



ElkHart Lake Client Platform

SPI Programming Guide

December 2020

Revision 1.25

Intel Confidential



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. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. 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>

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

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.

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details.

Intel, Core and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2020, Intel Corporation. All rights reserved.

Contents

1	Introduction	12
1.1	Overview	12
1.2	Terminology	13
1.3	Reference Documents	13
2	PCH SPI Flash Architecture	15
2.1	Descriptor Mode	15
2.2	Serial Flash Discoverable Parameter (SFDP)	15
2.3	SPI Fast Read	15
2.4	Boot Flow for Elkhart Lake Family	15
2.5	Flash Regions	15
2.5.1	Flash Region Layout	16
2.5.2	Flash Region Sizes	18
2.6	Hardware Sequencing	18
3	PCH SPI Flash Compatibility Requirement	19
3.1	Elkhart Lake PCH SPI Flash Requirements	19
3.1.1	General Requirements	19
3.1.2	SPI Flash Unlocking Requirements for Intel Converged Security Engine	20
3.1.3	Software / Firmware Requirements	20
3.1.4	JEDEC ID (Opcode 9Fh)	21
3.1.5	Multiple Page Write Usage Model	21
3.1.6	Hardware Sequencing Requirements	21
4	Descriptor	23
4.1	Flash Descriptor Overview	23
4.2	Flash Descriptor Content	24
4.2.1	Descriptor Signature and Map	25
4.2.1.1	FLVALSIG - Flash Valid Signature (Flash Descriptor Records)	25
4.2.1.2	FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)	25
4.2.1.3	FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)	26
4.2.1.4	FLMAP2—Flash Map 2 Register (Flash Descriptor Records)	26
4.2.1.5	FLMAP3—Flash Map 3 Register (Flash Descriptor Records)	26
4.2.2	Flash Descriptor Component Section	28
4.2.2.1	FLCOMP—Flash Components Register (Flash Descriptor Records)	28
4.2.2.2	FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)	31
4.2.2.3	FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)	31
4.2.3	Flash Descriptor Region Section	32
4.2.3.1	FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)	33
4.2.3.2	FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)	33
4.2.3.3	FLREG2—Flash Region 2 (IFWI / Intel® CSE ROM Bypass) Register (Flash Descriptor Records)	33

4.2.3.4	FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records)	34
4.2.4	Flash Descriptor Master Section.....	35
4.2.4.1	FLMSTR1—Flash Master 1 (Host CPU/ BIOS)	35
4.2.4.2	FLMSTR2—Flash Master 2 (Intel® CSE)	35
4.2.4.3	FLMSTR4—Flash Master 4 (Reserved)	35
4.2.5	PCH / CPU Softstraps	37
4.2.6	Descriptor Upper Map Section	37
4.2.6.1	FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)	37
4.2.6.2	IFWI / Intel® CSE ROM Bypass Size	37
4.2.6.3	MIP - Descriptor Table	37
4.2.7	Intel® CSE Vendor Specific Component Capabilities Table	38
4.2.7.1	JIDO—JEDEC-ID 0 Register (Flash Descriptor Records)	38
4.2.7.2	VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records)	39
4.2.7.3	JIDn—JEDEC-ID Register n (Flash Descriptor Records)	39
4.2.7.4	VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)	39
4.3	OEM Section	40
4.4	Region Access Control	40
4.4.1	Intel Recommended Permissions for Region Access	41
4.4.2	Overriding Region Access	41
4.5	Intel® CSE Vendor-Specific Component Capabilities (Intel® CSE VSCC) Table.....	42
4.5.1	How to Set a VSCC Entry in Intel® CSE VSCC Table for Elkhart Lake Platforms	42
4.5.2	Intel® CSE VSCC Table Settings for Elkhart Lake Family Systems	44
5	Serial Flash Discoverable Parameter (SFDP) Overview	45
5.1	Introduction	45
5.2	Discoverable Parameter Opcode and Flash Cycle.....	45
5.3	Parameter Table Supported on PCH	45
5.4	Detailed JEDEC Specification	46
6	Configuring BIOS for SPI Flash Access	47
6.1	Unlocking SPI Flash Device Protection for Elkhart Lake Platform.....	47
6.2	Locking SPI Flash via Status Register	48
6.3	SPI Protected Range Register Recommendations	48
6.4	Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits	48
6.4.1	Flash Configuration Lockdown	48
6.4.2	Vendor Component Lock	49
6.5	Host Vendor Specific Component Control Registers (VSCC)	49
6.6	Host VSCC Register Settings.....	53
7	IFWI / Intel® CSE Disable for Debug/Flash Burning Purposes.....	54
7.1	IFWI / Intel® CSE Disable	54
7.1.1	Erasing/Programming Intel® CSE Region	54
8	Recommendations for SPI Flash Programming in Manufacturing Environments	55
9	Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section	56
9.1	PCH Descriptor Record 0 (Flash Descriptor Records).....	56
9.2	PCH Descriptor Record 1 (Flash Descriptor Records).....	56
9.3	PCH Descriptor Record 2 (Flash Descriptor Records).....	56
9.4	PCH Descriptor Record 3 (Flash Descriptor Records).....	56
9.5	PCH Descriptor Record 4 (Flash Descriptor Records).....	57
9.6	PCH Descriptor Record 5 (Flash Descriptor Records).....	57

9.7	PCH Descriptor Record 6 (Flash Descriptor Records)	57
9.8	PCH Descriptor Record 7 (Flash Descriptor Records)	58
9.9	PCH Descriptor Record 8 (Flash Descriptor Records)	59
9.10	PCH Descriptor Record 9 (Flash Descriptor Records)	60
9.11	PCH Descriptor Record 10 (Flash Descriptor Records)	61
9.12	PCH Descriptor Record 11 (Flash Descriptor Records)	62
9.13	PCH Descriptor Record 12 (Flash Descriptor Records)	63
9.14	PCH Descriptor Record 13 (Flash Descriptor Records)	64
9.15	PCH Descriptor Record 14 (Flash Descriptor Records)	65
9.16	PCH Descriptor Record 15 (Flash Descriptor Records)	66
9.17	PCH Descriptor Record 16 (Flash Descriptor Records)	67
9.18	PCH Descriptor Record 17 (Flash Descriptor Records)	67
9.19	PCH Descriptor Record 18 (Flash Descriptor Records)	67
9.20	PCH Descriptor Record 19 (Flash Descriptor Records)	67
9.21	PCH Descriptor Record 20 (Flash Descriptor Records)	68
9.22	PCH Descriptor Record 21 (Flash Descriptor Records)	69
9.23	PCH Descriptor Record 22 (Flash Descriptor Records)	70
9.24	PCH Descriptor Record 23 (Flash Descriptor Records)	70
9.25	PCH Descriptor Record 24 (Flash Descriptor Records)	70
9.26	PCH Descriptor Record 25 (Flash Descriptor Records)	71
9.27	PCH Descriptor Record 26 (Flash Descriptor Records)	71
9.28	PCH Descriptor Record 27 (Flash Descriptor Records)	71
9.29	PCH Descriptor Record 28 (Flash Descriptor Records)	71
9.30	PCH Descriptor Record 29 (Flash Descriptor Records)	72
9.31	PCH Descriptor Record 30 (Flash Descriptor Records)	72
9.32	PCH Descriptor Record 31 (Flash Descriptor Records)	72
9.33	PCH Descriptor Record 32 (Flash Descriptor Records)	73
9.34	PCH Descriptor Record 33 (Flash Descriptor Records)	74
9.35	PCH Descriptor Record 34 (Flash Descriptor Records)	75
9.36	PCH Descriptor Record 35 (Flash Descriptor Records)	76
9.37	PCH Descriptor Record 36 (Flash Descriptor Records)	77
9.38	PCH Descriptor Record 37 (Flash Descriptor Records)	78
9.39	PCH Descriptor Record 38 (Flash Descriptor Records)	79
9.40	PCH Descriptor Record 39 (Flash Descriptor Records)	80
9.41	PCH Descriptor Record 40 (Flash Descriptor Records)	80
9.42	PCH Descriptor Record 41 (Flash Descriptor Records)	81
9.43	PCH Descriptor Record 42 (Flash Descriptor Records)	81
9.44	PCH Descriptor Record 43 (Flash Descriptor Records)	82
9.45	PCH Descriptor Record 44 (Flash Descriptor Records)	83
9.46	PCH Descriptor Record 45 (Flash Descriptor Records)	84
9.47	PCH Descriptor Record 46 (Flash Descriptor Records)	85
9.48	PCH Descriptor Record 47 (Flash Descriptor Records)	86
9.49	PCH Descriptor Record 48 (Flash Descriptor Records)	87
9.50	PCH Descriptor Record 49 (Flash Descriptor Records)	88
9.51	PCH Descriptor Record 50 (Flash Descriptor Records)	89
9.52	PCH Descriptor Record 51 (Flash Descriptor Records)	90
9.53	PCH Descriptor Record 52 (Flash Descriptor Records)	90
9.54	PCH Descriptor Record 53 (Flash Descriptor Records)	90
9.55	PCH Descriptor Record 54 (Flash Descriptor Records)	91
9.56	PCH Descriptor Record 55 (Flash Descriptor Records)	91
9.57	PCH Descriptor Record 56 (Flash Descriptor Records)	91
9.58	PCH Descriptor Record 57 (Flash Descriptor Records)	92
9.59	PCH Descriptor Record 58 (Flash Descriptor Records)	93
9.60	PCH Descriptor Record 59 (Flash Descriptor Records)	93
9.61	PCH Descriptor Record 60 (Flash Descriptor Records)	94

[illegible]

[illegible]

9.172 PCH Descriptor Record 171 (Flash Descriptor Records)	121
9.173 PCH Descriptor Record 172 (Flash Descriptor Records)	122
9.174 PCH Descriptor Record 173 (Flash Descriptor Records)	122
9.175 PCH Descriptor Record 174 (Flash Descriptor Records)	123
9.176 PCH Descriptor Record 175 (Flash Descriptor Records)	123
9.177 PCH Descriptor Record 176 (Flash Descriptor Records)	124
9.178 PCH Descriptor Record 177 (Flash Descriptor Records)	124
9.179 PCH Descriptor Record 178 (Flash Descriptor Records)	125
9.180 PCH Descriptor Record 179 (Flash Descriptor Records)	125
9.181 PCH Descriptor Record 180 (Flash Descriptor Records)	125
9.182 PCH Descriptor Record 181 (Flash Descriptor Records)	125
9.183 PCH Descriptor Record 182 (Flash Descriptor Records)	125
9.184 PCH Descriptor Record 183 (Flash Descriptor Records)	126
9.185 PCH Descriptor Record 184 (Flash Descriptor Records)	126
9.186 PCH Descriptor Record 185 (Flash Descriptor Records)	126
9.187 PCH Descriptor Record 186 (Flash Descriptor Records)	126
9.188 PCH Descriptor Record 187 (Flash Descriptor Records)	126
9.189 PCH Descriptor Record 188 (Flash Descriptor Records)	127
9.190 PCH Descriptor Record 189 (Flash Descriptor Records)	127
9.191 PCH Descriptor Record 190 (Flash Descriptor Records)	127
9.192 PCH Descriptor Record 191 (Flash Descriptor Records)	127
9.193 MIP Table Descriptor Record 0 (Flash Descriptor Records)	128
9.194 MIP Table Descriptor Record 1 (Flash Descriptor Records)	128
9.195 MIP Table Descriptor Record 2 (Flash Descriptor Records)	128
9.196 MIP Table Descriptor Record 3 (Flash Descriptor Records)	128
9.197 MIP Table Descriptor Record 4 (Flash Descriptor Records)	129
9.198 MIP Table Descriptor Record 5 (Flash Descriptor Records)	129
9.199 MIP Table Descriptor Record 6 (Flash Descriptor Records)	129
9.200 MIP Table Descriptor Record 7 (Flash Descriptor Records)	129
9.201 MIP Table Descriptor Record 8 (Flash Descriptor Records)	130
9.202 MIP Table Descriptor Record 9 (Flash Descriptor Records)	130
9.203 PMC Descriptor Record 0 (Flash Descriptor Records)	131
9.204 PMC Descriptor Record 1 (Flash Descriptor Records)	132
9.205 PMC Descriptor Record 2 (Flash Descriptor Records)	132
9.206 PMC Descriptor Record 3 (Flash Descriptor Records)	132
9.207 PMC Descriptor Record 4 (Flash Descriptor Records)	133
9.208 PMC Descriptor Record 5 (Flash Descriptor Records)	133
9.209 PMC Descriptor Record 6 (Flash Descriptor Records)	133
9.210 PMC Descriptor Record 7 (Flash Descriptor Records)	134
9.211 PMC Descriptor Record 8 (Flash Descriptor Records)	134
9.212 PMC Descriptor Record 9 (Flash Descriptor Records)	134
9.213 PMC Descriptor Record 10 (Flash Descriptor Records)	134
9.214 PMC Descriptor Record 11 (Flash Descriptor Records)	134
9.215 PMC Descriptor Record 12 (Flash Descriptor Records)	135
9.216 PMC Descriptor Record 13 (Flash Descriptor Records)	135
9.217 PMC Descriptor Record 14 (Flash Descriptor Records)	135
9.218 PMC Descriptor Record 15 (Flash Descriptor Records)	135
9.219 PMC Descriptor Record 16 (Flash Descriptor Records)	135
9.220 PMC Descriptor Record 17 (Flash Descriptor Records)	136
9.221 PMC Descriptor Record 18 (Flash Descriptor Records)	136
9.222 PMC Descriptor Record 19 (Flash Descriptor Records)	136
9.223 PMC Descriptor Record 20 (Flash Descriptor Records)	136
9.224 CPU Descriptor Record 0 (Flash Descriptor Records)	137
9.225 CPU Descriptor Record 1 (Flash Descriptor Records)	138
9.226 CPU Descriptor Record 2 (Flash Descriptor Records)	139

9.227	CPU Descriptor Record 3 (Flash Descriptor Records)	140
9.228	Intel® CSE Descriptor Record 0 (Flash Descriptor Records)	141
9.229	Intel® CSE Descriptor Record 1 (Flash Descriptor Records)	142
10	Configuration Dependencies	144
10.1	Descriptor Configuration Setting Enabling Dependencies	144
10.1.1	High Speed IO (HSIO) Port Enabling	144
10.1.2	Configuring PCIe on HSIO Dependencies	147
10.1.2.1	For PCIe Controller #1:	147
10.1.3	Configuring Multi VC PCIe on HSIO Dependencies	148
10.1.3.1	For Multi VC Controller #1:	148
10.1.3.2	For Multi VC Controller #2:	148
10.1.3.3	For Multi VC Controller #3:	149
10.1.4	TPM over SPI Enabling Dependencies	150
10.1.4.1	To enable TPM over SPI:	150
10.1.4.2	To disable TPM over SPI:	150
10.1.5	mSATA/M.2 / SATA Express Enabling Dependencies	150
10.1.5.1	SATA0 / PCIe10 mSATA /M.2 / SATA Express Enabling	150
10.1.5.2	SATA1 / PCIe11 mSATA /M.2 / SATA Express Enabling	150
10.1.6	3.1 Enabling Dependencies	151
10.1.6.1	USB 3.1 Port 2:	151
10.1.6.2	USB 3.1 Port 3:	151
10.1.7	UFS Enabling Dependencies	151
10.1.7.1	UFS Boot:	151
10.1.7.2	UFS Storage:	151
10.1.8	TSN GbE Port Select Enabling Dependencies	152
10.1.8.1	TSN Configuration:	152
11	RPMC Configuration	153
11.1	System Components - High-Level Architecture Block Diagram	153
11.2	Monotonic counters	154
11.3	Binding at End of Manufacturing (EOM)	154
11.3.1	RPMC binding on Dual SPI configuration	154
11.4	Refurbish flows impact	154
11.4.1	PCH replacement	154
11.4.2	SPI replacement	155
11.4.3	SPI re-flash	155
11.5	RPMC re-binding	155
A	FAQ and Troubleshooting	156

Figures

2-1 SPI Flash Region Layout	17
4-1 Flash Descriptor (Elkhart Lake)	23
5-1 SFDP Read Instruction Sequence.....	45

Tables

1-1 Terminology	13
1-2 Reference Documents.....	13
4-1 Region Access Control Table Options.....	40
4-2 Recommended Read/Write Permissions.....	41
4-3 Recommended Read/Write Settings for Platforms	41
4-4 Jidn - JEDEC ID Portion of Intel® CSE VSCC Table	42
4-5 Vscn - Vendor-Specific Component Capabilities Portion of the Elkhart Lake Platforms	42
6-1 VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0	49
6-2 VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1	51
6-3 Description of How WSR and WEWS is Used.....	52
10-1Elkhart Flex I/O Map	144
10-2HSIO Lane Muxing Selection	145

Revision History

Document Number	Revision Number	Description	Revision Date
	0.5	<ul style="list-style-type: none"> Initial Release 	October 2018
	0.6	<ul style="list-style-type: none"> Updated to 0.8 RDL 	January 2019
	0.61	<ul style="list-style-type: none"> Updated LOSL setting information 	February 2019
	0.62	<ul style="list-style-type: none"> Updated designations for GPIOs Updated EDS references Updated to firmware references to Intel® CSE Removed GbE and EC references Updated Configuration Dependencies chapter Removed eSPI information 	May 2019
	0.7	<ul style="list-style-type: none"> Revised to v0.7 	August 2019
	0.8	<ul style="list-style-type: none"> Updated with latest Harness changes 	December 2019
	0.81	<ul style="list-style-type: none"> Added additional note on Dual and Quad mode for SPI 	December 2019
	0.82	<ul style="list-style-type: none"> Updated Permissions table 	January 2020
	1.0	<ul style="list-style-type: none"> Update to v1.0 	April 2020
	1.1	<ul style="list-style-type: none"> Updates to remove Non POR information 	June 2020
	1.2	<ul style="list-style-type: none"> Updated offsets 0x174, 0x178 and 0x17C values to 0x8 for Multi-VC configuration Updated Multi VC Controller information in Configuration Dependencies chapter 	July 2020
	1.21	<ul style="list-style-type: none"> Corrected FLCOMP frequency values 	July 2020
	1.22	<ul style="list-style-type: none"> Top Swap Block Size encoding values 	August 2020
	1.23	<ul style="list-style-type: none"> Added RPMC Chapter 	October 2020
	1.24	<ul style="list-style-type: none"> Corrected encoding on MultiVC Controller 2 and 3 in Configuration Dependencies chapter 	November 2020
	1.25	<ul style="list-style-type: none"> Aligned USB2 and USB3 connector type settings with Harness 	December 2020

§ §

1 Introduction

1.1 Overview

This manual is intended for OEMs and software vendors to clarify various aspects of programming the SPI flash on PCH family based platforms. The current scope of this document is for Intel® processor code name Elkhart Lake only.

Chapter 2, "PCH SPI Flash Architecture"

- Overview of SPI flash, Descriptor, Flash Layout, compatible SPI flash.

Chapter 3, "PCH SPI Flash Compatibility Requirement"

- Overview of compatibility requirements for Elkhart Lake products.

Chapter 4, "Descriptor"

- Overview of the descriptor and Descriptor record definition

Chapter 5, "Serial Flash Discoverable Parameter (SFDP) Overview"

- Overview of the SFDP definition.

Chapter 6, "Configuring BIOS for SPI Flash Access"

- Describes how to configure BIOS/GbE for SPI flash access.

Chapter 7, "IFWI / Intel® CSE Disable for Debug/Flash Burning Purposes"

- Methods of disabling Intel Converged Security Engine for debug purposes.

Chapter 8, "Recommendations for SPI Flash Programming in Manufacturing Environments"

- Recommendations for manufacturing environments.

Chapter 9, "Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section"

- Flash Descriptor PCH / CPU Soft Strap Section.

Chapter 10, "Configuration Dependencies"

- Descriptor configuration dependencies for enabling Elkhart Lake Hardware I/O, Bus and GPIO components.

Appendix A, "FAQ and Troubleshooting"

- Frequently asked questions and Troubleshooting tips.

1.2 Terminology

Table 1-1. Terminology

Term	Description
BIOS	Basic Input-Output System
CRB	Customer Reference Board
Intel® FPT	Intel® Flash Programming Tool - programs the SPI flash
FIT	Intel® Flash Image Tool – creates a flash image from separate binaries
FW	Firmware
FWH	Firmware Hub – LPC based flash where BIOS may reside
GbE	Intel® Integrated 1000/100/10
HDCP	High-bandwidth Digital Content Protection
IFWI	Integrated Firmware Image Layout
Elkhart Lake	Elkhart Lake Platform Integrated I/O
Intel® Converged Security Engine Firmware (Intel® CSE FW)	Intel firmware that adds Castle Peak, Sentry Peak, etc.
Intel PCH	Intel® Platform Controller Hub
Intel PCHn family	All PCHn derivatives including PCHn (desktop) and PCHnM (mobile)
LPC	Low Pin Count Bus- bus on where legacy devices such a FWH reside
LVSCC	Lower Vendor Specific Component Capabilities
MCP	Multi-Chip package
MDTBA	MIP Descriptor Table Base Address
MIP	Master Image Profile
PCH	Platform Controller Hub
PCH-LP	Platform Controller Hub – Low Power
PMC	Power Management Controller (PCH)
SFDP	Serial Flash Discoverable Parameter
SPI	Serial Peripheral Interface – refers to serial flash memory in this document
UVSCC	Upper Vendor Specific Component Capabilities
VSCC	Vendor Specific Component Capabilities

1.3 Reference Documents

Table 1-2. Reference Documents

Document	Document # / Location
<i>Elkhart Lake External Design Specification (EDS), Volume 1 (RDC# 601458)</i> <i>Elkhart Lake External Design Specification (EDS), Volume 2 (RDC# 602633)</i>	Contact your Intel field representative.
<i>Intel® Flash Image Tool (FIT)</i>	\\System Tools\\Flash Image Tool of latest Intel® CSE kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.

Table 1-2. Reference Documents

Document	Document # / Location
<i>Flash Programming Tool (FPT)</i>	\System Tools\Flash Programming Tool of latest Intel® CSE from VIP. The Kit MUST match the platform you intend to use the flash tools for.
<i>FW Bring Up Guide</i>	Root directory of latest Intel® Converged Security Engine kit from VIP. The Kit MUST match the platform you intend to use the flash tools for.

§ §

2 PCH SPI Flash Architecture

2.1 Descriptor Mode

The Elkhart Lake Platform supports up to two SPI flash devices. The flash connected to Chip Select 0 must contain a valid Descriptor as defined in Section 4. The contents of the Descriptor provide platform configuration and enable the PCH to securely manage storage among multiple users/purposes.

SPI flash must be connected directly to the PCH SPI bus.

Note: Elkhart Lake only supports Descriptor mode.

See ***SPI Supported Feature Overview*** of the latest External Design Specification (EDS) for more detailed information.

2.2 Serial Flash Discoverable Parameter (SFDP)

Serial flash with SFDP have their supported capabilities and commands stored inside the serial flash devices. The controller will discover the attributes needed to operate.

Elkhart Lake PCH requires SPI flash devices support JEDEC standard JESD216 SDFDP (Serial Flash Discoverable Parameters, Revision A (JESD216A) or later is strongly recommended but not mandatory. SFDP provides a consistent method of describing the functional and feature capabilities of SPI devices in a standard set of internal parameter tables. These parameter tables can be interrogated by PCH to enable adjustment needed to accommodate divergent feature from multiple vendors.

Please refer to [Chapter 5, “Serial Flash Discoverable Parameter \(SFDP\) Overview”](#) for more information.

2.3 SPI Fast Read

Note: See ***SPI for Flash*** section of the latest External Design Specification (EDS) for more detailed information 100MHz support requires SPI component that meet 100MHz timing.

2.4 Boot Flow for Elkhart Lake Family

See Boot strap in the PIN Straps of the latest External Design Specification (EDS) for more detailed information.

See [Chapter 4, “Descriptor”](#) for more detailed information.

2.5 Flash Regions

The controller can divide the SPI flash into separate regions below.

Region	Content
0	Descriptor
1	BIOS
2	IFWI (Integrated Firmware Image) ¹
4	PDR – Platform Data Region (Optional) ²

Notes:

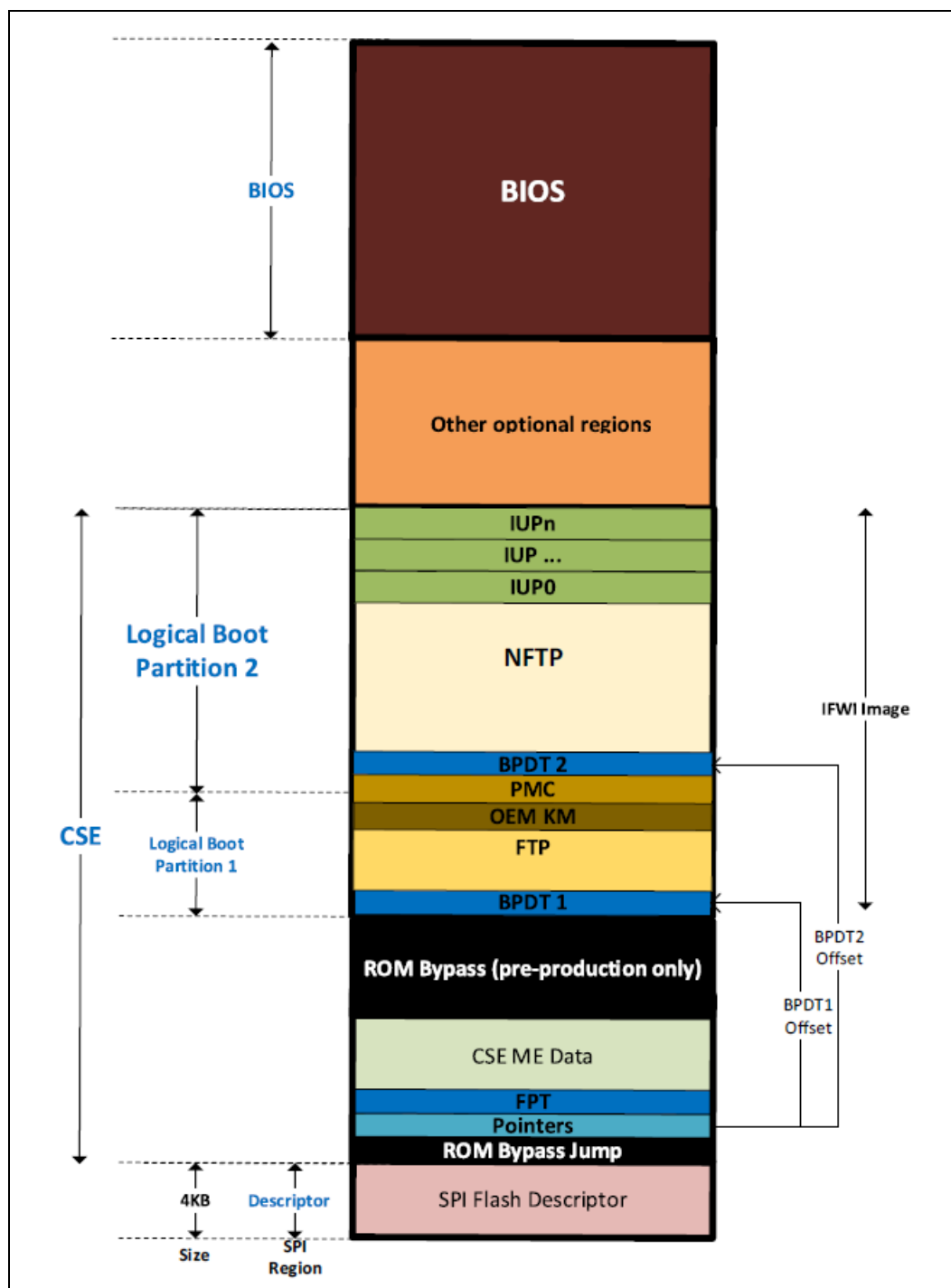
1. Also include as a part of IFWI in some instances is Intel® Converged Security Engine (Intel® CSE FW) ROM Bypass
2. The PDR region is optional and is not applicable for Elkhart Lake or not required for proper platform operation.

See ***SPI Flash Regions*** section of the External Design Specification (EDS) for more detailed information.

2.5.1 Flash Region Layout

In the SPI Controller; a 4K descriptor at the base of the SPI device splits the device into regions and defines the access control to each region.

Figure 2-1. SPI Flash Region Layout



As seen in Figure 2-1, the descriptor defines at least the following device regions:

1. **Intel® CSE ROM Bypass Region**: Starting from offset 4K. This region is used for Intel® CSE ROM Bypass. When Intel® CSE ROM Bypass does not exist, this region size is 0.
2. **IFWI Region**: This region starts after the Intel® CSE ROM Bypass region.
3. **BIOS Region**: This region starts after the IFWI region.

2.5.2 Flash Region Sizes

SPI flash space requirements differ by platform and configuration. Please refer to documentation specific to your platform for BIOS and Intel® CSE Region flash size estimates.

See ***SPI Flash Regions*** section of the latest *External Design Specification (EDS)* for more detailed information.

2.6 Hardware Sequencing

Host/BIOS and Intel® CSE may read/write /erase flash via Hardware Sequencing or Software Sequencing registers.

Elkhart Lake Hardware sequencing has been enhanced to include all operations the BIOS needs to perform.

Note: Host / BIOS Software Sequencing is not supported in Elkhart Lake.

Hardware sequencing has a predefined list of opcodes, the PCH discovers the 4k and 64k erase opcodes via SFDP.

See ***Serial Peripheral Interface Memory Mapped Configuration Registers*** in *External Design Specification (EDS)* for more details.

§ §

3 PCH SPI Flash Compatibility Requirement

3.1 Elkhart Lake PCH SPI Flash Requirements

- Elkhart Lake allows for up to two SPI flash devices to store BIOS, Intel® CSE FW and integrated LAN information.
 - **Intel® CSE FW is required for Elkhart Lake PCH Family-based platforms**
 - Each SPI component can support up to 64 MB (128 MB total addressable) using 26-bit addressing
- 3.3V or 1.8V SPI I/O buffer VCC
- SPI Fast Read instruction is supported at of 14MHz, 25MHz, 50MHz and 100MHz frequencies.
- SPI Dual Output and Dual I/O Fast Read instruction is supported at frequencies of 14MHz, 25MHz, 50MHz and 100MHz.
- SPI Quad Output and Quad I/O Fast read instruction is supported at frequencies of 14MHz, 25MHz, 50MHz and 100MHz.

If there are two SPI components, both components have to support fast read in order to enable Fast Read in PCH.

Enabling Quad mode reads may require special configuration of the flash device during platform manufacturing, prior to first boot. No special configuration is required for flash devices that support Quad mode but do not contain a Quad Enable (QE) bit. Flash devices that contain a QE bit must be configured with QE=1. Several manufacturers offer SKU's with QE=1 by default.

3.1.1 General Requirements

- Erase size capability of: 4 KBytes erase must be supported uniformly across the flash array. If 64k erase is also supported, then it must be supported uniformly across the flash array.
- Serial flash device must ignore the upper address bits such that an address of FFFFFFFh aliases to the top of the flash memory.
- SPI Compatible Mode 0 support: Clock phase is 0 and data is latched on the rising edge of the clock.
- If the device receives a command that is not supported or incomplete (less than 8 bits), the device must discard the cycle gracefully without any impact on the flash content.
- An erase command (page, sector, block, chip, etc.) must set all bits inside the designated area (page, sector, block, chip, etc.) to 1 (Fh).
- Status Register bit 0 must be set to 1 when a write, erase or write to status register is in progress and cleared to 0 when a write or erase is NOT in progress.
- Devices requiring the Write Enable command must automatically clear the Write Enable Latch at the end of Data Program instructions.

- The flexibility to perform a write between 1 byte to 64 bytes is required.
- SFDP fields: dword 1, bit 4 "Write Enable Instruction". Dword 1, bit 3 "Volatile Status Register", both bits must be 0.

Intel Management Firmware must meet the SPI flash based BIOS Requirements plus:

- [2.2 Serial Flash Discoverable Parameter \(SFDP\)](#)
- [3.1.4 JEDEC ID \(Opcode 9Fh\)](#)
- [3.1.5 Multiple Page Write Usage Model](#)
- [3.1.6 Hardware Sequencing Requirements](#)

Write protection scheme must meet the following guidelines [3.1.2 SPI Flash Unlocking Requirements for Intel Converged Security Engine](#).

3.1.2 SPI Flash Unlocking Requirements for Intel Converged Security Engine

- Flash devices must be globally unlocked (read, write and erase access on the Intel® CSE region) from power on by writing 0 to the Block Protect bits in the flash's status register to disable write protection.
- If the status register must be unprotected, it must use the write enable 06h instruction.
- Opcode 01h (write to status register) must then be used to write 0 to the Block Protect bits in the status register. If the device contains a Quad Enable bit in the status register, then firmware must perform a read-modify-write to prevent changing the state of the QE bit when writing to the status register. This must unlock the entire part. If the SPI flash's status register has non-volatile bits that must be written to, bits [5:2] of the flash's status register must be all 0h to indicate that the flash is unlocked.

3.1.3 Software / Firmware Requirements

The recommended Intel® CSE firmware flow for clearing block protect is:

- Determine the location of the Quad Enable (QE) bit using the SFDP table QER field (for devices that support SFDP rev A or later) or the VSCC table QER field (for SFDP rev 1.1)
- Read status registers 1 and 2.
- Modify status to clear Block Protect bits and leave QE bit unchanged.
- Write the status register using an atomic {write_enable, write_status} sequence (this happens automatically when hardware sequencing is used).
- Issue a write_disable instruction using software sequencing.

After global unlock, BIOS has the ability to lock down small sections of the flash as long as they do not involve the Intel® CSE region. See [6.1 Unlocking SPI Flash Device Protection for Elkhart Lake Platform](#) and [6.2 Locking SPI Flash via Status Register](#) for more information about flash based write/erase protection.

3.1.4 JEDEC ID (Opcode 9Fh)

Since each serial flash device may have unique capabilities and commands, the JEDEC ID is the necessary mechanism for identifying the device so the uniqueness of the device can be comprehended by the controller (master). The JEDEC ID uses the opcode 9Fh and a specified implementation and usage model. This JEDEC Standard Manufacturer and Device ID read method is defined in Standard JESD21-C, PRN03-NV1 and is available on the JEDEC website: www.jedec.org.

3.1.5 Multiple Page Write Usage Model

Intel platforms have firmware usage models which require that the serial flash device support multiple writes to a page (minimum of 512 writes) without requiring a preceding erase command. BIOS commonly uses capabilities such as counters that are used for error logging and system boot progress logging. These counters are typically implemented by using byte-writes to 'increment' the bits within a page that have been designated as the counter. The Intel firmware usage models require the capability for multiple data updates within any given page. These data updates occur via byte-writes without executing a preceding erase to the given page. Both the BIOS and Intel Converged Security Engine firmware multiple page write usage models apply to sequential and non-sequential data writes.

Flash parts must also support the writing of a single byte 1024 times in a single 256-byte page without erase. There will be 64 pages where this usage model will occur. These 64 pages will be every 16 kilobytes.

3.1.6 Hardware Sequencing Requirements

The following table contains a list of commands and the associated opcodes that a SPI-based serial flash device must support in order to be compatible with hardware sequencing.

Commands	OPCODE	Notes
Write to Status Register	01h	Writes a byte to SPI flash's status register. Enable Write to Status Register command must be run prior to this command
Program Data	02h	Single byte or 64 byte write as determined by flash part capabilities and software
Read Data	03h	
Write Disable	04h	
Read Status	05h	Outputs contents of SPI flash's status register
Write Enable	06h	
Fast Read	0Bh	
Enable Write to Status Register	06h	If write-status 01h requires a write-enable, then 06h must enable write-status.
Erase	Programmable/ Discoverable	4 Kbyte erase. Uses the value from SFDP (if available) else value from VSCCN Erase Opcode register value
Chip Erase	C7h and/or 60	
JEDEC ID	9Fh	See Section 3.1.4 for more information
Dual Output Fast Read	3Bh/ Discoverable	Discoverable opcodes are obtained from each component's SFDP table
Dual I/O Fast Read	Discoverable	Opcode is obtained from each component's SFDP table
Quad I/O Fast Read	Discoverable	Opcode is obtained from each component's SFDP table

|

§ §

|

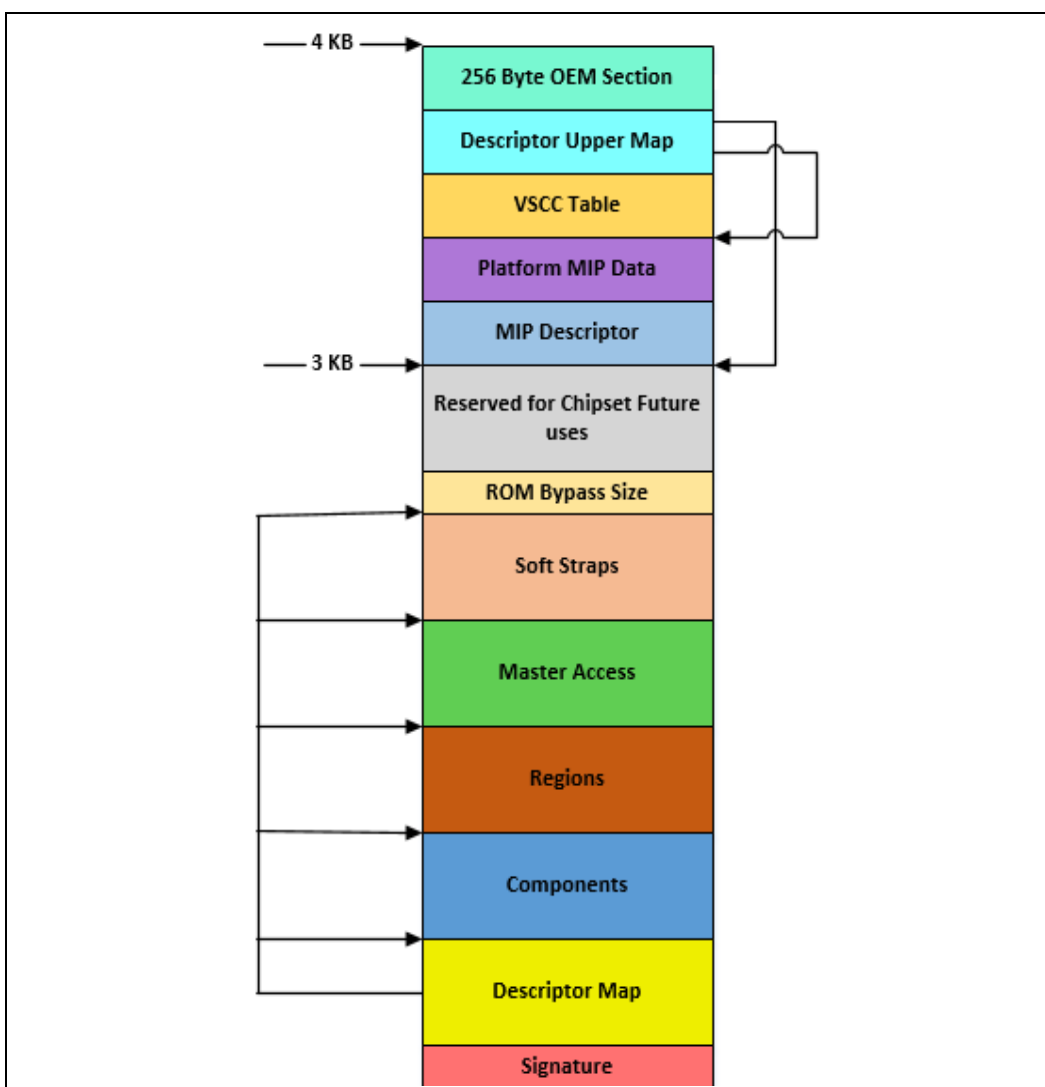
4 Descriptor

4.1 Flash Descriptor Overview

The Flash Descriptor is a data structure that is programmed on the SPI flash part on Elkhart Lake PCH based platforms. The Descriptor data structure describes the layout of the flash as well as defining configuration parameters for the PCH. The descriptor is on the SPI flash itself and is not in memory mapped space like PCH programming registers. The maximum size of the Flash Descriptor is 4 KBytes. It requires its own discrete erase block, so it may need greater than 4 KBytes of flash space depending on the flash architecture that is on the target system.

The information stored in the Flash Descriptor can only be written during the manufacturing process as its read/write permissions must be set to Read Only when the computer leaves the manufacturing floor.

Figure 4-1. Flash Descriptor (Elkhart Lake)



- The Flash signature at the bottom of the flash (offset 10h) must be 0FF0A55Ah in order to be in Descriptor mode.
- The Descriptor map has pointers to the lower five descriptor sections as well as the size of each.
- The Component section has information about the SPI flash part(s) the system. It includes the number of components, density of each component, read, write and erase frequencies and invalid instructions.
- The Region section defines the base and the limit of the BIOS, IFWI, PDR (Optional) regions as well as their size.
- The master region contains the hardware security settings for the flash, granting read/write permissions for each region and identifying each master.
- PCH chipset soft strap sections contain PCH configurable parameters.
- The Reserved region is for future chipset usage.
- The Descriptor Upper Map determines the length and base address of the Intel® CSE VSCC Table.
- The Intel® CSE VSCC Table holds the JEDEC ID and the Intel® CSE VSCC information for all the SPI Flash part(s) supported by the NVM image. BIOS write and erase capabilities depend on VSCC0 and VSCC1 registers in SPIBAR memory space.
- OEM Section is 256 Byte section reserved at the top of the Flash Descriptor for use by the OEM.

See ***SPI Supported Feature Overview*** and ***Flash Descriptor Records*** in the *External Design Specification (EDS)*.

4.2 Flash Descriptor Content

The following sections describe the data structure of the Flash Descriptor on the SPI device. These are not registers or memory space within PCH. FDBAR - is address 0x0 on the SPI flash device on chip select 0.

Recommended flash descriptor map:

Region Name	Starting Address
Signature	0x10
Component FCBA	0x30
Regions FRBA	0x40
Masters FMBA	0x80
PCH Straps FPSBA	0x100
MDTBA	0xC00
PMC Straps	0xC14
CPU Straps	0xC68
Intel® CSE Straps	0xC78
Register Init FIBA	0x340

4.2.1 Descriptor Signature and Map

4.2.1.1 FLVALSIG - Flash Valid Signature (Flash Descriptor Records)

Memory Address: FDBAR + 010h

Size: 32 bits

Recommended Value: 0FF0A55Ah

Bits	Description	FIT Visible
31:0	Flash Valid Signature. This field identifies the Flash Descriptor sector as valid. If the contents at this location contains 0FF0A55Ah, then the Flash Descriptor is considered valid and it will operate in Descriptor Mode (Note: Non-Descriptor mode is not supported).	No

4.2.1.2 FLMAP0 - Flash Map 0 Register (Flash Descriptor Records)

Memory Address: FDBAR + 014h

Size: 32 bits

Bits	Description	FIT Visible
31:27	Reserved	No
26:24	Reserved	No
23:16	Flash Region Base Address (FRBA). This identifies address bits [11:4] for the Region portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this value to 04h. This will define FRBA as 40h.	No
15:12	Reserved	No
11	Touch on dedicated SPI bus 0 = No Touch device is connected to the dedicated Touch SPI bus 1 = Touch device is connected to the dedicated Touch SPI bus Note: Hardware does not use this field. This value must be read directly from flash. It's not available via Host FDOC/FDOD registers.	Yes
10	Reserved	No
9:8	Number Of Components (NC). This field identifies the total number of Flash Components. Each supported Flash Component requires a separate chip select. 00 = 1 Component 01 = 2 Components All other settings = Reserved Note: With the introduction of DnX mode support, the flash controller ignores this descriptor field. It determines the number of attached flash components by virtue of SFDP discovery. Software may still use this field, therefore it must be properly initialized.	Yes
7:0	Flash Component Base Address (FCBA). This identifies address bits [11:4] for the Component portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. set this field to 03h. This will define FCBA as 30h	No

4.2.1.3 FLMAP1 - Flash Map 1 Register (Flash Descriptor Records)

Memory Address: FDBAR + 018h

Size: 32 bits

Bits	Description	FIT Visible
31:24	PCH Strap Length (PSL) . Identifies the 1s based number of Dwords of PCH Straps to be read, up to 255 DWs (1KB) max. A setting of all 0's indicates there are no PCH DW straps. This field MUST be set to 55h	No
23:16	Flash PCH Strap Base Address (FPSBA) . This identifies address bits [11:4] for the PCH Strap portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 10h. This will define FPSBA to 100h	No
15:11	Reserved	No
10:8	Number Of Masters (NM) . This field identifies the total number of Flash Masters. Note: This field is not used by the Flash Controller.	No
7:0	Flash Master Base Address (FMBA) . This identifies address bits [11:4] for the Master portion of the Flash Descriptor. Bits [24:12] and bits [3:0] are 0. Set this field to 08h. This will define FMBA as 80h	No

4.2.1.4 FLMAP2—Flash Map 2 Register (Flash Descriptor Records)

Memory Address: FDBAR + 01Ch

Size: 32 bits

Bits	Description	FIT Visible
31:24	Reserved	No
23:16	CPU Soft Strap Length Represents the total number of CPU Soft Strap Dwords Set to 0x11	No
15:12	Reserved	No
11:2	CPU Soft Strap Offset from PMC Base 4 bytes aligned -- Offset of CPU straps from PMC base i.e 0xC00 (MDTBA) CPU strap pointer = MDTBA + FLMAP[11:2] Set to 0x6C	No
1:0	Reserved	No

4.2.1.5 FLMAP3—Flash Map 3 Register (Flash Descriptor Records)

Memory Address: FDBAR + 020h

Size: 32 bits

Bits	Description	FIT Visible
31:21	Descriptor Major Revision ID	No
20:14	Descriptor Minor Revision ID	No

Bits	Description	FIT Visible
13:0	Reserved	No

4.2.2 Flash Descriptor Component Section

4.2.2.1 FLCOMP—Flash Components Register (Flash Descriptor Records)

The following section of the Flash Descriptor is used to identify the different SPI Flash Components and their capabilities.

Memory Address: FCBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30	Dual Output Fast Read Support 0 : Dual Output Fast Read is not supported 1 : Dual Output Fast Read is supported Notes: 1. This setting is no longer required.	No
29:27	Read ID and Read Status Clock Frequency. 001 = 50 MHz 100 = 33 MHz 101 = 20 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components.	Yes
26:24	Write and Erase Clock Frequency. 001 = 50 MHz 100 = 33 MHz 101 = 20 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components.	Yes
23:21	Fast Read Clock Frequency. This field identifies the frequency that can be used with the Fast Read instruction. This field is undefined if the Fast Read Support field is '0'. 001 = 50 MHz 100 = 33 MHz 101 = 20 MHz All other Settings = Reserved Notes: 1. If more than one Flash component exists, this field must be set to the lowest common frequency of the different Flash components.	Yes
20	Fast Read Support. 0 = Fast Read is not Supported 1 = Fast Read is supported If the Fast Read Support bit is a '1' and a device issues a Direct Read or issues a read command from the Hardware Sequencer and the length is greater than 4 bytes, then the SPI Flash instruction should be "Fast Read". If the Fast Read Support is a '0' or the length is 1-4 bytes, then the SPI Flash instruction should be "Read". Reads to the Flash Descriptor always use the Read command independent of the setting of this bit. Notes: 1. If more than one Flash component exists, this field can only be set to '1' if both components support Fast Read. 2. It is strongly recommended to set this bit to 1b	Yes
19:16	Reserved	No

Bits	Description	FIT Visible
15	Quad I/O Read Enable (QIORE): 0 = Quad I/O Read is disabled 1 = Quad I/O Read is enabled This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad I/O Read is controlled via the Flash Descriptor Component Section.	Yes
14	Quad Output Read Enable (QORE): 0 = Quad Output Read is disabled 1 = Quad Output Read is enabled This soft strap only has effect if Quad Output Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Quad Output Read is controlled via the Flash Descriptor Component Section.	Yes
13	Dual I/O Read Enable (DIORE): 0 = Dual I/O Read is disabled 1 = Dual I/O Read is enabled This soft strap only has effect if Dual I/O Read is discovered as supported via the SFDP If parameter table is not detected via SFDP, this bit has no effect and Dual Output I/O Read is controlled via the Flash Descriptor Component Section.	Yes
12	Dual Output Read Enable (DORE): 0 = Dual Output Read is disabled 1 = Dual Output Read is enabled This soft strap only has effect if Dual Output read is discovered as supported via the SFDP. If parameter table is not detected via SFDP, this bit has no effect and Dual Output Read is controlled via the Flash Descriptor Component Section.	Yes
11:10	Reserved	No
9:8	Reserved	No
7:4	Component 1 Density. (C1DEN) This field identifies the size of the 2nd Flash component connected directly to the PCH. If there is not 2nd Flash component, the contents of this field should be read as "1111b" 0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111- 1110 = Reserved Note: This field is defaulted to "1111b" after reset Note: C1DEN field will be ignored if FLMAPO.NC bit [9:8] is set to 00 i.e. 1 component only.	Yes

Bits	Description	FIT Visible
3:0	<p>Component 0 Density (CODEN). This field identifies the size of the 1st or only Flash component connected directly to the PCH.</p> <p>0000 = 512 KB 0001 = 1 MB 0010 = 2 MB 0011 = 4 MB 0100 = 8 MB 0101 = 16 MB 0110 = 32 MB 0111 - 1111 = Reserved</p> <p>Note: This field is defaulted to "0101b" (16MB) after reset.</p>	Yes

4.2.2.2 FLILL—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 004h

Size: 32 bits

Bits	Description	FIT Visible
31:24	Invalid Instruction 3. Default set to 0xAD See definition of Invalid Instruction 0	Yes
23:16	Invalid Instruction 2. Default set to 0x60 See definition of Invalid Instruction 0	Yes
15:8	Invalid Instruction 1. Default set to 0x42 See definition of Invalid Instruction 0	Yes
7:0	Invalid Instruction 0. Default set to 0x21 Note: Opcode for an instruction that the Flash Controller should protect against, such as Chip Erase. This byte should be set to 0 if there are no invalid instructions to protect against for this field. Opcodes programmed in the Software Sequencing Opcode Menu Configuration and Prefix-Opcode Configuration are not allowed to use any of the Invalid Instructions listed in this register.	Yes

4.2.2.3 FLILL1—Flash Invalid Instructions Register (Flash Descriptor Records)

Memory Address: FCBA + 008h

Size: 32 bits

Bits	Description	FIT Visible
31:24	Invalid Instruction 7. Default set to C7 See definition of Invalid Instruction 0	Yes
23:16	Invalid Instruction 6. Default set to 0xC4 See definition of Invalid Instruction 0	Yes
15:8	Invalid Instruction 5. Default set to 0xB9 See definition of Invalid Instruction 0	Yes

Bits	Description	FIT Visible
7:0	Invalid Instruction 4. Default set to 0xB7 See definition of Invalid Instruction 0	Yes

4.2.3 Flash Descriptor Region Section

The following section of the Flash Descriptor is used to identify the different Regions of the NVM image on the SPI flash.

Flash Regions:

- If a particular region is not using SPI Flash, the particular region should be disabled by setting the Region Base to all 1's, and the Region Limit to all 0's (base is higher than the limit)
- For each region except FLREG0, the Flash Controller must have a default Region Base of 7FFFh and the Region Limit to 0000h within the Flash Controller in case the Number of Regions specifies that a region is not used.

4.2.3.1 FLREG0—Flash Region 0 (Flash Descriptor) Register (Flash Descriptor Records)

Memory Address: FRBA + 000h

Size: 32 bits

Recommended Value: 00000000h

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> Set this field to 0b. This defines the ending address of descriptor as being FFFh. Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base. Note: Set this field to all 0s. This defines the descriptor address beginning at 0h.	No

4.2.3.2 FLREG1—Flash Region 1 (BIOS) Register (Flash Descriptor Records)

Memory Address: FRBA + 004h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> Must be set to 0000h if Intel® CSE ROM Bypass region is unused Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base. Note: If the BIOS region is not used, the Region Base must be programmed to 7FFFh	No

4.2.3.3 FLREG2—Flash Region 2 (IFWI / Intel® CSE ROM Bypass) Register (Flash Descriptor Records)

Memory Address: FRBA + 008h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> Ensure size is a correct reflection of IFWI size that will be used in the platform Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base.	No

4.2.3.4 FLREG4—Flash Region 4 (Platform Data) Register (Flash Descriptor Records)

Memory Address: FRBA + 010h

Size: 32 bits

Bits	Description	FIT Visible
31	Reserved	No
30:16	Region Limit. This specifies bits 26:12 of the ending address for this Region. Notes: <ol style="list-style-type: none"> 1. If PDR Region is not used, the Region Limit must be programmed to 0000h 2. Ensure BIOS region size is a correct reflection of actual BIOS image that will be used in the platform 3. Region limit address Bits[11:0] are assumed to be FFFh 	No
15	Reserved	No
14:0	Region Base. This specifies address bits 26:12 for the Region Base. Note: If the Platform Data region is not used, the Region Base must be programmed to 7FFFh	No

Note: Region 3 (FRBA + 00Ch) Region 6 (FRBA + 018h), Region 7 (FRBA + 01Ch), Region 8 (FRBA + 020h), Region 9 (FRBA + 024h), Region 10 (FRBA + 28h), Region 11 (FRBA + 2Ch), Region 12 (FRBA + 30h), Region 13 (FRBA + 34h), Region 14 (FRBA + 38h) and Region 15 (FRBA + 03Ch) are all reserved in client platform and should set to 7FFFh.

4.2.4 Flash Descriptor Master Section

4.2.4.1 FLMSTR1—Flash Master 1 (Host CPU/ BIOS)

Memory Address: FMBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31:20	Master Region Write Access: Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 21 and 26 are don't care as the primary master always has read/write permission to its primary region	Yes
19:8	Master Region Read Access: Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 9 and 14 are don't care as the primary master always read/write permission to its primary region.	Yes
7:4	Extended Region Write Access: Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes
3:0	Extended Region Read Access: Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes

4.2.4.2 FLMSTR2—Flash Master 2 (Intel® CSE)

Memory Address: FMBA + 004h

Size: 32 bits

Bits	Description	FIT Visible
31:20	Master Region Write Access: Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 22 is a don't care as the primary master always has read/write permission to its primary region	Yes
19:8	Master Region Read Access: Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 10 is a don't care as the primary master always read/write permission to its primary region.	Yes
7:4	Extended Region Write Access: Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes
3:0	Extended Region Read Access: Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	Yes

4.2.4.3 FLMSTR4—Flash Master 4 (Reserved)

Memory Address: FMBA + 00Ch

Size: 32 bits

Bits	Description	FIT Visible
31:20	Master Region Write Access: Each bit [31:20] corresponds to Regions [11:0]. If the bit is set, this master can erase and write that particular region through register accesses. Note: Bit 17 is a don't care as the primary master always has read/write permission to its primary region	No
19:8	Master Region Read Access: Each bit [19:8] corresponds to Regions [11:0]. If the bit is set, this master can read that particular region through register accesses. Note: Bit 13 is a don't care as the primary master always read/write permission to its primary region.	No

Bits	Description	FIT Visible
7:4	Extended Region Write Access: Each bit [7:4] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	No
3:0	Extended Region Read Access: Each bit [3:0] corresponds to Regions [15:12]. If the bit is set, this master can erase and write that particular region through register accesses.	No

4.2.5 PCH / CPU Softstraps

See Chapter 9, “Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section” for details.

4.2.6 Descriptor Upper Map Section

This section of the flash descriptor is used by Intel® CSE to find SPI VSCC information and MIP data.

4.2.6.1 FLUMAP1—Flash Upper Map 1 (Flash Descriptor Records)

Memory Address: FDBAR + EFCh

Size: 32 bits

Bits	Default	Description	FIT Visible
31:16	0xC1	MIP Descriptor Table Base Address (MDTBA) . This identifies base address bits [11:4] for the Platform Configuration Data Structure in the Flash Descriptor Bits [26:12] and bits [3:0] are 0.	No
23:16	0xFF	Reserved	No
15:8	0x1	Intel® CSE VSCC Table Length (VTL) . Identifies the 1s based number of DWORDS contained in the VSCC Table. Each SPI component entry in the table is 2 DWORDS long. Max recommended is 10 entries to allow for room for Platform Configuration Data (MIP)	No
7:0	0x1	Intel® CSE VSCC Table Base Address (VTBA) . This identifies address bits [11:4] for the VSCC Table portion of the Flash Descriptor. Bits [26:12] and bits [3:0] are 0.	No

4.2.6.2 IFWI / Intel® CSE ROM Bypass Size

Memory Address: FDBAR + C00h

Size: 32 bits

Bits	Default	Description	FIT Visible
31:0	0xFF	ROM BYPASS Size . ROM reads this value to determine the size of the region. Only applicable for A0 stepping.	No

4.2.6.3 MIP - Descriptor Table

Memory Address: FDBAR + MDTBA

Name	Offset	Size (bytes)	Description	FIT Visible
Number of Descriptors	0x0	2	Number of MIP blocks ('n') inside this MIP structure	Yes
Size of MIP	0x2	2	Size, in bytes, of this MIP structure (including the MDT structure)	Yes
Block 0 Type	0x4	2	Type of block 0. Can be one of the following: 0 = CSE (USB 2 PHY Configuration) 1 = PMC Soft Straps 2 = Reserved Note: In order to simplify handling a new block type can be defined for each usage	Yes
Block 0 Offset	0x6	2	Offset of block 0	Yes
Block 0 Length	0x8	2	Length of block 0 in bytes	Yes

Name	Offset	Size (bytes)	Description	FIT Visible
Block 0 Reserved	0xA	2	Must be 0	Yes
Block 1 Type	0xC	2	See Block 0 type	Yes
Block 1 Offset	0xE	2	Offset of block 1	Yes
Block 1 Length	0x10	2	Length of block 1 in bytes	Yes
Block 1 Reserved	0x12	2	Must be 0	Yes
.....				Yes
Block 'n' Type		2	See Block 0 type	Yes
Block 'n' Offset		2	Offset of block 'n'	Yes
Block 'n' Length		2	Length of block 'n' in bytes	Yes
Block 'n' Reserved		2	Must be 0	Yes

4.2.7 Intel® CSE Vendor Specific Component Capabilities Table

Entries in this table allow support for a SPI flash part for Intel Converged Security Engine capabilities including Intel® Active Management Technology.

Since Flash Partition Boundary Address (FPBA) has been removed, UVSCC and LVSCC has been replaced with VSCC0 and VSCC1 in Elkhart Lake. VSCC0 is for SPI component 0 and VSCC1 is for SPI component 1.

Each VSCC table entry is composed of two 32 bit fields: JEDEC IDn and the corresponding VSCCn value.

See 4.5 Intel® CSE Vendor-Specific Component Capabilities (Intel® CSE VSCC) Table for information on how to program individual entries.

4.2.7.1 JID0—JEDEC-ID 0 Register (Flash Descriptor Records)

Memory Address: VTBA + 000h

Size: 32 bits

Bits	Description	FIT Visible
31:24	Reserved	No
23:16	SPI Component Device ID 1. This field identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
15:8	SPI Component Device ID 0. This field identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
7:0	SPI Component Vendor ID. This field identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes

4.2.7.2 VSCC0—Vendor Specific Component Capabilities 0 (Flash Descriptor Records)

Memory Address: VTBA + 004h

Size: 32 bits

Note: VSCC0 applies to SPI flash that connected to CS0.

Bits	Description	FIT Visible
31:16	Reserved	No
15:8	Erase Opcode (EO) . This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.	No
7:5	Quad Enable Requirements (QER) 000 = Device does not have a QE bit. Device detects 1-1-4 and 1-4-4 reads based on instruction. DQ3 / HOLD# functions as hold during instruction phase. 001 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. Writing only one byte to the status register has the side effect of clearing status register 2, including the QE bit. The 100b code is used if writing one byte to the status register does not modify status register 2. 010 = QE is bit 6 of status register 1. It is set via Write Status with one data byte where bit 6 is one. It is cleared via Write Status with one data byte where bit 6 is zero. 011 = QE is bit 7 of status register 2. It is set via Write status register 2 instruction 3Eh with one data byte where bit 7 is one. It is cleared via Write status register 2 instruction 3Eh with one data byte where bit 7 is zero. The status register 2 is read using instruction 3Fh. 100 = QE is bit 1 of status register 2. It is set via Write Status with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. In contrast to the 001b code, writing one byte to the status register does not modify status register 2. 101 = QE is bit 1 of the status register 2. Status register 1 is read using Read Status instruction 05h. Status register 2 is read using instruction 35h. QE is set via Write Status instruction 01h with two data bytes where bit 1 of the second byte is one. It is cleared via Write Status with two data bytes where bit 1 of the second byte is zero. other = reserved Note: Please refer to Table note#1 below for details.	No
4:0	Reserved set to 00101b	No
Notes: 1. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's data sheet for exact requirements.		

4.2.7.3 JIDn—JEDEC-ID Register n (Flash Descriptor Records)

Memory Address: VTBA + (n*8)h

Size: 32 bits

"n" is an integer denoting the index of the Intel® CSE VSCC table. See **Table 4.1.7.1** for details.

4.2.7.4 VSCCn—Vendor Specific Component Capabilities n (Flash Descriptor Records)

Memory Address: VTBA + 0C4h + (n*8)h

Size: 32 bits

"n" is an integer denoting the index of the Intel® CSE VSCC table. See **Table 4.1.7.2** for details.

4.3 OEM Section

Memory Address: F00h

Size: 256 Bytes

256 Bytes are reserved at the top of the Flash Descriptor for use by the OEM. The information stored by the OEM can only be written during the manufacturing process as the Flash Descriptor read/write permissions must be set to Read Only when the computer leaves the manufacturing floor. The PCH Flash controller does not read this information. If no OEM data is stored in the OEM section, then programming the OEM section to all 1's (FFh) is suggested to reduce programming time.

4.4 Region Access Control

Regions of the flash can be protected from read or write access by setting a protection parameter in the Master section of the Descriptor. There are only two masters that have the ability to access other regions: CPU/BIOS, Intel® CSE Firmware software/driver running on CPU.

Table 4-1. Region Access Control Table Options

Master Read/Write Access		
Region (#)	CPU / BIOS	IFWI (Intel® CSE)
Descriptor (0)	Read Only	Read Only
BIOS (1)	CPU / BIOS can always read from and write to BIOS region prior to EOP	Not Accessible
IFWI / Intel® Converged Security Engine ROM Bypass (2)	Read / Write (BIOS Only)	Intel® CSE can always read from and write to IFWI region
PDR (4)	Not Accessible	Not Accessible
Notes: 1. The Region Access values listed above represent post manufacturing configuration only. 2. Descriptor and PDR region is not a master, so they will not have Master R/W access. 3. Descriptor should NOT have write access by any master in production systems. 4. PDR region should only have read and/or write access by CPU/Host. Intel® CSE should NOT have access to PDR region.		

4.4.1 Intel Recommended Permissions for Region Access

The following Intel recommended read/write permissions are necessary to secure Intel® CSE and Intel® CSE FW.

Table 4-2. Recommended Read/Write Permissions

Master Access	Descriptor Region Bit 0	BIOS Region Bit1	IFWI / Intel® CSE ROM Bypass Region Bit2	PDR Region Bit4
Intel® CSE read access	Y	N	Y	N
Intel® CSE read access	N	N	Y	N
BIOS read access	Y	Y	Y	‡
BIOS write access	N	Y	N	‡
Note: 1. ‡ = Host access to PDR is the discretion of the customer. Implementation of PDR is optional.				

The table below shows the values to be inserted into the Flash image tool. The values below will provide the access levels described in the table above.

Warning: Pre-configuring the flash image to Intel recommended read / write permission through the Intel® FIT tool and then flashing the resulting image will cause the platform to enter into end-of-manufacturing flow which will result in the FPFs being permanently set in the PCH if the platform is using production silicon and production Intel® CSE firmware with the PV bit set.

Table 4-3. Recommended Read/Write Settings for Platforms

	Intel® CSE	BIOS	EC
Read	0b 0000 0000 0000 1101 = 0x000D	0b 0000 0000 000‡ 1111 = 0x000F	0b 0000 0001 0000 0001 = 0x0101
Write	0b 0000 0000 0000 1100 = 0x0004	0b 0000 0000 000‡ 1010 = 0x00‡A	0b 0000 0001 0000 0000 = 0x0100
Note: 1. ‡ = Value dependent on if PDR is implemented and if Host access is desired			

4.4.2 Overriding Region Access

Once access Intel recommended Flash settings have been put into the flash descriptor, it may be necessary to update the Intel® CSE region with a Host program or write a new Flash descriptor.

Assert HDA_SDO Assert during the rising edge of PWROK to set the Flash descriptor override strap.

This strap should only be visible and available in manufacturing or during product development.

After this strap has been set you can use a host based flash programming tool like FPT to write/read any area of serial flash that is not protected by Protected Range Registers. Any area of flash protected by Protected range Registers will still NOT be writeable/readable.

See [6.3 SPI Protected Range Register Recommendations](#) for more details.

4.5 Intel® CSE Vendor-Specific Component Capabilities (Intel® CSE VSCC) Table

The Intel® CSE VSCC Table defines how the Intel® CSE will communicate with the installed SPI flash if there is no SFDP table found. This table is defined in the descriptor and is the responsibility of who puts together the NVM image. VSCCn registers are defined in memory space and must be set by BIOS. This table must define every flash part that is intended to be used. The size (number of max entries) of the table is defined in [4.2.6.1 FLUMAP1—Flash Upper Map 1 \(Flash Descriptor Records\)](#). Each Table entry is made of two parts: the JEDEC ID and VSCC setting.

Table 4-4. Jidn - JEDEC ID Portion of Intel® CSE VSCC Table

Bits	Description	FIT Visible
31:24	Reserved.	No
23:16	SPI Component Device ID 1: This identifies the second byte of the Device ID of the SPI Flash Component. This is the third byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
15:8	SPI Component Device ID 0: This identifies the first byte of the Device ID of the SPI Flash Component. This is the second byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes
7:0	SPI Component Vendor ID: This identifies the one byte Vendor ID of the SPI Flash Component. This is the first byte returned by the Read JEDEC-ID command (opcode 9Fh).	Yes

If using Flash Image Tool (FIT) refer to System Tools user guide in the Intel® CSE FW kit and the respective FW Bring up Guide on how to build the image. If not, refer to [4.2.6.1 FLUMAP1—Flash Upper Map 1 \(Flash Descriptor Records\)](#) thru [4.3 OEM Section](#).

4.5.1 How to Set a VSCC Entry in Intel® CSE VSCC Table for Elkhart Lake Platforms

VSCC0 needs to be programmed in instances where there is only SPI component in the system. When using an asymmetric flash component (part with two different sets of attributes based on address) VSCC0 and VSCC1 will need to be used. This includes if the system is intended to support both symmetric AND asymmetric SPI flash parts.

Refer to [4.5.2 Intel® CSE VSCC Table Settings for Elkhart Lake Family Systems](#).

See text below the table for explanation on how to determine Intel Converged Security Engine VSCC value.

Table 4-5. Vsccn – Vendor-Specific Component Capabilities Portion of the Elkhart Lake Platforms (Sheet 1 of 2)

Bits	Description	FIT Visible
31:16	Reserved	No
15:8	Erase Opcode (EO). This field must be programmed with the Flash erase instruction opcode that corresponds to the erase size that is in BES.	No

Table 4-5. Vscn – Vendor-Specific Component Capabilities Portion of the Elkhart Lake Platforms (Sheet 2 of 2)

Bits	Description	FIT Visible
7:5	Quad Enable Requirements (QER) 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). Note: Please refer to Table note#6 below for details.	No
4	Write Enable on Write Status (WEWS) 0 = 50h is the opcode used to unlock the status register on SPI flash if WSR (bit 3) is set to 1b. 1 = 06h is the opcode used to unlock the status register on SPI flash if WSR (bit 3) is set to 1b. Note: Please refer to Table Note #4 below for a description how this bit is used.	No
3	Write Status Required (WSR) 0 = No automatic write of 00h will be made to the SPI flash's status register) 1 = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase performed by Intel® CSE to the SPI flash. Note: Please refer to Table Note #5 below for a description how this bit is used.	No
2	Write Granularity (WG). 0 = 1 Byte 1 = 64 Bytes	No
1:0	Block/Sector Erase Size (BES). This field identifies the erasable sector size for all Flash components. 00 = 256 Bytes 01 = 4 K Bytes 10 = 8 K Bytes 11 = 64K Bytes	No
Notes: 1. Bit 3 (WEWS) and/or bit 4 (WSR) should not be set to '1' if there are non volatile bits in the SPI flash's status register. This may lead to premature flash wear out. 2. This is not an atomic (uninterrupted) sequence. The PCH will not wait for the status write to complete before issuing the next command, potentially causing SPI flash instructions to be disregarded by the SPI flash part. If the SPI flash component's status register is non-volatile, then BIOS should issue an atomic software sequence cycle to unlock the flash part. 3. If both bits 3 (WSR) and 4 (WEWS) are set to 1b, then sequence of 06h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Converged Security Engine firmware performs. 4. If bit 3 (WSR) is set to 1b and bit 4 (WEWS) is set to 0b then sequence of 50h 01h 00h is sent to unlock the SPI flash on EVERY write and erase that Intel Converged Security Engine firmware performs. 5. If bit 3 (WSR) is set to 0b and bit 4 (WEWS) is set to 0b or 1b then sequence of 60h is sent to unlock the SPI flash on EVERY write and erase that Processor. 6. The manufacturers information included in the QER list are for guidance purpose. Some manufacturer devices operate as shown in the table above. Check manufacturer's datasheet for exact requirements.		

Erase Opcode (EO) and Block/Sector Erase Size (BSES) should be set based on the flash part and the firmware on the platform. For Intel® CSE enabled platforms this should be 4 KB.

Write Status Required (WSR) or Write Enable on Write Status (WEWS) should be set on flash devices that require an opcode to enable a write to the status register. Intel® CSE Firmware will write a 00h to status register to unlock the flash part for every erase/write operation. If this bit is set on a flash part that has non-volatile bits in the status register then it may lead to pre-mature wear out of the flash.

- Set the **WSR** bit to 1b and **WEWS** to 0b if the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to SPI flash will bit 50h 01h 00h.
- Set the **WSR** bit to 1b AND **WEWS** bit to 1b if write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h 01h 00h.
- Set the **WSR** bit to 0b AND **WEWS** bit to 0b or 1b, if write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h
- **WSR or WEWS should be not be set on devices that use non volatile memory for their status register.** Setting this bit will cause operations to be ignored, which may cause undesired operation. Ask target flash vendor if this is the case for the target flash. See [6.1 Unlocking SPI Flash Device Protection for Elkhart Lake Platform](#) and [6.2 Locking SPI Flash via Status Register](#) for more information.

Erase Opcode (EO) and **Block/Sector Erase Size (BES)** should be set based on the flash part and the firmware on the platform.

Write Granularity (WG) bit should be set based on the capabilities of the flash device. If the flash part is capable of writing 1 to 64 bytes (or more) with the 02h command you can set this bit 0 or 1. Setting this bit high will result in faster write performance. If flash part only supports single byte write only, then set this bit to 0.

Bit ranges 31:16 and 7:5 are reserved and should set to all zeros.

4.5.2 Intel® CSE VSCC Table Settings for Elkhart Lake Family Systems

To understand general guidelines for BIOS VSCC settings on different SPI flash devices, please refer to **VSCCommn.bin Content application note** (VSCCommn_Hin Content.pdf under Flash Image Tool directory).

§ §

5 Serial Flash Discoverable Parameter (SFDP) Overview

5.1 Introduction

As the feature set of serial flash progresses, there is an increasing amount of divergence as individual vendors find different solution for adding new functionality such as speed and addressing.

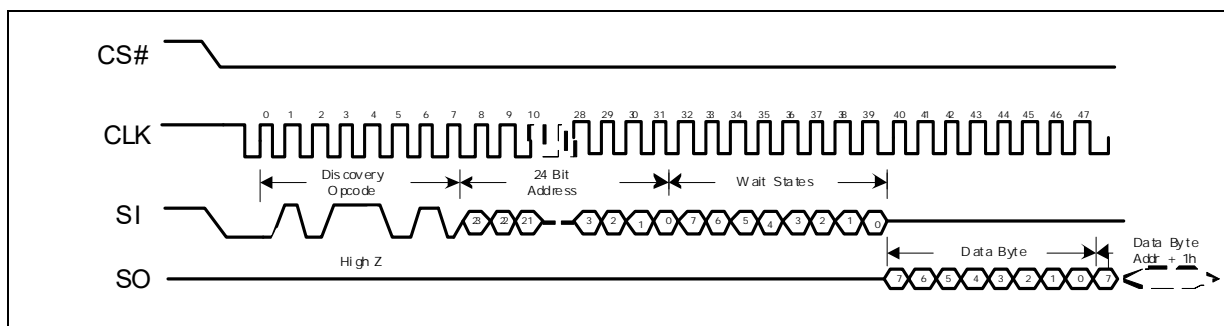
These guidelines are a standard that will allow for individual vendors to have their value add features, but will allow for a controller to discover the attributes needed to operate.

5.2 Discoverable Parameter Opcode and Flash Cycle

The discoverable parameter read opcode behaves like a fast read command. The opcode is 5Ah and the address cycle is 24 bit long. After the opcode 5Ah is clocked in, there are 24 bit of address clocked in. There will then be eight clock (8 wait states) before valid data is clocked out. There is flexibility in the number of wait states, but they must be byte aligned (multiple of 8 wait states).

SFDP read must update at a frequency between 14 MHz and 100 MHz with a single byte of wait state.

Figure 5-1. SFDP Read Instruction Sequence



5.3 Parameter Table Supported on PCH

The flash controller first checks for a valid SFDP header. The value of the major and minor revision fields in the SFDP header are don't care. If a valid SFDP header is found, the controller supports auto discovery of the Component Property Parameter Table (CPPT).

The following capabilities are only supported on PCH if CPPT is successfully discovered and parameter values indicate that they are supported. These capabilities are not supported as default.

- Quad I/O Read
- Quad Output Read

- Dual I/O read
- Dual Output Read
- Block /Sector Erase size

Note: If SFDP is valid and advertises 4 Kbyte erase capability, then BES is taken from the SFDP table, otherwise it is taken from the BIOS VCSS table.

PCH will also read the following opcode from parameter table and store to PCH if SFDP is valid and the following function is supported.

- Erase Opcode
- Dual Output Fast Read Opcode
- Dual I/O Fast Read Opcode
- Quad Output Fast Read Opcode
- Quad I/O Fast Read Opcode

5.4 Detailed JEDEC Specification

Please refer to www.jedec.com JESD216 for detailed SFDP specification on SPI.

§ §

6 Configuring BIOS for SPI Flash Access

6.1 Unlocking SPI Flash Device Protection for Elkhart Lake Platform

BIOS must account for any built in protection from the flash device itself. BIOS must ensure that any flash based protection will only apply to BIOS region only. It should not affect the Intel® CSE or GbE regions.

All the SPI flash devices that meet the SPI flash requirements in the *External Design Specification (EDS)* will be unlocked by writing a 00h to the SPI flash's status register. This command must be done via an atomic software sequencing to account for differences in flash architecture. Atomic cycles are uninterrupted in that it does not allow other commands to execute until a read status command returns a 'not busy' result from the flash.

Some flash vendors implement their status registers in NVM flash (non-volatile memory). This takes much more time than a write to volatile memory. During this write, the flash part will ignore all commands but a read to the status register (opcode 05h). The output of the read status register command will tell the PCH when the transaction is done.

Recommended flash unlocking sequence:

- Write enable (06h) command will have to be in the prefix opcode configuration register.
- The "write to status register" opcode (01h) will need to be an opcode menu configuration option.
- Opcode type for write to status register will be '01': a write cycle type with no address needed.
- The FDATA0 register should to be programmed to 0000 0000h.
- Data Byte Count (DBC) in Software Sequencing Flash Control register should be 000000b. Errors may occur if any non zero value is here.
- Set the Cycle Opcode Pointer (COP) to the "write to status register" opcode.
- Set to Sequence Prefix Opcode Pointer (SPOP) to Write Enable.
- Set the Data Cycle (DS) to 1.
- Set the Atomic Cycle Sequence (ACS) bit to 1.
- To execute sequence, set the SPI Cycle Go bit to 1.

Please see the ***Serial Peripheral Interface Memory Mapped Configuration Registers*** in the *External Design Specification (EDS)* for more detailed information.

6.2 Locking SPI Flash via Status Register

Flash vendors that implement their status register with non-volatile memory can be updated a limited number of times. This means that this register may wear out before the desired endurance for the rest of the flash. It is highly recommended that BIOS vendors and customers do NOT use the SPI flash's status register to protect the flash in multiple master systems.

BIOS should try to minimize the number of times that the system is locked and unlocked.

Care should be taken when using status register based SPI flash protection in multiple master systems such as Intel® CSE FW. BIOS must ensure that any flash based protection will apply to BIOS region only. It should not affect the Intel® CSE region.

Please contact your desired flash vendor to see if their status register protection bits volatile or non-volatile. Flash parts implemented with volatile systems do not have this concern.

6.3 SPI Protected Range Register Recommendations

The PCH has a mechanism to set up to 5 address ranges from HOST access. These are defined in PR0, PR1, PR2, PR3 and PR4 in the PCH EDS. These address ranges are NOT unlocked by assertion of Flash descriptor Override.

It is strongly recommended to use a protected range register to lock down the factory default portion of Intel® CSE FW region. The runtime portion should be left unprotected as to allow BIOS to update it.

It is strongly recommended that if Flash Descriptor Override strap (which can be checked by reading **FDOPSS (0b Flash Descriptor override is set, 1b not set) in PCH memory space (SPIBAR+ 4h bit 13))** is set, do not set a Protected range to cover the Intel® CSE FW factory defaults. This would allow a flashing of a complete image when the Flash descriptor Override strap is set.

6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits

6.4.1 Flash Configuration Lockdown

It is strongly recommended that BIOS sets the Host **Flash Configuration Lock-Down (FLOCKDN)** bits (located at SPIBAR + 04h and MBAR +04h respectively) to '1' on production platforms. If these bits are not set, it is possible to make register changes that can cause undesired host and Intel® CSE functionality as well as lead to unauthorized flash region access.

Refer to **HSFS— Hardware Sequencing Flash Status Register** in the Serial Peripheral Interface Memory Mapped Configuration Registers section and **HSFS— Hardware Sequencing Flash Status Register** in the SPI Flash Programming Registers section in the External Design Specification (EDS).

6.4.2 Vendor Component Lock

It is strongly recommended that BIOS sets the **Vendor Component Lock (VCL)** bits. These bits are located in the BIOS/GbE VSCC0 registers. VCL applies the lock to both VSCC0 and VSCC1 even if VSCC1 is not used. Without the VCL bits set, it is possible to make Host/GbE VSCC register(s) changes in that can cause undesired host and integrated GbE SPI flash functionality.

Refer to **VSCC— Vendor Specific Component Capabilities Register** in the *External Design Specification (EDS)* for more information.

6.5 Host Vendor Specific Component Control Registers (VSCC)

VSCC are memory mapped registers are used by the PCH when BIOS or Integrate LAN reads, programs or erases the SPI flash via Hardware sequencing.

Flash Partition Boundary Address (FBPBA) has been removed and UVSCC and LVSCC has been replaced with VSCC0 and VSCC1 in Elkhart Lake. VSCC0 is for SPI component 0 and VSCC1 is for SPI component 1. SPI controller will determine which VSCC (VSCC0 or VSCC1) to be used by comparing Flash Linear Address (FLA) with size of SPI component 0 (CODEN). When $FLA \leq CODEN$ then VSCC0 will be used; whereas $FLA > CODEN$ then VSCC1 will be used. If one SPI flash component used in the system, VSCC0 needs to be set.

Refer to **VSCC— Lower Vendor Specific Component Capabilities Register** and in the *External Design Specification (EDS)*.

See text below the tables for explanation on how to determine VSCC register values.

Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 1 of 3)

Bit	Description
31	Component Property Parameter Table Valid (CPPTV) - RO: This bit is set to a 1 if the Flash Controller detects a valid SFDP Component Property Parameter Table in SPI Component 0 If CPPTV bit is '0', software must configure the VSCC register appropriately. If CPPTV bit is '1', the corresponding parameter values discovered via SFDP will be used. In most cases, software is not required to configure the VSCC register. However, if the SFDP table indicates an erase size other than 4k byte, then the software is required to program the VSCC.EO register with the correct erase opcode.
30:24	Reserved
23	Vendor Component Lock (VCL): — RW/L: '0': The lock bit is not set '1': The Vendor Component Lock bit is set. This register locks itself when set. This bit applies to both VSCC0 and VSCC1 All bits locked by (VCL) will remained locked until a global reset.
22:16	Reserved

Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 2 of 3)

Bit	Description
15:8	<p>Erase Opcode (EO)— RW:</p> <p>This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. Software must program this register if the SFDP table for this component does not show 4 kByte erase capability</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: If CPPTV is 1 and the SPDP0 table shows 4k erase capability, the SFDP0 erase code is used instead of this register</p>
7:5	<p>Quad Enable Requirements (QER)</p> <p>000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx).</p> <p>001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion).</p> <p>010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix).</p> <p>011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel).</p> <p>100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond).</p> <p>Note: This register is locked by the Vendor Component Lock (VCL) bit.</p>
4	<p>Write Enable on Write Status (WEWS) — RW:</p> <p>'0' = 50h will be the opcode used to unlock the status register on the SPI flash if WSR (bit 3) is set to 1b.</p> <p>'1' = 06h will be the opcode used to unlock the status register on the SPI flash if WSR (bit 3) is set to 1b.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: Please refer to Table 6-3 for a description of how these bits is used.</p>
3	<p>Write Status Required (WSR) — RW:</p> <p>'0' = No automatic write of 00h will be made to the SPI flash's status register.</p> <p>'1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: Please refer to Table 6-3 for a description of how these bits is used.</p>
2	<p>Write Granularity (WG) — RW:</p> <p>0: 1 Byte</p> <p>1: 64 Byte</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Notes:</p> <ol style="list-style-type: none"> If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a feature in page writable SPI flash.

Table 6-1. VSCC0 - Vendor-Specific Component Capabilities Register for SPI Component 0 (Sheet 3 of 3)

Bit	Description
1:0	<p>Block/Sector Erase Size (BES)— RW: This field identifies the erasable sector size for Flash components. Valid Bit Settings: 00: 256 Byte 01: 4 KByte 10: 8 KByte 11: 64 K This register is locked by the Vendor Component Lock (VCL) bit. Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.</p>

Table 6-2. VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 (Sheet 1 of 2)

Bit	Description
31	<p>Component Property Parameter Table Valid (CPPTV) - RO: This bit is set to a 1 if the Flash Controller detects a valid SFDP Component Property Parameter Table in SPI Component 1 If CPPTV bit is '0', software must configure the VSCC register appropriately. If CPPTV bit is '1', the corresponding parameter values discovered via SFDP will be used. In most cases, software is not required to configure the VSCC register. However, if the SFDP table indicates an erase size other than 4k byte, then the software is required to program the VSCC.EO register with the correct erase opcode.</p>
30:16	Reserved
15:8	<p>Erase Opcode (EO)— RW: This register is programmed with the Flash erase instruction opcode required by the vendor's Flash component. This register is locked by the Vendor Component Lock (VCL) bit.</p>
7:5	<p>Quad Enable Requirements (QER) 000 = Part does not require a Quad Enable bit to be set, either because Quad is not supported or because the manufacturer permanently enables Quad capability (e.g. Micron, Numonyx). 001 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to status register clears all bits in register 2, therefore status register writes MUST be two bytes. If the status register is unlocked and SFDP bits WSR or VSCC WSR is 1 then SPI controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase. (e.g. Winbond, AMIC, Spansion). 010 = Part requires bit 6 of status register 1 to be set to enable quad IO. If the status register is unlocked and SFDP WSR bit or VSCC WSR is 1 then flash controller cannot use the quad output, quad IO features of this part because the hardware will automatically write one byte of zeros to status register with every write/erase (e.g. Macronix). 011 = Part requires bit 7 of the configuration register to be set to enable Quad (e.g. Atmel). 100 = Part requires bit 9 in status register 2 to be set to enable quad IO. Writing one byte to the status register does not clear the second byte (SST/Microchip, Winbond). Note: This register is locked by the Vendor Component Lock (VCL) bit.</p>
4	<p>Write Enable on Write to Status (WEWS) — RW: '0' = 50h will be the opcode used to unlock the status register if WSR (bit 3) is set to 1b. '1' = 06h will be the opcode used to unlock the status register if WSR (bit 3) is set to 1b. This register is locked by the Vendor Component Lock (VCL) bit. Please refer to Table 6-3 for a description of how these bits is used.</p>

Table 6-2. VSCC1 - Vendor Specific Component Capabilities Register for SPI Component 1 (Sheet 2 of 2)

Bit	Description
3	<p>Write Status Required (WSR) — RW:</p> <p>'0' = No automatic write of 00h will be made to the SPI flash's status register</p> <p>'1' = A write of 00h to the SPI flash's status register will be sent on EVERY write and erase to the SPI flash performed by Host and GbE.</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Note: Please refer to Table 6-3 for a description of how these bits is used.</p>
2	<p>Write Granularity (WG) — RW:</p> <p>0: 1 Byte</p> <p>1: 64 Byte</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>If more than one Flash component exists, this field must be set to the lowest common write granularity of the different Flash components.</p> <p>If using 64 B write, BIOS must ensure that multiple byte writes do not occur over 256 B boundaries. This will lead to corruption as the write will wrap around the page boundary on the SPI flash part. This is a feature in page writeable SPI flash.</p>
1:0	<p>Block/Sector Erase Size (BES)— RW: This field identifies the erasable sector size for all Flash components.</p> <p>Valid Bit Settings:</p> <p>00: 256 Byte</p> <p>01: 4 KByte</p> <p>10: 8 KByte</p> <p>11: 64 K</p> <p>This register is locked by the Vendor Component Lock (VCL) bit.</p> <p>Hardware takes no action based on the value of this register. The contents of this register are to be used only by software and can be read in the HSFSTS.BERASE register in both the BIOS and the GbE program registers if FLA is less than FPBA.</p>

Erase Opcode (EO) and **Block/Sector Erase Size (BSES)** should be set based on the flash part and the firmware on the platform.

- Either **Write Status Required (WSR)** or **Write Enable on Write Status (WEWS)** should be set on flash devices that require an opcode to enable a write to the status register. BIOS and GbE will write a 00h to the SPI flash's status register to unlock the flash part for every erase/write operation. If this bit is set on a flash part that has non-volatile bits in the status register then it may lead to pre-mature wear out of the flash and may result in undesired flash operation. Please refer to [Table 6-3](#) for a description of how these bits is set and what is the expected operation from the controller during erase/write operation.

Table 6-3. Description of How WSR and WEWS is Used

WSR	WEWS	Flash Operation
1b	0b	If the Enable Write Status Register opcode (50h) is needed to unlock the status register. Opcodes sequence sent to SPI flash will bit 50h 01h 00h.
1b	1b	If write enable (06h) will unlock the status register. Opcodes sequence sent to SPI flash will bit 06h 01h 00h.
0b	0 or 1b	Sequence of 60h is sent to unlock the SPI flash on EVERY write and erase that Processor or Intel GbE FW performs.

Note: **WSR or WEWS should be not be set on devices that use non volatile memory for their status register.** Setting this bit will cause operations to be ignored, which may cause undesired operation. Ask target flash vendor if this is the case for the target flash. See [6.1 Unlocking SPI Flash Device Protection for Elkhart Lake Platform](#) and [6.2 Locking SPI Flash via Status Register](#) for more information.

Write Granularity (WG) bit should be set based on the capabilities of the flash device. If the flash part is capable of writing 1 to 64 bytes (or more) with the 02h command you can set this bit 0 or 1. Setting this bit high will result in faster write performance. If flash part only supports single byte write only, then set this bit to 0. Setting this bit high requires that BIOS ensure that no multiple byte write operation does not cross a 256 Byte page boundary, as it will have unintended results. This is a feature of page programming capable flash parts.

Vendor Component Lock (VCL) should remain unlocked during development, but locked in shipping platforms. When **VCL** and **FLOCKDN** are set, it is possible that you may not be able to use in system programming methodologies including Intel Flash Programming Tool if programmed improperly. It will require a system reset to unlock this register and BIOS not to set this bits. See [6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits](#) for more details.

All reserved bits should set to zeros.

6.6 Host VSCC Register Settings

To understand general guidelines for VSCC settings with different SPI flash devices, please refer to **VSCCommn.bin content application note** (VSCCommn_Hin Content.pdf under Flash Image Tool directory). VSCCommn.bin contains SPI devices vendor ID, device ID and recommended VSCC values.

§ §

7 IFWI / Intel® CSE Disable for Debug/Flash Burning Purposes

This section is purely for debug purposes. Intel® CSE FW is the only supported configuration for Elkhart Lake based system.

7.1 IFWI / Intel® CSE Disable

Here are the ways one can disable the Intel® CSE for purposes of in system programming the flash.

1. HDA_SDO (Manufacturing mode jumper or Flash descriptor override jumper) asserted HIGH on the rising edge of PWROK. Power off or cold reset. Note: this is only valid as long as you do not specifically set the variable Flash Descriptor Override Pin-Strap Ignore in the Flash Image Tool to false.
2. HECI Intel® CSE region unlock - There is a HECI command that allows Intel® CSE FW to boot up in a temporarily disabled state and allows for a host program to overwrite the Intel® CSE region.

7.1.1 Erasing/Programming Intel® CSE Region

If CPU/Host has access to Intel® CSE region, then one could either erase/program the Intel® CSE region to all FFh. If there is no access, then one must assert HDA_SDO (Flash descriptor override strap) HIGH during the rising edge of PWROK. If there are Protected Range registers set, then you will not be able to program this w/o a BIOS option to turn off this protected range. (See [6.3 SPI Protected Range Register Recommendations](#)) for more detail.

This depends on the board booting HW defaults for clock configuration. If any clock configuration is required for booting the platform that is not in the HW defaults, then this option may not work for you.

FPT will automatically disable SPI writing by the Intel® CSE when erasing any address in IFWI region.

§ §

8 Recommendations for SPI Flash Programming in Manufacturing Environments

It is recommended that the Intel® CSE be disabled when you are programming the Intel® CSE region. Intel® CSE FW performs regular writes/erases to the Intel® CSE region. Therefore some bits may be changed after programming. Please note that not all of these options will be optimal for your manufacturing process.

Any method of programming SPI flash where the system is not powered will not result in any interference from Intel® CSE FW. The following methods are for Intel® CSE FW:

- Program via In Circuit Test – System is not fully powered here.
- Program via external flash burn-in solution.
- Assert HDA_SDO HIGH (Flash Descriptor Override Jumper) on the rising edge of PWROK. Note: this is only valid as long as you do not specifically disable this functionality in fixed offset variable.

§ §

9 Flash Descriptor PCH / PMC / CPU and Intel® CSE Configuration Section

The following section describes functionality and how to set soft strapping for a target platform. Improper setting of soft straps can lead to undesired operation and may lead to returns/recalls.

9.1 PCH Descriptor Record 0 (Flash Descriptor Records)

Flash Address: FPSBA + 000h

Default Flash Address: 100h

Offset from 0	Bits	Description	Usage	FIT Visible
0x100h	31:0	Reserved, set to '0x4'		No

9.2 PCH Descriptor Record 1 (Flash Descriptor Records)

Flash Address: FPSBA + 004h

Default Flash Address: 104h

Offset from 0	Bits	Description	Usage	FIT Visible
0x104h	7:0	Reserved, set to '0'		No

9.3 PCH Descriptor Record 2 (Flash Descriptor Records)

Flash Address: FPSBA + 005h

Default Flash Address: 105h

Offset from 0	Bits	Description	Usage	FIT Visible
0x105h	7:0	Reserved, set to '0'		No

9.4 PCH Descriptor Record 3 (Flash Descriptor Records)

Flash Address: FPSBA + 006h

Default Flash Address: 106h

Offset from 0	Bits	Description	Usage	FIT Visible
0x106h	7:0	Reserved, set to '0'		No

9.5 PCH Descriptor Record 4 (Flash Descriptor Records)

Flash Address: FPSBA + 007h

Default Flash Address: 107h

Offset from 0	Bits	Description	Usage	FIT Visible
0x107h	7:0	Reserved, set to '0'		No

9.6 PCH Descriptor Record 5 (Flash Descriptor Records)

Flash Address: FPSBA + 008h

Default Flash Address: 108h

Offset from 0	Bits	Description	Usage	FIT Visible
0x108h	7:5	Reserved, set to '0'		No
	4	Intel® SMBus ASD Mode Configuration (SMBALERTB): 0 = Configured as GP_C2 1 = Configured as Intel® SMBus ASD	This setting determines the native mode for the SMBAlert signal.	Yes
	3:2	Reserved, set to '0'		No
	1:0	SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0): 00 = PCIe Port 10 is statically assigned to SATA Port 0 01 = PCIe Port 10 is statically assigned to PCIe Note: This strap and the PCIe / SATA Combo Port 0 (FIA/LOSL10) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.		No

9.7 PCH Descriptor Record 6 (Flash Descriptor Records)

Flash Address: FPSBA + 009h

Default Flash Address: 109h

Offset from 0	Bits	Description	Usage	FIT Visible
0x109h	7:0	Reserved, set to '0'		No

9.8 PCH Descriptor Record 7 (Flash Descriptor Records)

Flash Address: FPSBA + 00Ah

Default Flash Address: 10Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ah	7	GP_C7 Individual Voltage Select (GPPC_C7_VCCIO): 0 = GP_C7 Voltage set to 3.3v 1 = GP_C7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C7 GPIO pin.	Yes
	6	GP_C6 Individual Voltage Select (GPPC_C6_VCCIO): 0 = GP_C6 Voltage set to 3.3v 1 = GP_C6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C6 GPIO pin.	Yes
	5	GP_C5 Individual Voltage Select (GPPC_C5_VCCIO): 0 = GP_C5 Voltage set to 3.3v 1 = GP_C5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C5 GPIO pin.	Yes
	4	GP_C4 Individual Voltage Select (GPPC_C4_VCCIO): 0 = GP_C4 Voltage set to 3.3v 1 = GP_C4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C4 GPIO pin.	Yes
	3	GP_C3 Individual Voltage Select (GPPC_C3_VCCIO): 0 = GP_C3 Voltage set to 3.3v 1 = GP_C3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C3 GPIO pin.	Yes
	2	GP_C2 Individual Voltage Select (GPPC_C2_VCCIO): 0 = GP_C2 Voltage set to 3.3v 1 = GP_C2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C2 GPIO pin.	Yes
	1	GP_C1 Individual Voltage Select (GPPC_C1_VCCIO): 0 = GP_C1 Voltage set to 3.3v 1 = GP_C1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C1 GPIO pin.	Yes
	0	GP_C0 Individual Voltage Select (GPPC_C0_VCCIO): 0 = GP_C0 Voltage set to 3.3v 1 = GP_C0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C0 GPIO pin.	Yes

9.9 PCH Descriptor Record 8 (Flash Descriptor Records)

Flash Address: FPSBA + 00Bh

Default Flash Address: 10Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Bh	7	GP_C15 Individual Voltage Select (GPPC_C15_VCCIO): 0 = GP_C15 Voltage set to 3.3v 1 = GP_C15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C15 GPIO pin.	Yes
	6	GP_C14 Individual Voltage Select (GPPC_C14_VCCIO): 0 = GP_C14 Voltage set to 3.3v 1 = GP_C14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C14 GPIO pin.	Yes
	5	GP_C13 Individual Voltage Select (GPPC_C13_VCCIO): 0 = GP_C13 Voltage set to 3.3v 1 = GP_C13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C13 GPIO pin.	Yes
	4	GP_C12 Individual Voltage Select (GPPC_C12_VCCIO): 0 = GP_C12 Voltage set to 3.3v 1 = GP_C12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C12 GPIO pin.	Yes
	3	GP_C11 Individual Voltage Select (GPPC_C11_VCCIO): 0 = GP_C11 Voltage set to 3.3v 1 = GP_C11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C11 GPIO pin.	Yes
	2	GP_C10 Individual Voltage Select (GPPC_C10_VCCIO): 0 = GP_C10 Voltage set to 3.3v 1 = GP_C10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C10 GPIO pin.	Yes
	1	GP_C9 Individual Voltage Select (GPPC_C9_VCCIO): 0 = GP_C9 Voltage set to 3.3v 1 = GP_C9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C9 GPIO pin.	Yes
	0	GP_C8 Individual Voltage Select (GPPC_C8_VCCIO): 0 = GP_C8 Voltage set to 3.3v 1 = GP_C8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C8 GPIO pin.	Yes

9.10 PCH Descriptor Record 9 (Flash Descriptor Records)

Flash Address: FPSBA + 00Ch

Default Flash Address: 10Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Ch	7	GP_C23 Individual Voltage Select (GPPC_C23_VCCIO): 0 = GP_C23 Voltage set to 3.3v 1 = GP_C23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C23 GPIO pin.	Yes
	6	GP_C22 Individual Voltage Select (GPPC_C22_VCCIO): 0 = GP_C22 Voltage set to 3.3v 1 = GP_C22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C22 GPIO pin.	Yes
	5	GP_C21 Individual Voltage Select (GPPC_C21_VCCIO): 0 = GP_C21 Voltage set to 3.3v 1 = GP_C21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C21 GPIO pin.	Yes
	4	GP_C20 Individual Voltage Select (GPPC_C20_VCCIO): 0 = GP_C20 Voltage set to 3.3v 1 = GP_C20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C20 GPIO pin.	Yes
	3	GP_C19 Individual Voltage Select (GPPC_C19_VCCIO): 0 = GP_C16 Voltage set to 3.3v 1 = GP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C19 GPIO pin.	Yes
	2	GP_C18 Individual Voltage Select (GPPC_C18_VCCIO): 0 = GP_C16 Voltage set to 3.3v 1 = GP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C18 GPIO pin.	Yes
	1	GP_C17 Individual Voltage Select (GPPC_C17_VCCIO): 0 = GP_C16 Voltage set to 3.3v 1 = GP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C17 GPIO pin.	Yes
	0	GP_C16 Individual Voltage Select (GPPC_C16_VCCIO): 0 = GP_C16 Voltage set to 3.3v 1 = GP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_C16 GPIO pin.	Yes

9.11 PCH Descriptor Record 10 (Flash Descriptor Records)

Flash Address: FPSBA + 00Dh

Default Flash Address: 10Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Dh	7	GP_E7 Individual Voltage Select (GPPC_E7_VCCIO): 0 = GP_C16 Voltage set to 3.3v 1 = GP_C16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E7 GPIO pin.	Yes
	6	GP_E6 Individual Voltage Select (GPPC_E6_VCCIO): 0 = GP_E6 Voltage set to 3.3v 1 = GP_E6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E6 GPIO pin.	Yes
	5	GP_E5 Individual Voltage Select (GPPC_E5_VCCIO): 0 = GP_E5 Voltage set to 3.3v 1 = GP_E5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E5 GPIO pin.	Yes
	4	GP_E4 Individual Voltage Select (GPPC_E4_VCCIO): 0 = GP_E4 Voltage set to 3.3v 1 = GP_E4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E4 GPIO pin.	Yes
	3	GP_E3 Individual Voltage Select (GPPC_E3_VCCIO): 0 = GP_E3 Voltage set to 3.3v 1 = GP_E3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E3 GPIO pin.	Yes
	2	GP_E2 Individual Voltage Select (GPPC_E2_VCCIO): 0 = GP_E2 Voltage set to 3.3v 1 = GP_E2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E2 GPIO pin.	Yes
	1	GP_E1 Individual Voltage Select (GPPC_E1_VCCIO): 0 = GP_E1 Voltage set to 3.3v 1 = GP_E1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E1 GPIO pin.	Yes
	0	GP_E0 Individual Voltage Select (GPPC_E0_VCCIO): 0 = GP_E0 Voltage set to 3.3v 1 = GP_E0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E0 GPIO pin.	Yes

9.12 PCH Descriptor Record 11 (Flash Descriptor Records)

Flash Address: FPSBA + 00Eh

Default Flash Address: 10Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Eh	7	GP_E15 Individual Voltage Select (GPPC_E15_VCCIO): 0 = GP_E15 Voltage set to 3.3v 1 = GP_E15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E15 GPIO pin.	Yes
	6	GP_E14 Individual Voltage Select (GPPC_E14_VCCIO): 0 = GP_E14 Voltage set to 3.3v 1 = GP_E14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E14 GPIO pin.	Yes
	5	GP_E13 Individual Voltage Select (GPPC_E13_VCCIO): 0 = GP_E13 Voltage set to 3.3v 1 = GP_E13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E13 GPIO pin.	Yes
	4	GP_E12 Individual Voltage Select (GPPC_E12_VCCIO): 0 = GP_E12 Voltage set to 3.3v 1 = GP_E12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E12 GPIO pin.	Yes
	3	GP_E11 Individual Voltage Select (GPPC_E11_VCCIO): 0 = GP_E11 Voltage set to 3.3v 1 = GP_E11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E11 GPIO pin.	Yes
	2	GP_E10 Individual Voltage Select (GPPC_E10_VCCIO): 0 = GP_E10 Voltage set to 3.3v 1 = GP_E10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E10 GPIO pin.	Yes
	1	GP_E9 Individual Voltage Select (GPPC_E9_VCCIO): 0 = GP_E9 Voltage set to 3.3v 1 = GP_E9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E9 GPIO pin.	Yes
	0	GP_E8 Individual Voltage Select (GPPC_E8_VCCIO): 0 = GP_E8 Voltage set to 3.3v 1 = GP_E8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E8 GPIO pin.	Yes

9.13 PCH Descriptor Record 12 (Flash Descriptor Records)

Flash Address: FPSBA + 00Fh

Default Flash Address: 10Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x10Fh	7	GP_E23 Individual Voltage Select (GPPC_E23_VCCIO): 0 = GP_E23 Voltage set to 3.3v 1 = GP_E23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E23 GPIO pin.	Yes
	6	GP_E22 Individual Voltage Select (GPPC_E22_VCCIO): 0 = GP_E22 Voltage set to 3.3v 1 = GP_E22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E22 GPIO pin.	Yes
	5	GP_E21 Individual Voltage Select (GPPC_E21_VCCIO): 0 = GP_E21 Voltage set to 3.3v 1 = GP_E21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E21 GPIO pin.	Yes
	4	GP_E20 Individual Voltage Select (GPPC_E20_VCCIO): 0 = GP_E20 Voltage set to 3.3v 1 = GP_E20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E20 GPIO pin.	Yes
	3	GP_E19 Individual Voltage Select (GPPC_E19_VCCIO): 0 = GP_E19 Voltage set to 3.3v 1 = GP_E19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E19 GPIO pin.	Yes
	2	GP_E18 Individual Voltage Select (GPPC_E18_VCCIO): 0 = GP_E18 Voltage set to 3.3v 1 = GP_E18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E18 GPIO pin.	Yes
	1	GP_E17 Individual Voltage Select (GPPC_E17_VCCIO): 0 = GP_E17 Voltage set to 3.3v 1 = GP_E17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E17 GPIO pin.	Yes
	0	GP_E16 Individual Voltage Select (GPPC_E16_VCCIO): 0 = GP_E16 Voltage set to 3.3v 1 = GP_E16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_E16 GPIO pin.	Yes

9.14 PCH Descriptor Record 13 (Flash Descriptor Records)

Flash Address: FPSBA + 010h

Default Flash Address: 110h

Offset from 0	Bits	Description	Usage	FIT Visible
0x110h	7	GP_F7 Individual Voltage Select (GPPC_F7_VCCIO): 0 = GP_F7 Voltage set to 3.3v 1 = GP_F7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F7 GPIO pin.	Yes
	6	GP_F6 Individual Voltage Select (GPPC_F6_VCCIO): 0 = GP_F6 Voltage set to 3.3v 1 = GP_F6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F6 GPIO pin.	Yes
	5	GP_F5 Individual Voltage Select (GPPC_F5_VCCIO): 0 = GP_F5 Voltage set to 3.3v 1 = GP_F5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F5 GPIO pin.	Yes
	4	GP_F4 Individual Voltage Select (GPPC_F4_VCCIO): 0 = GP_F4 Voltage set to 3.3v 1 = GP_F4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F4 GPIO pin.	Yes
	3	GP_F3 Individual Voltage Select (GPPC_F3_VCCIO): 0 = GP_F3 Voltage set to 3.3v 1 = GP_F3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F3 GPIO pin.	Yes
	2	GP_F2 Individual Voltage Select (GPPC_F2_VCCIO): 0 = GP_F2 Voltage set to 3.3v 1 = GP_F2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F2 GPIO pin.	Yes
	1	GP_F1 Individual Voltage Select (GPPC_F1_VCCIO): 0 = GP_F1 Voltage set to 3.3v 1 = GP_F1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F1 GPIO pin.	Yes
	0	GP_F0 Individual Voltage Select (GPPC_F0_VCCIO): 0 = GP_F0 Voltage set to 3.3v 1 = GP_F0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F0 GPIO pin.	Yes

9.15 PCH Descriptor Record 14 (Flash Descriptor Records)

Flash Address: FPSBA + 011h

Default Flash Address: 111h

Offset from 0	Bits	Description	Usage	FIT Visible
0x111h	7	GP_F15 Individual Voltage Select (GPPC_F15_VCCIO): 0 = GP_F15 Voltage set to 3.3v 1 = GP_F15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F15 GPIO pin.	Yes
	6	GP_F14 Individual Voltage Select (GPPC_F14_VCCIO): 0 = GP_F14 Voltage set to 3.3v 1 = GP_F14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F14 GPIO pin.	Yes
	5	GP_F13 Individual Voltage Select (GPPC_F13_VCCIO): 0 = GP_F13 Voltage set to 3.3v 1 = GP_F13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F13 GPIO pin.	Yes
	4	GP_F12 Individual Voltage Select (GPPC_F12_VCCIO): 0 = GP_F12 Voltage set to 3.3v 1 = GP_F12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F12 GPIO pin.	Yes
	3	GP_F11 Individual Voltage Select (GPPC_F11_VCCIO): 0 = GP_F11 Voltage set to 3.3v 1 = GP_F11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F11 GPIO pin.	Yes
	2	GP_F10 Individual Voltage Select (GPPC_F10_VCCIO): 0 = GP_F10 Voltage set to 3.3v 1 = GP_F10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F10 GPIO pin.	Yes
	1	GP_F9 Individual Voltage Select (GPPC_F9_VCCIO): 0 = GP_F9 Voltage set to 3.3v 1 = GP_F9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F9 GPIO pin.	Yes
	0	GP_F8 Individual Voltage Select (GPPC_F8_VCCIO): 0 = GP_F8 Voltage set to 3.3v 1 = GP_F8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F8 GPIO pin.	Yes

9.16 PCH Descriptor Record 15 (Flash Descriptor Records)

Flash Address: FPSBA + 012h

Default Flash Address: 112h

Offset from 0	Bits	Description	Usage	FIT Visible
0x112h	7	GP_F23 Individual Voltage Select (GPPC_F23_VCCIO): 0 = GP_F23 Voltage set to 3.3v 1 = GP_F23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F23 GPIO pin.	Yes
	6	GP_F22 Individual Voltage Select (GPPC_F22_VCCIO): 0 = GP_F22 Voltage set to 3.3v 1 = GP_F22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F22 GPIO pin.	Yes
	5	GP_F21 Individual Voltage Select (GPPC_F21_VCCIO): 0 = GP_F21 Voltage set to 3.3v 1 = GP_F21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F21 GPIO pin.	Yes
	4	GP_F20 Individual Voltage Select (GPPC_F20_VCCIO): 0 = GP_F20 Voltage set to 3.3v 1 = GP_F20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F20 GPIO pin.	Yes
	3	GP_F19 Individual Voltage Select (GPPC_F19_VCCIO): 0 = GP_F19 Voltage set to 3.3v 1 = GP_F19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F19 GPIO pin.	Yes
	2	GP_F18 Individual Voltage Select (GPPC_F18_VCCIO): 0 = GP_F18 Voltage set to 3.3v 1 = GP_F18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F18 GPIO pin.	Yes
	1	GP_F17 Individual Voltage Select (GPPC_F17_VCCIO): 0 = GP_F17 Voltage set to 3.3v 1 = GP_F17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F17 GPIO pin.	Yes
	0	GP_F16 Individual Voltage Select (GPPC_F16_VCCIO): 0 = GP_F16 Voltage set to 3.3v 1 = GP_F16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_F16 GPIO pin.	Yes

9.17 PCH Descriptor Record 16 (Flash Descriptor Records)

Flash Address: FPSBA + 013h

Default Flash Address: 113h

Offset from 0	Bits	Description	Usage	FIT Visible
0x113h	7:0	Reserved, set to '0'		No

9.18 PCH Descriptor Record 17 (Flash Descriptor Records)

Flash Address: FPSBA + 014h

Default Flash Address: 114h

Offset from 0	Bits	Description	Usage	FIT Visible
0x114h	7:0	Reserved, set to '0'		No

9.19 PCH Descriptor Record 18 (Flash Descriptor Records)

Flash Address: FPSBA + 015h

Default Flash Address: 115h

Offset from 0	Bits	Description	Usage	FIT Visible
0x115h	7:0	Reserved, set to '0'		No

9.20 PCH Descriptor Record 19 (Flash Descriptor Records)

Flash Address: FPSBA + 016h

Default Flash Address: 116h

Offset from 0	Bits	Description	Usage	FIT Visible
0x116h	7	GP_A7 Individual Voltage Select (GPPC_A7_VCCIO): 0 = GP_A7 Voltage set to 3.3v 1 = GP_A7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A7 GPIO pin.	Yes
	6	GP_A6 Individual Voltage Select (GPPC_A6_VCCIO): 0 = GP_A6 Voltage set to 3.3v 1 = GP_A6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A6 GPIO pin.	Yes
	5	GP_A5 Individual Voltage Select (GPPC_A5_VCCIO): 0 = GP_A5 Voltage set to 3.3v 1 = GP_A5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A5 GPIO pin.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x116h (Cont)	4	GP_A4 Individual Voltage Select (GPPC_A4_VCCIO): 0 = GP_A4 Voltage set to 3.3v 1 = GP_A4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A4 GPIO pin.	Yes
	3	GP_A3 Individual Voltage Select (GPPC_A3_VCCIO): 0 = GP_A3 Voltage set to 3.3v 1 = GP_A3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A3 GPIO pin.	Yes
	2	GP_A2 Individual Voltage Select (GPPC_A2_VCCIO): 0 = GP_A2 Voltage set to 3.3v 1 = GP_A2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A2 GPIO pin.	Yes
	1	GP_A1 Individual Voltage Select (GPPC_A1_VCCIO): 0 = GP_A1 Voltage set to 3.3v 1 = GP_A1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A1 GPIO pin.	Yes
	0	GP_A0 Individual Voltage Select (GPPC_A0_VCCIO): 0 = GP_A0 Voltage set to 3.3v 1 = GP_A0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A0 GPIO pin.	Yes

9.21 PCH Descriptor Record 20 (Flash Descriptor Records)

Flash Address: FPSBA + 017h

Default Flash Address: 117h

Offset from 0	Bits	Description	Usage	FIT Visible
0x117h	7	GP_A15 Individual Voltage Select (GPPC_A15_VCCIO): 0 = GP_A15 Voltage set to 3.3v 1 = GP_A15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A15 GPIO pin.	Yes
	6	GP_A14 Individual Voltage Select (GPPC_A14_VCCIO): 0 = GP_A14 Voltage set to 3.3v 1 = GP_A14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A14 GPIO pin.	Yes
	5	GP_A13 Individual Voltage Select (GPPC_A13_VCCIO): 0 = GP_A13 Voltage set to 3.3v 1 = GP_A13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A13 GPIO pin.	Yes
	4	GP_A12 Individual Voltage Select (GPPC_A12_VCCIO): 0 = GP_A12 Voltage set to 3.3v 1 = GP_A12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A13 GPIO pin.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x117h (Cont)	3	GP_A11 Individual Voltage Select (GPPC_A11_VCCIO): 0 = GP_A11 Voltage set to 3.3v 1 = GP_A11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A11 GPIO pin.	Yes
	2	GP_A10 Individual Voltage Select (GPPC_A10_VCCIO): 0 = GP_A10 Voltage set to 3.3v 1 = GP_A10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A10 GPIO pin.	Yes
	1	GP_A9 Individual Voltage Select (GPPC_A9_VCCIO): 0 = GP_A9 Voltage set to 3.3v 1 = GP_A9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A9 GPIO pin.	Yes
	0	GP_A8 Individual Voltage Select (GPPC_A8_VCCIO): 0 = GP_A8 Voltage set to 3.3v 1 = GP_A8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A8 GPIO pin.	Yes

9.22 PCH Descriptor Record 21 (Flash Descriptor Records)

Flash Address: FPSBA + 018h

Default Flash Address: 118h

Offset from 0	Bits	Description	Usage	FIT Visible
0x118h	7	GP_A23 Individual Voltage Select (GPPC_A23_VCCIO): 0 = GP_A23 Voltage set to 3.3v 1 = GP_A23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A23 GPIO pin.	Yes
	6	GP_A22 Individual Voltage Select (GPPC_A22_VCCIO): 0 = GP_A22 Voltage set to 3.3v 1 = GP_A22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A22 GPIO pin.	Yes
	5	GP_A21 Individual Voltage Select (GPPC_A21_VCCIO): 0 = GP_A21 Voltage set to 3.3v 1 = GP_A21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A21 GPIO pin.	Yes
	4	GP_A20 Individual Voltage Select (GPPC_A20_VCCIO): 0 = GP_A20 Voltage set to 3.3v 1 = GP_A20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A20 GPIO pin.	Yes
	3	GP_A19 Individual Voltage Select (GPPC_A19_VCCIO): 0 = GP_A19 Voltage set to 3.3v 1 = GP_A19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A19 GPIO pin.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x118h (Cont)	2	GP_A18 Individual Voltage Select (GPPC_A18_VCCIO): 0 = GP_A18 Voltage set to 3.3v 1 = GP_A18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A18 GPIO pin.	Yes
	1	GP_A17 Individual Voltage Select (GPPC_A17_VCCIO): 0 = GP_A17 Voltage set to 3.3v 1 = GP_A17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A17 GPIO pin.	Yes
	0	GP_A16 Individual Voltage Select (GPPC_A16_VCCIO): 0 = GP_A16 Voltage set to 3.3v 1 = GP_A16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_A16 GPIO pin.	Yes

9.23 PCH Descriptor Record 22 (Flash Descriptor Records)

Flash Address: FPSBA + 019h

Default Flash Address: 119h

Offset from 0	Bits	Description	Usage	FIT Visible
0x119h	7:0	Reserved, set to '0'		No

9.24 PCH Descriptor Record 23 (Flash Descriptor Records)

Flash Address: FPSBA + 01Ah

Default Flash Address: 11Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ah	7:0	Reserved, set to '0'		No

9.25 PCH Descriptor Record 24 (Flash Descriptor Records)

Flash Address: FPSBA + 01Bh

Default Flash Address: 11Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Bh	7:0	Reserved, set to '0'		No

9.26 PCH Descriptor Record 25 (Flash Descriptor Records)

Flash Address: FPSBA + 01Ch

Default Flash Address: 11Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Ch	7:6	Reserved, set to '0'		No
	5	SLP_S5# / GDP10 Signal Configuration: 0b = Use as SLP_S5# 1b = Use as GPD10		Yes
	4:2	Reserved, set to '0x6'		No
	1	SLP_S4# / GPD5 Signal Configuration: 0b = Use as SLP_S4# 1b = Use as GPD5		Yes
	0	SLP_S3# / GPD4 Signal Configuration: 0b = Use as SLP_S3# 1b = Use as GPD4		Yes

9.27 PCH Descriptor Record 26 (Flash Descriptor Records)

Flash Address: FPSBA + 01Dh

Default Flash Address: 11Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Dh	7:0	Reserved, set to '0'		No

9.28 PCH Descriptor Record 27 (Flash Descriptor Records)

Flash Address: FPSBA + 01Eh

Default Flash Address: 11Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Eh	7:0	Reserved, set to '0'		No

9.29 PCH Descriptor Record 28 (Flash Descriptor Records)

Flash Address: FPSBA + 01Fh

Default Flash Address: 11Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x11Fh	7:0	Reserved, set to '0'		No

9.30 PCH Descriptor Record 29 (Flash Descriptor Records)

Flash Address: FPSBA + 020h

Default Flash Address: 120h

Offset from 0	Bits	Description	Usage	FIT Visible
0x120h	7:0	Reserved, set to '0'		No

9.31 PCH Descriptor Record 30 (Flash Descriptor Records)

Flash Address: FPSBA + 021h

Default Flash Address: 121h

Offset from 0	Bits	Description	Usage	FIT Visible
0x121h	7:0	Reserved, set to '0'		No

9.32 PCH Descriptor Record 31 (Flash Descriptor Records)

Flash Address: FPSBA + 022h

Default Flash Address: 122h

Offset from 0	Bits	Description	Usage	FIT Visible
0x122h	7	GP_D7 Individual Voltage Select (GPPC_D7_VCCIO): 0 = GP_D7 Voltage set to 3.3v 1 = GP_D7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D7 GPIO pin.	Yes
	6	GP_D6 Individual Voltage Select (GPPC_D6_VCCIO): 0 = GP_D6 Voltage set to 3.3v 1 = GP_D6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D6 GPIO pin.	Yes
	5	GP_D5 Individual Voltage Select (GPPC_D5_VCCIO): 0 = GP_D5 Voltage set to 3.3v 1 = GP_D5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D5 GPIO pin.	Yes
	4	GP_D4 Individual Voltage Select (GPPC_D4_VCCIO): 0 = GP_D4 Voltage set to 3.3v 1 = GP_D4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D4 GPIO pin.	Yes
	3	GP_D3 Individual Voltage Select (GPPC_D3_VCCIO): 0 = GP_D3 Voltage set to 3.3v 1 = GP_D3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D3 GPIO pin.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x122h (Cont)	2	GP_D2 Individual Voltage Select (GPPC_D2_VCCIO): 0 = GP_D2 Voltage set to 3.3v 1 = GP_D2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D2 GPIO pin.	Yes
	1	GP_D1 Individual Voltage Select (GPPC_D1_VCCIO): 0 = GP_D1 Voltage set to 3.3v 1 = GP_D1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D1 GPIO pin.	Yes
	0	GP_D0 Individual Voltage Select (GPPC_D0_VCCIO): 0 = GP_D0 Voltage set to 3.3v 1 = GP_D0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D0 GPIO pin.	Yes

9.33 PCH Descriptor Record 32 (Flash Descriptor Records)

Flash Address: FPSBA + 023h

Default Flash Address: 123h

Offset from 0	Bits	Description	Usage	FIT Visible
0x123h	7	GP_D15 Individual Voltage Select (GPPC_D15_VCCIO): 0 = GP_D15 Voltage set to 3.3v 1 = GP_D15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D15 GPIO pin.	Yes
	6	GP_D14 Individual Voltage Select (GPPC_D14_VCCIO): 0 = GP_D14 Voltage set to 3.3v 1 = GP_D14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D14 GPIO pin.	Yes
	5	GP_D13 Individual Voltage Select (GPPC_D13_VCCIO): 0 = GP_D13 Voltage set to 3.3v 1 = GP_D13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D13 GPIO pin.	Yes
	4	GP_D12 Individual Voltage Select (GPPC_D12_VCCIO): 0 = GP_D12 Voltage set to 3.3v 1 = GP_D12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D12 GPIO pin.	Yes
	3	GP_D11 Individual Voltage Select (GPPC_D11_VCCIO): 0 = GP_D11 Voltage set to 3.3v 1 = GP_D11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D11 GPIO pin.	Yes
	2	GP_D10 Individual Voltage Select (GPPC_D10_VCCIO): 0 = GP_D10 Voltage set to 3.3v 1 = GP_D10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D10 GPIO pin.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x123h (Cont)	1	GP_D9 Individual Voltage Select (GPPC_D9_VCCIO): 0 = GP_D9 Voltage set to 3.3v 1 = GP_D9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D9 GPIO pin.	Yes
	0	GP_D8 Individual Voltage Select (GPPC_D8_VCCIO): 0 = GP_D8 Voltage set to 3.3v 1 = GP_D8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D8 GPIO pin.	Yes

9.34 PCH Descriptor Record 33 (Flash Descriptor Records)

Flash Address: FPSBA + 024h

Default Flash Address: 124h

Offset from 0	Bits	Description	Usage	FIT Visible
0x124h	7:4	Reserved, set to '0'		No
	3	GP_D19 Individual Voltage Select (GPPC_D19_VCCIO): 0 = GP_D19 Voltage set to 3.3v 1 = GP_D19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D19 GPIO pin.	Yes
	2	GP_D18 Individual Voltage Select (GPPC_D18_VCCIO): 0 = GP_D18 Voltage set to 3.3v 1 = GP_D18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D18 GPIO pin.	Yes
	1	GP_D17 Individual Voltage Select (GPPC_D17_VCCIO): 0 = GP_D17 Voltage set to 3.3v 1 = GP_D17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D17 GPIO pin.	Yes
	0	GP_D16 Individual Voltage Select (GPPC_D16_VCCIO): 0 = GP_D16 Voltage set to 3.3v 1 = GP_D16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_D16 GPIO pin.	Yes

9.35 PCH Descriptor Record 34 (Flash Descriptor Records)

Flash Address: FPSBA + 025h

Default Flash Address: 125h

Offset from 0	Bits	Description	Usage	FIT Visible
0x125h	7	GP_H7 Individual Voltage Select (GPPC_H7 VCCIO): 0 = GP_H7 Voltage set to 3.3v 1 = GP_H7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H7 GPIO pin.	Yes
	6	GP_H6 Individual Voltage Select (GPPC_H6 VCCIO): 0 = GP_H6 Voltage set to 3.3v 1 = GP_H6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H6 GPIO pin.	Yes
	5	GP_H5 Individual Voltage Select (GPPC_H5 VCCIO): 0 = GP_H5 Voltage set to 3.3v 1 = GP_H5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H5 GPIO pin.	Yes
	4	GP_H4 Individual Voltage Select (GPPC_H4 VCCIO): 0 = GP_H4 Voltage set to 3.3v 1 = GP_H4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H4 GPIO pin.	Yes
	3	GP_H3 Individual Voltage Select (GPPC_H3 VCCIO): 0 = GP_H3 Voltage set to 3.3v 1 = GP_H3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H3 GPIO pin.	Yes
	2	GP_H2 Individual Voltage Select (GPPC_H2 VCCIO): 0 = GP_H2 Voltage set to 3.3v 1 = GP_H2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H2 GPIO pin.	Yes
	1	GP_H1 Individual Voltage Select (GPPC_H1 VCCIO): 0 = GP_H1 Voltage set to 3.3v 1 = GP_H1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H1 GPIO pin.	Yes
	0	GP_H0 Individual Voltage Select (GPPC_H0 VCCIO): 0 = GP_H0 Voltage set to 3.3v 1 = GP_H0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H0 GPIO pin.	Yes

9.36 PCH Descriptor Record 35 (Flash Descriptor Records)

Flash Address: FPSBA + 026h

Default Flash Address: 126h

Offset from 0	Bits	Description	Usage	FIT Visible
0x126h	7	GP_H15 Individual Voltage Select (GPPC_H15 VCCIO): 0 = GP_H15 Voltage set to 3.3v 1 = GP_H15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H15 GPIO pin.	Yes
	6	GP_H14 Individual Voltage Select (GPPC_H14 VCCIO): 0 = GP_H14 Voltage set to 3.3v 1 = GP_H14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H14 GPIO pin.	Yes
	5	GP_H13 Individual Voltage Select (GPPC_H13 VCCIO): 0 = GP_H13 Voltage set to 3.3v 1 = GP_H13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H13 GPIO pin.	Yes
	4	GP_H12 Individual Voltage Select (GPPC_H12 VCCIO): 0 = GP_H12 Voltage set to 3.3v 1 = GP_H12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H12 GPIO pin.	Yes
	3	GP_H11 Individual Voltage Select (GPPC_H11 VCCIO): 0 = GP_H11 Voltage set to 3.3v 1 = GP_H11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H11 GPIO pin.	Yes
	2	GP_H10 Individual Voltage Select (GPPC_H10 VCCIO): 0 = GP_H10 Voltage set to 3.3v 1 = GP_H10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H10 GPIO pin.	Yes
	1	GP_H9 Individual Voltage Select (GPPC_H9 VCCIO): 0 = GP_H9 Voltage set to 3.3v 1 = GP_H9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H9 GPIO pin.	Yes
	0	GP_H8 Individual Voltage Select (GPPC_H8 VCCIO): 0 = GP_H8 Voltage set to 3.3v 1 = GP_H8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H8 GPIO pin.	Yes

9.37 PCH Descriptor Record 36 (Flash Descriptor Records)

Flash Address: FPSBA + 027h

Default Flash Address: 127h

Offset from 0	Bits	Description	Usage	FIT Visible
0x127h	7	GP_H23 Individual Voltage Select (GPPC_H23 VCCIO): 0 = GP_H23 Voltage set to 3.3v 1 = GP_H23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H23 GPIO pin.	Yes
	6	GP_H22 Individual Voltage Select (GPPC_H22 VCCIO): 0 = GP_H22 Voltage set to 3.3v 1 = GP_H22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H22 GPIO pin.	Yes
	5	GP_H21 Individual Voltage Select (GPPC_H21 VCCIO): 0 = GP_H21 Voltage set to 3.3v 1 = GP_H21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H21 GPIO pin.	Yes
	4	GP_H20 Individual Voltage Select (GPPC_H20 VCCIO): 0 = GP_H20 Voltage set to 3.3v 1 = GP_H20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H20 GPIO pin.	Yes
	3	GP_H19 Individual Voltage Select (GPPC_H19 VCCIO): 0 = GP_H19 Voltage set to 3.3v 1 = GP_H19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H19 GPIO pin.	Yes
	2	GP_H18 Individual Voltage Select (GPPC_H18 VCCIO): 0 = GP_H18 Voltage set to 3.3v 1 = GP_H18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H18 GPIO pin.	Yes
	1	GP_H17 Individual Voltage Select (GPPC_H17 VCCIO): 0 = GP_H17 Voltage set to 3.3v 1 = GP_H17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H17 GPIO pin.	Yes
	0	GP_H16 Individual Voltage Select (GPPC_H16 VCCIO): 0 = GP_H16 Voltage set to 3.3v 1 = GP_H16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_H16 GPIO pin.	Yes

9.38 PCH Descriptor Record 37 (Flash Descriptor Records)

Flash Address: FPSBA + 028h

Default Flash Address: 128h

Offset from 0	Bits	Description	Usage	FIT Visible
0x128h	7	GP_U7 Individual Voltage Select (GPPC_U7 VCCIO): 0 = GP_U7 Voltage set to 3.3v 1 = GP_U7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U7 GPIO pin.	Yes
	6	GP_U6 Individual Voltage Select (GPPC_U6 VCCIO): 0 = GP_U6 Voltage set to 3.3v 1 = GP_U6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U6 GPIO pin.	Yes
	5	GP_U5 Individual Voltage Select (GPPC_U5 VCCIO): 0 = GP_U5 Voltage set to 3.3v 1 = GP_U5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U5 GPIO pin.	Yes
	4	GP_U4 Individual Voltage Select (GPPC_U4 VCCIO): 0 = GP_U4 Voltage set to 3.3v 1 = GP_U4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U4 GPIO pin.	Yes
	3	GP_U3 Individual Voltage Select (GPPC_U3 VCCIO): 0 = GP_U3 Voltage set to 3.3v 1 = GP_U3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U3 GPIO pin.	Yes
	2	GP_U2 Individual Voltage Select (GPPC_U2 VCCIO): 0 = GP_U2 Voltage set to 3.3v 1 = GP_U2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U2 GPIO pin.	Yes
	1	GP_U1 Individual Voltage Select (GPPC_U1 VCCIO): 0 = GP_U1 Voltage set to 3.3v 1 = GP_U1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U1 GPIO pin.	Yes
	0	GP_U0 Individual Voltage Select (GPPC_U0 VCCIO): 0 = GP_U0 Voltage set to 3.3v 1 = GP_U0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U0 GPIO pin.	Yes

9.39 PCH Descriptor Record 38 (Flash Descriptor Records)

Flash Address: FPSBA + 029h

Default Flash Address: 129h

Offset from 0	Bits	Description	Usage	FIT Visible
0x129h	7	GP_U15 Individual Voltage Select (GPPC_U15 VCCIO): 0 = GP_U15 Voltage set to 3.3v 1 = GP_U15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U15 GPIO pin.	Yes
	6	GP_U14 Individual Voltage Select (GPPC_U14 VCCIO): 0 = GP_U14 Voltage set to 3.3v 1 = GP_U14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U14 GPIO pin.	Yes
	5	GP_U13 Individual Voltage Select (GPPC_U13 VCCIO): 0 = GP_U13 Voltage set to 3.3v 1 = GP_U13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U13 GPIO pin.	Yes
	4	GP_U12 Individual Voltage Select (GPPC_U12 VCCIO): 0 = GP_U12 Voltage set to 3.3v 1 = GP_U12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U12 GPIO pin.	Yes
	3	GP_U11 Individual Voltage Select (GPPC_U11 VCCIO): 0 = GP_U11 Voltage set to 3.3v 1 = GP_U11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U11 GPIO pin.	Yes
	2	GP_U10 Individual Voltage Select (GPPC_U10 VCCIO): 0 = GP_U10 Voltage set to 3.3v 1 = GP_U10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U10 GPIO pin.	Yes
	1	GP_U9 Individual Voltage Select (GPPC_U9 VCCIO): 0 = GP_U9 Voltage set to 3.3v 1 = GP_U9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U9 GPIO pin.	Yes
	0	GP_U8 Individual Voltage Select (GPPC_U8 VCCIO): 0 = GP_U8 Voltage set to 3.3v 1 = GP_U8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U8 GPIO pin.	Yes

9.40 PCH Descriptor Record 39 (Flash Descriptor Records)

Flash Address: FPSBA + 02Ah

Default Flash Address: 12Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ah	7:4	Reserved, set to '0'		No
	3	GP_U19 Individual Voltage Select (GPPC_U19 VCCIO): 0 = GP_U19 Voltage set to 3.3v 1 = GP_U19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U19 GPIO pin.	Yes
	2	GP_U18 Individual Voltage Select (GPPC_U18 VCCIO): 0 = GP_U18 Voltage set to 3.3v 1 = GP_U18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U18 GPIO pin.	Yes
	1	GP_U17 Individual Voltage Select (GPPC_U17 VCCIO): 0 = GP_U17 Voltage set to 3.3v 1 = GP_U17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U17 GPIO pin.	Yes
	0	GP_U16 Individual Voltage Select (GPPC_U16 VCCIO): 0 = GP_U16 Voltage set to 3.3v 1 = GP_U16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_U16 GPIO pin.	Yes

9.41 PCH Descriptor Record 40 (Flash Descriptor Records)

Flash Address: FPSBA + 02Bh

Default Flash Address: 12Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Bh	7:0	Reserved, set to '0'		No

9.42 PCH Descriptor Record 41 (Flash Descriptor Records)

Flash Address: FPSBA + 02Ch

Default Flash Address: 12Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Ch	7:2	Reserved, set to '0'		No
	1:0	SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1): 00 = PCIe Port 11 is statically assigned to SATA Port 1 01 = PCIe Port 11 is statically assigned to PCIe	This strap must also be configured when setting the PCIe / SATA Combo Port 1 Strap (FIA/LOSL11). Note: This strap and the PCIe / SATA Combo Port 1 Strap (FIA/LOSL11) and (SATA_PCIE_SP1) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

9.43 PCH Descriptor Record 42 (Flash Descriptor Records)

Flash Address: FPSBA + 02Dh

Default Flash Address: 12Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Dh	7:0	Reserved, set to '0'		No

9.44 PCH Descriptor Record 43 (Flash Descriptor Records)

Flash Address: FPSBA + 02Eh

Default Flash Address: 12Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Eh	7	GP_B7 Individual Voltage Select (GPPC_B7 VCCIO): 0 = GP_B7 Voltage set to 3.3v 1 = GP_B7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B7 GPIO pin.	Yes
	6	GP_B6 Individual Voltage Select (GPPC_B6 VCCIO): 0 = GP_B6 Voltage set to 3.3v 1 = GP_B6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B6 GPIO pin.	Yes
	5	GP_B5 Individual Voltage Select (GPPC_B5 VCCIO): 0 = GP_B5 Voltage set to 3.3v 1 = GP_B5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B5 GPIO pin.	Yes
	4	GP_B4 Individual Voltage Select (GPPC_B4 VCCIO): 0 = GP_B4 Voltage set to 3.3v 1 = GP_B4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B4 GPIO pin.	Yes
	3	GP_B3 Individual Voltage Select (GPPC_B3 VCCIO): 0 = GP_B3 Voltage set to 3.3v 1 = GP_B3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B3 GPIO pin.	Yes
	2	GP_B2 Individual Voltage Select (GPPC_B2 VCCIO): 0 = GP_B2 Voltage set to 3.3v 1 = GP_B2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B2 GPIO pin.	Yes
	1	GP_B1 Individual Voltage Select (GPPC_B1 VCCIO): 0 = GP_B1 Voltage set to 3.3v 1 = GP_B1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B1 GPIO pin.	Yes
	0	GP_B0 Individual Voltage Select (GPPC_B0 VCCIO): 0 = GP_B0 Voltage set to 3.3v 1 = GP_B0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B0 GPIO pin.	Yes

9.45 PCH Descriptor Record 44 (Flash Descriptor Records)

Flash Address: FPSBA + 02Fh

Default Flash Address: 12Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x12Fh	7	GP_B15 Individual Voltage Select (GPPC_B15 VCCIO): 0 = GP_B15 Voltage set to 3.3v 1 = GP_B15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B15 GPIO pin.	Yes
	6	GP_B14 Individual Voltage Select (GPPC_B14 VCCIO): 0 = GP_B14 Voltage set to 3.3v 1 = GP_B14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B14 GPIO pin.	Yes
	5	GP_B13 Individual Voltage Select (GPPC_B13 VCCIO): 0 = GP_B13 Voltage set to 3.3v 1 = GP_B13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B13 GPIO pin.	Yes
	4	GP_B12 Individual Voltage Select (GPPC_B12 VCCIO): 0 = GP_B12 Voltage set to 3.3v 1 = GP_B12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B12 GPIO pin.	Yes
	3	GP_B11 Individual Voltage Select (GPPC_B11 VCCIO): 0 = GP_B11 Voltage set to 3.3v 1 = GP_B11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B11 GPIO pin.	Yes
	2	GP_B10 Individual Voltage Select (GPPC_B10 VCCIO): 0 = GP_B10 Voltage set to 3.3v 1 = GP_B10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B10 GPIO pin.	Yes
	1	GP_B9 Individual Voltage Select (GPPC_B9 VCCIO): 0 = GP_B9 Voltage set to 3.3v 1 = GP_B9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B9 GPIO pin.	Yes
	0	GP_B8 Individual Voltage Select (GPPC_B8 VCCIO): 0 = GP_B8 Voltage set to 3.3v 1 = GP_B8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B8 GPIO pin.	Yes

9.46 PCH Descriptor Record 45 (Flash Descriptor Records)

Flash Address: FPSBA + 030h

Default Flash Address: 130h

Offset from 0	Bits	Description	Usage	FIT Visible
0x130h	7	GP_B23 Individual Voltage Select (GPPC_B23 VCCIO): 0 = GP_B23 Voltage set to 3.3v 1 = GP_B23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B23 GPIO pin.	Yes
	6	GP_B22 Individual Voltage Select (GPPC_B22 VCCIO): 0 = GP_B22 Voltage set to 3.3v 1 = GP_B22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B22 GPIO pin.	Yes
	5	GP_B21 Individual Voltage Select (GPPC_B21 VCCIO): 0 = GP_B21 Voltage set to 3.3v 1 = GP_B21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B21 GPIO pin.	Yes
	4	GP_B20 Individual Voltage Select (GPPC_B20 VCCIO): 0 = GP_B20 Voltage set to 3.3v 1 = GP_B20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B20 GPIO pin.	Yes
	3	GP_B19 Individual Voltage Select (GPPC_B19 VCCIO): 0 = GP_B19 Voltage set to 3.3v 1 = GP_B19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B19 GPIO pin.	Yes
	2	GP_B18 Individual Voltage Select (GPPC_B18 VCCIO): 0 = GP_B18 Voltage set to 3.3v 1 = GP_B18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B18 GPIO pin.	Yes
	1	GP_B17 Individual Voltage Select (GPPC_B17 VCCIO): 0 = GP_B17 Voltage set to 3.3v 1 = GP_B17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B17 GPIO pin.	Yes
	0	GP_B16 Individual Voltage Select (GPPC_B16 VCCIO): 0 = GP_B16 Voltage set to 3.3v 1 = GP_B16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_B16 GPIO pin.	Yes

9.47 PCH Descriptor Record 46 (Flash Descriptor Records)

Flash Address: FPSBA + 031h

Default Flash Address: 131h

Offset from 0	Bits	Description	Usage	FIT Visible
0x131h	7	GP_T7 Individual Voltage Select (GPPC_T7 VCCIO): 0 = GP_T7 Voltage set to 3.3v 1 = GP_T7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T7 GPIO pin.	Yes
	6	GP_T6 Individual Voltage Select (GPPC_T6 VCCIO): 0 = GP_T6 Voltage set to 3.3v 1 = GP_T6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T6 GPIO pin.	Yes
	5	GP_T5 Individual Voltage Select (GPPC_T5 VCCIO): 0 = GP_T5 Voltage set to 3.3v 1 = GP_T5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T5 GPIO pin.	Yes
	4	GP_T4 Individual Voltage Select (GPPC_T4 VCCIO): 0 = GP_T4 Voltage set to 3.3v 1 = GP_T4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T4 GPIO pin.	Yes
	3	GP_T3 Individual Voltage Select (GPPC_T3 VCCIO): 0 = GP_T3 Voltage set to 3.3v 1 = GP_T3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T3 GPIO pin.	Yes
	2	GP_T2 Individual Voltage Select (GPPC_T2 VCCIO): 0 = GP_T2 Voltage set to 3.3v 1 = GP_T2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T2 GPIO pin.	Yes
	1	GP_T1 Individual Voltage Select (GPPC_T1 VCCIO): 0 = GP_T1 Voltage set to 3.3v 1 = GP_T1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T1 GPIO pin.	Yes
	0	GP_T0 Individual Voltage Select (GPPC_T0 VCCIO): 0 = GP_T0 Voltage set to 3.3v 1 = GP_T0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T0 GPIO pin.	Yes

9.48 PCH Descriptor Record 47 (Flash Descriptor Records)

Flash Address: FPSBA + 032h

Default Flash Address: 132h

Offset from 0	Bits	Description	Usage	FIT Visible
0x132h	7	GP_T15 Individual Voltage Select (GPPC_T15 VCCIO): 0 = GP_T15 Voltage set to 3.3v 1 = GP_T15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T15 GPIO pin.	Yes
	6	GP_T14 Individual Voltage Select (GPPC_T14 VCCIO): 0 = GP_T14 Voltage set to 3.3v 1 = GP_T14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T14 GPIO pin.	Yes
	5	GP_T13 Individual Voltage Select (GPPC_T13 VCCIO): 0 = GP_T13 Voltage set to 3.3v 1 = GP_T13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T13 GPIO pin.	Yes
	4	GP_T12 Individual Voltage Select (GPPC_T12 VCCIO): 0 = GP_T12 Voltage set to 3.3v 1 = GP_T12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T12 GPIO pin.	Yes
	3	GP_T11 Individual Voltage Select (GPPC_T11 VCCIO): 0 = GP_T11 Voltage set to 3.3v 1 = GP_T11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T11 GPIO pin.	Yes
	2	GP_T10 Individual Voltage Select (GPPC_T10 VCCIO): 0 = GP_T10 Voltage set to 3.3v 1 = GP_T10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T10 GPIO pin.	Yes
	1	GP_T9 Individual Voltage Select (GPPC_T9 VCCIO): 0 = GP_T9 Voltage set to 3.3v 1 = GP_T9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T9 GPIO pin.	Yes
	0	GP_T8 Individual Voltage Select (GPPC_T8 VCCIO): 0 = GP_T8 Voltage set to 3.3v 1 = GP_T8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_T8 GPIO pin.	Yes

9.49 PCH Descriptor Record 48 (Flash Descriptor Records)

Flash Address: FPSBA + 033h

Default Flash Address: 133h

Offset from 0	Bits	Description	Usage	FIT Visible
0x133h	7	GP_G7 Individual Voltage Select (GPPC_G7 VCCIO): 0 = GP_G7 Voltage set to 3.3v 1 = GP_G7 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G7 GPIO pin.	Yes
	6	GP_G6 Individual Voltage Select (GPPC_G6 VCCIO): 0 = GP_G6 Voltage set to 3.3v 1 = GP_G6 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G6 GPIO pin.	Yes
	5	GP_G5 Individual Voltage Select (GPPC_G5 VCCIO): 0 = GP_G5 Voltage set to 3.3v 1 = GP_G5 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G5 GPIO pin.	Yes
	4	GP_G4 Individual Voltage Select (GPPC_G4 VCCIO): 0 = GP_G4 Voltage set to 3.3v 1 = GP_G4 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G4 GPIO pin.	Yes
	3	GP_G3 Individual Voltage Select (GPPC_G3 VCCIO): 0 = GP_G3 Voltage set to 3.3v 1 = GP_G3 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G3 GPIO pin.	Yes
	2	GP_G2 Individual Voltage Select (GPPC_G2 VCCIO): 0 = GP_G2 Voltage set to 3.3v 1 = GP_G2 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G2 GPIO pin.	Yes
	1	GP_G1 Individual Voltage Select (GPPC_G1 VCCIO): 0 = GP_G1 Voltage set to 3.3v 1 = GP_G1 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G1 GPIO pin.	Yes
	0	GP_G0 Individual Voltage Select (GPPC_G0 VCCIO): 0 = GP_G0 Voltage set to 3.3v 1 = GP_G0 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G0 GPIO pin.	Yes

9.50 PCH Descriptor Record 49 (Flash Descriptor Records)

Flash Address: FPSBA + 034h

Default Flash Address: 134h

Offset from 0	Bits	Description	Usage	FIT Visible
0x134h	7	GP_G15 Individual Voltage Select (GPPC_G15 VCCIO): 0 = GP_G15 Voltage set to 3.3v 1 = GP_G15 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G15 GPIO pin.	Yes
	6	GP_G14 Individual Voltage Select (GPPC_G14 VCCIO): 0 = GP_G14 Voltage set to 3.3v 1 = GP_G14 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G14 GPIO pin.	Yes
	5	GP_G13 Individual Voltage Select (GPPC_G13 VCCIO): 0 = GP_G13 Voltage set to 3.3v 1 = GP_G13 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G13 GPIO pin.	Yes
	4	GP_G12 Individual Voltage Select (GPPC_G12 VCCIO): 0 = GP_G12 Voltage set to 3.3v 1 = GP_G12 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G12 GPIO pin.	Yes
	3	GP_G11 Individual Voltage Select (GPPC_G11 VCCIO): 0 = GP_G11 Voltage set to 3.3v 1 = GP_G11 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G11 GPIO pin.	Yes
	2	GP_G10 Individual Voltage Select (GPPC_G10 VCCIO): 0 = GP_G10 Voltage set to 3.3v 1 = GP_G10 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G10 GPIO pin.	Yes
	1	GP_G9 Individual Voltage Select (GPPC_G9 VCCIO): 0 = GP_G9 Voltage set to 3.3v 1 = GP_G9 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G9 GPIO pin.	Yes
	0	GP_G8 Individual Voltage Select (GPPC_G8 VCCIO): 0 = GP_G8 Voltage set to 3.3v 1 = GP_G8 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G8 GPIO pin.	Yes

9.51 PCH Descriptor Record 50 (Flash Descriptor Records)

Flash Address: FPSBA + 035h

Default Flash Address: 135h

Offset from 0	Bits	Description	Usage	FIT Visible
0x135h	7	GP_G23 Individual Voltage Select (GPPC_G23 VCCIO): 0 = GP_G23 Voltage set to 3.3v 1 = GP_G23 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G23 GPIO pin.	Yes
	6	GP_G22 Individual Voltage Select (GPPC_G22 VCCIO): 0 = GP_G22 Voltage set to 3.3v 1 = GP_G22 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G22 GPIO pin.	Yes
	5	GP_G21 Individual Voltage Select (GPPC_G21 VCCIO): 0 = GP_G21 Voltage set to 3.3v 1 = GP_G21 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G21 GPIO pin.	Yes
	4	GP_G20 Individual Voltage Select (GPPC_G20 VCCIO): 0 = GP_G20 Voltage set to 3.3v 1 = GP_G20 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G20 GPIO pin.	Yes
	3	GP_G19 Individual Voltage Select (GPPC_G19 VCCIO): 0 = GP_G19 Voltage set to 3.3v 1 = GP_G19 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G19 GPIO pin.	Yes
	2	GP_G18 Individual Voltage Select (GPPC_G18 VCCIO): 0 = GP_G18 Voltage set to 3.3v 1 = GP_G18 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G18 GPIO pin.	Yes
	1	GP_G17 Individual Voltage Select (GPPC_G17 VCCIO): 0 = GP_G17 Voltage set to 3.3v 1 = GP_G17 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G17 GPIO pin.	Yes
	0	GP_G16 Individual Voltage Select (GPPC_G16 VCCIO): 0 = GP_G16 Voltage set to 3.3v 1 = GP_G16 Voltage set to 1.8v	This setting controls the VCCIO voltage for the GP_G16 GPIO pin.	Yes

9.52 PCH Descriptor Record 51 (Flash Descriptor Records)

Flash Address: FPSBA + 036h

Default Flash Address: 136h

Offset from 0	Bits	Description	Usage	FIT Visible
0x136h	7:0	Reserved, set to '0'		No

9.53 PCH Descriptor Record 52 (Flash Descriptor Records)

Flash Address: FPSBA + 037h

Default Flash Address: 137h

Offset from 0	Bits	Description	Usage	FIT Visible
0x137h	7:0	Reserved, set to '0'		No

9.54 PCH Descriptor Record 53 (Flash Descriptor Records)

Flash Address: FPSBA + 038h

Default Flash Address: 138h

Offset from 0	Bits	Description	Usage	FIT Visible
0x138h	7:4	Reserved, set to '0'		No
	3	XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP): Strap to decide XHCI Port 4 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 4 configured as XHC 0x1 = XHC Port 4 configured as Non-XHC	This strap must also be configured when setting the USB3 / PCIe Combo Port 1 (FIA/LOSL3) . Note: When USB3 / PCIe Combo Port 1 (FIA/LOSL3) configured as USB3 this setting needs to be set to 0x0. When USB3 / PCIe Combo Port 1 (FIA/LOSL3) is configured as PCIe this setting needs to be set to 0x1.	No
	2	XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP): Strap to decide XHCI Port 3 Ownership between XHCI/PCIe/CSI. 0x0 = XHC Port 3 configured as XHC 0x1 = XHC Port 3 configured as Non-XHC	This strap must also be configured when setting the USB3 / PCIe Combo Port 0 (FIA/LOSL2) . Note: When USB3 / PCIe Combo Port 0 (FIA/LOSL2) configured as USB3 this setting needs to be set to 0x0. When USB3 / PCIe Combo Port 0 (FIA/LOSL2) is configured as PCIe this setting needs to be set to 0x1.	No
	1:0	Reserved, set to '0x3'		No

9.55 PCH Descriptor Record 54 (Flash Descriptor Records)

Flash Address: FPSBA + 039h

Default Flash Address: 139h

Offset from 0	Bits	Description	Usage	FIT Visible
0x139h	7:0	Reserved, set to '0'		No

9.56 PCH Descriptor Record 55 (Flash Descriptor Records)

Flash Address: FPSBA + 03Ah

Default Flash Address: 13Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Ah	7:4	Reserved, set to '0'		No
	3	USB3 Port 4 Speed Select: 0 = Port 4 is configured as USB3.1 Gen2 1 = Port 4 is configured as USB3.1 Gen1	This setting determines the USB3 Port 4 speed capabilities.	Yes
	2	USB3 Port 3 Speed Select: 0 = Port 3 is configured as USB3.1 Gen2 1 = Port 3 is configured as USB3.1 Gen1	This setting determines the USB3 Port 3 speed capabilities.	Yes
	1	USB3 Port 2 Speed Select: 0 = Port 2 is configured as USB3.1 Gen2 1 = Port 2 is configured as USB3.1 Gen1	This setting determines the USB3 Port 2 speed capabilities.	Yes
	0	USB3 Port 1 Speed Select: 0 = Port 1 is configured as USB3.1 Gen2 1 = Port 1 is configured as USB3.1 Gen1	This setting determines the USB3 Port 1 speed capabilities.	Yes

9.57 PCH Descriptor Record 56 (Flash Descriptor Records)

Flash Address: FPSBA + 03Bh

Default Flash Address: 13Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Bh	7:0	Reserved, set to '0'		No
	3	USB3 Port 4 Initialization Speed Select: 0 = Port 4 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 4 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 4 speed during platform power-up.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Bh (Cont)	2	USB3 Port 3 Initialization Speed Select: 0 = Port 3 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 3 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 3 speed during platform power-up.	Yes
	1	USB3 Port 2 Initialization Speed Select: 0 = Port 2 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 2 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 2 speed during platform power-up.	Yes
	0	USB3 Port 1 Initialization Speed Select: 0 = Port 1 will boot as USB 3.1 Gen1 and carry on LBPM if USB 3.1 Gen2 is enabled 1 = Port 1 will boot as USB 3.1 Gen2 and skip LBPM	This setting determines USB3 Port 1 speed during platform power-up.	Yes

9.58 PCH Descriptor Record 57 (Flash Descriptor Records)

Flash Address: FPSBA + 03Ch

Default Flash Address: 13Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Ch	7:4	USB3 Port 2 Connector Type Select: 0x0 = USB3 Port 2 connector set to Type C 0x1 = USB3 Port 2 connector set to Type AB 0x2 = USB3 Port 2 connector set to Type A or Type C (Host Mode Only)	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	USB3 Port 1 Connector Type Select: 0x0 = USB3 Port 1 connector set to Type C 0x1 = USB3 Port 1 connector set to Type AB 0x2 = USB3 Port 1 connector set to Type A or Type C (Host Mode Only)	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

9.59 PCH Descriptor Record 58 (Flash Descriptor Records)

Flash Address: FPSBA + 03Dh

Default Flash Address: 13Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Dh	7:4	USB3 Port 4 Connector Type Select: 0x0 = USB3 Port 4 connector set to Type C 0x1 = USB3 Port 4 connector set to Type AB 0x2 = USB3 Port 4 connector set to Type A or Type C (Host Mode Only)	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes
	3:0	USB3 Port 3 Connector Type Select: 0x0 = USB3 Port 3 connector set to Type C 0x1 = USB3 Port 3 connector set to Type AB 0x2 = USB3 Port 3 connector set to Type A or Type C (Host Mode Only)	This setting configures the physical connector type for where the USB port [Super Speed / Enhanced Super Speed] is routed.	Yes

9.60 PCH Descriptor Record 59 (Flash Descriptor Records)

Flash Address: FPSBA + 03Eh

Default Flash Address: 13Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Eh	7:4	USB2 Port 2 Connector Type Select: 0x0 = USB2 Port 2 connector set to Type C 0x1 = USB2 Port 2 connector set to Type AB 0x2 = USB2 Port 2 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 2 physical connector type for where the USB port is routed.	Yes
	3:0	USB2 Port 1 Connector Type Select: 0x0 = USB2 Port 1 connector set to Type C 0x1 = USB2 Port 1 connector set to Type AB 0x2 = USB2 Port 1 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 1 physical connector type for where the USB port is routed.	Yes

9.61 PCH Descriptor Record 60 (Flash Descriptor Records)

Flash Address: FPSBA + 03Fh

Default Flash Address: 13Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x13Fh	7:4	USB2 Port 4 Connector Type Select: 0x0 = USB2 Port 4 connector set to Type C 0x1 = USB2 Port 4 connector set to Type AB 0x2 = USB2 Port 4 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 4 physical connector type for where the USB port is routed.	Yes
	3:0	USB2 Port 3 Connector Type Select: 0x0 = USB2 Port 3 connector set to Type C 0x1 = USB2 Port 3 connector set to Type AB 0x2 = USB2 Port 3 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 3 physical connector type for where the USB port is routed.	Yes

9.62 PCH Descriptor Record 61 (Flash Descriptor Records)

Flash Address: FPSBA + 040h

Default Flash Address: 140h

Offset from 0	Bits	Description	Usage	FIT Visible
0x140h	7:4	USB2 Port 6 Connector Type Select: 0x0 = USB2 Port 6 connector set to Type C 0x1 = USB2 Port 6 connector set to Type AB 0x2 = USB2 Port 6 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 6 physical connector type for where the USB port is routed.	Yes
	3:0	USB2 Port 5 Connector Type Select: 0x0 = USB2 Port 7 connector set to Type C 0x1 = USB2 Port 7 connector set to Type AB 0x2 = USB2 Port 7 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 5 physical connector type for where the USB port is routed.	Yes

9.63 PCH Descriptor Record 62 (Flash Descriptor Records)

Flash Address: FPSBA + 041h

Default Flash Address: 141h

Offset from 0	Bits	Description	Usage	FIT Visible
0x141h	7:4	USB2 Port 8 Connector Type Select: 0x0 = USB2 Port 8 connector set to Type C 0x1 = USB2 Port 8 connector set to Type AB 0x2 = USB2 Port 8 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 8 physical connector type for where the USB port is routed.	Yes
	3:0	USB2 Port 7 Connector Type Select: 0x0 = USB2 Port 7 connector set to Type C 0x1 = USB2 Port 7 connector set to Type AB 0x2 = USB2 Port 7 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 7 physical connector type for where the USB port is routed.	Yes

9.64 PCH Descriptor Record 63 (Flash Descriptor Records)

Flash Address: FPSBA + 042h

Default Flash Address: 142h

Offset from 0	Bits	Description	Usage	FIT Visible
0x142h	7:4	USB2 Port 10 Connector Type Select: 0x0 = USB2 Port 10 connector set to Type C 0x1 = USB2 Port 10 connector set to Type AB 0x2 = USB2 Port 10 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 10 physical connector type for where the USB port is routed.	Yes
	3:0	USB2 Port 9 Connector Type Select: 0x0 = USB2 Port 9 connector set to Type C 0x1 = USB2 Port 9 connector set to Type AB 0x2 = USB2 Port 9 connector set to Type A or Type C (Host Mode Only)	This setting configures the USB2 Port 9 physical connector type for where the USB port is routed.	Yes

9.65 PCH Descriptor Record 64 (Flash Descriptor Records)

Flash Address: FPSBA + 043h

Default Flash Address: 143h

Offset from 0	Bits	Description	Usage	FIT Visible
0x143h	7:0	Reserved, set to '0'		No

9.66 PCH Descriptor Record 65 (Flash Descriptor Records)

Flash Address: FPSBA + 044h

Default Flash Address: 144h

Offset from 0	Bits	Description	Usage	FIT Visible
0x144h	7:0	Reserved, set to '0'		No

9.67 PCH Descriptor Record 66 (Flash Descriptor Records)

Flash Address: FPSBA + 045h

Default Flash Address: 145h

Offset from 0	Bits	Description	Usage	FIT Visible
0x145h	7:0	Reserved, set to '0'		No

9.68 PCH Descriptor Record 67 (Flash Descriptor Records)

Flash Address: FPSBA + 046h

Default Flash Address: 146h

Offset from 0	Bits	Description	Usage	FIT Visible
0x146h	7:0	Reserved, set to '0'		No

9.69 PCH Descriptor Record 68 (Flash Descriptor Records)

Flash Address: FPSBA + 047h

Default Flash Address: 147h

Offset from 0	Bits	Description	Usage	FIT Visible
0x147h	7:0	Reserved, set to '0'		No

9.70 PCH Descriptor Record 69 (Flash Descriptor Records)

Flash Address: FPSBA + 048h

Default Flash Address: 148h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148h	31:0	Reserved, set to '0'		No

9.71 PCH Descriptor Record 70 (Flash Descriptor Records)

Flash Address: FPSBA + 04Ch

Default Flash Address: 14Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Ch	15:0	Reserved, set to '0'		No

9.72 PCH Descriptor Record 71 (Flash Descriptor Records)

Flash Address: FPSBA + 04Eh

Default Flash Address: 14Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Eh	7:0	Reserved, set to '0xFF'		No

9.73 PCH Descriptor Record 72 (Flash Descriptor Records)

Flash Address: FPSBA + 04Fh

Default Flash Address: 14Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x14Fh	7:0	Reserved, set to '0'		No

9.74 PCH Descriptor Record 73 (Flash Descriptor Records)

Flash Address: FPSBA + 050h

Default Flash Address: 150h

Offset from 0	Bits	Description	Usage	FIT Visible
0x150h	7	Reserved, set to '0'		No
	6:4	Top Swap Block size (TSBS): 0x0 = 64 KB. Invert A16 if Top Swap is enabled 0x1 = 128 KB. Invert A17 if Top Swap is enabled 0x2 = 256 KB. Invert A18 if Top Swap is enabled 0x3 = 512 KB. Invert A19 if Top Swap is enabled 0x4 = 1 MB. Invert A20 if Top Swap is enabled 0x5 = 2MB. Invert A20 if Top Swap is enabled 0x6 = 4MB. Invert A20 if Top Swap is enabled 0x7 = 8MB. Invert A20 if Top Swap is enabled This setting is dependent on BIOS architecture and can be different per design. The BIOS developer for the target platform has to determine this value.	This allows for the system to use alternate code in order to boot a platform based upon the Top Swap (GPIO66/SDIO_D0 pulled high during the rising edge of PWROK .) strap being asserted. Top Swap inverts an address on access to SPI and firmware hub, so the processor fetches the alternate Top Swap block instead of the original boot-block. The size of the Top Swap block and setting of this field must be determined by the BIOS developer. If this is not set correctly, then BIOS boot-block recovery mechanism will not work. This setting is not the same for all designs, is dependent on the architecture of BIOS. The setting of this field must be determined by the BIOS developer.	Yes
	3:0	Reserved, set to '0'		No

9.75 PCH Descriptor Record 74 (Flash Descriptor Records)

Flash Address: FPSBA + 051h

Default Flash Address: 151h

Offset from 0	Bits	Description	Usage	FIT Visible
0x151h	7:0	Reserved, set to '0'		No

9.76 PCH Descriptor Record 75 (Flash Descriptor Records)

Flash Address: FPSBA + 052h

Default Flash Address: 152h

Offset from 0	Bits	Description	Usage	FIT Visible
0x152h	7:0	Reserved, set to '0'		No

9.77 PCH Descriptor Record 76 (Flash Descriptor Records)

Flash Address: FPSBA + 053h

Default Flash Address: 153h

Offset from 0	Bits	Description	Usage	FIT Visible
0x153h	7:6	SPI Maximum write and erase Resume to Suspend intervals: 0x0 = 128us 0x1 = 256us 0x2 = 512us 0x3 = No Ceiling	This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	Yes
	5	SPI Out of Order operation Enable: 0 = Out or Order operation Enabled 1 = Out of Order operation Disabled	When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	Yes
	4	SPI Suspend / Resume Enable: 0 = Enable suspend / resume 1 = Disable suspend / resume	When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	Yes
	3:1	SPI Resume Holdoff Delay: 0x0 = 0us 0x1 = 2us 0x2 = 4us 0x3 = 6us 0x4 = 8us 0x5 = 10us 0x6 = 12us 0x7 = 14us	Specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is re-initialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	Yes
	0	Reserved, set to '0'		No

9.78 PCH Descriptor Record 77 (Flash Descriptor Records)

Flash Address: FPSBA + 054h

Default Flash Address: 154h

Offset from 0	Bits	Description	Usage	FIT Visible
0x154h	7:4	Reserved, set to '0'		No
	3:0	SPI Idle to Deep Power Down Timeout: Set to '0x5'	SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Powerdown, time = 2^N microseconds	Yes

9.79 PCH Descriptor Record 78 (Flash Descriptor Records)

Flash Address: FPSBA + 055h

Default Flash Address: 155h

Offset from 0	Bits	Description	Usage	FIT Visible
0x155h	7:3	Reserved, set to '0'		No
	2:0	SPI TPM Clock Frequency (STCF): This field is defined with a broad range to support both SOC and PCH implementations. The listed frequencies are approximate. 000 = 100MHz 001 = 50MHz 100 = 25 MHz 110 = 14 MHz Notes: This field identifies the serial clock frequency for TPM on SPI. This field is undefined if the TPM on SPI is disabled either by soft-strap or fuse.		Yes

9.80 PCH Descriptor Record 79 (Flash Descriptor Records)

Flash Address: FPSBA + 056h

Default Flash Address: 156h

Offset from 0	Bits	Description	Usage	FIT Visible
0x156h	7:0	Reserved, set to '0'		No

9.81 PCH Descriptor Record 80 (Flash Descriptor Records)

Flash Address: FPSBA + 057h

Default Flash Address: 157h

Offset from 0	Bits	Description	Usage	FIT Visible
0x157h	7:0	Reserved, set to '0'		No

9.82 PCH Descriptor Record 81 (Flash Descriptor Records)

Flash Address: FPSBA + 058h

Default Flash Address: 158h

Offset from 0	Bits	Description	Usage	FIT Visible
0x158h	31:0	Global Protected Range Default (GPRD): Set to '0x0'	Sets the default value of the GPR0 register in the SPI Flash Controller.	Yes

9.83 PCH Descriptor Record 82 (Flash Descriptor Records)

Flash Address: FPSBA + 05Ch

Default Flash Address: 15Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Ch	7:0	Reserved, set to '0'		No

9.84 PCH Descriptor Record 83 (Flash Descriptor Records)

Flash Address: FPSBA + 05Dh

Default Flash Address: 15Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Dh	7:0	Reserved, set to '0'		No

9.85 PCH Descriptor Record 84 (Flash Descriptor Records)

Flash Address: FPSBA + 05Eh

Default Flash Address: 15Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Eh	7:0	Reserved, set to '0'		No

9.86 PCH Descriptor Record 85 (Flash Descriptor Records)

Flash Address: FPSBA + 05Fh

Default Flash Address: 15Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x15Fh	7:0	Reserved, set to '0'		No

9.87 PCH Descriptor Record 86 (Flash Descriptor Records)

Flash Address: FPSBA + 060h

Default Flash Address: 160h

Offset from 0	Bits	Description	Usage	FIT Visible
0x160h	7:0	Reserved, set to '0'		No

9.88 PCH Descriptor Record 87 (Flash Descriptor Records)

Flash Address: FPSBA + 061h

Default Flash Address: 161h

Offset from 0	Bits	Description	Usage	FIT Visible
0x161h	7:0	Reserved, set to '0'		No

9.89 PCH Descriptor Record 88 (Flash Descriptor Records)

Flash Address: FPSBA + 062h

Default Flash Address: 162h

Offset from 0	Bits	Description	Usage	FIT Visible
0x162h	7:0	Reserved, set to '0'		No

9.90 PCH Descriptor Record 89 (Flash Descriptor Records)

Flash Address: FPSBA + 063h

Default Flash Address: 163h

Offset from 0	Bits	Description	Usage	FIT Visible
0x163h	7:0	Reserved, set to '0'		No

9.91 PCH Descriptor Record 90 (Flash Descriptor Records)

Flash Address: FPSBA + 064h

Default Flash Address: 164h

Offset from 0	Bits	Description	Usage	FIT Visible
0x164h	7:0	Reserved, set to '0'		No

9.92 PCH Descriptor Record 91 (Flash Descriptor Records)

Flash Address: FPSBA + 065h

Default Flash Address: 165h

Offset from 0	Bits	Description	Usage	FIT Visible
0x165h	7:0	Reserved, set to '0'		No

9.93 PCH Descriptor Record 92 (Flash Descriptor Records)

Flash Address: FPSBA + 066h

Default Flash Address: 166h

Offset from 0	Bits	Description	Usage	FIT Visible
0x166h	7:0	Reserved, set to '0'		No

9.94 PCH Descriptor Record 93 (Flash Descriptor Records)

Flash Address: FPSBA + 067h

Default Flash Address: 167h

Offset from 0	Bits	Description	Usage	FIT Visible
0x167h	7:0	Reserved, set to '0'		No

9.95 PCH Descriptor Record 94 (Flash Descriptor Records)

Flash Address: FPSBA + 068h

Default Flash Address: 168h

Offset from 0	Bits	Description	Usage	FIT Visible
0x168h	7:0	Reserved, set to '0'		No

9.96 PCH Descriptor Record 95 (Flash Descriptor Records)

Flash Address: FPSBA + 069h

Default Flash Address: 169h

Offset from 0	Bits	Description	Usage	FIT Visible
0x169h	7:0	Reserved, set to '0'		No

9.97 PCH Descriptor Record 96 (Flash Descriptor Records)

Flash Address: FPSBA + 06Ah

Default Flash Address: 16Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Ah	7:0	Reserved, set to '0'		No

9.98 PCH Descriptor Record 97 (Flash Descriptor Records)

Flash Address: FPSBA + 06Bh

Default Flash Address: 16Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Bh	7:0	Reserved, set to '0'		No

9.99 PCH Descriptor Record 98 (Flash Descriptor Records)

Flash Address: FPSBA + 06Ch

Default Flash Address: 16Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Ch	7:0	Reserved, set to '0'		No

9.100 PCH Descriptor Record 99 (Flash Descriptor Records)

Flash Address: FPSBA + 06Dh

Default Flash Address: 16Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Dh	7:5	Reserved, set to '0'		No
	4:3	PCIe Controller 1 (Port 0-3): Straps to set the default value of the PCI Express Port Configuration 1 register covering PCIe ports 0-3. 0x0 = 4x1 0x1 = 1x2, 2x1 0x2 = 2x2 0x3 = 1x4	Setting of this field depend on what PCIe ports 0-3 configurations are desired by the board manufacturer. Note: This field must be determined by the PCI Express port requirements of the design. The platform hardware designer must determine this setting. Note: Refer to EDS for PCIe supported port configurations.	Yes
	2	PCIe Controller 1 Lane Reversal: 0x0 = PCIe Lanes are not reversed. 0x1 = PCIe Lanes are reversed. Note: Refer to EDS supported Lane reversal configuration.	This bit controls lane reversal behavior for PCIe Controller 1 for PCIe. PCI Express port lane reversal can be done to aid in the laying out of the board. Note: This setting is dependent on the board design. The platform hardware designer must determine if this port needs lane reversal.	Yes
	1:0	Reserved, set to '0'		No

9.101 PCH Descriptor Record 100 (Flash Descriptor Records)

Flash Address: FPSBA + 06Eh

Default Flash Address: 16Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Eh	7:0	Reserved, set to '0'		No

9.102 PCH Descriptor Record 101 (Flash Descriptor Records)

Flash Address: FPSBA + 06Fh

Default Flash Address: 16Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x16Fh	7:0	Reserved, set to '0'		No

9.103 PCH Descriptor Record 102 (Flash Descriptor Records)

Flash Address: FPSBA + 070h

Default Flash Address: 170h

Offset from 0	Bits	Description	Usage	FIT Visible
0x170h	7:0	Reserved, set to '0'		No

9.104 PCH Descriptor Record 103 (Flash Descriptor Records)

Flash Address: FPSBA + 071h

Default Flash Address: 171h

Offset from 0	Bits	Description	Usage	FIT Visible
0x171h	7:0	Reserved, set to '0'		No

9.105 PCH Descriptor Record 104 (Flash Descriptor Records)

Flash Address: FPSBA + 072h

Default Flash Address: 172h

Offset from 0	Bits	Description	Usage	FIT Visible
0x172h	7:0	Reserved, set to '0'		No

9.106 PCH Descriptor Record 105 (Flash Descriptor Records)

Flash Address: FPSBA + 073h

Default Flash Address: 173h

Offset from 0	Bits	Description	Usage	FIT Visible
0x173h	7:0	Reserved, set to '0'		No

9.107 PCH Descriptor Record 106 (Flash Descriptor Records)

Flash Address: FPSBA + 074h

Default Flash Address: 174h

Offset from 0	Bits	Description	Usage	FIT Visible
0x174h	7:0	Reserved, set to '0x8'		No

9.108 PCH Descriptor Record 107 (Flash Descriptor Records)

Flash Address: FPSBA + 075h

Default Flash Address: 175h

Offset from 0	Bits	Description	Usage	FIT Visible
0x175h	7:0	Reserved, set to '0'		No

9.109 PCH Descriptor Record 108 (Flash Descriptor Records)

Flash Address: FPSBA + 076h

Default Flash Address: 176h

Offset from 0	Bits	Description	Usage	FIT Visible
0x176h	7:0	Reserved, set to '0'		No

9.110 PCH Descriptor Record 109 (Flash Descriptor Records)

Flash Address: FPSBA + 077h

Default Flash Address: 177h

Offset from 0	Bits	Description	Usage	FIT Visible
0x177h	7:0	Reserved, set to '0'		No

9.111 PCH Descriptor Record 110 (Flash Descriptor Records)

Flash Address: FPSBA + 078h

Default Flash Address: 178h

Offset from 0	Bits	Description	Usage	FIT Visible
0x178h	7:0	Reserved, set to '0x8'		No

9.112 PCH Descriptor Record 111 (Flash Descriptor Records)

Flash Address: FPSBA + 079h

Default Flash Address: 179h

Offset from 0	Bits	Description	Usage	FIT Visible
0x179h	7:0	Reserved, set to '0'		No

9.113 PCH Descriptor Record 112 (Flash Descriptor Records)

Flash Address: FPSBA + 07Ah

Default Flash Address: 17Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Ah	7:0	Reserved, set to '0'		No

9.114 PCH Descriptor Record 113 (Flash Descriptor Records)

Flash Address: FPSBA + 07Bh

Default Flash Address: 17Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Bh	7:0	Reserved, set to '0'		No

9.115 PCH Descriptor Record 114 (Flash Descriptor Records)

Flash Address: FPSBA + 07Ch

Default Flash Address: 17Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Ch	7:0	Reserved, set to '0x8'		No

9.116 PCH Descriptor Record 115 (Flash Descriptor Records)

Flash Address: FPSBA + 07Dh

Default Flash Address: 17Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Dh	7:0	Reserved, set to '0'		No

9.117 PCH Descriptor Record 116 (Flash Descriptor Records)

Flash Address: FPSBA + 07Eh

Default Flash Address: 17Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17Eh	7:0	Reserved, set to '0'		No

9.118 PCH Descriptor Record 117 (Flash Descriptor Records)

Flash Address: FPSBA + 07Fh

Default Flash Address: 17Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x17F	7:0	Reserved, set to '0'		No

9.119 PCH Descriptor Record 118 (Flash Descriptor Records)

Flash Address: FPSBA + 080h

Default Flash Address: 180h

Offset from 0	Bits	Description	Usage	FIT Visible
0x180h	7:0	Reserved, set to '0'		No

9.120 PCH Descriptor Record 119 (Flash Descriptor Records)

Flash Address: FPSBA + 081h

Default Flash Address: 181h

Offset from 0	Bits	Description	Usage	FIT Visible
0x181h	7	Reserved, set to '0'		No
	6:0	Reserved, set to '0x33'		No

9.121 PCH Descriptor Record 120 (Flash Descriptor Records)

Flash Address: FPSBA + 082h

Default Flash Address: 182h

Offset from 0	Bits	Description	Usage	FIT Visible
0x148h	7:5	Reserved, set to '0'		No
	4:2	Reserved, set to '0x1'		No
	1:0	Reserved, set to '0'		No
	7	Reserved, set to '0'		No
	7	Reserved, set to '0'		No

9.122 PCH Descriptor Record 121 (Flash Descriptor Records)

Flash Address: FPSBA + 083h

Default Flash Address: 183h

Offset from 0	Bits	Description	Usage	FIT Visible
0x183h	7:4	Reserved, set to '0'		No
	2:1	Reserved, set to '0x1'		No
	0	Reserved, set to '0'		No

9.123 PCH Descriptor Record 122 (Flash Descriptor Records)

Flash Address: FPSBA + 084h

Default Flash Address: 184h

Offset from 0	Bits	Description	Usage	FIT Visible
0x184h	31:22	Reserved, set to '0'		No
	21	Intel® Trace Hub - Emergency Mode: 0 = ROM Tracing Emergency mode disabled 1 = ROM Tracing Emergency mode enabled	This option enables ROM Tracing in the base platform image.	Yes
	20:18	Reserved, set to '0'		No
	17	Direct Connect Interface (DCI) Enabled: 0 = DCI Disabled 1 = DCI Enabled		Yes
	16	Reserved, set to '0'		Yes
	15:12	Reserved, set to '0'		No
	11	Intel® CSE AFS Flash Idle Reclaim Enable: 0 = AFS Flash Reclaim enabled 1 = AFS Flash Reclaim disabled	This controls enabling / disabling of Intel® CSE AFS Idle flash reclaim capabilities. Note: This setting should be used for debug purposes only	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x184h (Cont)	10	Intel® CSE Reset Behavior: 0 = Intel® CSE shall attempt to boot from the next available image, if exists. 1 = Intel® CSE will halt		Yes
	9:1	Reserved, set to '0x1C'		No
	0	Firmware ROM Bypass Enable Softstrap: 0 = ROM Bypass disabled 1 = ROM Bypass enabled	Firmware ROM Bypass Enable Softstrap.	Yes

9.124 PCH Descriptor Record 123 (Flash Descriptor Records)

Flash Address: FPSBA + 088h

Default Flash Address: 188h

Offset from 0	Bits	Description	Usage	FIT Visible
0x188h	7:0	Reserved, set to '0'		No

9.125 PCH Descriptor Record 124 (Flash Descriptor Records)

Flash Address: FPSBA + 089h

Default Flash Address: 189h

Offset from 0	Bits	Description	Usage	FIT Visible
0x189h	7:0	Reserved, set to '0'		No

9.126 PCH Descriptor Record 125 (Flash Descriptor Records)

Flash Address: FPSBA + 08Ah

Default Flash Address: 18Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Ah	7:0	Reserved, set to '0'		No

9.127 PCH Descriptor Record 126 (Flash Descriptor Records)

Flash Address: FPSBA + 08Bh

Default Flash Address: 18Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Bh	7:0	Reserved, set to '0'		No

9.128 PCH Descriptor Record 127 (Flash Descriptor Records)

Flash Address: FPSBA + 08Ch

Default Flash Address: 18Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Ch	7	Reserved, set to '0'		No
	6:0	Reserved, set to '0x64'		No

9.129 PCH Descriptor Record 128 (Flash Descriptor Records)

Flash Address: FPSBA + 08Dh

Default Flash Address: 18Dh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Dh	7:0	Reserved, set to '0'		No

9.130 PCH Descriptor Record 129 (Flash Descriptor Records)

Flash Address: FPSBA + 08Eh

Default Flash Address: 18Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Eh	7:0	Reserved, set to '0'		No

9.131 PCH Descriptor Record 130 (Flash Descriptor Records)

Flash Address: FPSBA + 08Fh

Default Flash Address: 18Fh

Offset from 0	Bits	Description	Usage	FIT Visible
0x18Fh	7:0	Reserved, set to '0'		No

9.132 PCH Descriptor Record 131 (Flash Descriptor Records)

Flash Address: FPSBA + 090h

Default Flash Address: 190h

Offset from 0	Bits	Description	Usage	FIT Visible
0x190h	7:0	Reserved, set to '0'		No

9.133 PCH Descriptor Record 132 (Flash Descriptor Records)

Flash Address: FPSBA + 091h

Default Flash Address: 191h

Offset from 0	Bits	Description	Usage	FIT Visible
0x191h	7:0	Reserved, set to '0'		No

9.134 PCH Descriptor Record 133 (Flash Descriptor Records)

Flash Address: FPSBA + 092h

Default Flash Address: 192h

Offset from 0	Bits	Description	Usage	FIT Visible
0x192h	7:0	Reserved, set to '0'		No

9.135 PCH Descriptor Record 134 (Flash Descriptor Records)

Flash Address: FPSBA + 093h

Default Flash Address: 193h

Offset from 0	Bits	Description	Usage	FIT Visible
0x193h	7:0	Reserved, set to '0'		No

9.136 PCH Descriptor Record 135 (Flash Descriptor Records)

Flash Address: FPSBA + 094h

Default Flash Address: 194h

Offset from 0	Bits	Description	Usage	FIT Visible
0x194h	7	Reserved, set to '0'		No
	6:0	Reserved, set to '0x64'		No

9.137 PCH Descriptor Record 136 (Flash Descriptor Records)

Flash Address: FPSBA + 095h

Default Flash Address: 195h

Offset from 0	Bits	Description	Usage	FIT Visible
0x195h	7:0	Reserved, set to '0'		No

9.138 PCH Descriptor Record 137 (Flash Descriptor Records)

Flash Address: FPSBA + 096h

Default Flash Address: 196h

Offset from 0	Bits	Description	Usage	FIT Visible
0x196h	7:0	Reserved, set to '0'		No

9.139 PCH Descriptor Record 138 (Flash Descriptor Records)

Flash Address: FPSBA + 097h

Default Flash Address: 197h

Offset from 0	Bits	Description	Usage	FIT Visible
0x197h	7:0	Reserved, set to '0'		No

9.140 PCH Descriptor Record 139 (Flash Descriptor Records)

Flash Address: FPSBA + 098h

Default Flash Address: 198h

Offset from 0	Bits	Description	Usage	FIT Visible
0x198h	7:0	Reserved, set to '0'		No

9.141 PCH Descriptor Record 140 (Flash Descriptor Records)

Flash Address: FPSBA + 099h

Default Flash Address: 199h

Offset from 0	Bits	Description	Usage	FIT Visible
0x199h	7:0	Reserved, set to '0'		No

9.142 PCH Descriptor Record 141 (Flash Descriptor Records)

Flash Address: FPSBA + 09Ah

Default Flash Address: 19Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Ah	7:0	Reserved, set to '0'		No

9.143 PCH Descriptor Record 142 (Flash Descriptor Records)

Flash Address: FPSBA + 09Bh

Default Flash Address: 19Bh

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Bh	7:0	Reserved, set to '0'		No

9.144 PCH Descriptor Record 143 (Flash Descriptor Records)

Flash Address: FPSBA + 09Ch

Default Flash Address: 19Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0x19Ch	31:0	Reserved, set to '0'		No

9.145 PCH Descriptor Record 144 (Flash Descriptor Records)

Flash Address: FPSBA + 0A0h

Default Flash Address: 1A0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A0h	31:0	Reserved, set to '0'		No

9.146 PCH Descriptor Record 145 (Flash Descriptor Records)

Flash Address: FPSBA + 0A4h

Default Flash Address: 1A4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A4h	7:4	Reserved, set to '0'		No
	3	DCI BSSB over USB3 Port3 Configuration (EXI_PTSS_PORT3): 0 = BSSB is enabled on USB3 Port3 1 = BSSB is disabled on USB3 Port3	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes
	2	DCI BSSB over USB3 Port2 Configuration (EXI_PTSS_PORT2): 0 = BSSB is enabled on USB3 Port2 1 = BSSB is disabled on USB3 Port2	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A4h (Cont)	1	DCI BSSB over USB3 Port1 Configuration (EXI_PTSS_PORT1): 0 = BSSB is enabled on USB3 Port1 1 = BSSB is disabled on USB3 Port1	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes
	0	DCI BSSB over USB3 Port0 Configuration (EXI_PTSS_PORT0): 0 = BSSB is enabled on USB3 Port0 1 = BSSB is disabled on USB3 Port0	This setting determines if the USB port being used for DCI operations has BSSB (Boundary Scan Side Band) enabled. Note: For S0ix and reset flows BSSB should be enabled.	Yes

9.147 PCH Descriptor Record 146 (Flash Descriptor Records)

Flash Address: FPSBA + 0A5h

Default Flash Address: 1A5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A5h	7:0	Reserved, set to '0'		No

9.148 PCH Descriptor Record 147 (Flash Descriptor Records)

Flash Address: FPSBA + 0A6h

Default Flash Address: 166h

Offset from 0	Bits	Description	Usage	FIT Visible
0x166h	7:0	Reserved, set to '0'		No

9.149 PCH Descriptor Record 148 (Flash Descriptor Records)

Flash Address: FPSBA + 0A7h

Default Flash Address: 1A7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A7h	7:0	Reserved, set to '0'		No

9.150 PCH Descriptor Record 149 (Flash Descriptor Records)

Flash Address: FPSBA + 0A8h

Default Flash Address: 1A8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1A8h	24:0	Reserved, set to '0'		No

9.151 PCH Descriptor Record 150 (Flash Descriptor Records)

Flash Address: FPSBA + 0ABh

Default Flash Address: 1ABh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ABh	7:4	Reserved, set to '0x6'		No
	3	Reserved, set to '0x1'		No
	2:0	Reserved, set to '0'		No

9.152 PCH Descriptor Record 151 (Flash Descriptor Records)

Flash Address: FPSBA + 0ACh

Default Flash Address: 1ACh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ACh	7:3	Reserved, set to '0x15'		No
	2:0	Reserved, set to '0'		No

9.153 PCH Descriptor Record 152 (Flash Descriptor Records)

Flash Address: FPSBA + 0ADh

Default Flash Address: 1ADh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1ADh	7:5	Reserved, set to '0'		No
	4:0	Reserved, set to '0x16'		No

9.154 PCH Descriptor Record 153 (Flash Descriptor Records)

Flash Address: FPSBA + 0AEh

Default Flash Address: 1AEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1AEh	15:0	Reserved, set to '0xDEAD'		No

9.155 PCH Descriptor Record 154 (Flash Descriptor Records)

Flash Address: FPSBA + 0B0h

Default Flash Address: 1B0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B0h	31:0	Reserved, set to '0xBDBDBDBD'		No

9.156 PCH Descriptor Record 155 (Flash Descriptor Records)

Flash Address: FPSBA + 0B4h

Default Flash Address: 1B4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B4h	7:3	Reserved, set to '0x15'		No
	2:0	Reserved, set to '0'		No

9.157 PCH Descriptor Record 156 (Flash Descriptor Records)

Flash Address: FPSBA + 0B5h

Default Flash Address: 1B5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B5h	7:5	Reserved, set to '0'		No
	4:0	Reserved, set to '0x16'		No

9.158 PCH Descriptor Record 157 (Flash Descriptor Records)

Flash Address: FPSBA + 0B6h

Default Flash Address: 1B6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B6h	15:0	Reserved, set to '0x5A5A'		No

9.159 PCH Descriptor Record 158 (Flash Descriptor Records)

Flash Address: FPSBA + 0B8h

Default Flash Address: 1B8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1B8h	31:0	Reserved, set to '0xA5A5A5A5'		No

9.160 PCH Descriptor Record 159 (Flash Descriptor Records)

Flash Address: FPSBA + 0BCh

Default Flash Address: 1BCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1BCh	31:0	Reserved, set to '0'		No

9.161 PCH Descriptor Record 160 (Flash Descriptor Records)

Flash Address: FPSBA + 0C0h

Default Flash Address: 1C0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C0h	7:0	Reserved, set to '0'		No

9.162 PCH Descriptor Record 161 (Flash Descriptor Records)

Flash Address: FPSBA + 0C1h

Default Flash Address: 1C1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C1h	7:0	Reserved, set to '0'		No

9.163 PCH Descriptor Record 162 (Flash Descriptor Records)

Flash Address: FPSBA + 0C2h

Default Flash Address: 1C2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C2h	7:0	Reserved, set to '0'		No

9.164 PCH Descriptor Record 163 (Flash Descriptor Records)

Flash Address: FPSBA + 0C3h

Default Flash Address: 1C3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C3h	7:0	Reserved, set to '0'		No

9.165 PCH Descriptor Record 164 (Flash Descriptor Records)

Flash Address: FPSBA + 0C4h

Default Flash Address: 1C4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C4h	7:2	Reserved, set to '0'		No
	1	BIOS Guard protection override enable (LPC/spi_strap_prr_ts_ovr): 0 = BIOS Guard Fault Tolerant Update Capability is disabled 1 = BIOS guard Fault Tolerant Update Capability is enabled	This setting allows BIOS Guard to bypass the SPI Flash controller protections such as protected range registers and top swap. Note: For further details please review Intel® Platform Protection Technology with BIOS Guard 2.0 BIOS Specification regarding Fault Tolerant Update (FTU).	Yes
	0	TPM Over SPI Bus Enabled (TOS): 0 = TPM is not on SPI 1 = TPM is on SPI	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap	Yes

9.166 PCH Descriptor Record 165 (Flash Descriptor Records)

Flash Address: FPSBA + 0C5h

Default Flash Address: 1C5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C5h	7:0	Reserved, set to '0'		No

9.167 PCH Descriptor Record 166 (Flash Descriptor Records)

Flash Address: FPSBA + 0C6h

Default Flash Address: 1C6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C6h	7:0	Reserved, set to '0'		No

9.168 PCH Descriptor Record 167 (Flash Descriptor Records)

Flash Address: FPSBA + 0C7h

Default Flash Address: 1C7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C7h	7:0	Reserved, set to '0'		No

9.169 PCH Descriptor Record 168 (Flash Descriptor Records)

Flash Address: FPSBA + 0C8h

Default Flash Address: 1C8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C8h	7:2	Reserved, set to '0x1'		No
	1	PCIe Port Staggering Enable: 0 = Disabled 1 = Enabled		Yes
	0	Reserved, set to '0x1'		No

9.170 PCH Descriptor Record 169 (Flash Descriptor Records)

Flash Address: FPSBA + 0C9h

Default Flash Address: 1C9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1C9h	7:4	USB3 / PCIe Combo Port 0 (FIA/LOSL2): 0x1 = statically assigned as USB Port 2 0x5 = statically assigned as PCIe Port 0 0xB = statically assigned as Multi VC 0	This setting determine if USB3 / PCIe Combo Port 0 is configured natively for USB3, PCIe or Multi VC. Note: When configuring this setting you must also configure XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP) .	Yes
	3:0	Reserved, set to '0x1'		No

9.171 PCH Descriptor Record 170 (Flash Descriptor Records)

Flash Address: FPSBA + 0CAh

Default Flash Address: 1CAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CAh	7:4	FIA_LOSL4 (FIA/LOSL4): 0x5 = statically assigned as PCIe Port 4 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL4 is configured natively for PCIe or Multi VC.	No
	3:0	USB3 / PCIe Combo Port 1 (FIA/LOSL3): 0x1 = statically assigned as USB Port 3 0x5 = statically assigned as PCIe Port 3 0xB = statically assigned as Multi VC Note: When configuring this setting you must also configure XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP) .	This setting determine if USB3 / PCIe Combo Port 1 is configured natively for USB3, PCIe or Multi VC.	Yes

9.172 PCH Descriptor Record 171 (Flash Descriptor Records)

Flash Address: FPSBA + 0CBh

Default Flash Address: 1CBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CBh	7:4	FIA_LOSL6 (FIA/LOSL6): 0x9 = assigned as UFS 1 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL6 is configured natively for PCIe, UFS or Multi VC.	No
	3:0	FIA_LOSL5 (FIA/LOSL5): 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL5 is configured natively for PCIe or Multi VC.	No

9.173 PCH Descriptor Record 172 (Flash Descriptor Records)

Flash Address: FPSBA + 0CCh

Default Flash Address: 1CCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CCh	7:4	FIA_LOSL8 (FIA/LOSL8): 0x5 = assigned as PCIe Port 8 0x9 = assigned as UFS 2 0xA = assigned as TSN 2 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL8 is configured natively for PCIe, UFS or TSN or Multi VC.	No
	3:0	FIA_LOSL7 (FIA/LOSL7): 0x5 = assigned as PCIe Port 7 0x9 = assigned as UFS 1 0xA = assigned as TSN 0 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL7 is configured natively for PCIe, UFS, TSN or Multi VC.	No

9.174 PCH Descriptor Record 173 (Flash Descriptor Records)

Flash Address: FPSBA + 0CDh

Default Flash Address: 1CDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CDh	7:4	SATA / PCIe Combo Port 0 (FIA/LOSL10): 0x5 = PCIe Port 10 is statically assigned as PCIe 0x7 = PCIe Port 10 is statically assigned as SATA Port 0 0xA = assigned as TSN 2 0xB = statically assigned as Multi VC	This setting determine if SATA / PCIe Combo Port 0 is configured natively for SATA , PCIe or TSN. Note: If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS0). Note: The settings for this strap and the SATA / PCIe Select for Port 0 (SATA_PCIE_SPO) and (SATA_PCIE_GPO) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	Yes
	3:0	FIA_LOSL9 (FIA/LOSL9): 0x5 = assigned as PCIe Port 9 0x9 = assigned as UFS 3 0xA = assigned as TSN 1 0xB = statically assigned as Multi VC	This setting determine if FIA_LOSL9 is configured natively for PCIe, UFS or TSN or Multi VC.	No

9.175 PCH Descriptor Record 174 (Flash Descriptor Records)

Flash Address: FPSBA + 0CEh

Default Flash Address: 1CEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CEh	7:4	Reserved, set to '0'		No
	3:0	SATA / PCIe Combo Port 1 (FIA/LOSL11): 0x5 = PCIe Port 11 is statically assigned as PCIe 0x7 = PCIe Port 11 is statically assigned as SATA Port 1 0xA = assigned as TSN 1 0xB = statically assigned as Multi VC	This setting determine if SATA / PCIe Combo Port 1 is configured natively for SATA, PCIe or TSN. Note: If using GPIO Polarity control settings '0xC' or '0xD' must match the (SPS1). Note: The settings for this strap and the SATA / PCIe Select for Port 1 (SATA_PCIE_SP1) and (SATA_PCIE_GP1) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	Yes

9.176 PCH Descriptor Record 175 (Flash Descriptor Records)

Flash Address: FPSBA + 0CFh

Default Flash Address: 1CFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1CFh	7:0	Reserved, set to '0'		No

9.177 PCH Descriptor Record 176 (Flash Descriptor Records)

Flash Address: FPSBA + 0D0h

Default Flash Address: 1D0h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D0h	7:4	Reserved, set to '0'		No
	3:2	SATA / PCIe Select for Port 1 (SATA_PCIE_SP1): 00 = PCIe Port 11 is statically assigned to SATA Port 1 01 = PCIe Port 11 is statically assigned to PCIe	This strap must also be configured when setting the PCIe / SATA Combo Port 1 Strap (SATA/PCIe Combo Port 1 Strap). Note: This strap and the PCIe / SATA Combo Port 1 Strap (SATA/PCIe Combo Port 1 Strap) and (SATA_PCIE_GP1) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No
	1:0	SATA / PCIe Select for Port 0 (SATA_PCIE_SPO): 00 = PCIe Port 10 is statically assigned to SATA Port 0 01 = PCIe Port 10 is statically assigned to PCIe	This strap must also be configured when setting the PCIe / SATA Combo Port 0 (SATA/PCIe Combo Port 0 Strap). Note: This strap and the PCIe / SATA Combo Port 0 (SATA/PCIe Combo Port 0 Strap) and (SATA_PCIE_GP0) must match for proper port function. Note: For unused SATA/PCIe* Combo Lanes, Flex I/O Lanes that can be configured as PCIe* or SATA, the lanes must be statically assigned to SATA or PCIe*. These unused SATA/PCIe* Combo Lanes must not be assigned as polarity based.	No

9.178 PCH Descriptor Record 177 (Flash Descriptor Records)

Flash Address: FPSBA + 0D1h

Default Flash Address: 1D1h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D1h	7:0	Reserved, set to '0'		No

9.179 PCH Descriptor Record 178 (Flash Descriptor Records)

Flash Address: FPSBA + 0D2h

Default Flash Address: 1D2h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D2h	7:0	Reserved, set to '0'		No

9.180 PCH Descriptor Record 179 (Flash Descriptor Records)

Flash Address: FPSBA + 0D3h

Default Flash Address: 1D3h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D3h	7:0	Reserved, set to '0'		No

9.181 PCH Descriptor Record 180 (Flash Descriptor Records)

Flash Address: FPSBA + 0D4h

Default Flash Address: 1D4h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D4h	7:0	Reserved, set to '0x64'		No

9.182 PCH Descriptor Record 181 (Flash Descriptor Records)

Flash Address: FPSBA + 0D5h

Default Flash Address: 1D5h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D5h	7:0	Reserved, set to '0x5'		No

9.183 PCH Descriptor Record 182 (Flash Descriptor Records)

Flash Address: FPSBA + 0D6h

Default Flash Address: 1D6h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D6h	7:0	Reserved, set to '0xF5'		No

9.184 PCH Descriptor Record 183 (Flash Descriptor Records)

Flash Address: FPSBA + 0D7h

Default Flash Address: 1D7h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D7h	7:0	Reserved, set to '0x16'		No

9.185 PCH Descriptor Record 184 (Flash Descriptor Records)

Flash Address: FPSBA + 0D8h

Default Flash Address: 1D8h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D8h	7:0	Reserved, set to '0x21'		No

9.186 PCH Descriptor Record 185 (Flash Descriptor Records)

Flash Address: FPSBA + 0D9h

Default Flash Address: 1D9h

Offset from 0	Bits	Description	Usage	FIT Visible
0x1D9h	7:0	Reserved, set to '0x43'		No

9.187 PCH Descriptor Record 186 (Flash Descriptor Records)

Flash Address: FPSBA + 0DAh

Default Flash Address: 1DAh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DAh	7:0	Reserved, set to '0x65'		No

9.188 PCH Descriptor Record 187 (Flash Descriptor Records)

Flash Address: FPSBA + 0DBh

Default Flash Address: 1DBh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DBh	7:0	Reserved, set to '0x87'		No

9.189 PCH Descriptor Record 188 (Flash Descriptor Records)

Flash Address: FPSBA + 0DCh

Default Flash Address: 1DCh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DCh	7:0	Reserved, set to '0xA9'		No

9.190 PCH Descriptor Record 189 (Flash Descriptor Records)

Flash Address: FPSBA + 0DDh

Default Flash Address: 1DDh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DDh	7:0	Reserved, set to '0xCB'		No

9.191 PCH Descriptor Record 190 (Flash Descriptor Records)

Flash Address: FPSBA + 0DEh

Default Flash Address: 1DEh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DEh	7:0	Reserved, set to '0x88'		No

9.192 PCH Descriptor Record 191 (Flash Descriptor Records)

Flash Address: FPSBA + 0DFh

Default Flash Address: 1DFh

Offset from 0	Bits	Description	Usage	FIT Visible
0x1DFh	7:0	Reserved, set to '0x88'		No

9.193 MIP Table Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 000h

Default Flash Address: C00h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC00h	15:0	Number of MIP Table Descriptor Entries: Set to '0x2'	This setting determines the total number of MIP Table Descriptor entries present in the SPI image.	Yes

9.194 MIP Table Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 002h

Default Flash Address: C02h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC02h	15:0	Size of MIP Descriptor Entry: Set to '0x6C'	This setting determines the size in bytes of the MIP Descriptor Entry structure.	Yes

9.195 MIP Table Descriptor Record 2 (Flash Descriptor Records)

Flash Address: MDTBA + 004h

Default Flash Address: C04h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC04h	15:0	MIP Descriptor Block 0: Set to '0x1'	This setting determines what the data type is for the MIP Descriptor.	Yes

9.196 MIP Table Descriptor Record 3 (Flash Descriptor Records)

Flash Address: MDTBA + 006h

Default Flash Address: C06h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC06h	15:0	MIP Descriptor Block 0 Offset: Set to '0x14'	This setting determines the offset location of the MIP Descriptor Table Entries.	Yes

9.197 MIP Table Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 008h

Default Flash Address: C08h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC08h	15:0	MIP Descriptor Block 0 Length: Set to '0x64'	This setting determine the length of the MIP Descriptor Block 0.	Yes

9.198 MIP Table Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ah

Default Flash Address: C0Ah

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Ah	15:0	Reserved, set to '0'		No

9.199 MIP Table Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 00Ch

Default Flash Address: C0Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Ch	15:0	MIP Descriptor Block 1 Type: Set to '0'	This setting determines what the data type is for the MIP Descriptor.	Yes

9.200 MIP Table Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 00Eh

Default Flash Address: C0Eh

Offset from 0	Bits	Description	Usage	FIT Visible
0xC0Eh	15:0	MIP Descriptor Block 1 Offset: Set to '0x74'	This setting determines the offset location of the MIP Descriptor Table Entries.	Yes

9.201 MIP Table Descriptor Record 8 (Flash Descriptor Records)

Flash Address: MDTBA + 010h

Default Flash Address: C10h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC10h	15:0	MIP Descriptor Block 1 Length: Set to '0x8h'	This setting determine the length of the MIP Descriptor Block 0.	Yes

9.202 MIP Table Descriptor Record 9 (Flash Descriptor Records)

Flash Address: MDTBA + 012h

Default Flash Address: C12h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC12h	15:0	Reserved, set to '0'		No

9.203 PMC Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 014h

Default Flash Address: C14h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC14h	31:28	Reserved, set to '0'		No
	27	Intel® Trace Hub Debug Messages Enable: 0 = PCH Tracing debug messages Disabled 1 = PCH Tracing debug messages Enabled	This setting enables debug messages on the Intel® Trace Hub. Note: You will also need to set the Intel® Trace Hub Soft Enable to "Enabled"	Yes
	26	Reserved, set to '0'		No
	25	Power Reporting Enable (THERM_PWR_REP_DIS): 0 = Power Reporting is enabled. 1 = Power Reporting is completely disabled, regardless of the settings in the Thermal Power Reporting configuration registers. Note: When this setting is disabled the once-per-second timer interrupt associated with this feature must not be turned on.	This bit, when set, causes the PMC FW to completely turn off the Power Reporting feature. Note: A once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers.	Yes
	24	PCIe* Power Stable Timer (tPCH33 timer): 0 = tPCH33 timer is disabled 1 = PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted.	Board dependent. Default is disabled, Platform is required to ensure timing of PWROK and SYS_PWROK in such a way that it satisfies the PCIe timing requirement of power stable to reset de-assertion.	Yes
	23:21	Reserved, set to '0'		No
	20	DeepSx Platform Configuration (DEEPSX_PLT_CFG_SS): 0 = The platform does not support DeepSx. 1 = The platform supports DeepSx		Yes
	19:12	Reserved, set to '0'		No
	11:10	tPCH46 Timing: 00 = 1 ms 01 = Reserved 10 = 5 ms 11 = 2 ms	tPch46: PROCPWRGD and SYS_PWROK high to SUS_STAT# deassertion. Refer to EDS for details.	Yes
	9:8	tPCH45 Timing: 00 = 100 ms 01 = 50 ms 10 = 5 ms 11 = 1 ms	tPCH45: PCH clock output stable to PROCPWRGD high. Refer to EDS for details.	Yes
	7:0	Reserved, set to '0x7c'		No

9.204 PMC Descriptor Record 1 (Flash Descriptor Records)

Flash Address:MDTBA + 018h

Default Flash Address: C18h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC18h	31:8	Reserved, set to '0xF000000'		No
	6:1	Reserved, set to '0x4'		No
	0	Intel® Integrated wired LAN Enable (IWL_EN): 0 = Enabled Intel® Integrated wired LAN Solution 1 = Disabled Intel® Integrated wired LAN Solution Note: This must be set to '0' if the platform is using Intel's integrated wired LAN solution. Set to '1' if not using Intel integrated wired LAN solution or if disabling it.	This must be set to '0' if the platform is using the Intel® Integrated wired LAN solution. This must be set to '1' if not using the Intel® Integrated wired LAN solution or if disabling it.	Yes

9.205 PMC Descriptor Record 2 (Flash Descriptor Records)

Flash Address:MDTBA + 01Ch

Default Flash Address: C1Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC1Ch	31:0	Reserved, set to '0x1078802'		No

9.206 PMC Descriptor Record 3 (Flash Descriptor Records)

Flash Address:MDTBA + 020h

Default Flash Address: C20h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC20h	31:0	Reserved, set to '0x0'		No

9.207 PMC Descriptor Record 4 (Flash Descriptor Records)

Flash Address:MDTBA + 024h

Default Flash Address: C24h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC24h	31:17	Reserved, set to '0x100'		No
	16:18	Reserved, set to '0'		No
	7:3	USB2 DbC port enable: 0x00 = No USB2 ports are assigned to DbC 0x80 = USB2 Port 1 DbC enabled 0x88 = USB2 Port 2 DbC enabled 0x90 = USB2 Port 3 DbC enabled 0x98 = USB2 Port 4 DbC enabled 0xA0 = USB2 Port 5 DbC enabled 0xA8 = USB2 Port 6 DbC enabled 0xB0 = USB2 Port 7 DbC enabled 0xB8 = USB2 Port 8 DbC enabled 0xC0 = USB2 Port 9 DbC enabled 0xC8 = USB2 Port 10 DbC enabled All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	No
	2:0	Reserved, set to '0'		No

9.208 PMC Descriptor Record 5 (Flash Descriptor Records)

Flash Address:MDTBA + 028h

Default Flash Address: C28h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC28h	31:0	Reserved, set to '0x79000000'		No

9.209 PMC Descriptor Record 6 (Flash Descriptor Records)

Flash Address:MDTBA + 02Ch

Default Flash Address: C2Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC2Ch	31:0	Reserved, set to '0'		No

9.210 PMC Descriptor Record 7 (Flash Descriptor Records)

Flash Address:MDTBA + 030h

Default Flash Address: C30h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC30h	31:0	Reserved, set to '0'		No

9.211 PMC Descriptor Record 8 (Flash Descriptor Records)

Flash Address:MDTBA + 034h

Default Flash Address: C34h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC34h	31:15	Reserved, set to '0'		No
	14:8	Reserved, set to '0x64'		No
	7:0	Reserved, set to '0'		No

9.212 PMC Descriptor Record 9 (Flash Descriptor Records)

Flash Address:MDTBA + 038h

Default Flash Address: C38h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC38h	31:0	Reserved, set to '0'		No

9.213 PMC Descriptor Record 10 (Flash Descriptor Records)

Flash Address:MDTBA + 03Ch

Default Flash Address: C3Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC3Ch	31:0	Reserved, set to '0'		No

9.214 PMC Descriptor Record 11 (Flash Descriptor Records)

Flash Address:MDTBA + 040h

Default Flash Address: C40h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC40h	31:0	Reserved, set to '0'		No

9.215 PMC Descriptor Record 12 (Flash Descriptor Records)

Flash Address:MDTBA + 044h

Default Flash Address: C44h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC44h	31:0	Reserved, set to '0'		No

9.216 PMC Descriptor Record 13 (Flash Descriptor Records)

Flash Address:MDTBA + 048h

Default Flash Address: C48h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC48h	31:0	Reserved, set to '0'		No

9.217 PMC Descriptor Record 14 (Flash Descriptor Records)

Flash Address:MDTBA + 04Ch

Default Flash Address: C4Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC4Ch	31:0	Reserved, set to '0'		No

9.218 PMC Descriptor Record 15 (Flash Descriptor Records)

Flash Address:MDTBA + 050h

Default Flash Address: C50h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC50h	31:0	Reserved, set to '0'		No

9.219 PMC Descriptor Record 16 (Flash Descriptor Records)

Flash Address:MDTBA + 054h

Default Flash Address: C54h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC54h	31:0	Reserved, set to '0'		No

9.220 PMC Descriptor Record 17 (Flash Descriptor Records)

Flash Address:MDTBA + 058h

Default Flash Address: C58h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC58h	31:0	Reserved, set to '0'		No

9.221 PMC Descriptor Record 18 (Flash Descriptor Records)

Flash Address:MDTBA + 05Ch

Default Flash Address: C5Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC5Ch	31:0	Reserved, set to '0'		No

9.222 PMC Descriptor Record 19 (Flash Descriptor Records)

Flash Address:MDTBA + 060h

Default Flash Address: C60h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC60h	31:0	Reserved, set to '0'		No

9.223 PMC Descriptor Record 20 (Flash Descriptor Records)

Flash Address:MDTBA + 064h

Default Flash Address: C64h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC64h	31:0	Reserved, set to '0'		No

9.224 CPU Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 068h

Default Flash Address: C68h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC68h	31:27	CPU Strap Length (CPUSL): Identifies the 1's based number of Dwords of Processor Straps to be read, up to 31 DWs (1KB) max. A setting of all 0's indicates there are no Processor DW straps. Set this field to 0x3h		No
	26:0	Reserved, set to '0'		No

9.225 CPU Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 06Ch

Default Flash Address: C6Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC6Ch	31	Reserved, set to '0x1'		No
	30:16	Reserved, set to '0'		No
	17	Encrypted Debug Enable: 0 = Encrypted Debug Enabled 1 = Encrypted Debug Disabled	This setting determines if encrypted debugging is enabled Note: This strap is intended for debugging purposes only.	Yes
	14:15	Reserved, set to '0'		No
	13	JTAG Power Disable: 0 = Disable JTAG Power for C10 and deeper states 1 = Enable JTAG Power for C10 and deeper states	This setting determines if JTAG power will be maintained on C10 or lower power states. Note: This strap is intended for debugging purposed only.	Yes
	12	Processor Boot Max Non-Turbo Frequency: 0 = Disable Boot Non-Turbo Max Frequency 1 = Enable Boot Non-Turbo Max Frequency	This setting determines if the processor will operate at maximum Non-Turbo frequency at power-on and boot. Note: This strap is intended for debugging purposed only.	Yes
	11:6	Flex Ratio: '0x0'	This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for debugging purposed only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	Yes
	5	BIST Initialization: 0 = Disable BIST at Reset 1 = Enable BIST at Reset	This setting determines if BIST will be run at platform reset after BIOS requested actions. Note: This strap is intended for debugging purposed only.	Yes
	4:1	Number of Active Cores: 0x0 = All Cores active 0x1 = One core active 0x2 = Two cores active 0x3 = Three cores active 0x4 = Four cores active	This setting controls the number of active processor cores. Note: This strap is intended for debugging purposed only. See BIOS Spec for more details on enabling / disabling processor cores.	Yes
	0	Reserved, set to '0'		No

9.226 CPU Descriptor Record 2 (Flash Descriptor Records)

Flash Address: MDTBA + 070h

Default Flash Address: C70h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC70h	31	Platform IMON: 0 = IMON Enabled 1 = IMON Disabled	Note: This strap should be left at the recommended default setting.	Yes
	30	Reserved, set to '0'		No
	29	VCC IN SVID VR Type: 0 = VCC IN SVID VR Type SVID 1 = VCC IN SVID VR Type is fixed VR	This setting determines the VCC IN SVID VR. See Processor EDS for details.	Yes
	28:25	VCC IN SVID VR Address: '0'	This setting determines the VCC IN SVID VR Address for the platform.	Yes
	24:5	Reserved, set to '0'		No
	4	VCC SFR OC PG Present: 0 = VCC SFR OC PG Present 1 = VCC SFR OC PG Not Present	This setting determines if VCC SFR OC PG is present on the platform.	Yes
	3	VCC ST PG Present: 0 = VCC ST PG Present 1 = VCC ST PG Not Present	This setting determines if VCC ST PG is present on the platform	Yes
	2	VCC STG PG Present: 0 = VCC STG PG Present 1 = VCC STG PG Not Present	This setting determines the SA power plane topology. See Processor EDS for details. Note: This strap should be left at the recommended default setting.	Yes
	1	VDDQ TX Rail Supply: 0 = Tied to VDDQ (1.1/1.2v) 1 = Tied to LP4x (0.6v)	This setting determines if the VDDQ TX Rail supply is tied to VDDQ or LP4x.	Yes
	0	VCC Aux Present: 0 = VCC Aux is not Present 1 = VCC Aux is Present	This setting determines if VCC Aux exists as a separate VR.	Yes

9.227 CPU Descriptor Record 3 (Flash Descriptor Records)

Flash Address: MDTBA + 074h

Default Flash Address: C74h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC74h	31:0	SE Key Mode: '0x0'	Note: This strap should be left at the recommended default setting.	Yes

9.228 Intel® CSE Descriptor Record 0 (Flash Descriptor Records)

Flash Address: MDTBA + 078h

Default Flash Address: C78h

Offset from 0	Bits	Description	Usage	FIT Visible
0xC78h	31:0	Reserved, set to '0'		No

9.229 Intel® CSE Descriptor Record 1 (Flash Descriptor Records)

Flash Address: MDTBA + 07Ch

Default Flash Address: C7Ch

Offset from 0	Bits	Description	Usage	FIT Visible
0xC7Ch	31:24	Reserved, set to '0'		No
	23:16	Early USB DbC Intel® CSE Boot Stall Enable: 0 = Intel® CSE Boot Stall not enabled 1 = Intel® CSE Boot Stall enabled	This setting enables a delay during Intel® CSE FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	Yes
	15:8	USB Connector's Associated USB3 Port enable: 0x0 = USB3 Port 0 DbC enabled 0x1 = USB3 Port 1 DbC enabled 0x2 = USB3 Port 2 DbC enabled 0x3 = USB3 Port 3 DbC enabled 0xff = No USB3 ports are assigned to DbC All other values are Reserved	This setting determines which USB3 port goes to the target USB2 ports connector for Early DbC debugging.	Yes
	7:0	USB2 DbC port enable: 0x0 = USB2 Port 0 DbC enabled 0x1 = USB2 Port 1 DbC enabled 0x2 = USB2 Port 2 DbC enabled 0x3 = USB2 Port 3 DbC enabled 0x4 = USB2 Port 4 DbC enabled 0x5 = USB2 Port 5 DbC enabled 0x6 = USB2 Port 6 DbC enabled 0x7 = USB2 Port 7 DbC enabled 0x8 = USB2 Port 8 DbC enabled 0x9 = USB2 Port 9 DbC enabled 0xff = No USB2 ports are assigned to DbC All other values are Reserved	This setting determines which USB2 ports are enabled for Early DbC debugging.	Yes



10 Configuration Dependencies

10.1 Descriptor Configuration Setting Enabling Dependencies

This chapter outlines the descriptor configuration dependencies for enabling Elkhart Lake Hardware I/O, Bus and GPIO components.

10.1.1 High Speed IO (HSIO) Port Enabling

Below diagram provides better illustration on HSIO muxing and next table shows how to enable each mux functionality on HSIO lane.

Note: Refer to EDS for further details.

Table 10-1. Elkhart Flex I/O Map

ModPHY Lanes											
0	1	2	3	4	5	6	7	8	9	10	11
USB SuperSpeed							SGMII GbE				
0	1	2	3				PSE 0	Host 0	PSE 1	Host 0	PSE 1
PCIe 0				UFS 0		UFS 1		SATA			
0	1	2	3	0	1	0	1	0	1	0	1
PCIe 2		PCIe 2		PCIe 3		PCIe 1		PCIe 1			
0	1	0	1	0	1	0	1	0	1	0	1
						PCIe 1					
						0					

Table 10-2. HSIO Lane Muxing Selection (Sheet 1 of 2)

HSIO Lane (Port#)	Strap Offset	Description
Lane 0 (USB P0)	No muxing	
Lane 1 (USB P1)	No muxing	
Lane 2 (USB P2)	FPSBA + C9h	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
	FPSBA + 38h	XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP)
Lane 2 (PCIe 0 (Single VC P0))	FPSBA + C9h	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
	FPSBA + 6Dh	PCIe Controller 1 (Port 0-3)
Lane 2 (PCIe 2 (Multi VC P0))	FPSBA + C9h	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
	FPSBA + 78h	PCIe Multi VC Controller 2
Lane 3 (USB P3)	FPSBA + CAh	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
	FPSBA + 38h	XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP)
Lane 3 (PCIe Controller 1 P1)	FPSBA + CAh	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
	FPSBA + 6Dh	PCIe Controller 1 (Port 0-3)
Lane 3 (Multi VC #2 P1)	FPSBA + CAh	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
	FPSBA + 78h	PCIe Multi VC Controller 2
Lane 4 (PCIe Controller 1 P2)	FPSBA + CAh	FIA_LOSL4 (FIA/LOSL4)
	FPSBA + 6Dh	PCIe Controller 1 (Port 0-3)
Lane 4 (Multi VC #2 P0)	FPSBA + CAh	FIA_LOSL4 (FIA/LOSL4)
	FPSBA + 78h	PCIe Multi VC Controller 2
Lane 5 (PCIe Controller 1 P3)	FPSBA + CAh	FIA_LOSL5 (FIA/LOSL5)
	FPSBA + 6Dh	PCIe Controller 1 (Port 0-3)
Lane 5 (Multi VC #2 P1)	FPSBA + CAh	FIA_LOSL5 (FIA/LOSL5)
	FPSBA + 78h	PCIe Multi VC Controller 2
Lane 6 (PCIe P6)	FPSBA + CBh	FIA_LOSL6 (FIA/LOSL6)
Lane 6 (Multi VC #3 P0)	FPSBA + CBh	FIA_LOSL6 (FIA/LOSL6)
	FPSBA + 7Ch	PCIe Multi VC Controller 3
Lane 6 (UFS Storage 0)	FPSBA + CBh	FIA_LOSL6 (FIA/LOSL6)
Lane 7 (PCIe P7)	FPSBA + CCh	FIA_LOSL7 (FIA/LOSL7)
Lane 7 (Multi VC #1 P0)	FPSBA + CCh	FIA_LOSL7 (FIA/LOSL7)
	FPSBA + 74h	PCIe Multi VC Controller 1
Lane 7 (Multi VC #3 P1)	FPSBA + CCh	FIA_LOSL7 (FIA/LOSL7)
	FPSBA + 7Ch	PCIe Multi VC Controller 3
Lane 7 (UFS Storage 1)	FPSBA + CCh	FIA_LOSL7 (FIA/LOSL7)
Lane 7 (TSN PSE 0)	FPSBA + CCh	FIA_LOSL7 (FIA/LOSL7)
Lane 8 (PCIe P8)	FPSBA + CCh	FIA_LOSL8 (FIA/LOSL8)
Lane 8 (Multi VC #1 P0)	FPSBA + CCh	FIA_LOSL8 (FIA/LOSL8)
	FPSBA + 74h	PCIe Multi VC Controller 1
Lane 8 (UFS Boot 0)	FPSBA + CCh	FIA_LOSL8 (FIA/LOSL8)
Lane 8 (TSN Host 0)	FPSBA + CCh	FIA_LOSL8 (FIA/LOSL8)
Lane 9 (PCIe P9)	FPSBA + CDh	FIA_LOSL9 (FIA/LOSL9)

Table 10-2. HSIO Lane Muxing Selection (Sheet 2 of 2)

HSIO Lane (Port#)	Strap Offset	Description
Lane 9 (Multi VC #1 P1)	FPSBA + CDh	FIA_LOSL9 (FIA/LOSL9)
	FPSBA + 74h	PCIe Multi VC Controller 1
Lane 9 (UFS Boot 1)	FPSBA + CDh	FIA_LOSL9 (FIA/LOSL9)
Lane 9 (TSN PSE 1)	FPSBA + CDh	FIA_LOSL9 (FIA/LOSL9)
Lane 10 (PCIe P10)	FPSBA + CDh	SATA / PCIe Combo Port 0 (FIA/LOSL10)
Lane 10 (Multi VC #1 P0)	FPSBA + CDh	SATA / PCIe Combo Port 0 (FIA/LOSL10)
	FPSBA + 74h	PCIe Multi VC Controller 1
Lane 10 (SATA P0)	FPSBA + CDh	SATA / PCIe Combo Port 0 (FIA/LOSL10)
	FPSBA + 08h	SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0)
	FPSBA + D0h	SATA / PCIe Select for Port 0 (SATA_PCIE_SP0)
Lane 10 (TSN Host 0)	FPSBA + CDh	SATA / PCIe Combo Port 0 (FIA/LOSL10)
Lane 11 (PCIe P11)	FPSBA + CEh	SATA / PCIe Combo Port 1 (FIA/LOSL11)
Lane 11 (Multi VC #1 P1)	FPSBA + CEh	SATA / PCIe Combo Port 1 (FIA/LOSL11)
	FPSBA + 74h	PCIe Multi VC Controller 1
Lane 11 (SATA P1)	FPSBA + CEh	SATA / PCIe Combo Port 1 (FIA/LOSL11)
	FPSBA + 2Ch	SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1)
	FPSBA + D0h	SATA / PCIe Select for Port 1 (SATA_PCIE_SP1)
Lane 11 (TSN PSE 1)	FPSBA + CEh	SATA / PCIe Combo Port 1 (FIA/LOSL11)

10.1.2 Configuring PCIe on HSI O Dependencies

10.1.2.1 For PCIe Controller #1:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
4x1 on Lanes 0-3			
FPSBA + 6Dh	4:3	0x0	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x0	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
1x2, 2x1 on Lane 0-3			
FPSBA + 6Dh	4:3	0x1	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x0	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
2x1, 1x2 on Lanes 0-3 (Lane Reversed)			
FPSBA + 6Dh	4:3	0x1	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x1	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
2x2 on Lanes 0-3			
FPSBA + 6Dh	4:3	0x2	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x0	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
1x4 on Lanes 0-3			
FPSBA + 6Dh	4:3	0x3	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x0	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
1x4 on Lanes 0-3 (Lane Reversed)			
FPSBA + 6Dh	4:3	0x3	PCIe Controller 1 (Port 0-3)
FPSBA + 6Dh	2	0x1	PCIe Controller 1 Lane Reversal
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)

10.1.3 Configuring Multi VC PCIe on HSI O Dependencies

10.1.3.1 For Multi VC Controller #1:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
x1 PCIe on Lane 7			
FPSBA + 74h	3:1	0x4	PCIe Multi VC Controller 1
FPSBA + CCh	3:0	0xB	FIA_LOSL7 (FIA/LOSL7)
x1 PCIe on Lane 8			
FPSBA + 74h	3:1	0x4	PCIe Multi VC Controller 1
FPSBA + CCh	7:4	0xB	FIA_LOSL8 (FIA/LOSL8)
x1 PCIe on Lane 10			
FPSBA + 74h	3:1	0x4	PCIe Multi VC Controller 1
FPSBA + CDh	7:4	0xB	SATA / PCIe Combo Port 0 (FIA/LOSL10)
x2 on Lanes 8 and 9			
FPSBA + 74h	3:1	0x4	PCIe Multi VC Controller 1
FPSBA + CCh	7:4	0xB	FIA_LOSL8 (FIA/LOSL8)
FPSBA + CDh	3:0	0xB	FIA_LOSL9 (FIA/LOSL9)
x2 on Lanes 10 and 11			
FPSBA + 74h	3:1	0x4	PCIe Multi VC Controller 1
FPSBA + CDh	7:4	0xB	SATA / PCIe Combo Port 0 (FIA/LOSL10)
FPSBA + CEh	3:0	0xB	SATA / PCIe Combo Port 1 (FIA/LOSL11)

10.1.3.2 For Multi VC Controller #2:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
x1 on Lane 2			
FPSBA + 78h	3:1	0x4	PCIe Multi VC Controller 2
FPSBA + C9h	7:4	0xB	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
x1 on Lane 4			
FPSBA + 78h	3:1	0x4	PCIe Multi VC Controller 2
FPSBA + CAh	7:4	0xB	FIA_LOSL4 (FIA/LOSL4)
x2 on Lanes 2 and 3			
FPSBA + 78h	3:1	0x4	PCIe Multi VC Controller 2
FPSBA + C9h	7:4	0xB	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
FPSBA + CAh	3:0	0xB	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
x2 on Lanes 4 and 5			
FPSBA + 78h	3:1	0x4	PCIe Multi VC Controller 2
FPSBA + CAh	7:4	0xB	FIA_LOSL4 (FIA/LOSL4)
FPSBA + CBh	3:0	0xB	FIA_LOSL5 (FIA/LOSL5)

10.1.3.3 For Multi VC Controller #3:

Offset from 0	Bits	Lane Configuration	Descriptor Configuration Parameter
x1 on Lane 6			
FPSBA + 7Ch	3:1	0x4	PCIe Multi VC Controller 3
FPSBA + CBh	7:4	0xB	FIA_LOSL6 (FIA/LOSL6)
x2 on Lanes 6 and 7			
FPSBA + 7Ch	3:1	0x4	PCIe Multi VC Controller 3
FPSBA + CBh	7:4	0xB	FIA_LOSL6 (FIA/LOSL6)
FPSBA + CCh	3:0	0xB	FIA_LOSL7 (FIA/LOSL7)

10.1.4 TPM over SPI Enabling Dependencies

10.1.4.1 To enable TPM over SPI :

Offset from 0	Bits	Required Value	Frequency	Descriptor Configuration Parameter
FPSBA + C4h	0	0x1	N/A	TPM Over SPI Bus Enabled (TOS)
FPSBA + 55h	2:0	0x0	100MHz	SPI TPM Clock Frequency (STCF)
		0x1	50MHz	
		0x4	25MHz	
		0x6	14MHz	

10.1.4.2 To disable TPM over SPI :

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
FPSBA + C4h	0	0x0	TPM Over SPI Bus Enabled (TOS)

10.1.5 mSATA/M.2 / SATA Express Enabling Dependencies

10.1.5.1 SATA0 / PCIe10 mSATA /M.2 / SATA Express Enabling

Port 0 if running in configurable mode for SATAXPCEIO (e.g. mSATA/M.2 / SATA Express):

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
Port 10 Configured as SATA			
FPSBA + CDh	7:4	0x7	SATA / PCIe Combo Port 0 (FIA/LOSL10)
FPSBA + 08h	1:0	0x0	SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0)
FPSBA + D0h	1:0	0x0	SATA / PCIe Select for Port 0 (SATA_PCIE_SP0)
Port 10 Configured as PCIe			
FPSBA + CDh	7:4	0x5	SATA / PCIe Combo Port 0 (FIA/LOSL10)
FPSBA + 08h	1:0	0x1	SATA / PCIe GP Select for Port 0 (SATA_PCIE_GP0)
FPSBA + D0h	1:0	0x1	SATA / PCIe Select for Port 0 (SATA_PCIE_SP0)

10.1.5.2 SATA1 / PCIe11 mSATA /M.2 / SATA Express Enabling

Port 0 if running in configurable mode for SATAXPCEIO (e.g. mSATA/M.2 / SATA Express):

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
Port 11 Configured as SATA			
FPSBA + CEh	3:0	0x7	SATA / PCIe Combo Port 1 (FIA/LOSL11)
FPSBA + 2Ch	1:0	0x0	SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1)
FPSBA + D0h	3:2	0x0	SATA / PCIe Select for Port 1 (SATA_PCIE_SP1)
Port 11 Configured as PCIe			
FPSBA + CEh	3:0	0x5	SATA / PCIe Combo Port 1 (FIA/LOSL11)
FPSBA + 2Ch	1:0	0x1	SATA / PCIe GP Select for Port 1 (SATA_PCIE_GP1)
FPSBA + D0h	3:2	0x1	SATA / PCIe Select for Port 1 (SATA_PCIE_SP1)

10.1.6 3.1 Enabling Dependencies

10.1.6.1 USB 3.1 Port 2:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
Port 2 Configured as USB 3.1			
FPSBA + C9h	7:4	0x1	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
FPSBA + 38h	2	0x0	XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP)
Port 2 Configured as PCIe #2			
FPSBA + C9h	7:4	0x5	USB3 / PCIe Combo Port 0 (FIA/LOSL2)
FPSBA + 38h	1	0x1	XHCI Port 3 Ownership Strap (XHC_PORT3_OWNERSHIP_STRAP)

10.1.6.2 USB 3.1 Port 3:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
Port 3 Configured as USB 3.1			
FPSBA + CAh	3:0	0x1	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
FPSBA + 38h	3	0x0	XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP)
Port 3 Configured as PCIe #3			
FPSBA + CAh	3:0	0x5	USB3 / PCIe Combo Port 1 (FIA/LOSL3)
FPSBA + 38h	3	0x1	XHCI Port 4 Ownership Strap (XHC_PORT4_OWNERSHIP_STRAP)

10.1.7 UFS Enabling Dependencies

10.1.7.1 UFS Boot:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
x1 UFS			
FPSBA + CCh	7:4	0x9	FIA_LOSL8 (FIA/LOSL8)
FPSBA + CDh	3:0	0x0	FIA_LOSL9 (FIA/LOSL9)
x2 UFS			
FPSBA + CCh	7:4	0x9	FIA_LOSL8 (FIA/LOSL8)
FPSBA + CDh	3:0	0x9	FIA_LOSL9 (FIA/LOSL9)

10.1.7.2 UFS Storage:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
x1 UFS			
FPSBA + CBh	7:4	0x9	FIA_LOSL6 (FIA/LOSL6)
FPSBA + CCh	3:0	0x0	FIA_LOSL7 (FIA/LOSL7)
x2 UFS			
FPSBA + CBh	7:4	0x9	FIA_LOSL6 (FIA/LOSL6)
FPSBA + CCh	3:0	0x9	FIA_LOSL7 (FIA/LOSL7)

10.1.8 TSN GbE Port Select Enabling Dependencies

10.1.8.1 TSN Configuration:

Offset from 0	Bits	Required Value	Descriptor Configuration Parameter
TSN / PSE on Lane 7 and 9			
FPSBA + CCh	3:0	0xA	FIA_LOSL7 (FIA/LOSL7)
FPSBA + CDh	3:0	0xA	FIA_LOSL9 (FIA/LOSL9)
TSN / PSE on Lanes 7 & 11			
FPSBA + CCh	3:0	0xA	FIA_LOSL7 (FIA/LOSL7)
FPSBA + CEh	3:0	0xA	SATA / PCIe Combo Port 1 (FIA/LOSL11)
TSN / Host on Lane 8			
FPSBA + CCh	7:4	0xA	FIA_LOSL8 (FIA/LOSL8)
TSN Host on Lane 10			
FPSBA + CDh	7:4	0xA	SATA / PCIe Combo Port 0 (FIA/LOSL10)

11 RPMC Configuration

Replay Protection Monotonic Counter (RPMC) is a capability providing Anti-Replay Protection using Monotonic Counters inside SPI Flash.

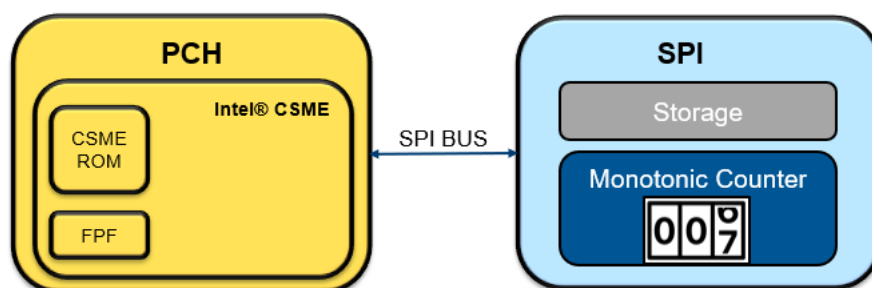
RPMC protection relies on:

- Special RPMC HW and logic inside the SPI Flash
- Intel® CSME FW support that utilizes RPMC capabilities within Flash

RPMC support in SPI Flash and Intel® CSME FW ensures the integrity of the data and mitigates rollback attacks.

Replay protection based RPMC is immune to power loss in case it's reset or corrupted and therefore more robust than using PRTC based monotonic counters.

11.1 System Components - High-Level Architecture Block Diagram



Legend	
	Existing Intel Component
	Existing Third Party Component
	New Third Party Component

Acronyms:	
MC	= Monotonic Counter
BC	= Binding Counter
SK	= Session Key
BK	= Binding Key

Main R&R:	
CSME ROM:	Derive BK, SK
FPF:	Hold binding counter
SPI MC:	hold monotonic counter in SPI HW
CSME FW:	Manage counters

11.2 Monotonic counters

Monotonic counters are counters on the SPI Flash maintained by Intel® CSME FW.

SPI Flash has a set of four 32-bit monotonic counters, where Intel® CSME FW uses two of these counters

Intel® CSME FW ensures FW write operations will not exceed SPI RPMC monotonic counter increment rate specified by RPMC HW during platform lifetime supported by Intel

Reading and incrementing the counters in the Flash is done using authenticated commands with a key known to both: SPI Flash and Intel® CSME FW

11.3 Binding at End of Manufacturing (EOM)

RPMC Binding pairs between SPI Flash and PCH by provisioning the Binding key produced by PCH into SPI Flash. This pairing is done as part of the EOM flow which usually takes place at the manufacturing line.

In cases where EOM is set in Intel® FIT to be performed on first boot, the binding will happen at first boot, after a complete configuration was defined using Intel® FIT, and access permission were set in the image.

In cases where EOM is not set in Intel® FIT configuration, the binding is performed using FPT tool systems when 'Intel® FPT -closemnf' is executed.

On platforms outside the manufacturing line (non PRQ parts), the binding happens when 'Intel® FPT -closemnf' is executed only if 'HW BINDING enabled' flag is set to 'Enabled' in Intel® FIT.

Prior to the binding operation, the Intel® CSME data is Anti Replay protected using a default key.

11.3.1 RPMC binding on Dual SPI configuration

When only one of the two SPIs supports RPMC, it will be selected by the SPI Controller.

If both SPIs support RPMC, then the lower addressed chip will be selected.

When the selected SPI is being replaced, a rebinding flow is required.

11.4 Refurbish flows impact

11.4.1 PCH replacement

Before EOM:

PCH replacement without SPI replacement/re-flashing is supported (up to 5 replacements). RPMC is functional with a default key.

Post EOM:

PCH replacement requires SPI replacement as well as running the EOM.

11.4.2 SPI replacement

Before Binding (Pre-EOM):

SPI part can be replaced infinite number of times (default key is used).

After Binding (Post-EOM):

In cases where SPI Flash was removed, it cannot be used with another PCH.

If RPMC rebinding is enabled - New SPI Flash will be automatically paired with PCH.

If RPMC rebinding is disabled - RPMC will not be used. Applications whose data requires RPMC protection will not be fully functional.

11.4.3 SPI re-flash

Binding key not re-flashed. Monotonic counter will not be reset, data will be lost.

11.5 RPMC re-binding

Rebinding is essential to all platforms that support refurbishing in the field.

After the initial bind has been performed, if the SPI Flash part is replaced and rebinding is enabled, the Intel® CSME FW will bind the new RPMC Flash part automatically as part of the 1st boot flow.

Intel® CSME FW detects that Flash is using the default key. It then triggers rebinding flow that produces a new Binding key and sends it to the Flash

The PCH can be paired with up to 16 RPMC enabled SPI Flash parts during the platform life cycle.

Rebinding is assumed to be done in a safe & secure environment (e.g., ODM/OEM manufacturing site, or OEM service center).

A FAQ and Troubleshooting

A.1 FAQ

Q: How do I find the Intel® Flash Programming Tool (Intel® FPT) and Intel® Flash Image Tool (Intel® FIT) for my platform?

A: The aforementioned flash tools are included in the system tools directory in Intel® CSE FW kit. Please ensure that you download the appropriate kit for the target platform.

Target	Platform Name In VIP	Kit Name
Elkhart Lake	Elkhart Lake Platform	Intel® Converged Security Engine 15.40.x (use latest version)

Q: How do I build an Image for my Intel PCH based platform?

A: Elkhart Lake family based platforms, you can follow the appropriate instructions in the FW Bringup Guide which is located in the root directory of the appropriate Intel® CSE KIT.

Q: Is my flash part supported by the Intel® Flash Programming Tool (Intel® FPT)? How can I add support for a new flash to Intel® FPT?

A: Look at fparts.txt to see if the intended flash part is present. If the intended flash part meets the guidelines defined in the *External Design Specification (EDS)*, Intel® Converged Security Engine (Intel® CSE) Firmware SPI Flash Requirements and support may be added to FPT by adding an entry for the part into the Fparts.txt file.

Q: Is my flash part supported by Intel® CSE Firmware? How can I add support for a new flash to Intel® CSE Firmware?

A: As long as the SPI flash devices meets the requirements defined in the *External Design Specification (EDS)*, support may be added for the device. BIOS will have to set up the Host VSCC registers. The Intel Converged Security Engine VSCC table in the descriptor will also have to be set up in order to get Intel® CSE firmware to work.

Adding support does not imply validation or guarantee a flash part will work. Platform designers/integrators will have to validate all flash parts with their platforms to ensure full functionality and reliability.

Q: Do I have to use SFDP enabled SPI flash parts?

A: Yes you will need to use SFDP enabled SPI flash parts regardless of using the VSCC table entries Elkhart Lake does not support VSCC only SPI flash parts.

Q: Why does FPT/verify fail for my system even when I wrote nothing to flash?

A: Intel® CSE Firmware performs periodic writes to SPI flash when it is active. Due to this the Intel® CSE region may not match the source file. There are also other system activities beside the Intel® CSE that can change the data on the flash vs the original image. For example, the GbE check sum is updated on flash part whenever the value is incorrect.

Q: How can I overwrite the descriptor when FPT does not have write access? How can I overwrite a region that is locked down by descriptor protections? How do I write to flash space that is not defined by the descriptor?

A: By asserting HDA_SDO (flash descriptor override strap) low on the rising edge of PWROK, you can read, write and erase all of SPI flash space regardless of descriptor protections. Any protections imposed by BIOS or directly to the SPI flash part still apply. This should only be used in debug or manufacturing environments. End customers should **NOT** receive systems with this strap engaged.

Q: I have two flash parts installed on the board. Why does fpt /i only show one flash part?

A: Elkhart Lake will not recognize the second SPI flash part unless it is in descriptor mode and the Component section of the descriptor properly describes the flash. Another possibility is that you have two different flash parts and the second flash part is not defined in fparts.txt.

A.2 Troubleshooting

Q: I'm seeing the following error:

```
Intel(R) Flash Programming Tool. Version:  x.x.x.xxxx
Copyright (c) 2007-2015, Intel Corporation. All rights reserved.
Platform: Intel(R) Qxx Express Chipset
Reading HSFSTS register... Flash Descriptor: Invalid

--- Flash Devices Found ---

Error: Timeout waiting for hardware to complete read operation!
      SSFSTS register: 0x00

Error: Timeout waiting for hardware to complete read operation!
      SSFSTS register: 0x00

Error: Timeout waiting for hardware to complete read operation!
      SSFSTS register: 0x00

Error: Failed to read the device ID from the flash part!
```

A: You may be using the wrong version of FPT. Please ensure that you are using the flash tools that were provided in the kit for the target systems.

Q: What does following FPT error message mean?

Error: The host does not have write access to the target flash memory!

A: In order for FPT to read or write to a given region, BIOS/Host must have read/write permissions to that target region. This access is set in the descriptor. Look closely at all the addresses defined in the output of FPT /i. If there are any gaps in flash space defined you cannot perform a full flash write. You have to update region by region. Refer to [4.4 Region Access Control](#) for more information. You may have to reflash the descriptor to get the proper access.

Q: What does following FPT error message mean?

Error: Flash program registers are locked! HSFSTS[15] (FLOCKDN).

A: The Flash Configuration Lock-Down (FLCOKDN) bit was set HSFS (hardware sequencing flash status register). This locks down all the program registers in the ICH. If your BIOS and descriptor do not set up Hardware Sequencing, you will have to leave this bit unset in order to use FPT. You may have to upgrade the latest version of FPT as older versions do not support Hardware Sequencing. Please refer to [Hardware Sequencing Flash Status Register](#) in the *External Design Specification (EDS)* for the location for the HSFS. Try reflashing the SPI device with a 3rd Party programmer. If you still see this error message, please contact your BIOS vendor to ensure that they are not setting this bit.

Q: What does following FPT error message mean?

Error: There is no supported SPI flash device installed.

A: See the answer to the question above: *Is my flash part supported by the Flash Programming Tool (FPT)? How can I add support for a new flash to FPT?*

If the tool correctly identifies the flash part installed and still gives an error message like:

--- Flash Devices Found ---

SPI 1234 ID:0x123456 Size: 4096KB (32768Kb)

Device ID: 0xFFFF not supported.

Error 405: There is no supported SPI flash device installed

This error will result when the descriptor has two flash parts defined. Edit the image via FIT/FITC and set the number of flash components to 1.

See [6.4 Recommendations for Flash Configuration Lockdown and Vendor Component Lock Bits](#) for Opcodes required for FPT operation.

§ §