FspsUpd.h.

8.7.2.4 UINT8 FSP_S_TEST_CONFIG::C1e

Offset 0x07D9 - Enable or Disable Enhanced C-states Enable or Disable Enhanced C-states.

0: Disable; 1: Enable \$EN_DIS

Definition at line 2509 of file FspsUpd.h.

8.7.2.5 UINT8 FSP_S_TEST_CONFIG::ConfigTdpBios

Offset 0x07B8 - Load Configurable TDP SSDT Configure whether to load Configurable TDP SSDT; **0: Disable**; 1: Enable.

\$EN DIS

Definition at line 2321 of file FspsUpd.h.

8.7.2.6 UINT16 FSP_S_TEST_CONFIG::CstateLatencyControl0Irtl

Offset 0x083C - Interrupt Response Time Limit of C-State LatencyContol0 Interrupt Response Time Limit of C-State LatencyContol0.

Range of value 0 to 0x3FF

Definition at line 2628 of file FspsUpd.h.

8.7.2.7 UINT8 FSP_S_TEST_CONFIG::CStatePreWake

Offset 0x07DC - Enable or Disable CState-Pre wake Enable or Disable CState-Pre wake.

Disable; 1: Enable \$EN DIS

Definition at line 2529 of file FspsUpd.h.

8.7.2.8 UINT8 FSP_S_TEST_CONFIG::CstCfgCtrloMwaitRedirection

Offset 0x07DE - Enable or Disable IO to MWAIT redirection Enable or Disable IO to MWAIT redirection; **0: Disable**; 1: Enable.

\$EN DIS

Definition at line 2541 of file FspsUpd.h.

8.7.2.9 UINT8 FSP_S_TEST_CONFIG::Custom1ConfigTdpControl

Offset 0x07B0 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2279 of file FspsUpd.h.

8.7.2.10 UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit1

Offset 0x085C - Short term Power Limit value for custom cTDP level 1 Short term Power Limit value for custom cTDP level 1.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2689 of file FspsUpd.h.

8.7.2.11 UINT8 FSP_S_TEST_CONFIG::Custom1PowerLimit1Time

Offset 0x07AE - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 1.

Valid Range 0 to 128

Definition at line 2269 of file FspsUpd.h.

8.7.2.12 UINT32 FSP_S_TEST_CONFIG::Custom1PowerLimit2

Offset 0x0860 - Long term Power Limit value for custom cTDP level 1 Long term Power Limit value for custom cTDP level 1.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2695 of file FspsUpd.h.

8.7.2.13 UINT8 FSP_S_TEST_CONFIG::Custom1TurboActivationRatio

Offset 0x07AF - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 1.

Valid Range 0 to 255

Definition at line 2274 of file FspsUpd.h.

8.7.2.14 UINT8 FSP_S_TEST_CONFIG::Custom2ConfigTdpControl

Offset 0x07B3 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2294 of file FspsUpd.h.

8.7.2.15 UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit1

Offset 0x0864 - Short term Power Limit value for custom cTDP level 2 Short term Power Limit value for custom cTDP level 2.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2701 of file FspsUpd.h.

8.7.2.16 UINT8 FSP_S_TEST_CONFIG::Custom2PowerLimit1Time

Offset 0x07B1 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 2.

Valid Range 0 to 128

Definition at line 2284 of file FspsUpd.h.

8.7.2.17 UINT32 FSP_S_TEST_CONFIG::Custom2PowerLimit2

Offset 0x0868 - Long term Power Limit value for custom cTDP level 2 Long term Power Limit value for custom cTDP level 2.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2707 of file FspsUpd.h.

8.7.2.18 UINT8 FSP_S_TEST_CONFIG::Custom2TurboActivationRatio

Offset 0x07B2 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 2.

Valid Range 0 to 255

Definition at line 2289 of file FspsUpd.h.

8.7.2.19 UINT8 FSP_S_TEST_CONFIG::Custom3ConfigTdpControl

Offset 0x07B6 - Custom Config Tdp Control Config Tdp Control (0/1/2) value for custom cTDP level 1.

Valid Range is 0 to 2

Definition at line 2309 of file FspsUpd.h.

8.7.2.20 UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit1

Offset 0x086C - Short term Power Limit value for custom cTDP level 3 Short term Power Limit value for custom cTDP level 3.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2713 of file FspsUpd.h.

8.7.2.21 UINT8 FSP_S_TEST_CONFIG::Custom3PowerLimit1Time

Offset 0x07B4 - Custom Short term Power Limit time window Short term Power Limit time window value for custom CTDP level 3.

Valid Range 0 to 128

Definition at line 2299 of file FspsUpd.h.

8.7.2.22 UINT32 FSP_S_TEST_CONFIG::Custom3PowerLimit2

Offset 0x0870 - Long term Power Limit value for custom cTDP level 3 Long term Power Limit value for custom cTDP level 3.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2719 of file FspsUpd.h.

8.7.2.23 UINT8 FSP_S_TEST_CONFIG::Custom3TurboActivationRatio

Offset 0x07B5 - Custom Turbo Activation Ratio Turbo Activation Ratio for custom cTDP level 3.

Valid Range 0 to 255

Definition at line 2304 of file FspsUpd.h.

8.7.2.24 UINT8 FSP_S_TEST_CONFIG::Cx

Offset 0x07D7 - Enable or Disable CPU power states (C-states) Enable or Disable CPU power states (C-states).

0: Disable; 1: Enable \$EN_DIS

Definition at line 2497 of file FspsUpd.h.

8.7.2.25 UINT8 FSP_S_TEST_CONFIG::DebugInterfaceEnable

Offset 0x07C2 - Enable or Disable processor debug features Enable or Disable processor debug features; $0 \leftarrow$: Disable; 1: Enable.

\$EN DIS

Definition at line 2374 of file FspsUpd.h.

8.7.2.26 UINT8 FSP_S_TEST_CONFIG::DebugInterfaceLockEnable

Offset 0x07C3 - Lock or Unlock debug interface features Lock or Unlock debug interface features; 0: Disable; 1: Enable.

\$EN DIS

Definition at line 2380 of file FspsUpd.h.

8.7.2.27 UINT8 FSP_S_TEST_CONFIG::DisableProcHotOut

Offset 0x07D2 - Enable or Disable PROCHOT# signal being driven externally Enable or Disable PROCHOT# signal being driven externally; 0: Disable; 1: Enable.

\$EN DIS

Definition at line 2467 of file FspsUpd.h.

8.7.2.28 UINT8 FSP_S_TEST_CONFIG::DisableVrThermalAlert

Offset 0x07D4 - Enable or Disable VR Thermal Alert Enable or Disable VR Thermal Alert; 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 2479 of file FspsUpd.h.

8.7.2.29 UINT8 FSP_S_TEST_CONFIG::Eist

Offset 0x07CD - Enable or Disable Intel SpeedStep Technology Enable or Disable Intel SpeedStep Technology.

0: Disable; 1: Enable \$EN_DIS

Definition at line 2435 of file FspsUpd.h.

8.7.2.30 UINT8 FSP_S_TEST_CONFIG::EndOfPostMessage

Offset 0x088B - End of Post message Test, Send End of Post message.

Disable(0x0): Disable EOP message, Send in PEI(0x1): EOP send in PEI, Send in DXE(0x2)(Default): EOP send in PEI 0:Disable, 1:Send in PEI, 2:Send in DXE, 3:Reserved

Definition at line 2765 of file FspsUpd.h.

8.7.2.31 UINT8 FSP_S_TEST_CONFIG::EnergyEfficientPState

Offset 0x07CE - Enable or Disable Energy Efficient P-state Enable or Disable Energy Efficient P-state will be applied in Turbo mode.

Disable; 1: Enable \$EN_DIS

Definition at line 2442 of file FspsUpd.h.

8.7.2.32 UINT8 FSP_S_TEST_CONFIG::EnergyEfficientTurbo

Offset 0x07CF - Enable or Disable Energy Efficient Turbo Enable or Disable Energy Efficient Turbo, will be applied in Turbo mode.

Disable; 1: Enable \$EN_DIS

Definition at line 2449 of file FspsUpd.h.

8.7.2.33 UINT8 FSP_S_TEST_CONFIG::HdcControl

Offset 0x07A2 - Hardware Duty Cycle Control Hardware Duty Cycle Control configuration.

0: Disabled; 1: Enabled 2-3:Reserved \$EN_DIS

Definition at line 2194 of file FspsUpd.h.

8.7.2.34 UINT8 FSP_S_TEST_CONFIG::Hwp

Offset 0x07A1 - Enable or Disable HWP Enable or Disable HWP(Hardware P states) Support.

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

Definition at line 2188 of file FspsUpd.h.

8.7.2.35 UINT8 FSP_S_TEST_CONFIG::MachineCheckEnable

Offset 0x07C1 - Enable or Disable initialization of machine check registers Enable or Disable initialization of machine check registers; 0: Disable; **1: Enable**.

\$EN DIS

Definition at line 2368 of file FspsUpd.h.

8.7.2.36 UINT8 FSP_S_TEST_CONFIG::MicStreamerPrefetcher

Offset 0x07BE - Enable or Disable MLC Streamer Prefetcher Enable or Disable MLC Streamer Prefetcher; 0←: Disable; **1: Enable**.

\$EN DIS

Definition at line 2350 of file FspsUpd.h.

8.7.2.37 UINT8 FSP_S_TEST_CONFIG::MonitorMwaitEnable

Offset 0x07C0 - Enable or Disable Monitor /MWAIT instructions Enable or Disable Monitor /MWAIT instructions; 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 2362 of file FspsUpd.h.

8.7.2.38 UINT8 FSP_S_TEST_CONFIG::NumberOfEntries

Offset 0x07AD - Custom Ratio State Entries The number of custom ratio state entries, ranges from 0 to 40 for a valid custom ratio table. Sets the number of custom P-states.

At least 2 states must be present

Definition at line 2264 of file FspsUpd.h.

8.7.2.39 UINT8 FSP_S_TEST_CONFIG::OneCoreRatioLimit

Offset 0x079C - 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 2156 of file FspsUpd.h.

8.7.2.40 UINT16 FSP_S_TEST_CONFIG::PchHdaResetWaitTimer

Offset 0x088E - HD Audio Reset Wait Timer The delay timer after Azalia reset, the value is number of microseconds. Default is 600.

Definition at line 2783 of file FspsUpd.h.

8.7.2.41 UINT8 FSP_S_TEST_CONFIG::PchLockDownBiosInterface

Offset 0x0890 - Enable LOCKDOWN BIOS Interface Enable BIOS Interface Lock Down bit to prevent writes to the Backup Control Register.

\$EN_DIS

Definition at line 2789 of file FspsUpd.h.

8.7.2.42 UINT8 FSP_S_TEST_CONFIG::PchLockDownGlobalSmi

Offset 0x088D - Enable LOCKDOWN SMI Enable SMI LOCK bit to prevent writes to the Global SMI Enable bit.

\$EN DIS

Definition at line 2778 of file FspsUpd.h.

8.7.2.43 UINT8 FSP_S_TEST_CONFIG::PchLockDownRtcLock

Offset 0x0891 - RTC CMOS RAM LOCK Enable RTC lower and upper 128 byte Lock bits to lock Bytes 38h-3Fh in the upper and and lower 128-byte bank of RTC RAM.

\$EN DIS

Definition at line 2796 of file FspsUpd.h.

8.7.2.44 UINT8 FSP_S_TEST_CONFIG::PchPmDisableEnergyReport

Offset 0x0A2E - PCH Pm Disable Energy Report Disable/Enable PCH to CPU enery report feature.

\$EN_DIS

Definition at line 2886 of file FspsUpd.h.

8.7.2.45 UINT8 FSP_S_TEST_CONFIG::PchPmPmcReadDisable

Offset 0x0A2F - PCH Pm Pmc Read Disable When set to true, this bit disallows host reads to PMC XRAM.

\$EN_DIS

Definition at line 2892 of file FspsUpd.h.

8.7.2.46 UINT8 FSP_S_TEST_CONFIG::PchSbAccessUnlock

Offset 0x0893 - PCH Psf lock bit The PSF registers will be locked before 3rd party code execution.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 2808 of file FspsUpd.h.

8.7.2.47 UINT8 FSP_S_TEST_CONFIG::PchSbiUnlock

Offset 0x0892 - PCH Sbi lock bit This unlock the SBI lock bit to allow SBI after post time.

0: Disable; 1: Enable. \$EN DIS

Definition at line 2802 of file FspsUpd.h.

8.7.2.48 UINT8 FSP_S_TEST_CONFIG::PcieEnablePort8xhDecode

Offset 0x0A2C - PCIE RP Enable Port8xh Decode This member describes whether PCIE root port Port 8xh Decode is enabled.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 2875 of file FspsUpd.h.

8.7.2.49 UINT8 FSP_S_TEST_CONFIG::PcieRpDptp[24]

Offset 0x0A14 - PCIE RP Downstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 7.

Definition at line 2868 of file FspsUpd.h.

8.7.2.50 UINT8 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitScale[24]

Offset 0x09B4 - PCIE RP Slot Power Limit Scale Specifies scale used for slot power limit value.

Leave as 0 to set to default.

Definition at line 2853 of file FspsUpd.h.

8.7.2.51 UINT16 FSP_S_TEST_CONFIG::PcieRpSlotPowerLimitValue[24]

Offset 0x09CC - PCIE RP Slot Power Limit Value Specifies upper limit on power supplie by slot.

Leave as 0 to set to default.

Definition at line 2858 of file FspsUpd.h.

8.7.2.52 UINT8 FSP_S_TEST_CONFIG::PcieRpUptp[24]

Offset 0x09FC - PCIE RP Upstream Port Transmiter Preset Used during Gen3 Link Equalization.

Used for all lanes. Default is 5.

Definition at line 2863 of file FspsUpd.h.

8.7.2.53 UINT8 FSP_S_TEST_CONFIG::PkgCStateDemotion

Offset 0x07DA - Enable or Disable Package C-State Demotion Enable or Disable Package C-State Demotion.

0: Disable; 1: Enable; 2: Auto (Auto: Enabled for Skylake; Disabled for Kabylake) \$EN DIS

Definition at line 2516 of file FspsUpd.h.

8.7.2.54 UINT8 FSP_S_TEST_CONFIG::PkgCStateLimit

Offset 0x07DF - Set the Max Pkg Cstate Set the Max Pkg Cstate.

Default set to Auto which limits the Max Pkg Cstate to deep C-state. Valid values 0 - C0/C1, 1 - C2, 2 - C3, 3 - C6, 4 - C7, 5 - C7S, 6 - C8, 7 - C9, 8 - C10, 254 - CPU Default, 255 - Auto

Definition at line 2548 of file FspsUpd.h.

8.7.2.55 UINT8 FSP_S_TEST_CONFIG::PkgCStateUnDemotion

Offset 0x07DB - Enable or Disable Package C-State UnDemotion Enable or Disable Package C-State UnDemotion.

0: Disable; 1: Enable; 2: Auto (Auto: Enabled for Skylake; Disabled for Kabylake) \$EN_DIS

Definition at line 2523 of file FspsUpd.h.

8.7.2.56 UINT8 FSP_S_TEST_CONFIG::PmgCstCfgCtrlLock

Offset 0x07D8 - Configure C-State Configuration Lock Configure C-State Configuration Lock; 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 2503 of file FspsUpd.h.

8.7.2.57 UINT32 FSP_S_TEST_CONFIG::PowerLimit1

Offset 0x0848 - Package Long duration turbo mode power limit Package Long duration turbo mode power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit. Valid Range 0 to 4095875 in Step size of 125

Definition at line 2659 of file FspsUpd.h.

8.7.2.58 UINT8 FSP_S_TEST_CONFIG::PowerLimit1Time

Offset 0x07A3 - Package Long duration turbo mode time Package Long duration turbo mode time window in seconds

Valid values(Unit in seconds) 0 to 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128 Definition at line 2200 of file FspsUpd.h.

8.7.2.59 UINT8 FSP_S_TEST_CONFIG::PowerLimit2

Offset 0x07A4 - Short Duration Turbo Mode Enable or Disable short duration Turbo Mode.

0 : Disable; 1: Enable \$EN_DIS

Definition at line 2206 of file FspsUpd.h.

8.7.2.60 UINT32 FSP_S_TEST_CONFIG::PowerLimit2Power

Offset 0x084C - Package Short duration turbo mode power limit Package Short duration turbo mode power limit. Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2665 of file FspsUpd.h.

8.7.2.61 UINT32 FSP_S_TEST_CONFIG::PowerLimit3

Offset 0x0850 - Package PL3 power limit Package PL3 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2671 of file FspsUpd.h.

8.7.2.62 UINT8 FSP_S_TEST_CONFIG::PowerLimit3Time

Offset 0x07A6 - Package PL3 time window Package PL3 time window range for this policy in milliseconds.

Valid values are 0, 3 to 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 55, 56, 64

Definition at line 2218 of file FspsUpd.h.

8.7.2.63 UINT32 FSP_S_TEST_CONFIG::PowerLimit4

Offset 0x0854 - Package PL4 power limit Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2677 of file FspsUpd.h.

8.7.2.64 UINT8 FSP_S_TEST_CONFIG::ProcHotResponse

Offset 0x07D3 - Enable or Disable PROCHOT# Response Enable or Disable PROCHOT# Response; **0: Disable**; 1: Enable.

\$EN DIS

Definition at line 2473 of file FspsUpd.h.

8.7.2.65 UINT8 FSP_S_TEST_CONFIG::ProcTraceEnable

Offset 0x07C9 - Enable or Disable Processor Trace feature Enable or Disable Processor Trace feature; **0: Disable**; 1: Enable.

\$EN DIS

Definition at line 2408 of file FspsUpd.h.

8.7.2.66 UINT8 FSP_S_TEST_CONFIG::ProcTraceOutputScheme

Offset 0x07C8 - Control on Processor Trace output scheme Control on Processor Trace output scheme; **0: Single Range Output**; 1: ToPA Output.

0:Single Range Output, 1:ToPA Output

Definition at line 2402 of file FspsUpd.h.

8.7.2.67 UINT16 FSP_S_TEST_CONFIG::PsysPmax

Offset 0x087C - Platform Power Pmax PCODE MMIO Mailbox: Platform Power Pmax.

0 - Auto Specified in 1/8 Watt increments. Range 0-1024 Watts. Value of 800 = 100W

Definition at line 2737 of file FspsUpd.h.

8.7.2.68 UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit1

Offset 0x07B9 - PL1 Enable value PL1 Enable value to limit average platform power.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 2327 of file FspsUpd.h.

8.7.2.69 UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit1Power

Offset 0x0874 - Platform PL1 power Platform PL1 power.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2725 of file FspsUpd.h.

8.7.2.70 UINT8 FSP_S_TEST_CONFIG::PsysPowerLimit2

Offset 0x07BB - PL2 Enable Value PL2 Enable activates the PL2 value to limit average platform power.

0: Disable; 1: Enable. \$EN_DIS

Definition at line 2340 of file FspsUpd.h.

8.7.2.71 UINT32 FSP_S_TEST_CONFIG::PsysPowerLimit2Power

Offset 0x0878 - Platform PL2 power Platform PL2 power.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2731 of file FspsUpd.h.

8.7.2.72 UINT8 FSP_S_TEST_CONFIG::RaceToHalt

Offset 0x07E9 - Race To Halt Enable/Disable Race To Halt feature.

RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)Disable; **1: Enable** \$EN_DIS

Definition at line 2611 of file FspsUpd.h.

8.7.2.73 UINT8 FSP_S_TEST_CONFIG::SataTestMode

Offset 0x0A30 - PCH Sata Test Mode Allow entrance to the PCH SATA test modes.

\$EN_DIS

Definition at line 2898 of file FspsUpd.h.

8.7.2.74 UINT16 FSP_S_TEST_CONFIG::StateRatio[40]

Offset 0x07EC - Maximum P-state ratio to use in the custom P-state table Maximum P-state ratio to use in the custom P-state table.

NumOfCustomPStates has valid range between 0 to 40. For no. of P-States supported(NumOfCustomPStates), StateRatio[NumOfCustomPStates] are configurable. Valid Range of value is 0 to 0x7F

Definition at line 2623 of file FspsUpd.h.

8.7.2.75 UINT8 FSP_S_TEST_CONFIG::TccActivationOffset

Offset 0x07AA - TCC Activation Offset TCC Activation Offset.

Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated. TCC will be activated at TCC Activation Temperature, in volts.For SKL Y SKU, the recommended default for this policy is **10**, For all other SKUs the recommended default are **0**

Definition at line 2243 of file FspsUpd.h.

8.7.2.76 UINT8 FSP_S_TEST_CONFIG::TccOffsetClamp

Offset 0x07AB - Tcc Offset Clamp Enable/Disable Tcc Offset Clamp for Runtime Average Temperature Limit (RATL) allows CPU to throttle below P1.For SKL Y SKU, the recommended default for this policy is **1: Enabled**, For all other SKUs the recommended default are **0: Disabled**.

\$EN DIS

Definition at line 2251 of file FspsUpd.h.

8.7.2.77 UINT8 FSP_S_TEST_CONFIG::TccOffsetLock

Offset 0x07AC - Tcc Offset Lock Tcc Offset Lock for Runtime Average Temperature Limit (RATL) to lock temperature target; **0: Disabled**; 1: Enabled.

\$EN_DIS

Definition at line 2258 of file FspsUpd.h.

8.7.2.78 UINT32 FSP_S_TEST_CONFIG::TccOffsetTimeWindowForRatl

Offset 0x0858 - Tcc Offset Time Window for RATL Package PL4 power limit.

Units are based on POWER_MGMT_CONFIG.CustomPowerUnit.Valid Range 0 to 4095875 in Step size of 125 Definition at line 2683 of file FspsUpd.h.

8.7.2.79 UINT8 FSP_S_TEST_CONFIG::TimedMwait

Offset 0x07DD - Enable or Disable TimedMwait Support.

Enable or Disable TimedMwait Support. Disable; 1: Enable \$EN_DIS

Definition at line 2535 of file FspsUpd.h.

8.7.2.80 UINT8 FSP_S_TEST_CONFIG::TStates

Offset 0x07D0 - Enable or Disable T states Enable or Disable T states; 0: Disable; 1: Enable.

\$EN_DIS

Definition at line 2455 of file FspsUpd.h.

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

· FspsUpd.h

8.8 FSP_T_CONFIG Struct Reference

Fsp T Configuration.

#include <FsptUpd.h>

Public Attributes

UINT8 PcdSerialIoUartDebugEnable

Offset 0x0040 - PcdSerialloUartDebugEnable Enable Seriallo Uart debug library with/without initializing Seriallo Uart device in FSP.

UINT8 PcdSerialloUartNumber

Offset 0x0041 - PcdSerialloUartNumber Select Seriallo Uart Controller for debug.

UINT8 UnusedUpdSpace0 [2]

Offset 0x0042.

UINT32 PcdSerialIoUartInputClock

Offset 0x0044.

UINT64 PcdPciExpressBaseAddress

Offset 0x0048 - Pci Express Base Address Base address to be programmed for Pci Express.

UINT32 PcdPciExpressRegionLength

Offset 0x0050 - Pci Express Region Length Region Length to be programmed for Pci Express.

UINT8 ReservedFsptUpd1 [12]

Offset 0x0054.

8.8.1 Detailed Description

Fsp T Configuration.

Definition at line 68 of file FsptUpd.h.

8.8.2 Member Data Documentation

8.8.2.1 UINT8 FSP_T_CONFIG::PcdSerialloUartDebugEnable

Offset 0x0040 - PcdSerialloUartDebugEnable Enable Seriallo Uart debug library with/without initializing Seriallo Uart device in FSP.

0:Disable, 1:Enable and Initialize, 2:Enable without Initializing

Definition at line 74 of file FsptUpd.h.

8.8.2.2 UINT8 FSP_T_CONFIG::PcdSerialloUartNumber

Offset 0x0041 - PcdSerialloUartNumber Select Seriallo Uart Controller for debug.

0:SerialloUart0, 1:SerialloUart1, 2:SerialloUart2

Definition at line 80 of file FsptUpd.h.

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

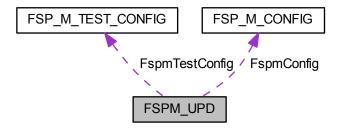
• FsptUpd.h

8.9 FSPM UPD Struct Reference

Fsp M UPD Configuration.

#include <FspmUpd.h>

Collaboration diagram for FSPM_UPD:



Public Attributes

- FSP_UPD_HEADER FspUpdHeader
 Offset 0x0000.
- FSPM_ARCH_UPD FspmArchUpd

Offset 0x0020.

FSP_M_CONFIG FspmConfig

Offset 0x0040.

• FSP_M_TEST_CONFIG FspmTestConfig

Offset 0x0520.

UINT8 UnusedUpdSpace10 [134]

Offset 0x05C0.

UINT16 UpdTerminator

Offset 0x0646.

8.9.1 Detailed Description

Fsp M UPD Configuration.

Definition at line 1613 of file FspmUpd.h.

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

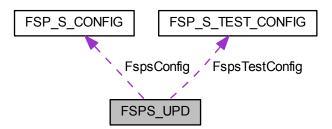
• FspmUpd.h

8.10 FSPS_UPD Struct Reference

Fsp S UPD Configuration.

#include <FspsUpd.h>

Collaboration diagram for FSPS_UPD:



Public Attributes

FSP_UPD_HEADER FspUpdHeader

Offset 0x0000.

• FSP_S_CONFIG FspsConfig

Offset 0x0020.

FSP_S_TEST_CONFIG FspsTestConfig

Offset 0x0780.

• UINT8 UnusedUpdSpace26 [470]

Offset 0x0A40.

UINT16 UpdTerminator

Offset 0x0C16.

8.10.1 Detailed Description

Fsp S UPD Configuration.

Definition at line 2907 of file FspsUpd.h.

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

· FspsUpd.h

8.11 FSPT_CORE_UPD Struct Reference

Fsp T Core UPD.

```
#include <FsptUpd.h>
```

Public Attributes

UINT32 MicrocodeRegionBase

Offset 0x0020.

· UINT32 MicrocodeRegionSize

Offset 0x0024.

• UINT32 CodeRegionBase

Offset 0x0028.

• UINT32 CodeRegionSize

Offset 0x002C.

• UINT8 Reserved [16]

Offset 0x0030.

8.11.1 Detailed Description

Fsp T Core UPD.

Definition at line 43 of file FsptUpd.h.

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

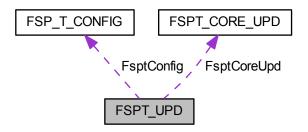
• FsptUpd.h

8.12 FSPT_UPD Struct Reference

Fsp T UPD Configuration.

```
#include <FsptUpd.h>
```

Collaboration diagram for FSPT_UPD:



Public Attributes

• FSP_UPD_HEADER FspUpdHeader

Offset 0x0000.

FSPT_CORE_UPD FsptCoreUpd

Offset 0x0020.

FSP_T_CONFIG FsptConfig

Offset 0x0040.

• UINT8 UnusedUpdSpace1 [6]

Offset 0x0060.

UINT16 UpdTerminator

Offset 0x0066.

8.12.1 Detailed Description

Fsp T UPD Configuration.

Definition at line 107 of file FsptUpd.h.

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

• FsptUpd.h

8.13 GPIO_CONFIG Struct Reference

GPIO configuration structure used for pin programming.

#include <GpioConfig.h>

Public Attributes

• UINT32 PadMode: 5

Pad Mode Pad can be set as GPIO or one of its native functions.

• UINT32 HostSoftPadOwn: 2

Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.

· UINT32 Direction: 6

GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.

• UINT32 OutputState: 2

Output State Set Pad output value.

UINT32 InterruptConfig: 9

GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).

• UINT32 PowerConfig: 8

GPIO Power Configuration.

• UINT32 ElectricalConfig: 9

GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.

• UINT32 LockConfig: 4

GPIO Lock Configuration This setting controls pads lock.

• UINT32 OtherSettings: 2

Additional GPIO configuration Refer to definition of GPIO_OTHER_CONFIG for supported settings.

• UINT32 RsvdBits: 17

Reserved bits for future extension.

8.13.1 Detailed Description

GPIO configuration structure used for pin programming.

Structure contains fields that can be used to configure pad.

Definition at line 55 of file GpioConfig.h.

8.13.2 Member Data Documentation

8.13.2.1 UINT32 GPIO_CONFIG::Direction

GPIO Direction Can choose between In, In with inversion, Out, both In and Out, both In with inversion and out or disabling both.

Refer to definition of GPIO DIRECTION for supported settings.

Definition at line 76 of file GpioConfig.h.

8.13.2.2 UINT32 GPIO_CONFIG::ElectricalConfig

GPIO Electrical Configuration This setting controls pads termination and voltage tolerance.

Refer to definition of GPIO_ELECTRICAL_CONFIG for supported settings.

Definition at line 102 of file GpioConfig.h.

8.13.2.3 UINT32 GPIO_CONFIG::HostSoftPadOwn

Host Software Pad Ownership Set pad to ACPI mode or GPIO Driver Mode.

Refer to definition of GPIO_HOSTSW_OWN.

Definition at line 70 of file GpioConfig.h.

8.13.2.4 UINT32 GPIO_CONFIG::InterruptConfig

GPIO Interrupt Configuration Set Pad to cause one of interrupts (IOxAPIC/SCI/SMI/NMI).

This setting is applicable only if GPIO is in GpioMode with input enabled. Refer to definition of GPIO_INT_CONFIG for supported settings.

Definition at line 90 of file GpioConfig.h.

8.13.2.5 UINT32 GPIO_CONFIG::LockConfig

GPIO Lock Configuration This setting controls pads lock.

Refer to definition of GPIO_LOCK_CONFIG for supported settings.

Definition at line 108 of file GpioConfig.h.

8.13.2.6 UINT32 GPIO_CONFIG::OutputState

Output State Set Pad output value.

Refer to definition of GPIO_OUTPUT_STATE for supported settings. This setting takes place when output is enabled.

Definition at line 83 of file GpioConfig.h.

8.13.2.7 UINT32 GPIO_CONFIG::PadMode

Pad Mode Pad can be set as GPIO or one of its native functions.

When in native mode setting Direction (except Inversion), OutputState, InterruptConfig, Host Software Pad Ownership and OutputStateLock are unnecessary. Refer to definition of GPIO_PAD_MODE. Refer to EDS for each native mode according to the pad.

Definition at line 64 of file GpioConfig.h.

8.13.2.8 UINT32 GPIO_CONFIG::PowerConfig

GPIO Power Configuration.

This setting controls Pad Reset Configuration. Refer to definition of GPIO_RESET_CONFIG for supported settings. Definition at line 96 of file GpioConfig.h.

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

• GpioConfig.h

8.14 MEMORY PLATFORM DATA Struct Reference

Memory Platform Data Hob.

#include <MemInfoHob.h>

8.14.1 Detailed Description

Memory Platform Data Hob.

Revision 1:

- Initial version. Revision 2:
- Added TsegBase, PrmrrSize, PrmrrBase, Gttbase, MmioSize, PciEBaseAddress fields

Definition at line 245 of file MemInfoHob.h.

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

· MemInfoHob.h

8.15 SI_CHIPSET_INIT_INFO Struct Reference

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

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

8.15.1 Detailed Description

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

Definition at line 46 of file FspmUpd.h.

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

• FspmUpd.h

8.16 SI_PCH_DEVICE_INTERRUPT_CONFIG Struct Reference

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

```
#include <FspsUpd.h>
```

Public Attributes

UINT8 Device

Device number.

UINT8 Function

Device function.

UINT8 IntX

Interrupt pin: INTA-INTD (see SI_PCH_INT_PIN)

• UINT8 Irq

IRQ to be set for device.

8.16.1 Detailed Description

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device. Definition at line 75 of file FspsUpd.h.

The documentation for this struct was generated from the following file:

• FspsUpd.h

8.17 SMBIOS_CACHE_INFO Struct Reference

SMBIOS Cache Info HOB Structure.

#include <SmbiosCacheInfoHob.h>

Public Attributes

• UINT16 NumberOfCacheLevels

Based on Number of Cache Types L1/L2/L3.

• UINT8 SocketDesignationStrIndex

String Index in the string Buffer. Example "L1-CACHE".

• UINT16 CacheConfiguration

Format defined in SMBIOS Spec v3.0 Section7.8 Table36.

UINT16 MaxCacheSize

Format defined in SMBIOS Spec v3.0 Section7.8.1.

• UINT16 InstalledSize

Format defined in SMBIOS Spec v3.0 Section7.8.1.

• UINT16 SupportedSramType

Format defined in SMBIOS Spec v3.0 Section7.8.2.

UINT16 CurrentSramType

Format defined in SMBIOS Spec v3.0 Section7.8.2.

UINT8 CacheSpeed

Cache Speed in nanoseconds. 0 if speed is unknown.

UINT8 ErrorCorrectionType

ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.3.

UINT8 SystemCacheType

ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.4.

UINT8 Associativity

ENUM Format defined in SMBIOS Spec v3.0 Section 7.8.5.

8.17.1 Detailed Description

SMBIOS Cache Info HOB Structure.

Definition at line 32 of file SmbiosCacheInfoHob.h.

The documentation for this struct was generated from the following file:

• SmbiosCacheInfoHob.h

8.18 SMBIOS_PROCESSOR_INFO Struct Reference

SMBIOS Processor Info HOB Structure.

#include <SmbiosProcessorInfoHob.h>

Public Attributes

UINT8 ProcessorType

ENUM defined in SMBIOS Spec v3.0 Section 7.5.1.

UINT16 ProcessorFamily

This info is used for both ProcessorFamily and ProcessorFamily2 fields See ENUM defined in SMBIOS Spec v3.0 Section 7.5.2.

UINT8 ProcessorManufacturerStrIndex

Index of the String in the String Buffer.

UINT64 ProcessorId

ENUM defined in SMBIOS Spec v3.0 Section 7.5.3.

• UINT8 ProcessorVersionStrIndex

Index of the String in the String Buffer.

UINT8 Voltage

Format defined in SMBIOS Spec v3.0 Section 7.5.4.

• UINT16 ExternalClockInMHz

External Clock Frequency. Set to 0 if unknown.

• UINT16 CurrentSpeedInMHz

Snapshot of current processor speed during boot.

• UINT8 Status

Format defined in the SMBIOS Spec v3.0 Table 21.

• UINT8 ProcessorUpgrade

ENUM defined in SMBIOS Spec v3.0 Section 7.5.5.

UINT16 CoreCount

This info is used for both CoreCount & CoreCount2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.6.

UINT16 EnabledCoreCount

This info is used for both CoreEnabled & CoreEnabled2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.7.

• UINT16 ThreadCount

This info is used for both ThreadCount & ThreadCount2 fields See detailed description in SMBIOS Spec v3.0 Section 7.5.8.

UINT16 ProcessorCharacteristics

Format defined in SMBIOS Spec v3.0 Section 7.5.9.

8.18.1 Detailed Description

SMBIOS Processor Info HOB Structure.

Definition at line 32 of file SmbiosProcessorInfoHob.h.

The documentation for this struct was generated from the following file:

SmbiosProcessorInfoHob.h

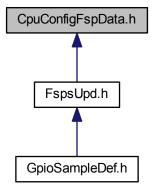
Chapter 9

File Documentation

9.1 CpuConfigFspData.h File Reference

FSP CPU Data Config Block.

This graph shows which files directly or indirectly include this file:



9.1.1 Detailed Description

FSP CPU Data Config Block.

Copyright

INTEL CONFIDENTIAL Copyright 2016 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon

you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

9.2 DoxygenFspIntegrationGuide.h File Reference

This file contains doxygen KabylakeFspIntegration Guide.

9.2.1 Detailed Description

This file contains doxygen KabylakeFspIntegration Guide.

Copyright

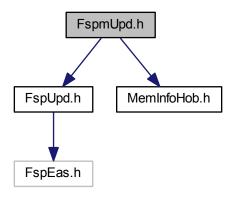
Copyright (c) 2015 - 2017 Intel Corporation. All rights reserved This software and associated documentation (if any) is furnished under a license and may only be used or copied in accordance with the terms of the license. Except as permitted by such license, no part of this software or documentation may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation. This file contains an 'Intel Peripheral Driver' and uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement

9.3 FspmUpd.h File Reference

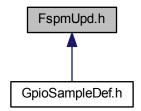
Copyright (c) 2017, Intel Corporation.

#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 SI_CHIPSET_INIT_INFO

The ChipsetInit Info structure provides the information of ME ChipsetInit CRC and BIOS ChipsetInit CRC.

• struct FSP_M_CONFIG

Fsp M Configuration.

• struct FSP_M_TEST_CONFIG

Fsp M Test Configuration.

struct FSPM_UPD

Fsp M UPD Configuration.

9.3.1 Detailed Description

Copyright (c) 2017, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

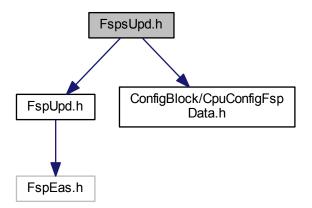
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHE ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS 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 !!!

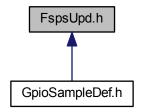
9.4 FspsUpd.h File Reference

Copyright (c) 2017, Intel Corporation.

#include <FspUpd.h>
#include <ConfigBlock/CpuConfigFspData.h>
Include dependency graph for FspsUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

struct AZALIA HEADER

Azalia Header structure.

struct AUDIO_AZALIA_VERB_TABLE

Audio Azalia Verb Table structure.

struct SI PCH DEVICE INTERRUPT CONFIG

The PCH_DEVICE_INTERRUPT_CONFIG block describes interrupt pin, IRQ and interrupt mode for PCH device.

struct FSP S CONFIG

Fsp S Configuration.

• struct FSP S TEST CONFIG

Fsp S Test Configuration.

struct FSPS UPD

Fsp S UPD Configuration.

Macros

#define SI_PCH_MAX_DEVICE_INTERRUPT_CONFIG 64
 Number of all PCH devices.

Enumerations

• enum SI_PCH_INT_PIN

Refer to the definition of PCH_INT_PIN.

9.4.1 Detailed Description

Copyright (c) 2017, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the

following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHE ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS 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 !!!

9.4.2 Enumeration Type Documentation

9.4.2.1 enum SI PCH INT PIN

Refer to the definition of PCH_INT_PIN.

Enumerator

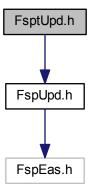
SiPchNoInt No Interrupt Pin.

Definition at line 65 of file FspsUpd.h.

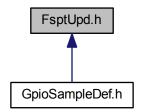
9.5 FsptUpd.h File Reference

Copyright (c) 2017, Intel Corporation.

#include <FspUpd.h>
Include dependency graph for FsptUpd.h:



This graph shows which files directly or indirectly include this file:



Classes

struct FSPT CORE UPD

Fsp T Core UPD.

struct FSP_T_CONFIG

Fsp T Configuration.

struct FSPT UPD

Fsp T UPD Configuration.

9.5.1 Detailed Description

Copyright (c) 2017, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

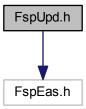
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHE ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURED MENT 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 !!!

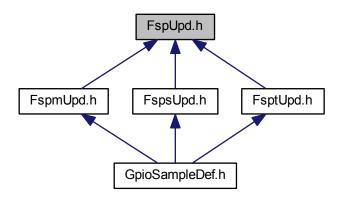
9.6 FspUpd.h File Reference

Copyright (c) 2017, Intel Corporation.

#include <FspEas.h>
Include dependency graph for FspUpd.h:



This graph shows which files directly or indirectly include this file:



9.6.1 Detailed Description

Copyright (c) 2017, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INT ERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This file is automatically generated. Please do NOT modify !!!

9.7 GpioConfig.h File Reference

Header file for GpioConfig structure used by GPIO library.

Classes

struct GPIO CONFIG

GPIO configuration structure used for pin programming.

Macros

#define B_GPIO_INT_CONFIG_INT_SOURCE_MASK 0x1F

Mask for GPIO_INT_CONFIG for interrupt source.

• #define B GPIO INT CONFIG INT TYPE MASK 0xE0

Mask for GPIO_INT_CONFIG for interrupt type.

#define B_GPIO_ELECTRICAL_CONFIG_TERMINATION_MASK 0x1F

Mask for GPIO_ELECTRICAL_CONFIG for termination value.

#define B_GPIO_ELECTRICAL_CONFIG_1V8_TOLERANCE_MASK 0x60

Mask for GPIO_ELECTRICAL_CONFIG for 1v8 tolerance setting.

#define B_GPIO_LOCK_CONFIG_PAD_CONF_LOCK_MASK 0x3

Mask for GPIO LOCK CONFIG for Pad Configuration Lock.

• #define B GPIO LOCK CONFIG OUTPUT LOCK MASK 0x5

Mask for GPIO_LOCK_CONFIG for Pad Output Lock.

#define B GPIO OTHER CONFIG RXRAW MASK 0x3

Mask for GPIO_OTHER_CONFIG for RxRaw1 setting.

Typedefs

• typedef UINT32 GPIO_PAD

For any GpioPad usage in code use GPIO_PAD type.

typedef UINT32 GPIO_GROUP

For any GpioGroup usage in code use GPIO_GROUP type.

Enumerations

- enum GPIO HARDWARE DEFAULT
- enum GPIO_PAD_MODE

GPIO Pad Mode Refer to GPIO documentation on native functions available for certain pad.

• enum GPIO_HOSTSW_OWN

Host Software Pad Ownership modes This setting affects GPIO interrupt status registers.

• enum GPIO_DIRECTION

GPIO Direction.

• enum GPIO_OUTPUT_STATE

GPIO Output State This field is relevant only if output is enabled.

enum GPIO_INT_CONFIG

GPIO interrupt configuration This setting is applicable only if pad is in GPIO mode and has input enabled.

• enum GPIO RESET CONFIG

GPIO Power Configuration GPIO_RESET_CONFIG allows to set GPIO Reset type (PADCFG_DW0.PadRstCfg) which will be used to reset certain GPIO settings.

enum GPIO ELECTRICAL CONFIG

GPIO Electrical Configuration Set GPIO termination and Pad Tolerance (applicable only for some pads) Field from GpioTermNone to GpioTermNative can be OR'ed with GpioTolerance1v8.

enum GPIO LOCK CONFIG

GPIO LockConfiguration Set GPIO configuration lock and output state lock.

enum GPIO_OTHER_CONFIG

Other GPIO Configuration GPIO_OTHER_CONFIG is used for less often settings and for future extensions Supported settings:

9.7.1 Detailed Description

Header file for GpioConfig structure used by GPIO library.

Copyright

INTEL CONFIDENTIAL Copyright 2014 - 2016 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

Specification Reference:

9.7.2 Enumeration Type Documentation

9.7.2.1 enum GPIO_DIRECTION

GPIO Direction.

Enumerator

GpioDirDefault Leave pad direction setting unmodified.

GpioDirInOut Set pad for both output and input.

GpioDirInInvOut Set pad for both output and input with inversion.

GpioDirIn Set pad for input only.

GpioDirInInv Set pad for input with inversion.

GpioDirOut Set pad for output only.

GpioDirNone Disable both output and input.

Definition at line 167 of file GpioConfig.h.

9.7.2.2 enum GPIO_ELECTRICAL_CONFIG

GPIO Electrical Configuration Set GPIO termination and Pad Tolerance (applicable only for some pads) Field from GpioTermNone to GpioTermNative can be OR'ed with GpioTolerance1v8.

Enumerator

GpioTermDefault Leave termination setting unmodified.

GpioTermNone none

GpioTermWpd5K 5kOhm weak pull-down

GpioTermWpd20K 20kOhm weak pull-down

GpioTermWpu1K 1kOhm weak pull-up

GpioTermWpu2K 2kOhm weak pull-up

GpioTermWpu5K 5kOhm weak pull-up

GpioTermWpu20K 20kOhm weak pull-up

GpioTermWpu1K2K 1kOhm & 2kOhm weak pull-up

GpioTermNative Native function controls pads termination This setting is applicable only to some native modes. Please check EDS to determine which native functionality can control pads termination

GpioNoTolerance1v8 Disable 1.8V pad tolerance.

GpioTolerance1v8 Enable 1.8V pad tolerance.

Definition at line 296 of file GpioConfig.h.

9.7.2.3 enum GPIO_HARDWARE_DEFAULT

Enumerator

GpioHardwareDefault Leave setting unmodified.

Definition at line 118 of file GpioConfig.h.

9.7.2.4 enum GPIO HOSTSW OWN

Host Software Pad Ownership modes This setting affects GPIO interrupt status registers.

Depending on chosen ownership some GPIO Interrupt status register get updated and other masked. Please refer to EDS for HOSTSW_OWN register description.

Enumerator

GpioHostOwnDefault Leave ownership value unmodified.

GpioHostOwnAcpi Set HOST ownership to ACPI. Use this setting if pad is not going to be used by GPIO OS driver. If GPIO is configured to generate SCI/SMI/NMI then this setting must be used for interrupts to work

GpioHostOwnGpio Set HOST ownership to GPIO Driver mode. Use this setting only if GPIO pad should be controlled by GPIO OS Driver. GPIO OS Driver will be able to control the pad if appropriate entry in ACPI exists (refer to ACPI specification for Gpiolo and GpioInt descriptors)

Definition at line 146 of file GpioConfig.h.

9.7.2.5 enum GPIO_INT_CONFIG

GPIO interrupt configuration This setting is applicable only if pad is in GPIO mode and has input enabled.

GPIO_INT_CONFIG allows to choose which interrupt is generated (IOxAPIC/SCI/SMI/NMI) and how it is triggered (edge or level). Refer to PADCFG_DW0 register description in EDS for details on this settings. Field from Gpio IntNmi to GpioIntApic can be OR'ed with GpioIntLevel to GpioIntBothEdge to describe an interrupt e.g. GpioIntApic | GpioIntLevel If GPIO is set to cause an SCI then also GPI_GPE_EN is enabled for this pad. If GPIO is set to cause an NMI then also GPI_NMI_EN is enabled for this pad. Not all GPIO are capable of generating an SMI or NMI interrupt. When routing GPIO to cause an IOxAPIC interrupt care must be taken, as this interrupt cannot be shared and its IRQn number is not configurable. Refer to EDS for GPIO pads IRQ numbers (PADCFG_DW1.Int Sel) If GPIO is under GPIO OS driver control and appropriate ACPI GpioInt descriptor exist then use only trigger type setting (from GpioIntLevel to GpioIntBothEdge). This type of GPIO Driver interrupt doesn't have any additional routing setting required to be set by BIOS. Interrupt is handled by GPIO OS Driver.

Enumerator

GpioIntDefault Leave value of interrupt routing unmodified.

GpioIntDis Disable IOxAPIC/SCI/SMI/NMI interrupt generation.

GpioIntNmi Enable NMI interrupt only. **GpioIntSmi** Enable SMI interrupt only.

GpioIntSci Enable SCI interrupt only.

GpioIntApic Enable IOxAPIC interrupt only.GpioIntLevel Set interrupt as level triggered.

GpioIntEdge Set interrupt as edge triggered (type of edge depends on input inversion)

GpioIntLvIEdgDis Disable interrupt trigger.

GpioIntBothEdge Set interrupt as both edge triggered.

Definition at line 207 of file GpioConfig.h.

9.7.2.6 enum GPIO LOCK CONFIG

GPIO LockConfiguration Set GPIO configuration lock and output state lock.

GpioLockPadConfig and GpioLockOutputState can be OR'ed. Lock settings reset is in Powergood domain. Care must be taken when using this setting as fields it locks may be reset by a different signal and can be controllable by what is in GPIO_RESET_CONFIG (PADCFG_DW0.PadRstCfg). GPIO library provides functions which allow to unlock a GPIO pad.

Enumerator

GpioLockDefault Leave lock setting unmodified.

GpioPadConfigLock Lock Pad Configuration.

GpioOutputStateLock Lock GPIO pad output value.

Definition at line 329 of file GpioConfig.h.

9.7.2.7 enum GPIO_OTHER_CONFIG

Other GPIO Configuration GPIO_OTHER_CONFIG is used for less often settings and for future extensions Supported settings:

• RX raw override to '1' - allows to override input value to '1' This setting is applicable only if in input mode (both in GPIO and native usage). The override takes place at the internal pad state directly from buffer and before the RXINV.

Enumerator

GpioRxRaw1Default Use default input override value.

GpioRxRaw1Dis Don't override input.

GpioRxRaw1En Override input to '1'.

Definition at line 346 of file GpioConfig.h.

9.7.2.8 enum GPIO_OUTPUT_STATE

GPIO Output State This field is relevant only if output is enabled.

Enumerator

GpioOutDefault Leave output value unmodified.

GpioOutLow Set output to low.

GpioOutHigh Set output to high.

Definition at line 181 of file GpioConfig.h.

```
9.7.2.9 enum GPIO PAD MODE
```

GPIO Pad Mode Refer to GPIO documentation on native functions available for certain pad.

If GPIO is set to one of NativeX modes then following settings are not applicable and can be skipped:

- · Interrupt related settings
- · Host Software Ownership
- · Output/Input enabling/disabling
- Output lock

Definition at line 132 of file GpioConfig.h.

```
9.7.2.10 enum GPIO_RESET_CONFIG
```

GPIO Power Configuration GPIO_RESET_CONFIG allows to set GPIO Reset type (PADCFG_DW0.PadRstCfg) which will be used to reset certain GPIO settings.

Refer to EDS for settings that are controllable by PadRstCfg.

Enumerator

GpioResetDefault Leave value of pad reset unmodified.

GpioResetPwrGood Deprecated settings. Maintained only for compatibility.GPP: RSMRST; GPD: DSW_← PWROK; (PadRstCfg = 00b = "Powergood")

GpioResetDeep Deep GPIO Reset (PadRstCfg = 01b = "Deep GPIO Reset")

GPIO Reset (PadRstCfg = 10b = "GPIO Reset")

GPI: Reserved; GPD: RSMRST; (PadRstCfg = 11b = "Resume Reset")

GpioResumeReset New GPIO reset configuration options. Resume Reset (RSMRST) GPP: PadRstCfg = 00b = "Powergood" GPD: PadRstCfg = 11b = "Resume Reset" Pad setting will reset on:

- · DeepSx transition
- · G3 Pad settings will not reset on:
- S3/S4/S5 transition

· Warm/Cold/Global reset

GpioHostDeepReset Host Deep Reset PadRstCfg = 01b = "Deep GPIO Reset" Pad settings will reset on:

- · Warm/Cold/Global reset
- · DeepSx transition
- G3 Pad settings will not reset on:
- S3/S4/S5 transition

GpioPlatformReset Platform Reset (PLTRST) PadRstCfg = 10b = "GPIO Reset" Pad settings will reset on:

- S3/S4/S5 transition
- · Warm/Cold/Global reset
- · DeepSx transition
- G3

GpioDswReset Deep Sleep Well Reset (DSW_PWROK) GPP: not applicable GPD: PadRstCfg = 00b = "← Powergood" Pad settings will reset on:

- · G3 Pad settings will not reset on:
- S3/S4/S5 transition
- · Warm/Cold/Global reset
- · DeepSx transition

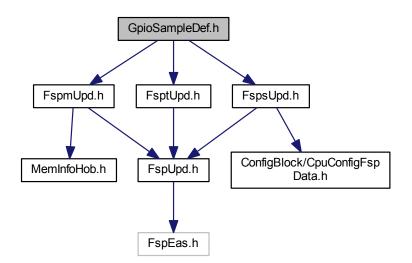
Definition at line 229 of file GpioConfig.h.

9.8 GpioSampleDef.h File Reference

Copyright (c) 2015, Intel Corporation.

```
#include <FsptUpd.h>
#include <FspmUpd.h>
#include <FspsUpd.h>
```

Include dependency graph for GpioSampleDef.h:



9.8.1 Detailed Description

Copyright (c) 2015, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

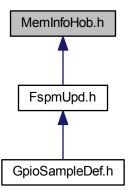
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHE ALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCURE MENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS 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 !!!

9.9 MemInfoHob.h File Reference

This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs.

This graph shows which files directly or indirectly include this file:



Classes

struct DIMM INFO

Memory SMBIOS & OC Memory Data Hob.

struct MEMORY_PLATFORM_DATA

Memory Platform Data Hob.

Macros

• #define WARM BOOT 2

Host reset states from MRC.

• #define MAX_SPD_SAVE 29

Defines taken from MRC so avoid having to include MrcInterface.h.

9.9.1 Detailed Description

This file contains definitions required for creation of Memory S3 Save data, Memory Info data and Memory Platform data hobs.

Copyright

INTEL CONFIDENTIAL Copyright 1999 - 2016 Intel Corporation.

The source code contained or described herein and all documents related to the source code ("Material") are owned by Intel Corporation or its suppliers or licensors. Title to the Material remains with Intel Corporation or its suppliers and licensors. The Material may contain trade secrets and proprietary and confidential information of Intel Corporation and its suppliers and licensors, and is protected by worldwide copyright and trade secret laws and treaty provisions. No part of the Material may be used, copied, reproduced, modified, published, uploaded, posted, transmitted, distributed, or disclosed in any way without Intel's prior express written permission.

No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the Materials, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Intel in writing.

Unless otherwise agreed by Intel in writing, you may not remove or alter this notice or any other notice embedded in Materials by Intel or Intel's suppliers or licensors in any way.

This file contains an 'Intel Peripheral Driver' and is uniquely identified as "Intel Reference Module" and is licensed for Intel CPUs and chipsets under the terms of your license agreement with Intel or your vendor. This file may be modified by the user, subject to additional terms of the license agreement.

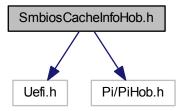
Specification Reference:

9.10 SmbiosCacheInfoHob.h File Reference

Header file for SMBIOS Cache Info HOB.

```
#include <Uefi.h>
#include <Pi/PiHob.h>
```

Include dependency graph for SmbiosCacheInfoHob.h:



Classes

struct SMBIOS_CACHE_INFO

SMBIOS Cache Info HOB Structure.

9.10.1 Detailed Description

Header file for SMBIOS Cache Info HOB.

Copyright (c) 2015, Intel Corporation. All rights reserved.

This program and the accompanying materials are licensed and made available under the terms and conditions of the BSD License which accompanies this distribution. The full text of the license may be found at http-://opensource.org/licenses/bsd-license.php

THE PROGRAM IS DISTRIBUTED UNDER THE BSD LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED.

Specification Reference:

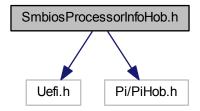
System Management BIOS (SMBIOS) Reference Specification v3.0.0 dated 2015-Feb-12 (DSP0134) http \leftarrow ://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.0. \leftarrow pdf

9.11 SmbiosProcessorInfoHob.h File Reference

Header file for SMBIOS Processor Info HOB.

```
#include <Uefi.h>
#include <Pi/PiHob.h>
```

Include dependency graph for SmbiosProcessorInfoHob.h:



Classes

• struct SMBIOS_PROCESSOR_INFO

SMBIOS Processor Info HOB Structure.

9.11.1 Detailed Description

Header file for SMBIOS Processor Info HOB.

Copyright (c) 2015, Intel Corporation. All rights reserved.

This program and the accompanying materials are licensed and made available under the terms and conditions of the BSD License which accompanies this distribution. The full text of the license may be found at httpe://opensource.org/licenses/bsd-license.php

THE PROGRAM IS DISTRIBUTED UNDER THE BSD LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED.

Specification Reference:

System Management BIOS (SMBIOS) Reference Specification v3.0.0 dated 2015-Feb-12 (DSP0134) http \leftarrow ://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.0. \leftarrow pdf

Index

AUDIO_AZALIA_VERB_TABLE, 23	CmdTriStateDis
AZALIA_HEADER, 24	FSP_M_CONFIG, 36
AcLoadline	ConfigTdpBios
FSP_S_CONFIG, 71	FSP_S_TEST_CONFIG, 107
AcousticNoiseMitigation	CoreMaxOcRatio
FSP_S_CONFIG, 71	FSP_M_CONFIG, 36
ActiveCoreCount	CorePllVoltageOffset
FSP_M_CONFIG, 35	FSP_M_CONFIG, 36
AmtEnabled	CoreVoltageAdaptive
FSP_S_CONFIG, 72	FSP_M_CONFIG, 36
AmtSolEnabled	CoreVoltageMode
FSP_S_CONFIG, 72	FSP_M_CONFIG, 36
ApHandoffManner	CoreVoltageOverride
FSP_S_TEST_CONFIG, 107	FSP_M_CONFIG, 36
ApidleManner	CpuConfigFspData.h, 129
FSP_S_TEST_CONFIG, 107	CpuRatio
ApertureSize	FSP_M_CONFIG, 37
FSP_M_CONFIG, 35	CpuRatioOverride
AsfEnabled	FSP_M_CONFIG, 37
FSP_S_CONFIG, 72	CstCfgCtrIoMwaitRedirection
AutoThermalReporting FSP_S_TEST_CONFIG, 107	FSP_S_TEST_CONFIG, 108
Avx2RatioOffset	CstateLatencyControl0Irtl
FSP_M_CONFIG, 35	FSP_S_TEST_CONFIG, 107
1 3F_M_CONTIG, 33	Custom1ConfigTdpControl
BclkAdaptiveVoltage	FSP_S_TEST_CONFIG, 108
FSP_M_CONFIG, 35	Custom1PowerLimit1
BdatEnable	FSP_S_TEST_CONFIG, 108
FSP_M_TEST_CONFIG, 49	Custom1PowerLimit1Time
BiosAcmBase	FSP_S_TEST_CONFIG, 108
FSP_M_TEST_CONFIG, 49	Custom1PowerLimit2
BiosAcmSize	FSP_S_TEST_CONFIG, 108
FSP_M_TEST_CONFIG, 49	Custom1TurboActivationRatio
BiosGuard	FSP_S_TEST_CONFIG, 108
FSP_M_CONFIG, 35	Custom2ConfigTdpControl
BiosSize	FSP_S_TEST_CONFIG, 108
FSP_M_TEST_CONFIG, 49	Custom2PowerLimit1
BistOnReset	FSP_S_TEST_CONFIG, 109
FSP_M_CONFIG, 35	Custom2PowerLimit1Time
BootFrequency	FSP_S_TEST_CONFIG, 109
FSP_M_CONFIG, 35	Custom2PowerLimit2
BypassPhySyncReset	FSP_S_TEST_CONFIG, 109
FSP_M_TEST_CONFIG, 49	Custom2TurboActivationRatio
	FSP_S_TEST_CONFIG, 109
C1e	Custom3ConfigTdpControl
FSP_S_TEST_CONFIG, 107	FSP_S_TEST_CONFIG, 109
CStatePreWake	Custom3PowerLimit1
FSP_S_TEST_CONFIG, 107	FSP_S_TEST_CONFIG, 109
ChipsetInitMessage	Custom3PowerLimit1Time
FSP M TEST CONFIG. 49	FSP S TEST CONFIG. 109

Custom3PowerLimit2	FSP_S_TEST_CONFIG, 111
FSP_S_TEST_CONFIG, 110	ElectricalConfig
Custom3TurboActivationRatio	GPIO CONFIG, 123
FSP_S_TEST_CONFIG, 110	EnableC6Dram
Cx	FSP M CONFIG, 38
FSP_S_TEST_CONFIG, 110	EnableSgx
	FSP_M_CONFIG, 38
DIMM_INFO, 24	EnableTcoTimer
DcLoadline	FSP_S_CONFIG, 73
FSP_S_CONFIG, 72	
DdrFreqLimit	EnableTraceHub
FSP_M_CONFIG, 37	FSP_M_CONFIG, 38
	EndOfPostMessage
DebugInterfaceEnable	FSP_S_TEST_CONFIG, 111
FSP_S_TEST_CONFIG, 110	EnergyEfficientPState
DebugInterfaceLockEnable	FSP_S_TEST_CONFIG, 111
FSP_S_TEST_CONFIG, 110	EnergyEfficientTurbo
DelayUsbPdoProgramming	FSP_S_TEST_CONFIG, 111
FSP_S_CONFIG, 72	EsataSpeedLimit
DevIntConfigPtr	FSP_S_CONFIG, 73
FSP_S_CONFIG, 72	EvLoader
Direction	FSP M CONFIG, 38
GPIO_CONFIG, 123	/
DisableHeciRetry	FClkFrequency
FSP_M_TEST_CONFIG, 49	FSP_M_CONFIG, 38
DisableMessageCheck	FSP M CONFIG, 25
FSP M TEST CONFIG, 49	ActiveCoreCount, 35
DisableProcHotOut	ApertureSize, 35
FSP_S_TEST_CONFIG, 110	Avx2RatioOffset, 35
DisableVrThermalAlert	BclkAdaptiveVoltage, 35
	BiosGuard, 35
FSP_S_TEST_CONFIG, 110	BistOnReset, 35
DmiDeEmphasis	BootFrequency, 35
FSP_M_CONFIG, 37	• •
DmiGen3EndPointHint	CmdTriStateDis, 36
FSP_M_CONFIG, 37	CoreMaxOcRatio, 36
DmiGen3EndPointPreset	CorePllVoltageOffset, 36
FSP_M_CONFIG, 37	CoreVoltageAdaptive, 36
DmiGen3EqPh2Enable	CoreVoltageMode, 36
FSP_M_TEST_CONFIG, 50	CoreVoltageOverride, 36
DmiGen3EqPh3Method	CpuRatio, 37
FSP_M_TEST_CONFIG, 50	CpuRatioOverride, 37
DmiGen3ProgramStaticEq	DdrFreqLimit, 37
FSP M CONFIG, 37	DmiDeEmphasis, 37
DmiGen3RootPortPreset	DmiGen3EndPointHint, 37
FSP M CONFIG, 38	DmiGen3EndPointPreset, 37
DmiSuggestedSetting	DmiGen3ProgramStaticEq, 37
FSP S CONFIG, 72	DmiGen3RootPortPreset, 38
DmiVc1	EnableC6Dram, 38
	EnableSgx, 38
FSP_M_TEST_CONFIG, 50	EnableTraceHub, 38
DmiVcm	
FSP_M_TEST_CONFIG, 50	EvLoader, 38
DoxygenFspIntegrationGuide.h, 130	FClkFrequency, 38
Fault 100F4Clast Cation = Fire all a	FlashWearOutProtection, 38
Early8254ClockGatingEnable	HeciTimeouts, 39
FSP_S_CONFIG, 73	IgdDvmt50PreAlloc, 39
EcCmdLock	InitPcieAspmAfterOprom, 39
FSP_S_CONFIG, 73	InternalGfx, 39
EcCmdProvisionEav	JtagC10PowerGateDisable, 39
FSP_S_CONFIG, 73	MmioSize, 39
Eist	OcLock, 39

	PcdDebugInterfaceFlags, 39		Gen3SwEqJitterErrorTarget, 51
	PcdlsaSerialUartBase, 40		Gen3SwEqNumberOfPresets, 51
	PcdSerialDebugBaudRate, 40		Gen3SwEqVocDwellTime, 51
	PcdSerialDebugLevel, 40		Gen3SwEqVocErrorTarget, 51
	PcdSerialIoUartNumber, 40		HeciCommunication2, 51
	PchAcpiBase, 40		IderDeviceEnable, 52
	PchHpetBase, 40		KtDeviceEnable, 52
	PchHpetBdfValid, 40		LockPTMregs, 52
	PchHpetBusNumber, 41		PanelPowerEnable, 52
	PchHpetDeviceNumber, 41		PchDciEn, 52
	PchHpetEnable, 41		Peg0Gen3EqPh2Enable, 52
	PchHpetFunctionNumber, 41		Peg0Gen3EqPh3Method, 52
	PchLpcEnhancePort8xhDecoding, 41		Peg1Gen3EqPh2Enable, 53
	PchNumRsvdSmbusAddresses, 41		Peg1Gen3EqPh3Method, 53
	PchPmPciePllSsc, 41		Peg2Gen3EqPh2Enable, 53
	PchPort80Route, 42		Peg2Gen3EqPh3Method, 53
	PcieRpEnableMask, 42		PegGen3EndPointHint, 53
	PeciC10Reset, 42		PegGen3EndPointPreset, 53
	PeciSxReset, 42		PegGen3ProgramStaticEq, 54
	PegDataPtr, 42		PegGen3RootPortPreset, 54
	PegDisableSpreadSpectrumClocking, 42		PegGenerateBdatMarginTable, 54
	PrmrrSize, 42		PegRxCemLoopbackLane, 54
	ProbelessTrace, 43		PegRxCemNonProtocolAwareness, 54
	RMT, 43		ScanExtGfxForLegacyOpRom, 54
	Ratio, 43		SkipMbpHob, 55
	RefClk, 43		SmbusDynamicPowerGating, 55
	RingMaxOcRatio, 43		SmbusSpdWriteDisable, 55
	RingMinOcRatio, 43		TgaSize, 55
	SaGv, 43		TotalFlashSize, 55
	SinitMemorySize, 44		TxtLcpPdBase, 55
	SmbusArpEnable, 44		TxtLcpPdSize, 55
	SmbusEnable, 44		WdtDisableAndLock, 56
	SpdProfileSelected, 44	FSP	_S_CONFIG, 56
	tRTP, 44		AcLoadline, 71
	TsegSize, 44		AcousticNoiseMitigation, 71
	Txt, 44		AmtEnabled, 72
	TxtDprMemoryBase, 44		AmtSolEnabled, 72
	TxtDprMemorySize, 45		AsfEnabled, 72
	TxtHeapMemorySize, 45		DcLoadline, 72
	TxtImplemented, 45		DelayUsbPdoProgramming, 72
	VddVoltage, 45		DevIntConfigPtr, 72
	VmxEnable, 45		DmiSuggestedSetting, 72
FSP	_M_TEST_CONFIG, 45		Early8254ClockGatingEnable, 73
	BdatEnable, 49		EcCmdLock, 73
	BiosAcmBase, 49		EcCmdProvisionEav, 73
	BiosAcmSize, 49		EnableTcoTimer, 73
	BiosSize, 49		EsataSpeedLimit, 73
	BypassPhySyncReset, 49		FastPkgCRampDisableGt, 73
	ChipsetInitMessage, 49		FastPkgCRampDisablela, 73
	DisableHeciRetry, 49		FastPkgCRampDisableSa, 74
	DisableMessageCheck, 49		FwProgress, 74
	DmiGen3EqPh2Enable, 50		GpioIrqRoute, 74
	DmiGen3EqPh3Method, 50		Heci3Enabled, 74
	DmiVc1, 50		IccMax, 74
	DmiVcm, 50		ImonOffset, 74
	Gen3SwEqAlwaysAttempt, 50		ImonSlope, 74
	Gen3SwEqEnableVocTest, 50		ManageabilityMode, 75
	Gen3SwEqJitterDwellTime, 51		MeUnconfigIsValid, 75

MicrocodePatchAddress, 75	PchPmSlpAMinAssert, 83
NumOfDevIntConfig, 75	PchPmSlpLanLowDc, 83
PchCio2Enable, 75	PchPmSlpS0Enable, 83
PchCrid, 75	PchPmSlpS0VmEnable, 83
PchDisableComplianceMode, 75	PchPmSlpS3MinAssert, 83
PchDmiAspm, 76	PchPmSlpS4MinAssert, 84
PchDmiTsawEn, 76	PchPmSlpStrchSusUp, 84
PchHdaDspEnable, 76	PchPmSlpSusMinAssert, 84
PchHdaDspEndpointBluetooth, 76	PchPmWoWlanDeepSxEnable, 84
PchHdaDspEndpointl2s, 76	PchPmWoWlanEnable, 84
PchHdaDspFeatureMask, 76	PchPmWolEnableOverride, 84
PchHdaDspUaaCompliance, 76	PchPmWolOvrWkSts, 84
PchHdaEnable, 77	PchPort61hEnable, 85
PchHdalDispCodecDisconnect, 77	PchPwrOptEnable, 85
PchHdaloBufferOwnership, 77	PchScsEmmcHs400DllDataValid, 85
PchHdaPme, 77	PchScsEmmcHs400TuningRequired, 85
PchloApicBdfValid, 77	PchSirqEnable, 85
PchloApicBusNumber, 77	PchSirqMode, 85
PchloApicDeviceNumber, 77	PchSkyCamPortACtleEnable, 85
PchloApicEntry24_119, 78	PchSkyCamPortATermOvrEnable, 86
PchloApicFunctionNumber, 78	PchSkyCamPortATrimEnable, 86
PchloApicId, 78	PchSkyCamPortBCtleEnable, 86
PchloApicla, 78 PchloApicRangeSelect, 78	PchSkyCamPortBTermOvrEnable, 86
PchlshEnable, 78	
	PchSkyCamPortBTrimEnable, 86
PchlshGp0GpioAssign, 78	PchSkyCamPortCDCtleEnable, 86
PchlshGp1GpioAssign, 78	PchSkyCamPortCTermOvrEnable, 86
PchlshGp2GpioAssign, 79	PchSkyCamPortCTrimEnable, 87
PchlshGp3GpioAssign, 79	PchSkyCamPortDTermOvrEnable, 87
PchlshGp4GpioAssign, 79	PchSkyCamPortDTrimEnable, 87
PchlshGp5GpioAssign, 79	PchSubSystemId, 87
PchlshGp6GpioAssign, 79	PchSubSystemVendorld, 87
PchlshGp7GpioAssign, 79	PchTTEnable, 87
Pchlshl2c0GpioAssign, 79	PchTTLock, 88
Pchlshl2c1GpioAssign, 79	PchTTState13Enable, 88
Pchlshl2c2GpioAssign, 80	PchThermalDeviceEnable, 87
PchlshPdtUnlock, 80	PchTsmicLock, 87
PchlshSpiGpioAssign, 80	PcieAllowNoLtrlccPllShutdown, 88
PchlshUart0GpioAssign, 80	PcieComplianceTestMode, 88
PchlshUart1GpioAssign, 80	PcieDisableRootPortClockGating, 88
PchLanClkReqSupported, 80	PcieEnablePeerMemoryWrite, 88
PchLanEnable, 80	PcieEqPh3LaneParamCm, 88
PchLanK1OffEnable, 81	PcieEqPh3LaneParamCp, 89
PchLanLtrEnable, 81	PcieRpAspm, 89
PchLockDownBiosLock, 81	PcieRpClkReqNumber, 89
PchLockDownSpiEiss, 81	PcieRpClkReqSupport, 89
PchMemoryThrottlingEnable, 81	PcieRpCompletionTimeout, 89
PchPcieDeviceOverrideTablePtr, 81	PcieRpDeviceResetPad, 89
PchPmCapsuleResetType, 81	PcieRpFunctionSwap, 89
PchPmDeepSxPol, 82	PcieRpGen3EqPh3Method, 90
PchPmDisableDsxAcPresentPulldown, 82	PcieRpL1Substates, 90
PchPmDisableNativePowerButton, 82	PcieRpPcieSpeed, 90
PchPmLanWakeFromDeepSx, 82	PcieRpPhysicalSlotNumber, 90
PchPmLpcClockRun, 82	PcieSwEqCoeffListCm, 90
PchPmMeWakeSts, 82	PcieSwEqCoeffListCp, 90
PchPmPcieWakeFromDeepSx, 82	PortUsb20Enable, 90
PchPmPmeB0S5Dis, 82	PortUsb30Enable, 91
PchPmPwrBtnOverridePeriod, 83	Psi1Threshold, 91
PchPmPwrCycDur, 83	Psi2Threshold, 91

Psi3Enable, 91	WatchDogTimerOs, 99
Psi3Threshold, 91	XdciEnable, 99
PsysOffset, 91	FSP_S_TEST_CONFIG, 99
PsysSlope, 91	ApHandoffManner, 107
PxRcConfig, 92	ApldleManner, 107
SataEnable, 92	AutoThermalReporting, 107
SataMode, 92	C1e, 107
SataP0TDispFinit, 92	CStatePreWake, 107
SataP1TDispFinit, 92	ConfigTdpBios, 107
SataPortsDevSlp, 92	CstCfgCtrloMwaitRedirection, 108
SataPortsDmVal, 92	CstateLatencyControl0Irtl, 107
SataPortsEnable, 93	Custom1ConfigTdpControl, 108
SataPwrOptEnable, 93	Custom1PowerLimit1, 108
SataRstHddUnlock, 93	Custom1PowerLimit1Time, 108
SataRstIrrt, 93	Custom1PowerLimit2, 108
SataRstIrrtOnly, 93	Custom1TurboActivationRatio, 108
SataRstLedLocate, 93	Custom2ConfigTdpControl, 108
SataRstOromUiBanner, 93	Custom2PowerLimit1, 109
SataRstPcieDeviceResetDelay, 93	Custom2PowerLimit1Time, 109
SataRstRaid0, 94	Custom2PowerLimit2, 109
SataRstRaid1, 94	Custom2TurboActivationRatio, 109
SataRstRaid10, 94	Custom3ConfigTdpControl, 109
SataRstRaid5, 94	Custom3PowerLimit1, 109
SataRstRaidAlternateId, 94	Custom3PowerLimit1Time, 109
SataRstSmartStorage, 94	Custom3PowerLimit2, 110
SataSalpSupport, 94	Custom3TurboActivationRatio, 110
SataThermalSuggestedSetting, 95	Cx, 110
ScilrqSelect, 95	DebugInterfaceEnable, 110
ScsEmmcEnabled, 95	DebugInterfaceLockEnable, 110
ScsEmmcHs400Enabled, 95	DisableProcHotOut, 110
ScsSdCardEnabled, 95	DisableVrThermalAlert, 110
SendEcCmd, 95	Eist, 111
SendVrMbxCmd, 95	EndOfPostMessage, 111
SendVrMbxCmd1, 96	EnergyEfficientPState, 111
SerialloDebugUartNumber, 96	EnergyEfficientTurbo, 111
SerialloDevMode, 96	HdcControl, 111
SerialloGpio, 96	Hwp, 111
ShowSpiController, 96	MachineCheckEnable, 111
SlowSlewRateForGt, 96	MlcStreamerPrefetcher, 112
SlowSlewRateForla, 96	MonitorMwaitEnable, 112
SlowSlewRateForSa, 97	NumberOfEntries, 112
SsicPortEnable, 97	OneCoreRatioLimit, 112
TTSuggestedSetting, 97	PchHdaResetWaitTimer, 112
TcolrqSelect, 97	PchLockDownBiosInterface, 112
TdcPowerLimit, 97	PchLockDownGlobalSmi, 113
TdcTimeWindow, 97	PchLockDownRtcLock, 113
TurboMode, 97	PchPmDisableEnergyReport, 113
Usb2AfePehalfbit, 97	PchPmPmcReadDisable, 113
Usb2AfePetxiset, 98	PchSbAccessUnlock, 113
Usb2AfePredeemp, 98	PchSbiUnlock, 113
Usb2AfeTxiset, 98	PcieEnablePort8xhDecode, 113
Usb3HsioTxDeEmph, 98	PcieRpDptp, 113
Usb3HsioTxDeEmphEnable, 98	PcieRpSlotPowerLimitScale, 114
Usb3HsioTxDownscaleAmp, 98	PcieRpSlotPowerLimitValue, 114
Usb3HsioTxDownscaleAmpEnable, 98	PcieRpUptp, 114
VrVoltageLimit, 99	PkgCStateDemotion, 114
WatchDog, 99	PkgCStateLimit, 114
WatchDogTimerBios, 99	PkgCStateUnDemotion, 114
,	,

PmgCstCfgCtrlLock, 114	GpioConfig.h, 138
PowerLimit1, 115	GPIO_ELECTRICAL_CONFIG
PowerLimit1Time, 115	GpioConfig.h, 139
PowerLimit2, 115	GPIO_HARDWARE_DEFAULT
PowerLimit2Power, 115	GpioConfig.h, 139
PowerLimit3, 115	GPIO HOSTSW OWN
PowerLimit3Time, 115	GpioConfig.h, 139
PowerLimit4, 115	GPIO INT CONFIG
ProcHotResponse, 115	GpioConfig.h, 139
ProcTraceEnable, 116	GPIO_LOCK_CONFIG
ProcTraceOutputScheme, 116	GpioConfig.h, 140
PsysPmax, 116	GPIO_OTHER_CONFIG
PsysPowerLimit1, 116	GpioConfig.h, 140
PsysPowerLimit1Power, 116	GPIO OUTPUT STATE
PsysPowerLimit2, 116	GpioConfig.h, 141
PsysPowerLimit2Power, 116	GPIO_PAD_MODE
RaceToHalt, 117	GpioConfig.h, 141
SataTestMode, 117	GPIO_RESET_CONFIG
StateRatio, 117	
TStates, 118	GpioConfig.h, 141
TccActivationOffset, 117	Gen3SwEqAlwaysAttempt
TccOffsetClamp, 117	FSP_M_TEST_CONFIG, 50
TccOffsetLock, 117	Gen3SwEqEnableVocTest
TccOffsetTimeWindowForRatl, 118	FSP_M_TEST_CONFIG, 50
TimedMwait, 118	Gen3SwEqJitterDwellTime
FSP_T_CONFIG, 118	FSP_M_TEST_CONFIG, 51
PcdSerialloUartDebugEnable, 119	Gen3SwEqJitterErrorTarget
PcdSerialloUartNumber, 119	FSP_M_TEST_CONFIG, 51
FSPM_UPD, 119	Gen3SwEqNumberOfPresets
FSPS_UPD, 120	FSP_M_TEST_CONFIG, 51
FSPT_CORE_UPD, 121	Gen3SwEqVocDwellTime
FSPT_UPD, 121	FSP_M_TEST_CONFIG, 51
FastPkgCRampDisableGt	Gen3SwEqVocErrorTarget
FSP_S_CONFIG, 73	FSP_M_TEST_CONFIG, 51
FastPkgCRampDisablela	GpioConfig.h, 137
FSP_S_CONFIG, 73	GPIO_DIRECTION, 138 GPIO_ELECTRICAL_CONFIG, 139
FastPkgCRampDisableSa	
FSP_S_CONFIG, 74	GPIO_HARDWARE_DEFAULT, 139 GPIO HOSTSW OWN, 139
FlashWearOutProtection	GPIO_INT_CONFIG, 139
FSP_M_CONFIG, 38	GPIO_LOCK_CONFIG, 140
FspUpd.h, 135	GPIO OTHER CONFIG, 140
FspmUpd.h, 130	GPIO OUTPUT STATE, 141
FspsUpd.h, 132	GPIO_PAD_MODE, 141
SI_PCH_INT_PIN, 134	
SiPchNoInt, 134	GPIO_RESET_CONFIG, 141
FsptUpd.h, 134	GpioDirDefault, 138
FwProgress	GpioDirln, 138 GpioDirlnlnv, 139
FSP_S_CONFIG, 74	GpioDirliniv, 139 GpioDirlnInvOut, 138
ODIO CONFIG. 100	GpioDirlinVOut, 138
GPIO_CONFIG, 122	•
Direction, 123	GpioDirNone, 139
ElectricalConfig, 123	GpioDirOut, 139
HostSoftPadOwn, 123	GpioDswReset, 142
InterruptConfig, 123	GpioHardwareDefault, 139
LockConfig, 124	GpioHostOwnAppi, 130
OutputState, 124	GpioHostOwnAcpi, 139
PadMode, 124	GpioHostOwnCpio 139
PowerConfig, 124	GpioHostOwnGpio, 139
GPIO_DIRECTION	GpioIntApic, 140

ChiclatPothEdge 140	ChiaCantia h 100
GpioIntBothEdge, 140	GpioConfig.h, 139
GpioIntDefault, 140	GpioHostOwnDefault
GpioIntDis, 140	GpioConfig.h, 139
GpioIntEdge, 140	GpioHostOwnGpio
GpioIntLevel, 140	GpioConfig.h, 139
GpioIntLvlEdgDis, 140	GpioIntApic
GpioIntNmi, 140	GpioConfig.h, 140
GpioIntSci, 140	GpioIntBothEdge
GpioIntSmi, 140	GpioConfig.h, 140
GpioLockDefault, 140	GpioIntDefault
GpioNoTolerance1v8, 139	GpioConfig.h, 140
GpioOutDefault, 141	GpioIntDis
GpioOutHigh, 141	GpioConfig.h, 140
GpioOutLow, 141	GpioIntEdge
GpioOutputStateLock, 140	GpioConfig.h, 140
GpioPadConfigLock, 140	GpioIntLevel
GpioPlatformReset, 142	GpioConfig.h, 140
GpioResetDeep, 141	GpioIntLvlEdgDis
GpioResetDefault, 141	GpioConfig.h, 140
GpioResetNormal, 141	GpioIntNmi
GpioResetPwrGood, 141	GpioConfig.h, 140
GpioResetResume, 141	GpioIntSci
•	•
GpioResumeReset, 141	GpioConfig.h, 140
GpioRxRaw1Default, 141	GpioIntSmi
GpioRxRaw1Dis, 141	GpioConfig.h, 140
GpioRxRaw1En, 141	GpiolrqRoute
GpioTermDefault, 139	FSP_S_CONFIG, 74
GpioTermNative, 139	GpioLockDefault
GpioTermNone, 139	GpioConfig.h, 140
GpioTermWpd20K, 139	GpioNoTolerance1v8
GpioTermWpd5K, 139	GpioConfig.h, 139
GpioTermWpu1K, 139	GpioOutDefault
GpioTermWpu1K2K, 139	GpioConfig.h, 141
GpioTermWpu20K, 139	GpioOutHigh
GpioTermWpu2K, 139	GpioConfig.h, 141
GpioTermWpu5K, 139	GpioOutLow
GpioTolerance1v8, 139	GpioConfig.h, 141
GpioDirDefault	GpioOutputStateLock
GpioConfig.h, 138	GpioConfig.h, 140
GpioDirIn	GpioPadConfigLock
GpioConfig.h, 138	GpioConfig.h, 140
GpioDirInInv	GpioPlatformReset
GpioConfig.h, 139	GpioConfig.h, 142
GpioDirInInvOut	GpioResetDeep
GpioConfig.h, 138	GpioConfig.h, 141
GpioDirInOut	GpioResetDefault
GpioConfig.h, 138	GpioConfig.h, 141
GpioDirNone	GpioResetNormal
GpioConfig.h, 139	GpioConfig.h, 141
GpioDirOut	GpioResetPwrGood
•	•
GpioConfig.h, 139 GpioDswReset	GpioConfig.h, 141 GpioResetResume
•	•
GpioConfig.h, 142	GpioConfig.h, 141
GpioHardwareDefault	GpioResumeReset
GpioConfig.h, 139	GpioConfig.h, 141
GpioHostDeepReset	GpioRxRaw1Default
GpioConfig.h, 142	GpioConfig.h, 141
GpioHostOwnAcpi	GpioRxRaw1Dis

GpioConfig.h, 141	KtDeviceEnable
GpioRxRaw1En	FSP_M_TEST_CONFIG, 52
GpioConfig.h, 141	
GpioSampleDef.h, 142	LockConfig
GpioTermDefault	GPIO_CONFIG, 124
GpioConfig.h, 139	LockPTMregs
GpioTermNative	FSP_M_TEST_CONFIG, 52
•	1 01 _M_1201_00141 14, 02
GpioConfig.h, 139	MEMORY_PLATFORM_DATA, 124
GpioTermNone	MachineCheckEnable
GpioConfig.h, 139	FSP_S_TEST_CONFIG, 111
GpioTermWpd20K	
GpioConfig.h, 139	ManageabilityMode
GpioTermWpd5K	FSP_S_CONFIG, 75
GpioConfig.h, 139	MeUnconfiglsValid
GpioTermWpu1K	FSP_S_CONFIG, 75
GpioConfig.h, 139	MemInfoHob.h, 143
GpioTermWpu1K2K	MicrocodePatchAddress
GpioConfig.h, 139	FSP_S_CONFIG, 75
GpioTermWpu20K	MlcStreamerPrefetcher
GpioConfig.h, 139	FSP_S_TEST_CONFIG, 112
GpioTermWpu2K	MmioSize
GpioConfig.h, 139	FSP_M_CONFIG, 39
GpioTermWpu5K	MonitorMwaitEnable
•	FSP_S_TEST_CONFIG, 112
GpioConfig.h, 139	101_0_1201_0014110, 112
GpioTolerance1v8	NumOfDevIntConfig
GpioConfig.h, 139	FSP S CONFIG, 75
III-OtI	
HdcControl	NumberOfEntries
FSP_S_TEST_CONFIG, 111	FSP_S_TEST_CONFIG, 112
Heci3Enabled	
FSP_S_CONFIG, 74	OcLock
	FSP_M_CONFIG, 39
FSP_S_CONFIG, 74	FSP_M_CONFIG, 39 OneCoreRatioLimit
FSP_S_CONFIG, 74 HeciCommunication2	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51	FSP_M_CONFIG, 39 OneCoreRatioLimit
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 lccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialIoUartDebugEnable
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialIoUartDebugEnable FSP_T_CONFIG, 119
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialIoUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74 InitPcieAspmAfterOprom	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialIoUartDebugEnable FSP_T_CONFIG, 119
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74 InitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialIoUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx FSP_M_CONFIG, 39	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSeriallOurtDebugEnable FSP_T_CONFIG, 119 PcdSeriallOUartNumber FSP_M_CONFIG, 40
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74 InitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx FSP_M_CONFIG, 39 InterruptConfig	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialloUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber FSP_M_CONFIG, 40 FSP_T_CONFIG, 119 PchAcpiBase
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx FSP_M_CONFIG, 39	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialloUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber FSP_M_CONFIG, 40 FSP_T_CONFIG, 119 PchAcpiBase FSP_M_CONFIG, 40
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74 InitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx FSP_M_CONFIG, 39 InterruptConfig GPIO_CONFIG, 123	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialloUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber FSP_M_CONFIG, 40 FSP_T_CONFIG, 119 PchAcpiBase FSP_M_CONFIG, 40 PchCio2Enable
FSP_S_CONFIG, 74 HeciCommunication2 FSP_M_TEST_CONFIG, 51 HeciTimeouts FSP_M_CONFIG, 39 HostSoftPadOwn GPIO_CONFIG, 123 Hwp FSP_S_TEST_CONFIG, 111 IccMax FSP_S_CONFIG, 74 IderDeviceEnable FSP_M_TEST_CONFIG, 52 IgdDvmt50PreAlloc FSP_M_CONFIG, 39 ImonOffset FSP_S_CONFIG, 74 ImonSlope FSP_S_CONFIG, 74 InitPcieAspmAfterOprom FSP_M_CONFIG, 39 InternalGfx FSP_M_CONFIG, 39 InterruptConfig	FSP_M_CONFIG, 39 OneCoreRatioLimit FSP_S_TEST_CONFIG, 112 OutputState GPIO_CONFIG, 124 PadMode GPIO_CONFIG, 124 PanelPowerEnable FSP_M_TEST_CONFIG, 52 PcdDebugInterfaceFlags FSP_M_CONFIG, 39 PcdIsaSerialUartBase FSP_M_CONFIG, 40 PcdSerialDebugBaudRate FSP_M_CONFIG, 40 PcdSerialDebugLevel FSP_M_CONFIG, 40 PcdSerialloUartDebugEnable FSP_T_CONFIG, 119 PcdSerialloUartNumber FSP_M_CONFIG, 40 FSP_T_CONFIG, 119 PchAcpiBase FSP_M_CONFIG, 40

FSP_S_CONFIG, 75	FSP_S_CONFIG, 78
PchDciEn	PchlshGp1GpioAssign
FSP_M_TEST_CONFIG, 52	FSP S CONFIG, 78
PchDisableComplianceMode	PchlshGp2GpioAssign
FSP S CONFIG, 75	FSP S CONFIG, 79
PchDmiAspm	PchlshGp3GpioAssign
FSP_S_CONFIG, 76	FSP S CONFIG, 79
PchDmiTsawEn	PchlshGp4GpioAssign
FSP_S_CONFIG, 76	FSP_S_CONFIG, 79
PchHdaDspEnable	PchlshGp5GpioAssign
FSP S CONFIG, 76	FSP S CONFIG, 79
:	PchlshGp6GpioAssign
PchHdaDspEndpointBluetooth	
FSP_S_CONFIG, 76	FSP_S_CONFIG, 79
PchHdaDspEndpointl2s	PchlshGp7GpioAssign
FSP_S_CONFIG, 76	FSP_S_CONFIG, 79
PchHdaDspFeatureMask	Pchlshl2c0GpioAssign
FSP_S_CONFIG, 76	FSP_S_CONFIG, 79
PchHdaDspUaaCompliance	Pchlshl2c1GpioAssign
FSP_S_CONFIG, 76	FSP_S_CONFIG, 79
PchHdaEnable	Pchlshl2c2GpioAssign
FSP_S_CONFIG, 77	FSP_S_CONFIG, 80
PchHdaIDispCodecDisconnect	PchlshPdtUnlock
FSP_S_CONFIG, 77	FSP_S_CONFIG, 80
PchHdaloBufferOwnership	PchlshSpiGpioAssign
FSP_S_CONFIG, 77	FSP_S_CONFIG, 80
PchHdaPme	PchlshUart0GpioAssign
FSP_S_CONFIG, 77	FSP_S_CONFIG, 80
PchHdaResetWaitTimer	PchlshUart1GpioAssign
FSP_S_TEST_CONFIG, 112	FSP_S_CONFIG, 80
PchHpetBase	PchLanClkReqSupported
FSP_M_CONFIG, 40	FSP_S_CONFIG, 80
PchHpetBdfValid	PchLanEnable
FSP_M_CONFIG, 40	FSP_S_CONFIG, 80
PchHpetBusNumber	PchLanK1OffEnable
FSP_M_CONFIG, 41	FSP_S_CONFIG, 81
PchHpetDeviceNumber	PchLanLtrEnable
FSP_M_CONFIG, 41	FSP_S_CONFIG, 81
PchHpetEnable	PchLockDownBiosInterface
FSP M CONFIG, 41	FSP S TEST CONFIG, 112
PchHpetFunctionNumber	PchLockDownBiosLock
FSP_M_CONFIG, 41	FSP S CONFIG, 81
PchloApicBdfValid	PchLockDownGlobalSmi
FSP S CONFIG, 77	FSP_S_TEST_CONFIG, 113
PchloApicBusNumber	PchLockDownRtcLock
FSP S CONFIG, 77	FSP_S_TEST_CONFIG, 113
:	
PchloApicDeviceNumber	PchLockDownSpiEiss
FSP_S_CONFIG, 77	FSP_S_CONFIG, 81
PchloApicEntry24_119	PchLpcEnhancePort8xhDecoding
FSP_S_CONFIG, 78	FSP_M_CONFIG, 41
PchloApicFunctionNumber	PchMemoryThrottlingEnable
FSP_S_CONFIG, 78	FSP_S_CONFIG, 81
PchloApicId	PchNumRsvdSmbusAddresses
FSP_S_CONFIG, 78	FSP_M_CONFIG, 41
PchloApicRangeSelect	PchPcieDeviceOverrideTablePtr
FSP_S_CONFIG, 78	FSP_S_CONFIG, 81
PchlshEnable	PchPmCapsuleResetType
FSP_S_CONFIG, 78	FSP_S_CONFIG, 81
PchlshGp0GpioAssign	PchPmDeepSxPol

FSP_S_CONFIG, 82	FSP_S_TEST_CONFIG, 113
PchPmDisableDsxAcPresentPulldown	PchScsEmmcHs400DllDataValid
FSP S CONFIG, 82	FSP S CONFIG, 85
PchPmDisableEnergyReport	PchScsEmmcHs400TuningRequired
FSP S TEST CONFIG, 113	FSP S CONFIG, 85
PchPmDisableNativePowerButton	PchSirqEnable
FSP_S_CONFIG, 82	FSP_S_CONFIG, 85
PchPmLanWakeFromDeepSx	PchSirqMode
FSP_S_CONFIG, 82	FSP_S_CONFIG, 85
PchPmLpcClockRun	PchSkyCamPortACtleEnable
FSP_S_CONFIG, 82	FSP_S_CONFIG, 85
PchPmMeWakeSts	PchSkyCamPortATermOvrEnable
FSP_S_CONFIG, 82	FSP_S_CONFIG, 86
PchPmPciePllSsc	PchSkyCamPortATrimEnable FSP S CONFIG, 86
FSP_M_CONFIG, 41	
PchPmPcieWakeFromDeepSx	PchSkyCamPortBCtleEnable
FSP_S_CONFIG, 82	FSP_S_CONFIG, 86
PchPmPmcReadDisable	PchSkyCamPortBTermOvrEnable
FSP_S_TEST_CONFIG, 113	FSP_S_CONFIG, 86
PchPmPmeB0S5Dis	PchSkyCamPortBTrimEnable
FSP_S_CONFIG, 82	FSP_S_CONFIG, 86
PchPmPwrBtnOverridePeriod	PchSkyCamPortCDCtleEnable
FSP_S_CONFIG, 83	FSP_S_CONFIG, 86
PchPmPwrCycDur	PchSkyCamPortCTermOvrEnable
FSP_S_CONFIG, 83	FSP_S_CONFIG, 86
PchPmSlpAMinAssert	PchSkyCamPortCTrimEnable
FSP_S_CONFIG, 83	FSP_S_CONFIG, 87
PchPmSlpLanLowDc	PchSkyCamPortDTermOvrEnable
FSP_S_CONFIG, 83	FSP_S_CONFIG, 87
PchPmSlpS0Enable	PchSkyCamPortDTrimEnable
FSP_S_CONFIG, 83	FSP_S_CONFIG, 87
PchPmSlpS0VmEnable	PchSubSystemId
FSP_S_CONFIG, 83	FSP S CONFIG, 87
PchPmSlpS3MinAssert	PchSubSystemVendorld
FSP_S_CONFIG, 83	FSP_S_CONFIG, 87
PchPmSlpS4MinAssert	PchTTEnable
FSP_S_CONFIG, 84	FSP_S_CONFIG, 87
PchPmSlpStrchSusUp	PchTTLock
FSP_S_CONFIG, 84	FSP_S_CONFIG, 88
PchPmSlpSusMinAssert	PchTTState13Enable
FSP S CONFIG, 84	FSP S CONFIG, 88
PchPmWoWlanDeepSxEnable	PchThermalDeviceEnable
FSP S CONFIG, 84	FSP S CONFIG, 87
PchPmWoWlanEnable	PchTsmicLock
FSP S CONFIG, 84	FSP S CONFIG, 87
	PcieAllowNoLtrlccPllShutdown
PchPmWolEnableOverride	
FSP_S_CONFIG, 84	FSP_S_CONFIG, 88
PchPmWolOvrWkSts	PcieComplianceTestMode
FSP_S_CONFIG, 84	FSP_S_CONFIG, 88
PchPort61hEnable	PcieDisableRootPortClockGating
FSP_S_CONFIG, 85	FSP_S_CONFIG, 88
PchPort80Route	PcieEnablePeerMemoryWrite
FSP_M_CONFIG, 42	FSP_S_CONFIG, 88
PchPwrOptEnable	PcieEnablePort8xhDecode
FSP_S_CONFIG, 85	FSP_S_TEST_CONFIG, 113
PchSbAccessUnlock	PcieEqPh3LaneParamCm
FSP_S_TEST_CONFIG, 113	FSP_S_CONFIG, 88
PchSbiUnlock	PcieEqPh3LaneParamCp

FSP_S_CONFIG, 89	FSP_M_TEST_CONFIG, 53
PcieRpAspm	PegGen3ProgramStaticEq
FSP_S_CONFIG, 89	FSP_M_TEST_CONFIG, 54
PcieRpClkReqNumber	PegGen3RootPortPreset
FSP_S_CONFIG, 89	FSP_M_TEST_CONFIG, 54
PcieRpClkReqSupport	PegGenerateBdatMarginTable
FSP_S_CONFIG, 89	FSP_M_TEST_CONFIG, 54
PcieRpCompletionTimeout	PegRxCemLoopbackLane
FSP_S_CONFIG, 89	FSP M TEST CONFIG, 54
PcieRpDeviceResetPad	PegRxCemNonProtocolAwareness
FSP S CONFIG, 89	FSP_M_TEST_CONFIG, 54
PcieRpDptp	PkgCStateDemotion
	FSP_S_TEST_CONFIG, 114
FSP_S_TEST_CONFIG, 113	
PcieRpEnableMask	PkgCStateLimit
FSP_M_CONFIG, 42	FSP_S_TEST_CONFIG, 114
PcieRpFunctionSwap	PkgCStateUnDemotion
FSP_S_CONFIG, 89	FSP_S_TEST_CONFIG, 114
PcieRpGen3EqPh3Method	PmgCstCfgCtrlLock
FSP_S_CONFIG, 90	FSP_S_TEST_CONFIG, 114
PcieRpL1Substates	PortUsb20Enable
FSP_S_CONFIG, 90	FSP_S_CONFIG, 90
PcieRpPcieSpeed	PortUsb30Enable
FSP_S_CONFIG, 90	FSP_S_CONFIG, 91
PcieRpPhysicalSlotNumber	PowerConfig
FSP_S_CONFIG, 90	GPIO_CONFIG, 124
PcieRpSlotPowerLimitScale	PowerLimit1
FSP_S_TEST_CONFIG, 114	FSP_S_TEST_CONFIG, 115
PcieRpSlotPowerLimitValue	PowerLimit1Time
FSP_S_TEST_CONFIG, 114	FSP_S_TEST_CONFIG, 115
PcieRpUptp	PowerLimit2
FSP_S_TEST_CONFIG, 114	FSP_S_TEST_CONFIG, 115
PcieSwEqCoeffListCm	PowerLimit2Power
FSP_S_CONFIG, 90	FSP_S_TEST_CONFIG, 115
PcieSwEqCoeffListCp	PowerLimit3
FSP_S_CONFIG, 90	FSP_S_TEST_CONFIG, 115
PeciC10Reset	PowerLimit3Time
FSP_M_CONFIG, 42	FSP_S_TEST_CONFIG, 115
PeciSxReset	PowerLimit4
FSP_M_CONFIG, 42	FSP_S_TEST_CONFIG, 115
Peg0Gen3EqPh2Enable	PrmrrSize
FSP_M_TEST_CONFIG, 52	FSP_M_CONFIG, 42
Peg0Gen3EqPh3Method	ProbelessTrace
FSP_M_TEST_CONFIG, 52	FSP_M_CONFIG, 43
Peg1Gen3EqPh2Enable	ProcHotResponse
FSP_M_TEST_CONFIG, 53	FSP_S_TEST_CONFIG, 115
Peg1Gen3EqPh3Method	ProcTraceEnable
FSP_M_TEST_CONFIG, 53	FSP_S_TEST_CONFIG, 116
Peg2Gen3EqPh2Enable	ProcTraceOutputScheme
FSP_M_TEST_CONFIG, 53	FSP_S_TEST_CONFIG, 116
Peg2Gen3EqPh3Method	Psi1Threshold
FSP_M_TEST_CONFIG, 53	FSP_S_CONFIG, 91
PegDataPtr	Psi2Threshold
FSP_M_CONFIG, 42	FSP_S_CONFIG, 91
PegDisableSpreadSpectrumClocking	Psi3Enable
FSP M CONFIG, 42	FSP_S_CONFIG, 91
PegGen3EndPointHint	Psi3Threshold
FSP_M_TEST_CONFIG, 53	FSP S CONFIG, 91
PegGen3EndPointPreset	PsysOffset
-	•

FSP_S_CONFIG, 91	SataRstLedLocate
PsysPmax	FSP_S_CONFIG, 93
FSP_S_TEST_CONFIG, 116	SataRstOromUiBanner
PsysPowerLimit1	FSP S CONFIG, 93
FSP S TEST CONFIG, 116	SataRstPcieDeviceResetDelay
PsysPowerLimit1Power	FSP_S_CONFIG, 93
FSP_S_TEST_CONFIG, 116	SataRstRaid0
PsysPowerLimit2	
	FSP_S_CONFIG, 94
FSP_S_TEST_CONFIG, 116	SataRstRaid1
PsysPowerLimit2Power	FSP_S_CONFIG, 94
FSP_S_TEST_CONFIG, 116	SataRstRaid10
PsysSlope	FSP_S_CONFIG, 94
FSP_S_CONFIG, 91	SataRstRaid5
PxRcConfig	FSP_S_CONFIG, 94
FSP_S_CONFIG, 92	SataRstRaidAlternateId
	FSP_S_CONFIG, 94
RMT	SataRstSmartStorage
FSP_M_CONFIG, 43	FSP S CONFIG, 94
RaceToHalt	SataSalpSupport
FSP S TEST CONFIG, 117	
Ratio	FSP_S_CONFIG, 94
FSP M CONFIG, 43	SataTestMode
RefClk	FSP_S_TEST_CONFIG, 117
FSP_M_CONFIG, 43	SataThermalSuggestedSetting
RingMaxOcRatio	FSP_S_CONFIG, 95
S .	ScanExtGfxForLegacyOpRom
FSP_M_CONFIG, 43	FSP_M_TEST_CONFIG, 54
RingMinOcRatio	ScilrqSelect
FSP_M_CONFIG, 43	FSP_S_CONFIG, 95
OL OLUBORT INIT INFO 405	ScsEmmcEnabled
SI_CHIPSET_INIT_INFO, 125	FSP_S_CONFIG, 95
SI_PCH_DEVICE_INTERRUPT_CONFIG, 125	
SI_PCH_INT_PIN	ScsEmmcHs400Enabled
FspsUpd.h, 134	FSP_S_CONFIG, 95
SMBIOS_CACHE_INFO, 126	ScsSdCardEnabled
SMBIOS_PROCESSOR_INFO, 126	FSP_S_CONFIG, 95
SaGv	SendEcCmd
FSP_M_CONFIG, 43	FSP_S_CONFIG, 95
SataEnable	SendVrMbxCmd
FSP_S_CONFIG, 92	FSP_S_CONFIG, 95
SataMode	SendVrMbxCmd1
	FSP_S_CONFIG, 96
FSP_S_CONFIG, 92	SerialloDebugUartNumber
SataP0TDispFinit	FSP_S_CONFIG, 96
FSP_S_CONFIG, 92	
SataP1TDispFinit	SerialloDevMode
FSP_S_CONFIG, 92	FSP_S_CONFIG, 96
SataPortsDevSlp	SerialloGpio
FSP_S_CONFIG, 92	FSP_S_CONFIG, 96
SataPortsDmVal	ShowSpiController
FSP_S_CONFIG, 92	FSP_S_CONFIG, 96
SataPortsEnable	SiPchNoInt
FSP_S_CONFIG, 93	FspsUpd.h, 134
SataPwrOptEnable	SinitMemorySize
FSP_S_CONFIG, 93	FSP M CONFIG, 44
SataRstHddUnlock	SkipMbpHob
FSP_S_CONFIG, 93	FSP_M_TEST_CONFIG, 55
SataRstIrrt	SlowSlewRateForGt
FSP_S_CONFIG, 93	FSP_S_CONFIG, 96
SataRstIrrtOnly	SlowSlewRateForla
FSP_S_CONFIG, 93	FSP_S_CONFIG, 96

SlowSlewRateForSa FSP_S_CONFIG, 97	TxtLcpPdBase FSP_M_TEST_CONFIG, 55
SmbiosCacheInfoHob.h, 144	TxtLcpPdSize
SmbiosProcessorInfoHob.h, 145	FSP_M_TEST_CONFIG, 55
SmbusArpEnable	
FSP M CONFIG, 44	Usb2AfePehalfbit
SmbusDynamicPowerGating	FSP_S_CONFIG, 97
FSP_M_TEST_CONFIG, 55	Usb2AfePetxiset
SmbusEnable	FSP_S_CONFIG, 98
FSP M CONFIG, 44	Usb2AfePredeemp
SmbusSpdWriteDisable	FSP S CONFIG, 98
FSP_M_TEST_CONFIG, 55	Usb2AfeTxiset
SpdProfileSelected	FSP_S_CONFIG, 98
•	Usb3HsioTxDeEmph
FSP_M_CONFIG, 44	FSP_S_CONFIG, 98
SsicPortEnable 500 CONFIGURE	Usb3HsioTxDeEmphEnable
FSP_S_CONFIG, 97	•
StateRatio	FSP_S_CONFIG, 98
FSP_S_TEST_CONFIG, 117	Usb3HsioTxDownscaleAmp
+DTD	FSP_S_CONFIG, 98
trtp	Usb3HsioTxDownscaleAmpEnable
FSP_M_CONFIG, 44	FSP_S_CONFIG, 98
TStates	N/ 1 N/ 1:
FSP_S_TEST_CONFIG, 118	VddVoltage
TTSuggestedSetting	FSP_M_CONFIG, 45
FSP_S_CONFIG, 97	VmxEnable
TccActivationOffset	FSP_M_CONFIG, 45
FSP_S_TEST_CONFIG, 117	VrVoltageLimit
TccOffsetClamp	FSP_S_CONFIG, 99
FSP_S_TEST_CONFIG, 117	
TccOffsetLock	WatchDog
FSP_S_TEST_CONFIG, 117	FSP_S_CONFIG, 99
TccOffsetTimeWindowForRatl	WatchDogTimerBios
FSP_S_TEST_CONFIG, 118	FSP_S_CONFIG, 99
TcolrqSelect	WatchDogTimerOs
FSP_S_CONFIG, 97	FSP_S_CONFIG, 99
TdcPowerLimit	WdtDisableAndLock
FSP_S_CONFIG, 97	FSP_M_TEST_CONFIG, 56
TdcTimeWindow	
FSP_S_CONFIG, 97	XdciEnable
	FSP_S_CONFIG, 99
TgaSize	
FSP_M_TEST_CONFIG, 55	
TimedMwait	
FSP_S_TEST_CONFIG, 118	
TotalFlashSize	
FSP_M_TEST_CONFIG, 55	
TsegSize	
FSP_M_CONFIG, 44	
TurboMode	
FSP_S_CONFIG, 97	
Txt	
FSP_M_CONFIG, 44	
TxtDprMemoryBase	
FSP_M_CONFIG, 44	
TxtDprMemorySize	
FSP_M_CONFIG, 45	
TxtHeapMemorySize	
FSP_M_CONFIG, 45	
TxtImplemented	
FSP_M_CONFIG, 45	
 '	