Intel Confidential

Purley/SKX Platform CRB BIOS Release Notes

August 2nd, 2017
Revision: 142R08

Legal Information

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
This document contains information on products in the design phase of development.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Copyright (C) 2014-2017, Intel Corporation. All rights reserved.

Disclaimer

Intel attempts to release Server BIOS binaries, under NDA for testing on supported CRBs that adhere to the same security requirements as should be used in production. However, some BIOS differences exist. The differences, which do not adhere to security requirements, that should be addressed before releasing a product based on for this release are listed below:

1. GPIO lock: The current CRB BIOS binary leaves the GPIOs unlocked, with a setup control to change the default. In a true production BIOS, the GPIOs are locked and no setup control to override exists.

2. SPI Lock: The current CRB BIOS binary leaves SPI unlocked to allow ease of upgrade in the field using non-production applications to upgrade CRBS to non-production binaries. In a true production BIOS, SPI is locked. In particular, the SPI flash descriptor permissions should be set to least privilege.

3. Runtime Variables: The current CRB BIOS binary defines Several PCDs as Dynamic HII PCDs such that validation has maximum flexibility in debug by offering setup control over these features. In a true production BIOS, these PCDs should be static PCDs configured at build time.

4. SWSMI Interface: The current CRB BIOS binary exposes several SWSMI functions to support ease of configuration by internal validation applications. The source code to these functions has not been included, though they are present in the binary. In a true production BIOS, these interfaces should not exist.

Contents

BKC to BIOS mapping

BKC release	BIOS version	Ingredients	
WW31	142R08 *SPI image*: 2017.30.4.15	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000029
		ME SPS FW version (LBG)	SPS_E5_04.00.03.235.0
		LT.BIN (Startup ACM)	Production,v1.3.3_LBG
		SINIT.BIN	Production,v1.3.2_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW27	140R10 *SPI image*: 2017.26.5.16	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000026
		ME SPS FW version (LBG)	SPS_E5_04.00.03.219.0
		LT.BIN (Startup ACM)	Production,v1.3.2_LBG
		SINIT.BIN	Production,v1.3.2_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW25	139R09 *SPI image*: 2017.24.5.06	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000022
		ME SPS FW version (LBG)	SPS_E5_04.00.03.216.0
		LT.BIN (Startup ACM)	Production,v1.3.1_LBG
		SINIT.BIN	Production,v1.3.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2

WW23	137R08 *SPI image*: 2017.22.5.12	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000022
		ME SPS FW version (LBG)	SPS_E5_04.00.03.211.0
		LT.BIN (Startup ACM)	Production,v1.3.0_LBG
		SINIT.BIN	Production,v1.3.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW21	135R03 *SPI image*: 2017.20.3.14	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200001E
		ME SPS FW version (LBG)	SPS_E5_04.00.03.206.0
		LT.BIN (Startup ACM)	Production,v1.2.0_LBG
		SINIT.BIN	Production,v1.2.1_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW19	133R12 *SPI image*: 2017.18.5.08	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200001C
		ME SPS FW version (LBG)	SPS_E5_04.00.03.202.0
		LT.BIN (Startup ACM)	Production,v1.2.0_LBG
		SINIT.BIN	Production,v1.2.1_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW17	132R08 *SPI image*: 2017.16.4.17	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200001A
		ME SPS FW version (LBG)	SPS_E5_04.00.03.199.0
		LT.BIN (Startup ACM)	Production,v1.2.0_LBG
		SINIT.BIN	Production,v1.2.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2

<table>
<tr><td>WW15</td><td>131R09
SPI image: 2017.15.4.07</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000018</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.195.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.2.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.2.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table>
</td></tr>
<tr><td>WW15</td><td>130R06
SPI image: 2017.14.2.03</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000016</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.185.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table>
</td></tr>
<tr><td>WW13</td><td>128R08
SPI image: 2017.12.5.07</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A0/A1 uCode</td><td>m1350650_8000002b</td></tr>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000016</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.176.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>WW12</td><td>127R04
<i>SPI image</i>: 2017.11.3.03</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A0/A1 uCode</td><td>m1350650_8000002b</td></tr>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000015</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.174.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table></td></tr>
<tr><td>WW11</td><td>126R06
<i>SPI image</i>: 2017.10.4.05</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A0/A1 uCode</td><td>m1350650_8000002b</td></tr>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000014</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.169.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table></td></tr>
<tr><td>WW10</td><td>125R03
<i>SPI image</i>: 2017.09.4.02</td><td>KTI uniphy recipe: V3.0
PCIe uniphy recipe: V3.25
<table>
<tr><td>SKYLAKE A0/A1 uCode</td><td>m1350650_8000002b</td></tr>
<tr><td>SKYLAKE A2 uCode</td><td>m1350651_8000002b</td></tr>
<tr><td>SKYLAKE B0 uCode</td><td>m9750652_80000034</td></tr>
<tr><td>SKYLAKE H0 uCode</td><td>m9750654_02000013</td></tr>
<tr><td>ME SPS FW version (LBG)</td><td>SPS_E5_04.00.03.166.0</td></tr>
<tr><td>LT.BIN (Startup ACM)</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>SINIT.BIN</td><td>Production,v1.1.0_LBG</td></tr>
<tr><td>BIOS Guard</td><td>PC_v0_9</td></tr>
<tr><td>GbE</td><td>0.2</td></tr>
</table></td></tr>
</table>

WW09	124R07 *SPI image*: 2017.08.4.10	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000013
		ME SPS FW version (LBG)	SPS_E5_04.00.03.163.0
		LT.BIN (Startup ACM)	Production,v1.1.0_LBG
		SINIT.BIN	Production,v1.1.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW08	123R04 *SPI image*: 2017.07.3.03	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000011
		ME SPS FW version (LBG)	SPS_E5_04.00.03.160.0
		LT.BIN (Startup ACM)	Production,v1.1.0_LBG
		SINIT.BIN	Production,v1.1.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW06	121R04 *SPI image*: 2017.05.3.03	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_02000011
		ME SPS FW version (LBG)	SPS_E5_04.00.03.148.0
		LT.BIN (Startup ACM)	Production,v1.1.0_LBG
		SINIT.BIN	Production,v1.1.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2

WW04	119R05 *SPI image*: 2017.03.3.04	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200000f
		ME SPS FW version (LBG)	SPS_E5_04.00.03.142.0
		LT.BIN (Startup ACM)	Production,v1.0.0_LBG
		SINIT.BIN	Production,v1.0.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW03	118R01 *SPI image*: 2017.02.5.22	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200000C
		ME SPS FW version (LBG)	SPS_E5_04.00.03.142.0
		LT.BIN (Startup ACM)	Production,v1.0.0_LBG
		SINIT.BIN	Production,v1.0.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW02	117R02 *SPI image*: 2017.02.5.14	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000034
		SKYLAKE H0 uCode	m9750654_0200000C
		ME SPS FW version (LBG)	SPS_E5_04.00.03.137.0
		LT.BIN (Startup ACM)	Production,v1.0.0_LBG
		SINIT.BIN	Production,v1.0.0_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2

WW01	116R01 *SPI image*: 2016.53.5.12	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	SKYLAKE A0/A1 uCode	m1350650_8000002b
			SKYLAKE A2 uCode	m1350651_8000002b
			SKYLAKE B0 uCode	m9750652_80000034
			SKYLAKE H0 uCode	m9750654_0200000C
			ME SPS FW version (LBG)	SPS_E5_04.00.03.137.0
			LT.BIN (Startup ACM)	Production,v0.9.5_LBG
			SINIT.BIN	Production,v0.9.5_LBG
			BIOS Guard	PC_v0_9
			GbE	0.2
WW52	114R09 *SPI image*: 2016.51.5.06	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	SKYLAKE A0/A1 uCode	m1350650_8000002b
			SKYLAKE A2 uCode	m1350651_8000002b
			SKYLAKE B0 uCode	m9750652_80000034
			SKYLAKE H0 uCode	m9750654_0200000C
			ME SPS FW version (LBG)	SPS_E5_04.00.03.137.0
			LT.BIN (Startup ACM)	Production,v0.9.5_LBG
			SINIT.BIN	Production,v0.9.5_LBG
			BIOS Guard	PC_v0_9
			GbE	0.2
WW51	113D07 *SPI image*: 2016.50.4.03	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	SKYLAKE A0/A1 uCode	m1350650_8000002b
			SKYLAKE A2 uCode	m1350651_8000002b
			SKYLAKE B0 uCode	m9750652_80000034
			SKYLAKE H0 uCode	m9750654_02000009
			ME SPS FW version (LBG)	SPS_E5_04.00.03.133.0
			LT.BIN (Startup ACM)	Production,v0.9.5_LBG
			SINIT.BIN	Production,v0.9.5_LBG
			BIOS Guard	PC_v0_9
			GbE	0.2

WW50	112D10 *SPI image*: 2016.49.5.09	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.25	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000033
		SKYLAKE H0 uCode	m9750654_02000009
		ME SPS FW version (LBG)	SPS_E5_04.00.03.133.0
		LT.BIN (Startup ACM)	Production,v0.9.5_LBG
		SINIT.BIN	Production,v0.9.5_LBG
		BIOS Guard	PC_v0_9
		GbE	0.2
WW49	111D13 *SPI image*: 2016.48.5.05	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000031 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.114.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_4_20161011_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_4_20161011_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW47	109D12 *SPI image*: 2016.46.4.08	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000031 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.113.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_4_20161011_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_4_20161011_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW46	108D11 *SPI image*: 2016.45.5.08	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_8000002d (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.111.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_4_20161011_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_4_20161011_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2

WW45	107D07 *SPI image*: 2016.44.3.02	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_8000002d (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.103.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_4_20161011_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_4_20161011_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW44	106D11 *SPI image*: 2016.43.5.10	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_8000002d (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.103.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_4_20161011_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_4_20161011_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW43	105D11 *SPI image*: 2016.41.6.10	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_8000002d (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.103.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_3_20160830_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_3_20160830_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW42	104D12 *SPI image*: 2016.41.6.10	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_8000002c (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.03.101.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_3_20160830_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_3_20160830_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2

WW40	102D12 *SPI image*: 2016.39.6.06	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000029 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.088.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_3_20160830_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_3_20160830_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW39	101D04 *SPI image*: 2016.38.3.03	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000029 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.086.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_3_20160830_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_3_20160830_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW38	100D14 *SPI image*: 2016.37.6.15	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000029 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.086.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_3_20160830_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_3_20160830_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW37	99D14 *SPI image*: 2016.36.5.09	KTI uniphy recipe: V3.0 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000029 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.084.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_2_20160810_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_2_20160810_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2

WW36	98D02 *SPI image*: 2016.35.2.01	KTI uniphy recipe: V2.5 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000028 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.081.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_2_20160810_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_2_20160810_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW35	97D05 *SPI image*: 2016.34.4.16	KTI uniphy recipe: V2.5 PCIe uniphy recipe: V3.0	
		SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000028 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.081.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_2_20160810_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_2_20160810_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW34	96D23 *SPI image*: 2016.33.5.10	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000028 (debug signed)
		ME SPS FW version (LBG)	SPS_E5_04.00.02.081.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_2_20160810_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_2_20160810_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW33	96D03 *SPI image*: 2016.32.4.04	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000025
		ME SPS FW version (LBG)	SPS_E5_04.00.02.069.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_1_20160725_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_1_20160725_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2

WW30	93D07 *SPI image*: 2016.31.6.09	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000022
		ME SPS FW version (LBG)	SPS_E5_04.00.02.064.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_9_0_20160712_LBG_NT_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_9_0_20160712_LBG_NT_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW29	93D07 *SPI image*: 2016.28.3.04	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000022
		ME SPS FW version (LBG)	SPS_E5_04.00.02.064.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_3_20160524_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_3_20160524_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW28	92D09 *SPI image*: 2016.27.5.05	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m9750652_80000022
		ME SPS FW version (LBG)	SPS_E5_04.00.02.064.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_3_20160524_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_3_20160524_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW26	90D03 *SPI image*: 2016.26.3.04	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m0f50652_80000020
		ME SPS FW version (LBG)	SPS_E5_04.00.02.053.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_3_20160524_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_3_20160524_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2

WW24	88D09 *SPI image*: 2016.23.4.03	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m1350652_80000017
		ME SPS FW version (LBG)	SPS_E5_04.00.02.053.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_3_20160524_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_3_20160524_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW23	87D08 *SPI image*: 2016.22.2.02	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m1350652_80000016
		ME SPS FW version (LBG)	SPS_E5_04.00.02.053.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_2_20160517_LBG_TR_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_2_20160517_LBG_TR_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW22	85D17 *SPI image*: 2016.21.1.10	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m1350652_80000015
		ME SPS FW version (LBG)	SPS_E5_04.00.02.033.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_0_20160419_LBG_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_0_20160419_LBG_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW21	85D17 *SPI image*: 2016.21.1.10	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m1350652_80000015
		ME SPS FW version (LBG)	SPS_E5_04.00.02.033.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_8_0_20160419_LBG_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_8_0_20160419_LBG_debug_signed
		BIOS Guard	2.0 rev 0.7 Beta Candidate
		GbE	0.2
WW18	82D04 *SPI image*: 2016.17.3.12	SKYLAKE A0/A1 uCode	m1350650_8000002b
		SKYLAKE A2 uCode	m1350651_8000002b
		SKYLAKE B0 uCode	m1350652_80000010
		ME SPS FW version (LBG)	SPS_E5_04.00.02.033.0
		LT.BIN (Startup ACM)	PURLEY_BIOSACX_v0_7_4_20160314_LBG_debug_signed
		SINIT.BIN	PURLEY_SINIT_v0_7_4_20160314_LBG_debug_signed
		BIOS Guard	None
		GbE	0.2

Potential issues

**Note: below table lists sightings that are under investigation*

No.	id	title	classification	bios_version	cpu	step ping
1.	5385534	ADDDC Bank to Rank upgrade doesnt take effect on Region 1	Investigate	131.R09	SKX-EP SKX-EX	All
2.	5385635	BIOSSCRATCHPAD7[27] is used for two purposes	Investigate	131.R09	SKX-EP SKX-EX	All
3.	5385651	MRC: BIOS configures illegal MC mode when ADDDC mode=en and pagepolicy=adaptive page mode	Investigate	133.R06	SKX-EP SKX-EX	All
4.	5385777	Purley 8-way system running Linpack test in Linux 7.2 generates lots of "IERR" when in 3 way interleaving	Investigate		SKX-EP SKX-EX	All

BIOS Releases

*Note: this section lists issue fixes in each BIOS revision

BIOS revision: 142R08 – BKC WW31 (PLR1)

518100:5346366: Add Production Patch Version 0x29 for SKX H0 to IFWI (PROD)

BIOS revision: 142R07

No change

BIOS revision: 142R06

518007:5385766: Hard PPR Failure after Memory CE injection
517977:5385651: MRC: BIOS configures illegal MC mode when ADDDC mode=en and pagepolicy=adaptive page mode

BIOS revision: 142R05

517644:5385977: Finalize code that sets Bit 11 in SPIBAR+0x04

BIOS revision: 142R04

No change

BIOS revision: 142R03

No change

BIOS revision: 142R02

No change

BIOS revision: 142R01

515412: Back out changelist 512615 (Incorrectly submitted)

BIOS revision: 141R13

No change

BIOS revision: 141R12

No change

BIOS revision: 141R11

514071:5385635: BIOSSCRATCHPAD7[27] is used for two purposes

BIOS revision: 141R10

513660:5385736: DCU SRAR hangs in bios under windows 2016 with Gen1 mode enabled, no opt-in.
513654:5385724: Hot Plug PCIe late Device Present Detection and command complete interrupt
513625:5385534: ADDDC Bank to Rank upgrade doesnt take effect on Region 1
513605:5385365: MAILBOX_BIOS_CMD_WRITE_PCU_MISC_CONFIG (0x6), Bit[28] UFS Disable was to be removed

BIOS revision: 141R09

No change

BIOS revision: 141R08

No change

BIOS revision: 141R07

No change

BIOS revision: 141R06

No change

BIOS revision: 141R05

512615:5385636: SRAT table still exist after Disabled "Publish SRAT"

BIOS revision: 141R04

No change

BIOS revision: 141R03

No change

BIOS revision: 141R02

No change

BIOS revision: 141R01

No change

BIOS revision: 140R18

No change

BIOS revision: 140R17

No change

BIOS revision: 140R16

No change

BIOS revision: 140R15

No change

BIOS revision: 140R14

No change

BIOS revision: 140R13

No change

BIOS revision: 140R12

No change

BIOS revision: 140R11

No change

BIOS revision: 140R10 – BKC WW27 (PV MR5)

510519:5346304: Purley Patch: Add Production Patch Version 0x26 for SKX H0 to IFWI(PROD)

BIOS revision: 140R09

510495:5385886: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

BIOS revision: 140R08

510309:5385887: Disable XPT in MR5

BIOS revision: 140R07

No change

BIOS revision: 140R06

509775:5346302: Please update SPS FW to SPS_E5_04.00.03.219.0 as Purley PV MR5 release to BKC. PROD

BIOS revision: 140R05

509711:5346298: Fort Park NVM 3.45 image with new OROM to be included in IFWI for Purley 2S (Also 5346299 for LR) PROD
509695:5385863: Windows 2016 CATERRs when trying to boot in non-NUMA mode with 128GB DIMMs

BIOS revision: 140R04

No change

BIOS revision: 140R03

509647:5346276: Purley ACM Version 1.3.2 Release for Trunk and MR5 (PROD)

BIOS revision: 140R02

507254:5346277: [2S-SKX] Ctrl+P menu is not displayed at splash screen with ME11 BIOS (FIX of 5346250 soft strap .xml file change name spt_lbg_fit_Corporate.xml)

BIOS revision: 140R01

No change

BIOS revision: 139R09 – BKC WW25 (PV MR4)

506110:5385840: CLONE SKX Sighting: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

BIOS revision: 139R08

505845:5385840: CLONE SKX Sighting: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

BIOS revision: 139R07

No change

BIOS revision: 139R06

505416:5385825: [2S] FW Eval lost PCIe Error Injection capabilities

BIOS revision: 139R05

505067:5385787: [NVDIMM] JedecNvDimm Coverity issue

BIOS revision: 139R04

504786:5385697: AcpiIoApic incorrect for 8S

BIOS revision: 139R03

No change

BIOS revision: 139R02

504192:5385491: BuildImage.sh files Restricted Tags in PurleyRpPkg and BakervillePkg do not match

BIOS revision: 139R01

503682:5385796: Request to integrate WMP B0_RC47 and S0_RC8 recipes into the IFWI official release

BIOS revision: 138R03

No change

BIOS revision: 138R02

503024:5385789: [FPGA] Caterr and POST code displaying 72 when boot from S5 with FPGA disabled.

BIOS revision: 138R01

No change

BIOS revision: 137R10

502362:5346233: Purley Patch: Add Production Patch Version 0x22 for SKX H0 to IFWI (PROD)

BIOS revision: 137R09

502014: Back out changelist 501968

BIOS revision: 137R08 – BKC WW23 (PV MR3)

501968:NO SIGHTING: Integration of microcode m9750654_02000022 (PROD)

BIOS revision: 137R07

501674:5385744: ERRINJCON.ERRINJDIS should be set by BIOS in every boot to disable error injection
501573:5385685: Hitting 768G limitation with Mirror mode enabled + MMCFG base set to 1 + 768G DDR4 installed

BIOS revision: 137R06

501434:5385764: Set_Strap_Lock is not set after resume from S3

BIOS revision: 137R05

No change

BIOS revision: 137R04

501059:5346224: Purley Patch: Add Production Patch Version 0x21 for SKX H0 to IFWI (PROD)

BIOS revision: 137R03

No change

BIOS revision: 137R02

No change

BIOS revision: 137R01

No change

BIOS revision: 136R08

499551:5385285: [NVDIMM] NVDIMM marked as "?" in windows 2016 Device Manager.

BIOS revision: 136R07

No change

BIOS revision: 136R06

No change

BIOS revision: 136R05

498574:5385708: [FPGA] RSA cannot add SMBIOS type198 as Fpga Fv hob init is skipped on subsequent boot

BIOS revision: 136R04

No change

BIOS revision: 136R03

No change

BIOS revision: 136R02

497796:5385686: [NVDIMM] System hangs with exception 0x0 at PC 0xD4, when ADR Batterybacked mode is enabled

BIOS revision: 136R01

497327:5385644: IOU2 pcie bifurcation incorrect on Kyanite boards
497273:5385667: [FPGA] Request to add a setup option to control HSSI EQ tuning as DFX hooks

BIOS revision: 135R04

497119:5385666: s5372912 Needs to be extended for H0 and CLX

BIOS revision: 135R03 – BKC WW21 (PV MR2)

5346202: Please update SPS FW to SPS_E5_04.00.03.206.0

BIOS revision: 135R02

496715:5346198:Purley Patch: Add Production Patch Version 0x1e for SKX H0 to IFWI (Prod)
496519, 496517:5385619: Set Bit 11 in SPIBAR+0x04

BIOS revision: 135R01

495797:5385623: Add checks in RC to automatically disable SNC when proc with less than 12 slices

BIOS revision: 134R03

No change

BIOS revision: 134R02

495078:5385583: MRC: Incorrect programming of TxEq setting post TxEQ training

BIOS revision: 134R01

494492:5385564: [FPGA] Request to add BBS version in Setup menu and bios serial log
494485:5385633: [FPGA] add HSSI 4x10 EQ table to BIOS

BIOS revision: 133R12 – BKC WW19 (PV MR1)

493707: NO_SIGHTING: Capsule update broken (Back out changelist 492757)

BIOS revision: 133R11

No change

BIOS revision: 133R10

493238:5385488: TXT is currently limited to 255 threads, not functional in 8S

BIOS revision: 133R09

492981:5385643: MRC: BIOS does not cache capIDs correctly for single-threaded mode. Can lead to training failures with control and command signals.

BIOS revision: 133R08

492757:5385619: Set Bit 11 in SPIBAR+0x04

BIOS revision: 133R07

492572:5346162: Purley Patch: Add Production Patch Version 0x1c for SKX H0 to IFWI (PROD)

BIOS revision: 133R06

492526:5346161: Purley Patch: Add SKX B1 Production Patch Release 0x137 to IFWI (PROD)

BIOS revision: 133R05

492193:5385509: t_stagger_ref change 1/2 tRFC -> 1/3 tRFC
492174:5385178: CNFG_500_NANOSEC in PCU (D30,F5,RD8[9:0]) is incorrectly programmed based on DDR Freq

BIOS revision: 133R04

No change

BIOS revision: 133R03

No change

BIOS revision: 133R02

No change

BIOS revision: 133R01

No change

BIOS revision: 132R08 – BKC WW17 (PV)

489280: Addendum (Correcting uCode File) - 5346127:Purley Patch: Add Production Patch Version 0x1a for SKX H0 to IFWI

BIOS revision: 132R07

489229: Updating Skylake_Production BIOS IDs: 20170420_CP_PURLEY_PRODUCTION_132_R07
489222:5346127: Purley Patch: Add Production Patch Version 0x1a for SKX H0 to IFWI

BIOS revision: 132R06

No change

BIOS revision: 132R05

488734:5385554: [Security VT] IA32_FEATURE_CONTROL MSR is locked at ready to boot event instead of EndofDXE (or) PciEnuResourceAssigned event

BIOS revision: 132R04

No change

BIOS revision: 132R03

488534:5385584: [Klocwork] Array boundary violation in PurleySktPkg\Dxe\MemRas\AdddcSparing.c:IsRankInPlusOne
488416:5385563: <s4048 kin, Issue#1>Route Through WB winning arbitration without credits blocks local WBs from completing, can cause deadlocks

BIOS revision: 132R02

No change

BIOS revision: 132R01

No change

BIOS revision: 131R11

No change

BIOS revision: 131R10

487415:5385511: [FPGA] Link width recognized x4, when plug an x8 pcie card into slot 1(x8).

BIOS revision: 131R09 – BKC WW16 (PC10)

No change

BIOS revision: 131R08

486855:5346094: Purley Patch: Add Production Patch Version 0x18 for SKX H0 to IFWI (Production)

BIOS revision: 131R07

486847:5346095: Purley Patch: Add Production Patch Version 0x17 for SKX H0 to IFWI (Production)

BIOS revision: 131R06

486689:5385541: PCIE Corrected Error logging broken on 131_R02

BIOS revision: 131R05

486653:5385548: [FPGA] System boot broken when VT-D enabled with SKX-P on FPGA board.
486592:5385431: PSTH IOSF Primary Trunk Clock Gating Enable is set in recent release of BIOS

BIOS revision: 131R04

486518:Back out changelist 486234(this change only apply for Skylake_Trunk)
486234:5385413:Pci devices are not detected during Pci scan as temp buses programmed in IioLateInit are not cleared
486232:5385510: Purley BIOS not setting Problematic Port bit for NTB Ports
486146:5385468: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

BIOS revision: 131R03

486031:5385363:ProcMemEnableReporting() doesn't fully enable poisoning due to IIO_DFX_LCK_CTL.dbgbuslck being locked
485948:5385509: t_stagger_ref change 1/2 tRFC -> 1/3 tRFC
485940:5385487: RC isnt handling Corrected errors during VLS operation
485789:5385473: CLONE SKX Sighting: DPN-MRT0D 25Gb NIC failed PCIe LTSSM LED TEst w/ Riser 2A/Slot 4, Riser3A/Slot8
485766:5385299: CLONE SKX Sighting: Hot Remove causes CTO Windows BSOD;

BIOS revision: 131R02

485456:5385412: PPR Code fixing CE on Bad DIMM, but CPGC still reporting failure in 2nd RowTest
485427:5385496: "sddc +1 ecc mode" not working as expected in ADDDC(MR)+1
485383:5385385: Cache poison error could not be detected correctly
485357:5385251: DMI error not logged,0x98/0x9a offset is not calculated correctly;
485283:5385490:[Klocwork][Purley] out of boundary access (read/write) with max_socket =1 or 2

BIOS revision: 131R01

484944:5385509: t_stagger_ref change 1/2 tRFC -> 1/3 tRFC
484899:NO_SIGHTING: Purley Release 131 BIOSID Update
484801:5385485: [Security VT] SMM Security Issue in Crystal Ridge _DSM interfaces

BIOS revision: 130R07

484587:5385350: [Klocwork] ABV issues (and one NPD) in PurleyPlatPkg

BIOS revision: 130R06 – BKC WW15 (PC9)

484007:5385428 Ph3 TxEq override does not work when Gen3 Override mode set to "Manual" in IIO DFX
483996:5385427: IIO DFX Ph2 TxEq override does not work when Gen3 Override mode set to "Manual"
483986:5385350: [Klocwork] ABV issues (and one NPD) in PurleyPlatPkg
483984:5385349: [Klocwork] ABV issues (and one NPD) in ProcMemInit

BIOS revision: 130R05

483788:5372008: [FPGA] FPGA HSSI BIOS flows

BIOS revision: 130R04

No change

BIOS revision: 130R03

483189:5385469:[FPGA]BIOS is assigning incorrect interrupt pin to the second socket FPGA in _PRT method (INT_B instead of INT_A)

BIOS revision: 130R02

482928:5372219 MDQ/MDQS read centering for DDR4 LRDIMMs

BIOS revision: 130R01

482642:NO_SIGHTING: Purley Release 130 BIOSID Update

BIOS revision: 129R05

482374:5372994: [FPGA] use FME MMIO to program GENPROTRANGE2 instead of KTI CSR
482165:NO_SIGHTING: Out of process submite. Back out changelist 482034

BIOS revision: 129R04

482034:5372219 MDQ/MDQS read centering for DDR4 LRDIMMs

BIOS revision: 129R03

481525:5385430 :Memory PEIM missing minor codes for the following warnings
481513:5388359: system error With 16DIMM populated, Lightning Ridge CRB stop at 0xF8 after disable NUMA

BIOS revision: 129R02

481216:5385442: Observing lower than expected memory BW with 2DPC LRDIMM

BIOS revision: 129R01

481049:NO_SIGHTING: Purley Release 129 BIOSID Update
480981:5385351: NPD issues in PurleyRpPkg

BIOS revision: 128R09

480802:5385422: BIOS knob To enable WA for Rx Testing to be implemented
480746:5385226: Add Windows Azure Stack support for Purley platforms (KW fix)

BIOS revision: 128R08 – BKC WW13 (PC8)

480737:5346047: Purley Patch: Add Production Patch Version 0x16 for SKX H0 to IFWI
480693:5385424: Production DIMMs incorrectly being reported as non-production
480655:5385434: Dynamic L1 BIOS option needs to be disabled and removed from the EDKII menu
480585:5385447: "SetMaxNonTurboPReqFrequencymiss" override msr(0x1A0) value and corrupt feature bit enabled by other module
480567:5385450: CL475712 caused ME capsule update fail with ME recovery jumper in purley PC project

BIOS revision: 128R07

480415:5385226: Add Windows Azure Stack support for Purley platforms
480130: 5385409: [2017_WW11][BIOS:126R06][Neon city] No instance of PowerMeter queried by wbemtest.exe command in OS

BIOS revision: 128R06

479883:5385420: PkgC6 MC FIVR actions not happening with later BIOS versions

BIOS revision: 128R05

479699:5385343: intel code is returning incorrect error log, S5353499 is partially fixed.
479625:5385407: INTRD_DET bit in PCH_TCO2_STS incorrectly cleared in PchInitPeim.c [IPS 1209547474]

BIOS revision: 128R04

479218:5385389: Incorrect initalization of setup structure is causing instability in customer board.

BIOS revision: 128R03

479209:5385297: System is not able to boot with ECC Disabled.

BIOS revision: 128R02

478991:5385350: [Klocwork] ABV issues (and one NPD) in PurleyPlatPkg
478988:5385405: [Coverity] 1 Out of Bounds issue reported 100's of times
478815: 5385402: Function GetCtlMarginsSweep doens't scan rest of memory channel after a fail channel

BIOS revision: 128R01

477958:5385378: Intel code shouldnt support ADDDC and mirroring, it is not supported configuration
477722:NO_SIGHTING: Purley Release 128 BIOSID Update
477616:5385352: 3 ABV and 1 NPD KW issue in PurleySktPkg - not ProcMemInit
477615:5385351: NPD issues in PurleyRpPkg

BIOS revision: 127R04 – BKC WW12 (PC7 MR1)

477423:5346011: Purley Patch: Add Production Patch Version 0x15 for SKX H0 to IFWI

BIOS revision: 127R03

477243:5385349:[Klocwork] ABV issues (and one NPD) in ProcMemInit

BIOS revision: 127R02

476766:[5385246] SUT will hang when EFI network enabled
476582:5385375: Node 0 MemHob calculates first memory map rule incorrectly in NUMA mode.

BIOS revision: 127R01

476188:NO_SIGHTING: Purley Release 127 BIOSID Update

BIOS revision: 126R07

475730:5385360: Remove (mask) BIOS option to allow customers to not take VCCSA voltage actions in PC6
475711:5385380: 1209743892: HECI message timeouts when ME is in recovery mode

BIOS revision: 126R06 – BKC WW11 (PC7)

475424:5385239: Dimm to System Address conversion wrong in Mirror Mode

BIOS revision: 126R05

475375:5385342: Fully populated 2DPC Purley system with 24- 64GB LRDIMM hangs on UMA mode
475328:5385345: Address translation failures in A3DC mode [IPS 1209655467

BIOS revision: 126R04

475182:5385313: Additional security settings needed on Purley

BIOS revision: 126R03

474719:5385279: Malformed subspace in ACPI PCCT

BIOS revision: 126R02

474332:5385178: CNFG_500_NANOSEC in PCU (D30,F5,RD8[9:0]) is incorrectly programmed based on DDR Freq

BIOS revision: 126R01

473816:5385288: [ALL] Change IFWI color in SMBIOS Type 148

473771:NO_SIGHTING: Purley Release 126 BIOSID Update

BIOS revision: 125R03 – BKC WW10 (PC6 MR1)

No change

BIOS revision: 125R02

472202:5345951: Purley Patch: Add Production Patch Version 0x14 for SKX H0 to IFWI
472141:5385227: Consuming Recoverable Errors results in NMI storm - causes windows BSOD

BIOS revision: 125R01

470796:5385252: Storm of SMI in SVLS config
470768:NO_SIGHTING: Purley Release 125 BIOSID Update

BIOS revision: 124R08

No change

BIOS revision: 124R07 – BKC WW09 (PC6)

469631:5385301: GBT offline is broken on PLYDTRL IFWI

BIOS revision: 124R06

468927:5385258:[NVDIMM] ARS is not working if NVDIMMs are in slot1 of the channel.

BIOS revision: 124R05

No Change

BIOS revision: 124R04

468527:5345930: Purley Patch: Add Production Patch Version 0x13 for SKX H0 to IFWI (PRODUCTION)
468467:5385200: Bug in PMax Detector offset table implementation

BIOS revision: 124R03

468447:5385236: SRAT incorrect when SNC enabled in X2APIC mode
468334:5385266: WHQL tVerifyTCGEventLogMatchesPCR failed when enable BootGuard with TPM1.2
468327:5372325:Support for handling bus resource allocation failure when PCI milti segmentation is disabled
468255:5385234: [FPGA] configure PCH to generate SMI for RC_ERROR_N inputs
468254:5385261: [FPGA] FPGA socket disable bitmap Setup option did not functional.

BIOS revision: 124R02

467943:5385248: SDP: BMC version in the BIOS does not match the version showing in the BMC console
467698:5385270: [LBG Si Request] XHCI controller Parity Error Response (PER) must be set by BIOS/OS

BIOS revision: 124R01

467422:NO_SIGHTING: Purley Release 124 BIOSID Update
467417:5385243: If user set CPU Core Flex Ratio to unsupported value, system will reset continuously.
467238:5385158: IOT LLC Setup not working for U0

BIOS revision: 123R04 – BKC WW08 (PC5)

466692:5372981: 1209269155: updating dimmList mapout variable would act abnormal if ATTEMPT_FAST_BOOT_COLD is enabled
466691:5385193: Request for MRC workaround to support 1Xnm DDR4 errata affected DIMMs

BIOS revision: 123R01

No change

BIOS revision: 123R02

466046:5385186: CLONE SKX Sighting: Seeing silent data corruption when a particular defective DIMM is installed.
465960:5385164:[NVDIMM] PMO: MRC bug on JEDECArm function in NVDIMM.c
465859:5373114: "Processor BSP Revision" display L0 stepping processor as B0 stepping in Setup menu.
465785:5372889: [clone of ND SW HSD# 1804669917] Purley NeonCity - OS fails to attach LUN after first reboot on PF2 and higher due to broken iBFT from EDK2 stack

BIOS revision: 123R01

465482:5373068:[NVDIMM] Code logic error in JedecNVDimm driver cause NVDIMM cannot be seen with "Get-PhysicalDisk" under Windows 2016]
465467:5385189: ACPI _CPC.LowestPerformance shall revert mapping to IA32_HWP_CAPABILITIES[31:24]Lowest_Performance
465460:5373073: WHQL - TPM 2.0 Physical Presence test failing
465382:NO_SIGHTING: Purley Release 123 BIOSID Update

BIOS revision: 122R07

No change

BIOS revision: 122R06

464628:[NO SIGHTING] Back out changelist 464061: uCode not affecting TXT functionality
464439:5373032: [SKX M0 PO] BIOS fails to boot after IERR injection - Invalid Socket Id 0.

BIOS revision: 122R05

464085:5373115:JedecNVDIMM driver should not depend on memory RAS protocol

BIOS revision: 122R04

464061:5345883: [NC] SUT reboot when try to enable TXT (Back out changelist 462519)
464054:5373068:[NVDIMM]Code logic error in JedecNVDimm driver cause NVDIMM cannot be seen with "Get-PhysicalDisk" under Windows 2016
464020:5385185: HOST_EXI interfance needs to be disabled and locked by BIOS, build fix
463981:5385185: HOST_EXI interfance needs to be disabled and locked by BIOS
463980:5385215: [LBG Si Request] REVID for LBG is changing for LBG NS C0 and LBG SD T0 stepping

BIOS revision: 122R03

463710:5385164:[NVDIMM] PMO: MRC bug on JEDECArm function in NVDIMM.c
463671:5385152: Include LBG Sx MPHY RC versions in PurleyRpPkg/projectMap

BIOS revision: 122R02

463328:5372832:[NVDIMM] Data is not retained in NVDIMMs attached to the first CPU socket after a power cycle

BIOS revision: 122R01

462957:5385161:OemSetPlatformDataValues is corrupting setup data with MAX_SOCKET > 4
462844:NO_SIGHTING: Purley Release 122 BIOSID Update

BIOS revision: 121R04 – BKC WW06 (PC4)

462574:5385182 : [NVDIMM] NVDIMM restore fail due to insufficient timeout
462519:5345878: Purley Patch: Add Production Patch Version 0x11 for SKX H0 to IFWI
462482:5385184: CLONE SKX Sighting: (ADDDC) 2666 LRDIMM failing with CECC/UC/SDC when BC4 OTF is Enabled

BIOS revision: 121R03

462313:5385130: WHQL Tpm20SupplementalTest failed when BootGuard enabled
462213:5385169: [SKX H0 PRQ] paniccompdnmult incorrect in latest MRC
462204:5385181: [SKX H0 PRQ] CLONE SKX Sighting: <@RC> TOR TO w/ PC6 and External Network Card <Dynamic L1>

462193:5385166: [SKX H0 PRQ] CLONE SKX Sighting: <BIOSw/a IOU bandwidth drops when runing stress with x4/x8 concurrently
462137:5372782: [SKX H0 VV] Bimodal Cmd Timing Margins due to CmdRcomp and Scomp Codes

BIOS revision: 121R02

461845:5385175 [SKX H0 PRQ]MRC: Round Trip Latency Optimization broke RMT
461843:5373110 :vmse_err_latency should be programed for SKX H0 and later

BIOS revision: 121R01

461034:NO_SIGHTING: Purley Release 121 BIOSID Update
461032:5373069: [SKX M0 PO] Golden rule boot fails with memory populated on IMC1 - remove the IA32 in previous check in

BIOS revision: 120R05

460830:459720: [SKX M0 PO] Golden rule boot fails with memory populated on IMC1

BIOS revision: 120R04

460682:5345857: Capsule: PurleyRestrictedPkg\Roms\FpgaBbs BBS_GBE.bin and N4PE.bin need to be updated when new FPGA BBS/N4PE released

BIOS revision: 120R03

460412:5373038: System hangs up during warm boot cycle test with "Multi-Threaded MRC" set "Disable"
460357:5385129: Opal City platform shutdown at POST code 0x06 then follow by 0x9. with beep sounds when try to boot up with different LBG parts
460171:5373061: [IPS 1209428227] UPI Dead Lock occurs in 6/8 socket configuration, because VN1 is disabled

BIOS revision: 120R02

459822:5385137: [SKX U0 PO] BIOS hangs before it gets to DWR Stall after a Dirty-Warm-Reset Occurs on MultiSocket Platforms

BIOS revision: 120R01

459156:NO_SIGHTING: Purley Release 120 BIOSID Update

BIOS revision: 119R06

459044:5372924: NVDIMM Reverse Address translation confused by interleaving.

BIOS revision: 119R05 – BKC WW04 (PC3 MR1)

No change

BIOS revision: 119R04

458391:5345835: Purley Patch: Add Production Patch Version 0xF for SKX H0 to IFWI
458383:5385147: [NC] Bios does not return from S3 (Back out changelist 457289)

BIOS revision: 119R03

458070:5373031 DQS still driven after Read Preamble Training Mode exit on LRDIMMs
457907:NO_SIGHTING: Back out changelist 457806 (Not approved for Production)
457806:5372943 : USRA native implementation needs support for pseudo offsets.

BIOS revision: 119R02

457289:5372782: [SKX H0 VV] Bimodal Cmd Timing Margins due to CmdRcomp and Scomp Codes (Back out changelist 450140)

BIOS revision: 119R01

457022:NO_SIGHTING: Purley Release 119 BIOSID Update

BIOS revision: 118R01 – BKC WW03 (PC3)

5345821:Please update SPS FW to SPS_E5_04.00.03.142.0 as Purley PC3 planned release to BKC (SKX_PPRODUCTION)
456597:NO_SIGHTING: Purley Release 118 BIOSID Update
456518:5372828: [2016_WW47 BKC][BIOS:109_D12][Neon city FPGA]SUT will hang when add new boot option.

BIOS revision: 117R03

5345817: Fort Park NVM 3.26 signed image to be included in IFWI for Purley 2S (Also HSD 5345818 for LR)
456213:5345801: Need to fix WW in the IFWI ID
456113:5372827: BSSA: bug in the BiosServerSetSeqRankMapChip() (Back out changelist 453638)

BIOS revision: 117R02 – BKC WW02 (PC2 MR1)

No Change

BIOS revision: 117R01

454863: 5372913: GPE offset of SWGPE_STS and HOT_PLUG_STS is not correct in PlatformGpe.asi
454687:5373010: Need to map out Channel on several instances in MRC
454686:5373016: CLONE SKX Sighting: PkgC w/ FIVR ramp failed with CAP Errors
454685:5373008: thrt_allow_isoch should be set to 0
454664:5372978: 1209142301 DxeSetupLib bug
454663:5372793: PCH sends unmapped IO cycles to BMC making keyboard not functional when on eSPI mode on Linux bootloader (GRUB)
454662:5373039: 1405242380: KTI RC bug for programming snoop fanout registers
454646:NO_SIGHTING: Purley Release 117 BIOSID Update Modified microcode for release

BIOS revision: 116R01 – BKC WW01 (PC2)

453638:5373081: [2016_WW51][BIOS:113D07][Lightning Ridge] Occasionally System autologin be broke at Linux bootup during G3/S5 test (Back out changelist 447390)
453627:NO_SIGHTING: Purley Release 116 BIOSID Update

BIOS revision: 115R03

No change

BIOS revision: 115R02

452410:5373007: PMax Detector auto-correction table needs changes to accomodate new SKUs
452401:5372972: PC6 Feature Change to Enable VCCSA Power Actions Selectable by Customers
452270:5372899: Handler for SMI generated by eSPI master is not complete
451974:5372990 MRC: EarlyCmdClk training will hang cpgc if 1 channel previously failed in EarlyCtlClkLoopback

BIOS revision: 115R01

451866:5373045: [SKX M0 PO] MRC: FUSE_DISABLE_DDRT inconsistency across sockets
451795:NO_SIGHTING: Purley Release 115 BIOSID Update

BIOS revision: 114R11

451735:5371219: [Hackathon] WheaErrorLog.c doesn?t use safe SMM comm buffer
451732:5372834: Unexpected or unknown PMTT subtable type 0x2
451731:5372438: Enable XCHI SERR by default to not mask potential issues seen by external customers
451725:5372970: Elements.[Index].NodeId Field in systemMemoryMap Hob is incorrect.
451723:5372915: [Purley] Set BIOS option-Show SPI deivce as disabled, the SPI device (D31;F5) still be seen in O.S
451722:5372958: WMP S0 RC7 test BIOS
451721:5372150: SRAT - Memory affinity structure shows incorrect values when memory is fully populated
451720:5372914: WMP B0 RC46 test BIOS

451703:5373024: [2016_WW51][BIOS:113_D07][Lightning Ridge] System hangs after clear TPM and enable TXT and serial console shows "Tpm2 The send buffer too small?
451696:5372985: "Platform Configuration" setup in systems without BMC

BIOS revision: 114R10

450544:5373029: [SKX M0 PO] ADDDC for M0 not comprehending workaround for 5372419
Modified microcode for release

BIOS revision: 114R09 – BKC WW52 (PC1)

450140:5373028: [SKX M0 PO] Attempting S3 with BIOS 113.D05 results in a reset at OS hand-off (Back out changelist 444917)
450127:5345749: Purley Patch: Add Production Patch Version 0xC for SKYLAKE H0 to IFWI

BIOS revision: 114R08

No change

BIOS revision: 114R07

449589:5373014: Synchronization issue in DWR Implementation causing memory lock issues

BIOS revision: 114R06

449334:5372922: [SKX H0 VV]]111.D13 PEI_ASSERTED on partial mirror when SCN is disable

BIOS revision: 114R05

449173:5372971: Remove setting dis_2cyc_byp from BIOS for most steppings/configs

BIOS revision: 114R04

448927:5372831: Debug Interface/Privacy MSR (0xc80) Enable bit set by mistake
448801:5372868: DIMM to System Address conversion Broken on Purley

BIOS revision: 114R03

448420:5345727: Purley Patch: Add B0 ONLY Production Patch Release 0x131 for SKX to IFWI
448371:5372866: [SKX H0 VV] BIOS assert when running memory error injection tests
448253:5372796: Expand GenbiosID tool to accept R build type

BIOS revision: 114R02

No change

BIOS revision: 114R01

447911:NO_SIGHTING: Purley Release 114 BIOSID Update
447908:Change build type to R
447905:5372796: Expand GenbiosID tool to accept R build type
447903:5372796: Expand GenbiosID tool to accept R build type [Override Original Module]

BIOS revision: 113D07 – BKC WW51

447398:5372955:[SKX H0 VV] CLONE SKX Sighting: Supercollider Arden Data Verify Failures (due to IO CTO / System Slowdown)
447393:5372918: BIST failure causes endless reboots
447392:5372948: LBG USB2: Disconnect vref need to change to 812.5mV in latest BIOS
447390:5372827: BSSA: bug in the BiosServerSetSeqRankMapChip()

BIOS revision: 113D06

447157:5345717: Purley Patch: Add B0 ONLY SysDBG Patch Release 0x34 for SKX B0 to IFWI
447078:5372959: MRC: Round Trip Latency Optimization causing failures for LRDIMMs
447075:5372528: [CR ES0] CLONE SKX Sighting: (CR) TOR timeout + system Hang in Dram Rapl

447008:5371989:[NVDIMM] Win 2016 scmb.sys driver yellow banged out

BIOS revision: 113D05

446768:5372887:Change PCIe Gen3 Preset 10 default postcursor to 21

BIOS revision: 113D04

446629:5372940:[NVDIMM] SMBIOS table is not support NVDIMM manufacture ID.
446607:5372799: WS-PLY-CRB Workstation: PETS AMT 011, 014, 015, fail, No BAE sent or reaching PETS

BIOS revision: 113D03

No change

BIOS revision: 113D02

No change

BIOS revision: 113D01

446162:NO_SIGHTING: Purley Release 113 BIOSID Update
446156:5372800: Cleanup in T-states support in regard of HWP modes

BIOS revision: 112D11

445937:5372762: [IPS 1209157031] In CpuMpDxe, Uefi Services are used in multi-threaded environment that causes intermittent system hang

BIOS revision: 112D10 – BKC WW50

445857:UnDo:[5372487][CR_ES0] Cloned From SKX Si Bug Eco: Spurious Rd tracker deallocation in case of a bypassed demand read hit.
445850:[5372487][CR_ES0] Cloned From SKX Si Bug Eco: Spurious Rd tracker deallocation in case of a bypassed demand read hit.
445811:5372810: [Klocwork] Pointer 'mPlatformFpkPortToFuncMapPtr' checked for NULL at line 167, 227 can be dereferenced at lines 177, 231 respectively
445809:5372505: BIOS should not clear the doorbell bit in mailbox cmd register in NVMCTLR controller
445769:5372833: [LBG Si Request] Disable Dfx Power gating even when EXI and Firmware trace hub are disabled
445763:5372883: Unadvised warning message from PchSbiExecution on DWORD alignment

BIOS revision: 112D09

445566:5345683: Purley Patch: Add B0 ONLY SysDBG Patch Release 0x33 for SKX B0 to IFWI

BIOS revision: 112D08

445452:5372633: Inconsistency between socket_0_table and platform dimm configuration.
445410:5372771 Consuming broadcast MSMI causes some threads to get stuck in SMM. Sometimes BIOS ASSERTS
445377:5372787: CPU frequency couldn't keep on maximum after S3 resume.
445358:5372801:PCIE: PHY recipe v3.25
445355:5372912: Transient Errors with 2667Mhz RDIMMs and OSR Enabled
445354:5372825: Change 2666 2DPC DIMM check from stop boot to Warning only
445352:5372792: BIOS incorrectly setting t_shrtloop_num for 2H 3DS

BIOS revision: 112D07

No change

BIOS revision: 112D06

445094:5345651: Remove SKX A0/A1 patch from IFWI (adendum matching #uCode vs #DisplayNames)

BIOS revision: 112D05

No change

BIOS revision: 112D04

445005:5345651: Remove SKX A0/A1 patch from IFWI

BIOS revision: 112D03

444961:5372088: Total Memory Capacity based CPU SKU'ing 5372819: Memory Capacity SKU - BIOS should halt even when error escalation is disabled
444935:5372785 Remove restriction on MTG RCD Rev 2.5
444934:[5372783]PPR address won't get logged when any of RAS features (Rk_Spare,SDDC,ADDC) are enabled.;
444918:
444917:5372782: [SKX] Bimodal Cmd Timing Margins due to CmdRcomp and Scomp Codes
444892:5372696: Purley 2S system will CATERR when entering win 10 , if enable PCH pcie root port hot plug, releated to PCIE max payload size setting
444795: [EPSD100035578: [WFP] SMBIOS Type 17 Speed is 0x0000 with HMA451R7AFR8N-TF.]

BIOS revision: 112D02

No change

BIOS revision: 112D01

444664:5345600: Integrate Intel Apache Pass UEFI driver 01.00.01.1018
444658:5345594: Purley Patch: Add B0 ONLY SysDBG Patch Release 0x32 for SKX B0 to IFWI
444636:5372665: Occasionally System hangs at PC 0xDD and KTI assert occurrs during Linux S5 or G3 cycling tests - Addendum
444612:5372665: Occasionally System hangs at PC 0xDD and KTI assert occurrs during Linux S5 or G3 cycling tests
444608:5372731: CorrectedErrorSMIThrottling timestamp gets cleared because of insufficient bit fields allocated for Year in TIME_STAMP
444594:5372805: PPR flow is breaking with BIOS 109D12
444593:5372770: ADDDC test case causes MCE UC to occur
444591:5372797: [SKX H0 VV] change snoop fanout direction
444587:NO_SIGHTING: Purley Release 112 BIOSID Update
444586:5372763: [SDP: Purley 4S] Failed to use user account login to BMC web console

BIOS revision: 111D17

No change

BIOS revision: 111D16

No change

BIOS revision: 111D15

No change

BIOS revision: 111D14

No change

BIOS revision: 111D13 – BKC WW49

No change

BIOS revision: 111D12

444239:5372624: CR ARS - fix getting media error logs and add specific functionality for ARS
444213:5372894 [SKX-D]Merge Bakerville development source back to trunk.

BIOS revision: 111D11
443994:5371099: [SKX-D] Pch DIDs must be updated for new Bakerville platform

BIOS revision: 111D10
443732:5372874: [CR ES0] BIOS not restoring non BSP information for fast cold boot
443598:EPSD100255811 #CCB471[Purley Common BIOS]To support early VGA video display to show system informaiton

BIOS revision: 111D09
No change

BIOS revision: 111D08
No change

BIOS revision: 111D07
No change

BIOS revision: 111D06
442824:EPSD100035438 [WFP] There is no SLIC table after flash the BIOS which add OA key by ITK

BIOS revision: 111D05
No change

BIOS revision: 111D04
No change

BIOS revision: 111D03
No change

BIOS revision: 111D02
No change

BIOS revision: 111D01
441514:NO_SIGHTING: Purley Release 111 BIOSID Update
441294:5370546: Request: add Fort Park Ethernet IP "port disable" feature to Neon City BIOS
441264:[Purley] [EPSD100255616: [WFP] MMIOH size is incorrect after remove Xeon 7120P when MMIO size is auto in Setup.]

BIOS revision: 110D13
441216:5371220:[Hackathon] SpiFlashLock never reverified that SPI is locked again

BIOS revision: 110D22
440886:5372719: SKX U0 and M0 readiness - KTI and stepping
440871:5372716: Legacy Region C000h~FFFFFh still could be written after boot
440869: 5372768: [SKX U0 PO] MRC: Upload LCC package delay table

BIOS revision: 109D13
No change

BIOS revision: 109D12
No change

BIOS revision: 109D11
440642:5372778: [FPGA] Add dependency on gEfiPeiMpServicesPpiGuid in FpgalatformEarlyInit driver

BIOS revision: 109D19

No change

BIOS revision: 109D18

440461:5345583:Purley Patch: Add Production Signed Release Version 0x9 for SKYLAKE H0 to IFWI

BIOS revision: 109D17

440386:5372579 | Emca L1 Directory Address not provided to ACPI
440375:5372657 | Recent BIOS Versions breaks hot plug flow
440317: 5372706: IODC CSRs incorrectly set on H-step

BIOS revision: 109D16

No change

BIOS revision: 109D15

440141:5345568:BIOS Guard PC candidate add to IFWI

BIOS revision: 109D14

440014:[5372434] Request to add SKX core/uncore machine check reads as part of the Purley DWR flow
439980:5372718: min_ops increase for 3DS/LR-DIMM
439927:NO_SIGHTING: Purley Release 110 BIOSID Update
439911:5372730: [Klocwork]: #9601: Array 'WdbLinePtr' of size 16 may use index value(s) 16
439909:5372615: [2016_WW42][BIOS:105_D11][Neon city] The USB device can?t be detected in ?Device and Printers? when plugging it into upper 2.0 USB port on rear panel.
439905:5372724: P-states do not work properly on SKX H0

BIOS revision: 109D13

439593:5372377: Build Error in CpuPcieAccessCommon when MAX_SOCKET == 1

BIOS revision: 109D12 – BKC WW47

439572:5345569:Integrate Intel Apache Pass UEFI driver 01.00.01.1016

BIOS revision: 109D11

No change

BIOS revision: 109D10

439526:5345556: Purley Patch: Add Debug Patch Version 0x31 for SKYLAKE B0 to IFWI

BIOS revision: 109D09

No change

BIOS revision: 109D08

439141:5372727: x8_wpq_dly on SLV mode should be 8 + (Max-Min RoundTrip)
439140:5372588: Bios 105.D11 on 2DPC RDIMM fails with DXE Assert when partialMirror knob is set to 40 percent
439106:5372526:[NVDIMM] Add NVDIMM support in the MRC Mem Map simulator

BIOS revision: 109D07

439071:5345555:Purley Patch: Add Production Signed Release Version 0x7 for SKYLAKE H0 to IFWI
439010:5371697: Logging or tagging issues with Error / Warning implementation, causing inability to identify causation of platform malfunction.

BIOS revision: 109D06

438955:5372653: IE HECI PPI loaded too late thus DRAM_INIT_DONE not sent
438924:5372544: Injecting CE memory errors on a DIMM results in entire channel being mapped out
438832:5372431: [FPGA] temperature threshold defaults exceed BBS-imposed upper limit

BIOS revision: 109D05

438767:5372745:[CL438107 will cause SUT hang 0x96](Back out changelist 438107)
438704:5372727: x8_wpq_dly on SLV mode should be 8 + (Max-Min RoundTrip)

BIOS revision: 109D04

438504:5372622: CR ARS - Fix NvmCtlrErrorLogDetectError and NvmCtlrErrorLogProgramSignal functions
438338:5372491: Incorrect ImcUncErrorMsr lookup table break Fast Path
438334:5372407: [klocwork-equivalent] Vararg marker not closed in MrcHooksServicesLib

BIOS revision: 109D03

No change

BIOS revision: 109D02

438107:5372716: Legacy Region C000h~FFFFFh still could be written after boot

BIOS revision: 109D01

438092:5372725: (Mirror) Mirror Failover Ch1 -> Ch0 = SDC
438054:5372684: [Klocwork] Issue found in module PurleyPlatPkg\Platform\Dxe\SmbiosIFWIDxe
438053:5372685: [Klocwork] Issue found in module PurleySktPkg\Dxe\JedecNvDimm
438050:5372683: [Klocwork] Issues found in module PurleyPlatPkg\Platform\Dxe\MemorySubClass
438041:5372261: Remove Platform Pkg dependencies from Skt pkg
438029:[5372434]Request to add SKX core/uncore machine check reads as part of the Purley DWR flow;
438014:5372643:SDP: NVMe drives (Oculink Ports) are not available when QAT cables attached
438001:NO_SIGHTING: Purley Release 109 BIOSID Update
437987:[Klocwork]: 5372729 Array 'IIO_resource' of size 4 may use index value(s) 4
437981:5372638: Function GetMargins() in MemMargins.c can loop forever - needs retry count

BIOS revision: 108D12

437856:5372547: [FPGA] Pcie slot 2 socket 0 Reserved FPGA-slot should not detect devices with SKX-SP processor

BIOS revision: 108D11 – BKC WW46

437703: 5345540 : Purley Patch: Add Debug Signed Release Version 0x7 for SKYLAKE H0 to IFWI
437647:5372635: [CR_ES0] BIOS rejecting new partition requests, 5372637: [CR_ES0] BIOS CfgReq Validation FAILED

BIOS revision: 108D10

437617:5372577: [SKX H0 VV] CLONE SKX Sighting: MRS PDA WA removal to support NVDIMM causing failures during MRC
437602:5372702: BIOS 107d06 failed to resume from the first S3 cycle
437598:5372623: CR ARS - Fix NvmCtlrSetAddressRangeScrub and NvmCtlrGetAddressRangeScrub

BIOS revision: 108D09

No change

BIOS revision: 108D08

No change

BIOS revision: 108D07

437285:5372674: CPU Stepping checking is incorrect in SktScopemsrInit.c

437278:5372667: 3DS LRDIMM seeign illegal PRE and ACT during MPR sequence
437269:5372577: CLONE SKX Sighting: MRS PDA WA removal to support NVDIMM causing failures during MRC
437247:5372455: Wrong value for MBAR (SMBUS and GBE) after S3 [Neoncity]
437232:
437189:5372551: Concern in current WHEA error log handler
437177:5372531: Replace LogWarning() usage in RC with OutputWarning() as ENHANCED_WARNING_LOG support is Enabled by default

BIOS revision: 108D06

436995:5371224: [Hackathon] Strange check if allocated pointer is below 4G
436990:5372411: [klocwork-equivalent] Memory leak in BootMaint
436971:5372649:[NVDIMM] BIOS does not clear the ADR_RST_STS bit early in MRC
436960:5372421:[NVDIMM]Enable NVDIMM support in the BIOS binary
436878:5372655: Invalid number of T states reported by BIOS
436843:5372588: [SKX H0 VV] Bios 105.D11 on 2DPC RDIMM fails with DXE Assert when partialMirror knob is set to 40 percent
436799:5372567: SDP PXE Installation 'SNP' debug messages

BIOS revision: 108D05

436770:5371320: Add all advanced memory mode support for Address translation (forward and reverse)
436740:5372617: Building bios doesn't work with no amt support
436725:5372295: [SKX H0 PO] CLONE from skylake_server: [CR] B2P mailbox command MISC_WORKAROUND_ENABLE for uclk>dclk should not be sent on SKX H0 (Stepping check fix)
436594:5372432: [FPGA] Broadway 5 not properly recognized on Socket 1 Bus 2 (slot 8) with SKX-P

BIOS revision: 108D04

436561:[5372621][Rev:5][Size of SMBIOS Type 17 doesn't displayed correctly when installing 64GB LRDIMM
436558:5372429 :[FPGA] INTx interrupt mapping incorrect for PCIE endpoints
436432:5372534: (SAFE
436371:5372554: Performance tuning knob coded incorrectly

BIOS revision: 108D03

436340:5372450: DWR workaround: BIOS needs to avoid access to TPM on DWR
436336:5372216:IPS 1208972787: IioInit drivers are consuming more boot time
436330:5372461:ARI Forwarding Need to have a configurable option
436264:[EPSD100255360: POST LED will brighten when BMC cold reset with SUT power on.]
435953:5372385: Cloned from SKX-D: Interleaving not enabled with empty MC1 Ch0 / stuck in reset loop
435945:5372261: Remove Platform Pkg dependencies from Skt pkg (Back out changelist 435885 - Unapproved Checkin)
435885:5372261: Remove Platform Pkg dependencies from Skt pkg

BIOS revision: 108D02

435593:5372647: Pointer arithmetic vulnerability in OpaPlatCfgEntryPoint()

BIOS revision: 108D01

435517:5372127: OemTableId missing changes for all drivers
435485:NO_SIGHTING: Purley Release 108 BIOSID Update
435484:5372257: [SKX H0 PO] Enable m2mem TO
435470:5372647: Pointer arithmetic vulnerability in OpaPlatCfgEntryPoint()

BIOS revision: 107D09

435130:5372645: Support for GCC - second batch

BIOS revision: 107D08

434809:5372162: [FPGA] Need to add version number of SBL (Shell Bitstream Loader) and SBS(Shell Bitstream) to debug prints

BIOS revision: 107D07 – BKC WW45

434702:5372534: Updated to fix build error in PLYBGRVS2K8 - Add TPM1.2 and PTT support in OOB PPI-x
434688:5372266: Need a way to store a platform config file in the IFWI that is updatable using an utility from the customer side [Addendum]
434687:5372492: MemMapSim on current BIOS tip generates ASSERT
434686:5372208: Smbios Type16 - Maximum capacity shows incorrect information.
434679:5372479: Chipsec is reporting multiple failures
434503:5372230 Purley-SKX CRB BIOS DWR changes to skip IE/ME handshakes and enable PCODE surprise reset assertion (Late DWR changes)

BIOS revision: 107D06

434290:5372534: Add TPM1.2 and PTT support in OOB PPI-x

BIOS revision: 107D05

434185:5372620: GBT Offline is broken: XML Parse Error
434172:5372606: [klocwork]NULL pointer dereferences and array boundary violation in PurleyPlatPkg
434135:5372538: CLONE SKX Sighting: SKX UPI MCA loggged on 8S system
434120:5372403:Cloned From SKX Si Bug Eco: CLONE SKX Sighting: PCIE: SKX responds with UR instead of CA for non posted transactions that incur on an ACS violation
434104:5372408: [klocwork-equivalent] Memory leak in UbaPlatLib
434094:5372518: OppSrefEn=Disable needs to have all load lines to be clear on each channel populated
434093:5372474: CLONE SKX Sighting: PkgC w/ FIVR ramp failed with CAP Errors
434080:5371085: Enable Rack Scale 2.0 on Purley BIOS and ME/BMC fw

BIOS revision: 107D04

No change

BIOS revision: 107D03

No change

BIOS revision: 107D02

433839:5372549: CLONE SKX Sighting: [FPGA] Correctable and some uncorrectable errors seen on SKX UPI during boot
433778:5372536: [klocwork] #8528662: 'ProcessorLtsxEnableBit' is used uninitialized in this function.
433674:5372595: [WW38 BKC][BIOS 97.D06][NeonCity] WHEA log buffer was out of boundary when memory CE storm happened

BIOS revision: 107D01

433637:5372356: GPP_C_10 is requested not to be locked after EndOfDxe
433552:5372530: Unclear code clarification for PPR RAS code
433549:5372496: CR ARS - Remove old mocked code and clean the DSM interface
433524:NO_SIGHTING: Purley Release 107 BIOSID Update
433523:5372452: EWL Implementation error on EwlOutputType1
433513:5372554(5372466): Performance tuning knob coded incorrectly(main trunk)
433506:5372410: [klocwork-equivalent] Vararg marker not closed and uninitialized variable in ProcMemInit, OemProcMemInitLibPpi, and CrystalRidge
433505:5372405: [klocwork-equivalent] Uninitialized variable and memory leaks in PlatformCpuPolicy, SocketSetup, and PlatformInit

BIOS revision: 106D12

433308:5371788: KTIRC:False warning message logged for links in slow speed w/ FPGA parts
433302:5372583:[FPGA] Failed to load different BBS on different FPGA socket
433264:5372562: BIOS hang after enable sVLS with one DR DIMM populated
433253:5372400: [Klocwork] Issue found in file PurleyRpPkg\Platform\Pei\PlatformInfo\PlatformInfo.c

433237:5372533: [SKX H0 VV] CLONE SKX Sighting: <@RC.w/a>CATERR with Lock stuck in TOR while running Rocket
433236:5345479: Integrate Intel Apache Pass UEFI driver 01.00.01.1011

BIOS revision: 106D11 – BKC WW44

No change

BIOS revision: 106D10

432938:[EPSD100255668]GCC build fix cause PCPLYLBGIPCD and PCPLYLBGIPCR failed.

BIOS revision: 106D09

No change

BIOS revision: 106D08

432766:5372586: GCC: PurleyRpPkg - Binary Changes
432754:5372586: GCC: PurleySktPkg - No binary Changes
432742:5372586: GCC: ServerCommonPkg - No binary Changes
432734:5372586: GCC: PurleySktPkg - Binary Changes
432731:5372586: GCC: PurleyRpPkg - No binary Changes
432728:5372586: GCC: PurleyPlatPkg - Binary Changes
432726:5372586: GCC: PurleyPlatPkg - No binary Changes
432694:5372586: GCC: CpRcPkg - No binary Changes
432659:5372586: GCC: CpPlatPkg - Binary Changes
432645:5372586: GCC: CpPlatPkg - No binary Changes
432642:5372586: GCC: CpPcPlatPkg - No binary Changes
432641:5372586: GCC: BpCommon - No binary Changes

BIOS revision: 106D07

432629:5372553: [SKX H0 VV] 105D11 Post Code A3 Socket does not come out of reset (Back out changelist 430365)
432579:5372406: [klocwork-equivalent] Memory leaks in IE Policy and AMT
432578:5372439: 1209034862: Issues with HiiGetBrowser()/HiiSetBrowser() calls in Purley ExtractConfig() methods.
432513:5371942: USRA issue causing PCI_IO_PROTOCOL to fail on Purley when FILL/FIFO widths are used

BIOS revision: 106D06

432397:[5372426] [SKX H0 VV] RAS handler causing URs;
432384:5372571: LZ Boot times are being exceeded] (Back out changelist 431741)
432310:5372344: Debug message fixes undone in CL 422224
432307:5345476:Purley Patch: Add Debug Signed Release Version 0x5 for SKYLAKE H0 to IFWI

BIOS revision: 106D05

No change

BIOS revision: 106D04

432256:5372565: [Simics] GP Exception type on serial
432250:5372358: [CR H0] BIOS 102.D02 boot hang at nfit

BIOS revision: 106D03

432198:5371764: MRC: Add DDR-T BCOM margining support
432190:5371439: Core Count not correct based on respective CPUs
432184:5371881: [CR_Alpha] [HW - nvm PRE-ES0] Corrupted PCD after write/read operations - set/get PCD functions fixes
432144:5372521: BIOS got assertion in a 8 socket system (88R)
432141:5372266: Need a way to store a platform config file in the IFWI that is updatable using an utility from the customer side
432119:5370471: xHCI debug does not function as expected (part 2)
432117:5372260: Integrate WMP B0 RC45

432092:5372523: [FPGA] Remove the FpgaFwPkg tool to improve the code flow

BIOS revision: 106D02

431979:5372541: [FPGA] IPclean build can not create FPGA IFWI
431978:5372509 : Fix issue: PchAlternateAccessMode will invoke MmPciBase after many call layers causing potential issues.
431969:5371863 : USRA Native implementation for CpuInit.c in ProcMemInit Library.

BIOS revision: 106D01

431790:[5372304] [Klocwork] Issues found in module PurleyPlatPkg\Ras\Smm\HpIOXAccess;
431784:NO_SIGHTING: Purley Release 106 BIOSID Update
431771:5372374: Smart Health data only added to Memory Device To SPA Range Map Table for PMEM regions in certain configurations

BIOS revision: 105D17

431741:5372385: Cloned from SKX-D: Interleaving not enabled with empty MC1 Ch0 / stuck in reset loop
431726:5372254: Missing MTRR reduces Storage mode performance by 500x
431678:5372316: Neon City FPGA platform has CSME/BIOS GPIO ownership issues
431665:5372258: System fail to boot to OS with "PCH State after G3" = S5
431653:5372495: CR ARS - Add boottime ARS option to setup menu

BIOS revision: 105D16

No change

BIOS revision: 105D15

No change

BIOS revision: 105D14

431386:5345437:Integrate Intel Apache Pass UEFI driver 01.00.01.1005
431307:5372467: [SKX H0 VV]: Need LLC prefetch option exposed
431302:5372472: [IE] Configuring OEM defined subsystem ID for Innovation Engine device on PCI does not work
431287:5372147: [SKX H0 PO] Add Warning for non supported DDR4 DIMMs when testing 2DPC 2666

BIOS revision: 105D13

430985:5372513: Mirror Failover SMI handler needs to disable link fail on failover

BIOS revision: 105D12

430968:5370403: 6000120986 1207839503: No support for vol mem 2LM mode Address Translation - Addendum for 2k8 build issue
430951:5372529:[Klocwork]Array 'LaneMask[Bifurcation]' of size 4 may use index value(s) -254..-1,4..12
430926: 5372307: Wrong LCTL2 register's value for DMI speed: 5GT/s (Gen2) [NeonCity]
430916:5372409.[klocwork-equivalent] Vararg marker not closed in PeiDxeCommonIioInitLib
430910:5371563: Audio reporting front panel connections and Digital out causing WHQL tests to fail

BIOS revision: 105D11 – BKC WW43

430594:5372146: [FPGA] BIOS needs to set RCiEP bit for device 0xBCC0 when it hides the Root Port associated with this device

BIOS revision: 105D10

430533:5372419: [SKX H0 PO] retry_rd_err_log_address1 reporting incorrect rank
430532:5372513: Mirror Failover SMI handler needs to disable link fail on failover

BIOS revision: 105D09

430523:5345462:Purley Patch: Add Debug Signed Patch Version 0x4 for SKYLAKE H0 to IFWI

BIOS revision: 105D08

430491:5372099: [WHQL] USB exposed port test failing, showing 10 USB3 ports
430458:5372131: PcieRootPortEqPh3Method left without default
430437: 5372217:NTB pcicmd setup on secondary side
430415:5372468: Node Manager Power Optimized BIOS POST Mode configurations are overwritten before END_OF_POST.
430391:5372147: [SKX H0 PO] Add Warning for non supported DDR4 DIMMs when testing 2DPC 2666
430375:5372503: [SKX H0 PO] CLONE SKX Sighting: Unexpected failover seen with UC mirror scrub injection.
430366:5371677: 1207894231: PCH DMI ASPM setup option is under Restricted Flags
430365:5372450: DWR workaround: BIOS needs to avoid access to TPM on DWR

BIOS revision: 105D07

No change

BIOS revision: 105D06

430127:5372522: [FPGA] fpga IOMMU did not support ISOCH VTD, need to remove the ISOCH programming.

BIOS revision: 105D05

430051:5345456:Purley Patch: Add Debug Signed Version 0x2D for SKYLAKE B0 to IFWI

BIOS revision: 105D04

430012:5371085: Enable Rack Scale 2.0 on Purley BIOS and ME/BMC fw
430010:5372127: OemTableId missing changes for all drivers

BIOS revision: 105D03

429988:5372130: IsolatedFaultyDimm and system reset error
429899:5370403: [6000120986 1207839503: No support for vol mem 2LM mode Address Translation
429888:5372412: ME Operation State field should not be compared to ME Operation Mode define values.
429857:5372197: SMB_TSOD_CONFIG_CFG registers are not set correctly for NVM DIMMs with non-functional FW
429855:5372370: RAS Code incorrectly using OEM Scratchpad range, breaking customer designs
429832: [EPSD100034766: [WFP] SUT will auto reset at POST code 0x94 after set MMIO size to auto and attach a Xeon 7120P.]
429809:5372163: [FPGA] SBS(Shell Bitstream) and SBL(Shell Bitstream Loader) are loaded to DRAM again after a subsequent warm reset
429802:5371916: [FPGA] XML CLI - Cannot find FPGA knobs inforrmation when dumping platformconfig.xml

BIOS revision: 105D02

429710:5372339: [SKX H0 PO] Bios not completeing plus1 flow in ADDDC tc2a

BIOS revision: 105D01

429604:5372147 [SKX H0 PO] Add Warning for non supported DDR4 DIMMs when testing 2DPC 2666
429583:5372466: [SKX H0 VV]: Need DeadOnValid exposed in BIOS
429488:NO_SIGHTING: Purley Release 105 BIOSID Update
429481:5371487: probably BIOS didn?t add VMD at all in either DMA or interrupt remapping tables
429477:5372365: Please remove fabric_boot.efi from the Purley BIOS
429465:5371914: PPR failure due to the MRS snooping command in the BIOS PPR sequence
429464:5372331: Per socket based CompletionTimeout setup options incorrect

BIOS revision: 104D14

429368:5371818: Enabling SERM, PCH SERVER ERROR REPORTING MODE in F2 setup doesn't change SERM bit in GIC register

BIOS revision: 104D13

No change

BIOS revision: 104D12 – BKC WW42

429217:5372504:SUT restart after sending to S3 state (Back out changelist 428962)
429134:5372100: [[WHQL] Whea failing fatal error event]
429124:5372379: [2016_WW38][BIOS:100_D14][Lightning Ridge] System will restart and cannot boot into OS any more when installing QAT Linux driver

BIOS revision: 104D11

429011:NO_SIGHTING: Back out changelist 428668 uCode team Investigating a possible issue
428970:5372248. [klocwork] #8527369 - NULL Pointer Dereference (NPD) in CpuPciAccess.c::GetSbspSktId ()
428962:5372258: System fail to boot to OS with "PCH State after G3" = S5
428938:5372087: Change Extended Status Field to represent value returned by NVMCTLR FW instead of the UEFI return code.
428926:5332961: DPA/SPA conversion functionality in the NVMCTLR DXE driver does not function properly

BIOS revision: 104D10

428803:5372301:[Klocwork] Issues found in library PurleyPlatPkg\Ras\Library\mpsyncdatalib\

BIOS revision: 104D09

428710:5372451: Admin password is not working even entering correct password
428704:5372281:[SKX H0 PO] NTB Bar size doesn't allow value greater than 39

BIOS revision: 104D08

No change

BIOS revision: 104D07

428657:5372242: "Enable SMX" did not automatically set enabled if only enable "Enable Intel(R) TXT" in setup menu]
428638:5372402: [Klocwork] Issue found in file PurleyRpPkg\Library\AcpiPlatformTableLib\AcpiPlatformLibSlit.c
428637:5372401: [Klocwork] Issue found in file PurleyPlatPkg\Legacy\Dxe\LegacyBiosPlatform\LegacyBiosPlatform.c

BIOS revision: 104D06

428482:5371610: [clone of ND SW HSD# 10020641] FPK NeonCity - Lack of interrupt connection (no valid PCI config space int. line) causes PXE boot failure
428478:5372153: PCIe Max Payload Size determination broken

BIOS revision: 104D05

428222:5372303: [Klocwork] Issues found in module PurleyPlatPkg\Platform\Dxe\SmbiosIFWIDxe
428221:5372302: [Klocwork] Issues found in module PurleyRpPkg\Platform\Dxe\Setup
428220:5372232: [Klocwork] Issues found in module PurleyPlatPkg\Platform\Dxe\SmbiosMiscDxe
428182:5372427: CheckForOemResourceUpdate() does not detect gap between MMIOL and 64MB below 4GB (0xFBFFFFFF)
428174:5372456: [SKX H0 VV] Need a new BIOS knob to control the PACKAGE_RAPL_LIMIT CSR lock bit
428156:5372463: Need to Sync all AP MTRRs with BSP before Enable mcaonnonnemcacheablemmio in the end of PEI
428093:5372437: Incorrect Devhide on M3KTI Pmon Registers on 2-socket Systems (KTI Port2 Disabled)
427884:5372182: Request to disable nibble alignment (LRDIMM xtalk optimization) in back-side MREP training step (Addendum)
427876:5372182 - Request to disable nibble alignment (LRDIMM xtalk optimization) in back-side MREP training step
427853:5371085: Enable Rack Scale 2.0 on Purley BIOS and ME/BMC fw

BIOS revision: 104D04

427828:5372030:[SKX H0 PO] New BIOS knob to enable WA
427805:5372179: cachedLrBuf values not updated correctly during Back-side training
427666:5372175: TCO_BASE_LOCK not getting correctly set
427634:5372230: Purley-SKX CRB BIOS DWR changes to skip IE ME handshakes and enable PCODE surprise reset assertion
427631:5372264: MSR IA32_PERF_CTL programmed by Node Manager function not aligned with EDS.

BIOS revision: 104D03

427560:5372128: BIOS is not clearing memory on a Surprise reset from a TXT Trusted Boot.
427455:5372445: [SKX H0 PO] CLONE SKX Sighting: ADDDC/SVL fails with UC or thousands of CECC errors
427453:5345386:Integrate Intel Apache Pass UEFI driver 01.00.01.1004

BIOS revision: 104D02

427366:5372299: Request SKX MMRC spreasheet change for Data and CMDCTL Ron Comp Vref settings
427359:5372152: UEFI FW needs to publish HOB to identify HFI-to-socket mapping
427346:5345425:Purley Patch: Add Debug Signed Patch Version 0x3 for SKYLAKE H0 to IFWI
427342:5372101: SDP: Lightning Ridge is not booting with PCIe cards plugged in.
427338:5372425: [SKX H0 PO] CLONE SKX Sighting: Patrol Scrub Hang after Failover
427337:5371121: [NVDIMM] ADR Initialization code is duplicated in InitADR() and in LBG code also..
427324:5372239: [Perf] tPRQ - D2K credit setting for 2S3UPI
427309:5371965: Only one processor is limited when P-states are used
427308:5372188: CLONE from skylake_server: MTRRDefTypeUncachable does not properly map socket 1 NVMCTLR (CR) CSR space
427307:5332362: PurleyMRC De-configuring entire memory channel for CECC detected(Part 2)

BIOS revision: 104D01

427296:5372312: RC:Update headers w/ H0 XML
427292:NO_SIGHTING: Purley Release 104 BIOSID Update

BIOS revision: 103D07

426999:5371581: W/A not removed: Cloned From SKX Si Bug Eco: Deadlock when PWMM enabled during an ADR
426998:5372390: [NVDIMM] Host Partition Reset ADR Enable bit is always enabled in Pch. So it triggers NVDIMM SAVE on every cold boot
426994:5372161: Change default value of PchAdrEn setup option Enabled.
426989:5371320: Add all advanced memory mode support for Address translation (forward and reverse)
426974:5372318: [NVMCTLR_TI] [DDR-T] Enable BCOM Fast Path with matched NVMDIMM/DDR4 Timings
426969:5371742: [NVMCTLR_TI] Using wrong DdrtCASWriteLatency for DDR2667
426966: 5372436 : CLONE from skylake_server: System hangs at nonce during S3 resume
426959:5371403: [NVDIMM] ACPI 6.1 FADT Minor Version update
426937:5372352: Patrol Scrub Rank Disables setup on wrong MC on mirror failover

BIOS revision: 103D06

426842:5372435: SX2C caterr during boot with 102.D09 (Back out changelist 421835)

BIOS revision: 103D05

426835:5372413: WMP S0 RC1 BIOS
426833:5372306: [LBG Si Request] LBG S0 will have a RevID = 8h

BIOS revision: 103D04

426597:5372209: SKX XCC BIOS showing inconstistent results with XCC QDFs and BIOS 94D10 and 97D05 (L2 TF)
426576:5372334: HWPM ACPI _CPC object needs update to reflect pCode patch changes in v 0x2B and beyond
426517:5345381:Purley Patch: Sysdebug Patch Release Version 0x2C for SKYLAKE B0 to IFWI

BIOS revision: 103D03

426165:5372291:[SKX H0 PO] pcie injection through einj reporting incorrect B/D/F in RHEL
426106:5372246: [SKX H0 PO] Chicken bit to enable hot plug command complete fix
426105:5372367: [SKX H0 PO] PCI 64-bit resource Allocation setting will roll back to Enable after disable it in setup (MMIO above 4GB).

BIOS revision: 103D02

426055:5372351: CLONE from skylake_server: [CR] Slow Warm reset - Erird parity error logged during NVMDIMM training (pre-pc 0xBF)
426052:5371893: [CR_POE_05] CLONE from skylake_server: Address aliasing on 2skt 2ch interleave configuration in PMEM
426047:5372000: [CR_POE_04] CLONE SKX Sighting: (CR) 2DPC half cachline data miscompare on automation config CRP01
426040:5371520: [CR_POE_15] [CR PM] [CR ES_0] Request for bios to disable CKE, OSR & PkgC if there is a NVMDIMM present on the platform for any SKX stepping less than H0.
Removed build workaround files+Skylake_BIOS.pdf

BIOS revision: 103D01

425542:NO_SIGHTING: Purley Release 103 BIOSID Update
425464:EPSD100255287:[BNP SFP+]10G NIC NVM image integration and softstrap enabling.

BIOS revision: 102D15

425102:5372330: UPI: DFX knob "DfxVn1En" does not enable VN1 when set to "Enable"

BIOS revision: 102D14

No change

BIOS revision: 102D13

No change

BIOS revision: 102D12 – BKC WW40

424786:5372379: [2016_WW38][BIOS:100_D14][Lightning Ridge] System will restart and cannot boot into OS any more when installing QAT Linux driver (Back out changelist 419478)
424593:5372386: [SKX H0 PO] Purley Patch: Release version 82000002
424468:EPSD100033536:When injecting ECRC error, SUT still operates normally

BIOS revision: 102D11

No change

BIOS revision: 102D10

424207:5372288 | [2016_WW38 BKC][BIOS: 100_D14][Neon city] System will reset during hibernation
424056:5372349: [SKX H0 PO] Fuse override settings not working
Modified for release
Modified for release

BIOS revision: 102D09

No change

BIOS revision: 102D08

423362:NO_SIGHTING: Inadvertant submit past stream lock for H0 PO (Back out changelist 423149)
423351:5372273: [SKX H0 PO] CLONE SKX Sighting: 2DCP LRDIMM CAP m2mem TO
423149:HSD 5372179: cachedLrBuf values not updated correctly during Back-side training

BIOS revision: 102D07

423014:[EPSD100034382] [WFP] Memory size in Setup is incorrect when memory device mismatch

BIOS revision: 102D06

No change

BIOS revision: 102D05

422693: 5372337: [SKX H0 PO] Need to extend w/a to H-step for memory error handling.

BIOS revision: 102D04

No change

BIOS revision: 102D03

No change

BIOS revision: 102D02

422346:5372265:[SKX H0 PO] BIOS is not setting IA32_FEATURE_CONTROL[LMCE_ON] when LmceEn knob == Enable on SKU with LMCE fuse enabled
422345:5372333: Cat error booting DP Neon City configs with 101.D06 (Back out changelist 421570)
422303:5372294: [SKX H0 PO] Hang after MRC with 2666MHz 2DPC fully populated
422250:5372286: System hang "08" during boot up with 32GB 2666MHz memory (build fix)
422233:5372286: System hang "08" during boot up with 32GB 2666MHz memory
422224:5332508: [CR_POE_14] CR: Setup Option Default to Enable NGN Mgment Driver
422211:5372310: Heavy ECC Injection = TOR TO or HA unexpected response
422203:5372289: MRC Hang Max ranks per ch exceeded
422185:5372174: SSID/SVID not correctly programmed for some devices

BIOS revision: 102D01

422109:5372255: Include LBG MPHY RC versions in PurleyRpPkg/projectMap (doc-only change approved for evaluation by mrthomas)
421963:5371929: 3-sigma table entries missing for 3DS LR-DIMM
421835: 5372257:[SKX H0 PO] Enable m2mem TO
421807:NO_SIGHTING: Purley Release 102 BIOSID Update

BIOS revision: 101D06

421662:5372036 | Setup Option "Max CPUID Value Limit" does not work
421599:5372267: CheckForOemResourceUpdate() does not detect overlapping stack resources after limit is reached
421570:5371893: [CR_POE] CLONE from skylake_server: Address aliasing on 2skt 2ch interleave configuration in PMEM
421435:5372203: Request to Enable CMDCTL Scomp Override after Initial Comp Update
421418:5372295: [SKX H0 PO] CLONE from skylake_server: [CR] B2P mailbox command MISC_WORKAROUND_ENABLE for uclk>dclk should not be sent on SKX H0
421383:5372198: Sporadic error 'Cannot send EINJ_CONFIG request (Time out)'
Added missing SPS FlashImageTool files that were being ignored by Git

BIOS revision: 101D05

421296:5372205: [SKX-P FPGA] FPGA VFs getting associated with incorrect IOMMU

BIOS revision: 101D04 – BKC WW39

421099:5372274: [SKX H0 PO] BIOS not programming m2mem_pad0 for flush hint address
421093:5371626: CLONE from skylake_server: [TF] FAB1 DIMMs failing NVMDIMM Backside Write Delay Training
421062:5332677: [SKX H0 PO] LR 4S - NUMA distance in SLIT table is incorrect
421050:5372253: need to update stitched BSSA RMT to v3.19.4
420952:5372244: MRC: RMT CmdVref margins missing

BIOS revision: 101D03

420949:5372269: Completer Abort error from GbE in 100.D10
420918:5330842: NFIT: incorrectly reporting DPA base in MemDev Table when two PM regions exist on DIMM
420905:5372235: [Klocwork] Issues found in module PurleySktPkg\Dxe\CrystalRidge

BIOS revision: 101D02

420659:5372273: [SKX H0 PO] CLONE SKX Sighting: 2DCP LRDIMM CAP m2mem TO

BIOS revision: 101D01

420535:5372104: Memory Mapped I/O above 4G disable will cause system keep reset during POST
420511:5372211: Build errors when optimization enabled in DimmIsolationFlow
420501:5372144: MRC: ValRequestHandlerAtBreakPoint broken by 10nm changes
420498:5370185: IPS 1207841362/6000145972: Move the OSHP() method to respective PCxx.asl code to avoid redundant code
420471:5372114: [Klocwork] Issues found in module PurleySktPkg\Library\ProcMemInit\Chip
420470:5372263: Top of tree BIOSes no longer train NVMDIMM at Normal/Max Serial Log - PlatformWriteSmb / PlatformReadSmb messages
420466:NO_SIGHTING: Purley Release 101 BIOSID Update
420464:5371426: Request to Optimize < PurleySktPkg\Dxe\CrystalRidge\CrystalRidge.inf > performance

BIOS revision: 100D16

420303:[EPSD100034647: [WFP] SUT will auto reset at POST code 0x94 after disable MMIO.]

BIOS revision: 100D15

420223:5371782: [CR_POE_16] NVMDIMM nvmcontroller swizzling registers need to be programmed outside of WRCRC enabling
420221:5372068: SMI 0x26 Security Issues-fixed chipsec SMI 0x26 hang up issue.

BIOS revision: 100D14 – BKC WW38

No change

BIOS revision: 100D13

420003:5371520: [CR_POE_15] [CR PM] [CR ES_0] Request for bios to disable CKE, OSR & PkgC if there is a NVMDIMM present on the platform for any SKX stepping less than H0.
419994:5371450: [CR_POE_02] MRC: BIOS cannot program NVMCTLR registers before CKE goes high in fast warm reset flow

BIOS revision: 100D12

419989:5372191: RAPL package 0 domain package locked by BIOS
419987:5372262: LRDIMM not booting (Back out changelist 419343)
419954:5372252: CLONE from skylake_server: [CR H0] SKX H0 fails NVMDIMM training at recEn PI

BIOS revision: 100D11

419948:5371715: CLONE from skylake_server: BIOS not mapping MC to Vr correctly for BPK
419944:5372243: [SKX-P FPGA] FPGA hangs after warmreset when setting to 0 the Socket Enable bitmap
419942:5372139: platform has CSME/BIOS GPIO ownership issues

BIOS revision: 100D10

419670:5372206: USRA Enhancement to remove 'WIDTH' parameter from Macro USRA_CSR_OFFSET_ADDRESS.

BIOS revision: 100D09

No change

BIOS revision: 100D08

419528:5371983: [CLONE from skylake_server: BIOS gets a GP fault in 2LM on a one socket system]

BIOS revision: 100D07

No change

BIOS revision: 100D06

419478:5372100: [WHQL] Whea failing fatal error event
419453:5371971: Investigate training steps which are printing data with Min Message Enabled

BIOS revision: 100D05

419380:5372154: [SKX H0 PO] PCIE: Enable bug fix for NAK sent on L1 entry
419343:5371626: CLONE from skylake_server: [TF] FAB1 DIMMs failing NVMDIMM Backside Write Delay Training
419342:5371881: [HW - PRE-ES0] Corrupted PCD after write/read operations

BIOS revision: 100D04

419331:5345315: Integrate Intel Apache Pass UEFI driver 01.00.00.1712

BIOS revision: 100D03

419294:5372111: ICC_SETGET_CLOCK_SETTINGS Structure Does Not Match SPS Documentation
419279:5371944: [LBG Si Request] BIOS needs to update EPMASKx registers to restrict access thru P2SB on LBG
419277:5372222: [FPGA] Error handler failure prevents boot
419243:5371962: Softstrap Override to LR complying with SPS ME xml configuration
419235:5371616: Move MrcHooksServicesPpi out of MRC_OEM_HOOKS_PPI_SUPPORT switch.
419213:5372105: [SKX-P FPGA] MAX_FPGA_SOCKET is not same as MaxIIO/MAX_SOCKET definition

BIOS revision: 100D02

418865:5371918: Command/Control margining can lead to cpgc hang with full rpq
418848: Back out changelist 418808
418808: Bad major version number, rolling back daily 100d01.
418752:5372170: No PTSS table applied on LBG B1
418748:5370471: xHCI debug does not function as expected
418744:5371832: WMP B0 RC43 Test BIOS (NC PTSS update)
418739:5372168: ME-BIOS interface version trace missing
418735:5372118: [Klocwork] Issues found in module PurleySktPkg\Me\Heci
418730:5372221: [FPGA] Changing BIOS knobs from default prevents boot
418725:5372174: SSID/SVID not correctly programmed for some devices
418648: Fix build issue for VERSION_MAJOR after changelist 418576

BIOS revision: 100D01

418495:5372201: MRC asserts in FastWarmBoot path in ExitSelfRefresh() when single thread option is enabled
418492:5372199: BUILD_TYPE constrained to Hex characters due to RC_REVISION implementation
418467:5372081: Below code would cause GP fault when the SMM_MCA_CAP MSR not avaliable
418460:5371773: Replace WBG SPS builds with LBG SPS build in OEM code.
418459:5371085: Enable Rack Scale 2.0 on Purley BIOS and ME/BMC fw
418457:5372059: [Klocwork] Issues in PurleyPlatPkg\Ras\Smm\ErrHandling\FpgaErrorHandler
418455:NO_SIGHTING: Purley Release 100 BIOSID Update
418451:5371908: Update PCD Bios Partition Failure in CR
418356:5371833: [CR_POE_01] CLONE from skylake_server: [CR_B0] WA update for skylake sighting s5352857
418342:5331333: [SKX H0 PO BIOS] NTB pcicmd and BAR setup

BIOS revision: 99D18

No change

BIOS revision: 99D17

No change

BIOS revision: 99D16

417915:5372158: [SKX-P FPGA] ioapic has no mapping iommu

BIOS revision: 99D15

417754:5372156: [SKX H0 PO] SX2B Cat error during boot with 99.D06

BIOS revision: 99D14 – BKC WW37

No change

BIOS revision: 99D13

417211:5372159: InitADR() code must be called from Slave Table in MRC.
417203: Addendum 5372177: Request to revert Purley Trunk back to SKX B0 patch 0x29
417182:5372116: [Klocwork] Issues found in module PurleySktPkg\SouthClusterLbg\Library

BIOS revision: 99D12

No change

BIOS revision: 99D11

416937:5372177: Request to revert Purley Trunk back to SKX B0 patch 0x29
416906:5372096: LER Triggering during Warm Resets
416901:5372119: [Klocwork] Issues found in module PurleySktPkg\Library\CpuS3MsrLib

BIOS revision: 99D10

416794:5370255:MRS synchronization with Refresh commands after NVDIMM restore
416782:5372112: [CLV] Update BiosToPcodeMailboxSimulationLib CLV Library to support MISC_WORKAROUND_ENABLE Bios-to-Pcode Mailbox v1.09

BIOS revision: 99D09

416729:5371724:[NVDIMM] system can't work in neoncity board when plugging only one smart 2400 NVDIMM .]
416718:5371807 : CLONE from skylake_server: BIOS needs to restore nvm DIMM DQ duffer during S3 resume
416717:5372108: [FPGA] ME in Operational mode causes Inband PECI messages to FPGA
416713:5372149: [FPGA] Mixed Config SKX-SP and SKX-P not booting
416711:5372145: Initial SKX H0 PO Patch Integration
416701:5371732: OemTableId and OemID in ACPI tables should have unique OEM table ID

BIOS revision: 99D08

416698:5345308:Purley Patch: Sysdebug Patch Release Version 0x2B to IFWI
416631:EPSD100034623: [BNP] SUT cannot parallel flash and downgrade from BIOS D0262
416624:5372155: [FPGA] Address of ParmDirectory must be 8-byte aligned before passing on to FPGA_BBS_PARAM

BIOS revision: 99D07

416333:5371931: BIOS needs to know when to spare dev17 for ADDDC+1 sparing
416297:5332810: new definition of MSR 0x62 to merge multiple 1LM+Pmem workarounds (with SIMICS fix)
416227:5372140 [FPGA] Boot fails when Socket 1 Bitstream is set to None

BIOS revision: 99D06

416099:5371317: Cloned From SKX Si Bug Eco: Cloned Bug: CLONE SKX Sighting: IIO: PCIE - Correctable errors with DLW/ASPM L1 and Laguna/PLX
415990:5371578: PMax Detector Offset correction (FPGA)
415928:5371988: grayout setup options for SRAT when NUMA is disabled.

BIOS revision: 99D05

415916:5371859: [SKX H0 PO] WrCRC fails on some configs with addition of CL# 395796 in 92.D09
415912:5371871: PPI-x not reporting correct status of TPM when removed from platform
415907:5371577: Unable to save TCG menu options with LPC TPM1.2
415900:5332336: [SKX H0 PO BIOS] MRC: Update MMRC spreadsheet to configure RxVref to be in per-bit mode
415883:5332293: [SKX H0 PO BIOS] Cloned From SKX Si Bug Eco: CLONE SKX Sighting: CATERR with M2Mem timeout error on SP4
415877:[5371999][SKX H0 PO] RAS handler infinite loop;
415872:5372115: [Klocwork] Issues found in module PurleySktPkg\Iio\Library\PeiDxeCommonIioInitLib
415871:5372117: [Klocwork] Issues found in module PurleySktPkg\SouthClusterLbg
415860:5371341: [SKX H0 TI] CLONE SKX Sighting: (4S Only) Silent Data Corruption (SDC) in presence of Core C6 - include WA to H step
415856:5332810: New definition of MSR 0x62 to merge multiple 1LM+ Pmem workarounds

BIOS revision: 99D04

No change

BIOS revision: 99D03

No change

BIOS revision: 99D02

No change

BIOS revision: 99D01

415418:5372092: [SKX H0 PO] KTI Recipe 2.5 mismatches on BIOS D-label 98.D03
415417:5372123: [Simics] Assert present when booting with EX_DDRx_LBG_MAX configurations
415387:5372124: [FPGA]SUT has a slow perfomance into setup option Menu or when boots to OS
415303:NO_SIGHTING: Purley Release 99 BIOSID Update
415293:5372050: [Klocwork] Issues in PurleyPlatPkg\Library\OemProcMemInitLib
415292:5372049: [Klocwork] Issues in PurleyPlatPkg\Legacy\Dxe\LegacyBiosPlatform
415288:5372062: [Klocwork] [NVDIMM] Issues in PurleySktPkg\Dxe\JedecNvDimm
415272: 5372097: MRC: Single threaded mode fails in Dimm Detection
415263:5372026: [LBG] Thermal Reporting always gets disabled with default "PchThermalDeviceAuto"
415256:5372061: [Klocwork] Issues in PurleySktPkg\Dxe\CrystalRidge
415249:5372110: On DVP board drives connected to secondary SATA controller are not detected
415233:5371658: SMBIOS spec table Type 1 Wake-up type field is Unknown

BIOS revision: 98D10

415138:[EPSD100034448] [WFP] Memory size is incorrect in SMBIOS Type 19 on BIOS D0249
415047:5333019:BIOS Disables PCIe Link for Slot 2 When Hot Plug Enabled and Slot Empty At G3 Exit
415044:5372063: [Klocwork] Issues in PurleySktPkg\Library\ProcMemInit\Chip\Kti

BIOS revision: 98D09

415030:5345282: Integrate Intel Apache Pass UEFI driver 01.00.00.1710
414997:5372071:ADDDC failover to +1 after mirror failover causes UC and/or and assert
414991:5332907: IMC Error Injection Fails ~25% of the Time With Directory Mode Enabled on 2S
414988:5370459: [SKX H0 PO BIOS] CLONE SKX Sighting: [ADDDC/SVL] 2B writes and write merge causes UC errors
414979:5370568: [SKX H0 PO BIOS] CLONE SKX Sighting: (CR) DDR4 Cap Logged on 2DPC RDIMM+ Config

BIOS revision: 98D08

414937:5345281:Purley Patch: Sysdebug Patch Release Version 0x2A to IFWI
414928:5372028: KTI: PHY recipe v3.0
414918:5372068: SMI 0x26 Security Issues

414916:5370185: IPS 1207841362/6000145972: Move the OSHP() method to respective PCxx.asl code to avoid redundant code
414904:5372064: [Klocwork] Issues in PurleySktPkg\Library\ProcMemInit\Chip\Mem
414903:5372048: [Klocwork] Issues in CpRcPkg\Library\BaseMemoryCoreLib\Core\Common
414902:5371710: Fort Park NVM image for 4S BKC IFWI
414862:5371982: Remove Dangling BmcCaterrMonEn knob
414795:5371832: WMP B0 RC43 Test BIOS
414722:[EPSD100034310:[WFP] I350 which installed in Riser2_tripple slot riser_slot1 cannot boot to PXE in legacy mode.]
414703:5372067: Building bios doesn't work with no amt support
414702:5372034: 1208906739: Build Errors when Optimization disabled in 95.D20

BIOS revision: 98D07

414537:5372053: [Klocwork] Issues in PurleyPlatPkg\Me\AMT\Library\DxePolicyUpdateLib
414536:5372054: [Klocwork] Issues in PurleyPlatPkg\Me\Policy\Library\DxeSpsPolicy
414535:5372056: [Klocwork] Issues in PurleyPlatPkg\Override\MdeModulePkg\Library\PiDxeS3BootScriptLib
414534:5372052: [Klocwork] Issues in PurleyPlatPkg\Me\AMT\Library\AmtPlatformLib
414531:5372051: [Klocwork] Issues in PurleyPlatPkg\Library\PlatformSaltLib
414461:5371966: CpuMpPeimInit will cause MCE: SAD_ERR_NON_CORRUPTING_OTHER
414445:5372057: [Klocwork] Issues in PurleyPlatPkg\Override\SecurityPkg\Library\DxeTcg2PhysicalPresenceLib (part 2 - fix build issue)
414373:5372057: [Klocwork] Issues in PurleyPlatPkg\Override\SecurityPkg\Library\DxeTcg2PhysicalPresenceLib
414343:5371174: String name change for MMIO High Granularity Size
414327:5372071: ADDDC failover to +1 after mirror failover causes UC and/or and assert

BIOS revision: 98D06

414307:4929300:Cloned From SKX Si Bug Eco: DID mismatch for BDF 2,23,5

BIOS revision: 98D05

414304:5372084 - [Simics] Assert present when booting
414297:5372032: [SKX H0 PO] MRC handling of SKX/ICX SKU capability vs. detected memory on the platform
414296:5371408:[NVDIMM]BIOS needs to Unarm NVDIMMs before reset and training sequences.
414269:Back out changelist 412891
414255:EPSD100254461: BIOS Security enhancement for SMM communication buffer
414173:Backout changelist 376024 ,it cause a showstopper for Red Hat
Ran IPClean on source individually to delete unchecked flags.

BIOS revision: 98D04

413951:[Purley][Klocwork] Issues in CpPcPlatPkg\Library\BasePasswordEncodeLibSha2
413832:5371578: PMax Detector Offset correction
413780:EPSD100032463: [WFP] Backup BIOS can't be flash when online flash BIOS via "UpdateBackupBios+UpdateNvram" parameter-disable EISS to unlock SPI region in PEI.
413735: [EPSD100033813: Legacy PXE function is failed on Dual CPU config.]
413732:5371758: Request to
413651:5371925: [FPGA] reset loop when add an external VGA card in the Slot1

BIOS revision: 98D03

413643:5371996: [FPGA]:one fail of BBS load followed by a successful BBS load
413631:5371948: [FPGA] VF BAR is not being programmed correctly
413625:5371946:[SKX-P FPGA] IOMMU Driver Crashes on IOAPIC to IOMMU Mapping Check
413621:5371721: [Klocwork] Issues in PurleyPlatPkg\Platform\Dxe\FpgaSocketSetup
413620:5371981: [SKX-P FPGA] BIOS Prints only 4 bytes of FPGA_BBS_PARAM_MSR
413576:5371975: TAD Offset Computation is Incorrect when Memory Mapping code rounds to force GB Alignment in 3-way or 6-way Channel Interleave
413536:5345256:Purley Patch: Sysdebug Patch Release Version 0x29 to IFWI

413451:5371674: Flag "CR Halt/Warm Mixed SKU" does not work. Regardless of the setting of the flag "CR Halt/Warm Mixed SKU", while the SKU is mixed, BIOS stops booting.
413437:5371945: CLONE SKX Sighting: Memory Controller Returning Poison when Viral is triggered and Link Error FSM indicates 'Idle'
413436:5371874: 1208876134: A7 mode is enabled for Purley
413431:5371931: BIOS needs to know when to spare dev17 for ADDDC+1 sparing
413416:5371618: Setting up 2LM mode in BIOS prevents SIMICS simulation from further booting
413408:5371896: BIOS fails to set proper BAR address when NTB BAR size set to 4G (32) or greater

BIOS revision: 98D02 – BKC WW36

413405:5370805: DMAR faults logged in OS when loading NTB drivers with VTd enabled in the bios
413404:5371787: Move P1 init to SEC phase
413401:5371865: CLONE SKX Sighting: ADDDC retry_rd_err_log_address1.faildevice incorrect on 3
413399:5371919: CLONE SKX Sighting: SVL Plus1 sparing failing with UC Error
413362:5370517: [ADDDC/SVL] 2B writes and write merge causes UC errors [Addendum]
413328:5371827: Request to Enable Multithreading call on PiSmmCpuDxeSmm driver
413324:5370517: [SKX H0 PO BIOS] CLONE SKX Sighting: [ADDDC/SVL] 2B writes and write merge causes UC errors
413315:5371931: BIOS needs to know when to spare dev17 for ADDDC+1 sparing
413313:5371937: ADDDC testcase 3b causes UCE and machinecheck in memory
413309:5371680: PCI Multiseg Support Broken in 94D14
413306:5371904: Mismatched LegacyVgaSoc/LegacyVgaStack issues a warm reset
413298:5371030: L0_REV_SKX and B0_REV_SKX have the same value (2), need to separate the different Si stepping
413291:5371030: L0_REV_SKX and B0_REV_SKX have the same value (2), need to separate the different Si stepping

BIOS revision: 98D01

413280:5371889: CLONE SKX Sighting: 2DPC-2400 3DS-LRDIMM DRAM RAPL UC TOR TO
413279:5371926: MCTP will cause uEFI hang on system with 2 or more CPU installed
413278:5371941: KTI Read IAR routine clears write_en bit, should wait for HW to clear the write_en bit before reading IAR
413277:5372014: [IPS 00106536/1208847256] ME/HECI - Skip initializing IE HECI if configuring HECI device fails
413275:5371951: PtuLoader driver is not compiling
413273:5371481: Cloned From SKX Si Bug Eco: KTI LL is incorrectly flagging AK VNA overflow/underflow error indication when VN1 is enabled
412937:NO_SIGHTING: Purley Release 98 BIOSID Update
412891:5330123: NVMDIMM protocol cannot assume that for a 3-way channel interleave that the first address associate with a DRAM rule is decoded to CH0

BIOS revision: 97D06

No change

BIOS revision: 97D05 – BKC WW35

412063:5371351: [Klocwork] Issues in CpRcPkg\Library\BaseMemoryCoreLib
411996:5333028: violation to the PCH BWG - section 3.6 Flash Security Recommendation (Back out changelist 403298, that back out 401771)
411974:5371355: [Klocwork] Issues in PurleyPlatPkg\Legacy\Dxe\LegacyBiosPlatform
411949:5371665: [IPS 1208790934] RTC.DM bit may come up in un-initialized state and not matching the format of the data
411948:5371935: Information in setup did not reflect current RC_VERSION on IPC BIOS

BIOS revision: 97D04

411935:5370221: MRC: DDR4 host Coarse Write Leveling improvement for frequencies above 1866 MT/s

BIOS revision: 97D03

411774:[Purley] [Addendum to EPSD100033389:[WFP] Reinstall the VGA Driver will make W2K12 OS Blue screen in Legacy mode.]

BIOS revision: 97D02

No change

BIOS revision: 97D01

411499:5371849: Violation to BWG - ERRINJDIS in the ERRINJCON register at B(3).D0-3.F0 + 1D8h [0] is set if associated B(3) PCIe ports are enabled
411312:5371953: RC 95.D20 doesn't work with 12G DIMM
411274:5371858: 1208845774: Incorrect implementation to Read IO Port 70h NMI bit in RtcRead/RtcWrite function
411271:5371535: LBG B1 AFE settings for USB2. RVP boards
410936:5371921: Patrol scrubber Address 2hi/lo register init.
410932:5371915: GetPerformanceCounterProperties() function returning incorrect values
410926:5371852: Change MMCFG Base to 1.5G/1.75G/2.25G boot to RHEL7.2 system hang up, Windows2012 reboot.
410924:5371228: [Hackathon] Modification of Setup variable leading to PDOS (part 2 - bakerville)
410914:NO_SIGHTING: Purley Release 97 BIOSID Update

BIOS revision: 96D24

410526:5371962: Softstrap Override to LR complying to SPS ME xml configuration

BIOS revision: 96D23 – BKC WW34

No change

BIOS revision: 96D22

410223:5345234: Purley Patch: Add Production Signed Release Version 0x27 for SKYLAKE to IFWI

BIOS revision: 96D21

410038:5371930: Early Processor Startup Causes LLC Cache Errors
409983:5371228: [Hackathon] Modification of Setup variable leading to PDOS
409948:5371654: L0 Remote BW lower than expected (IRQ threshold required for L0 step)
409945:5371867: Overclock Lock setup question incorrectly inverted
409940:5371584: MRC: Dimminfo DDR Vdd Printing Bugs
409936:5370413: Enabled Autonomous Core C-State knob not disabling dependent knobs
409935:5371161: Remove/Update code for "All CPU Information Page"
409930:5371562: 3_PCOMMIT Defeature and ADR support for Purley
409928:5371736: NVMCTLR registers mb_smm_nonce_0/1 are left populated before BIOS hands off to EFI shell or OS
409926:5371950: No message "ERROR: ME is non functional" after disabling ME
409919:5371625: Purley-SKX CRB BIOS DWR changes - BIOS setup menu fix

BIOS revision: 96D20

409651:5371907: Incorrect #definition in syshostchip.h
409618:5371828: In a certain UEFI implementation, adding memory to CPUSock 1 results in MRC hang
409606:5332362: PurleyMRC De-configuring entire memory channel for CECC detected
409603:5371816: CPU page fault exception while booting BIOS with CBDMA disabled.
409598:5371905: Fast coold boot Failing after new dimms are added

BIOS revision: 96D19

No change

BIOS revision: 96D18

409560:

> 5371895: m2mem_defeatures1.ingeco incorrectly programmed when multithreaded MRC is enabled on some 2-way ch interleaved configs
> 5371839: OS boot hangs after BIOS splash screen - SAD_ERR_NON_CORRUPTING_OTHER- BIOS 95D16

BIOS revision: 96D17

409429:5371356: [Klocwork] Issues in PurleyPlatPkg\Library\CustomizedDisplayLib
409428:5371351: [Klocwork] Issues in CpRcPkg\Library\BaseMemoryCoreLib

BIOS revision: 96D16

409270:5345216: Integrate Intel Apache Pass UEFI driver 01.00.00.1708
409262:5371909: [SKX-P FPGA] SUT sends assert booting with jumper J8C1 on 2 and 3 after N4PE flow enabled.
409261:5371910: [SKX-P FPGA] Need to enable the N4PE flow by default for PO entry.

BIOS revision: 96D15

409161:5345215: Purley Patch: Sysdebug Patch Release Version 0x28 for SKYLAKE B0 to IFWI
409118:5371835: Intel RC code discards the OEM resource map and uses default resource map in 8S configuration esbridge
409108:5371924: Apply s5370936 change (memory WrCmp overflow workaround) to all SKX steppings
409103:5371357: [Klocwork] Issues in PurleyPlatPkg\Library\LtDxeLib
408965:5371441: SVID/SID registers of IIO & PCH devices are not programmed depending on PcdLockCsrSsidSvidRegister PCD
408899:EPSD100034233: [WFP] There is only one Type 19 in SMBIOS with full DIMM installed

BIOS revision: 96D14

408790:5371884: [SKX-P/FPGA] Need to integrate the FpgaFwPkgTool script into the build/stitch process
408774:5371897: [FPGA] Clone from BKC: SUT sends assert message

BIOS revision: 96D13

408649:5371923: [NC,LR] Sut Hangs after booting to OS (Back out changelist 407913)
408629:5371804: [SKX H0 PO] CLONE SKX Sighting: EP PCIe Timout Completion Synthesis results in TOR Timeout -- From BDX HSD
408625:5371857: Diffrent DMI Gen and Link Speed
408549:5371877: PcieCorErrThres define UINT8 does not match EDS XPCORERRTHRESHOLD[14:0] 15bit definition

BIOS revision: 96D12

408502:5370664: BIOS print out buffer gen, FM controller and Stepping
408441:5371837: Platform do not boot to OS - PEI_ASSERT
408439:5333034: CR: SMBIOS Type17 Record - MemoryDevice needs to set Cache attribute bit for DDR4 DIMMs in 2LM mode
408406:5371882: Wrong ME firmware in AMT
408404:5371880: Remove handling wrong length of SPS_GET_ME_BIOS_INTERFACE response
408338:5371834: [SKX-P FPGA]: BIOS isn't programming FPGA VTd-BAR for SKX-P

BIOS revision: 96D11

No change

BIOS revision: 96D10

No change

BIOS revision: 96D09

408050:5371719: [Klocwork] Issues in PurleyPlatPkg\Acpi\Dxe\AcpiPlatform\AcpiPlatformVTDHooks
407951:5371854: PlatformEwlInit() should be called after the new MrcHooksServicesPpi is installed

BIOS revision: 96D08

407947:
5371256: GB Alignment for SNC 1 cluster on systems with only 1 iMC populated and 3way ddr4 chn interleaving
5371662: NVMDIMM Memory size is not being GB aligned with prefetchers enabled
407928:5371844: [CLV] Fix false negative result of SDDC +1 and Patrol Scrub validation reoutines.
407913:5371787: Move P1 init to SEC phase
407906:5371625: Purley-SKX CRB BIOS DWR changes - "Prep Done" options update
407867:EPSD100033090: [WFP] There is a fail message in Setup after use F9 to load default when SAS module OpROM is disabled.
407829:5371892: [FPGA] SUT sends assert booting whit jumper J8C1 on 2 and 3 .

BIOS revision: 96D07

No change

BIOS revision: 96D06

407576:5345201: Purley Patch: Sysdebug Patch Release Version 0x27 for SKYLAKE B0 to IFWI

BIOS revision: 96D05

407415:5370803: [SKX-D] [ME] Send Thermal Throttling initialization data to ME
407369:5370602: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal (configure MAX_SOCKET via PCD) for Bakerville platform.
407355:EPSD100250680: Disable measuing exit boot service event into PCR5.

BIOS revision: 96D04

407031:5332867: S3 resume time are very long (11sec) (IioEarlyPostLinkInit Delay)

BIOS revision: 96D03

406896:5370521: [Security VT] GPIO Pad locks should be in place by EndOfDxe
406893:5371740: BIOS should integrate xHCI BWG Rev20
406870:5370602: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal (configure MAX_SOCKET via PCD).
406847:5371625: Purley-SKX CRB BIOS DWR changes
406834:5371800: PTT is not initialized properly
406831:5371592: Platform do not transit to S5 - stays in S0 - DXE_ASSERT - fix update
406793:5332265: UBA for KTI Tx Equalization Parameters

BIOS revision: 96D02

406764:5331276: [SKX-P FPGA] define FPGA-specific POST codes
406754:5371515: DXE ASSERT when attempting to enable BIOS Guard with 91.D04 and newer (variable fix)
406636:5370833: Add the support for PMTT table in Purley Reference Code (Part 2)
406633:5371366: [Klocwork] Issues in PurleyPlatPkg\Platform\Pei\PlatformInit
406624:5371761: Add MemDebugPrint() API Support in MrcHooksServicesPpi.

BIOS revision: 96D01

406597:5371795: Workaround for ADDDC +1 not being implemented correctly - t_ccd_wr=1
406595:5371745: Assert when VMD enabled and FDx8 in slot 1
406591:5371352: [Klocwork] Issues in CpRcPkg\Library\PcieCommonInitLib
406588:5371376: [Klocwork] Issues in PurleySktPkg\Library\ProcMemInit
406585:5371365: [Klocwork] Issues in PurleyPlatPkg\Platform\Dxe\SocketSetup
406584:5371353: [Klocwork] Issues in CpRcPkg\Library\UsraAccessLib and PurleySktPkg\Smm\SmmAccessPei
406583:5371718: [Klocwork] Issues in PurleyPlatPkg\Platform\Dxe\MemorySubClass
406580:5371655: Patrol scrubs target memory hidden behind MMIO hole on 3-way configs
406570:5371070: [addendum] PCIe port can't be disabled from setup if the slot is populated with a device (Device Hide logic in IioLateInitilaize.c)
406560:5370445: Remove redundant FPK rom from BIOS region in SPI flash map
406556:5371826: M2M TO and TOR TO not disabled when rank sparing enabled on SKX
406551:5371476: Memory More Reliable Attribute not set when the system boots in Partial Mirror Mode
406539:5371768: Sync to BP 1330.421 to address core security issue defined in PSIRT-TA-201607
406413:NO_SIGHTING: Purley Release 96 BIOSID Update
406343: Add override.txt for CL 405854

BIOS revision: 95D23

405854:EPSD100032590: [BNP] Only 3 addin VGA devices listed in device manager and show another one "skylake -E PCI Express root port 1A -2030" yellow mark in Device Manager with Multi Addin VGA on both sockets.
405849:EPSD100033389: [WFP] Reinstall the VGA Driver will make W2K12 OS Blue screen in Legacy mode.]
405836:EPSD100254413: [BNP] SUT boot normally at MFG jumper, remove jumper and power on, SUT will hang 9C.]

BIOS revision: 95D22

No change

BIOS revision: 95D21

No change

BIOS revision: 95D20 – BKC WW32

405436:5345160: Purley Patch: Add Production Signed Release Version 0x24 for SKYLAKE to IFWI
405405: roll back CL403014: because patch25 is roll back
405273:EPSD100033956 -- [WFP] Alpha2 - PCIE M.2 speed is incorrect on J2C3(M.2 x4) and J4C2(M.2 x2)

BIOS revision: 95D19

405147:5371256: GB Alignment for SNC 1 cluster on systems with only 1 iMC populated and 3way ddr4 chn interleaving
405123:EPSD100033656: [STP]There is usb failed log in dmesg log after install RHEL 7.2 x64.
405122: CL404385 will cause system hang at 0x15 with debug BIOS and hang at 0xE8 with release BIOS. (Back out changelist 404385)
405112:[EPSD100033910, EPSD100034025]: SMBIOS Type 19 show physical memory size and total DDR4 Memory show effective memory size when in mirror mode
405091:EPSD100033380: [STP] There is "conflicts with Video ROM" message in message log after install RHEL 7.2 x64.
405010:5371779: [BIOS:95_D04][Neon city] TPM is not available
404811:5371728: KTIRC: Move 4 knobs from Sv to DFX
404790:5371815: System hangs while entering S3 and system resets eventually (Back out changelist 404660)
404724:5371762: ECC is disabled when memory is populated on MC1 of either CPU sockets.
404723:5371770: Low TxV RMT at 1DPC 2667 due to high per rank RMT variation
404716:5371702: Disable all clock gating in SPI Flash function (dis bits 9,8,5,1)
404689:5371778: [ME] SPS PTU option ROM not invoked since 94D29
404661:5371738: Remove IE disable Softstrap override from Lightning Ridge SS fixup
404660:5371592: Platform do not transit to S5 - stays in S0 - DXE_ASSERT
404618:5371722: Update BakervillePkg to sync with Skylake_Trunk 95D04 PurleyRpPkg

BIOS revision: 95D18

404567: 5371708 [SKX-P FPGA]: FPGA: Need a knob to skip N4PE flow defaulted to skip the flow

BIOS revision: 95D17

404425:5371753: LERRCTL register is not getting masked for all Iio Stacks;
404424:5371767: BIOS Incorrectly Programming the RIR's after re-partitioning through the NVM Drivers
404423:5371772: PCIE: Fix mistake on TCRH w/a
404421:5371594: Missing Link Speed option in BIOS menu
404420:5371698: APs not meant to access the EWL HOB; to be accessed by only the BSP
404411:5371633: Persistent CAP errors causes Windows BSOD when in channel mirror mode
404409:5371795: Workaround for ADDDC +1 not being implemented correctly - t_ccd_wr=1
404408:5371529: BIOS overrides Prochot Assertion Ratio which was set by ME
404403:5371793: BIOS Build script cleanup
404386:5371667: [SKX H0 PO] MRC: GetSetDIMMODT function not correctly handling DRAM Drv Str
404385:5370221: MRC: DDR4 host Coarse Write Leveling improvement for frequencies above 1866 MT/s

BIOS revision: 95D16

No change

BIOS revision: 95D15

404376:5371802: BSOD with signature MEMORY MANAGMENT a after Cstates stress test (Back out changelist 403315)

BIOS revision: 95D14

404143: fix PC hang issue-Back out changelist 403753

BIOS revision: 95D13

403840:5371794: INT IFWI is not generated (Back out changelist 403274)
403839:5371757: BIOS to set xpdfxsparereg[drop_poison_cmpl] when enabling LER
403773:EPSD100034043: ACPI BDAT Table exist in ACPI log.
403761:EPSD100254321: Disable FRB2 timer when waiting for entering Power On Password or the System Boot Timeout is waiting to continue will cause CPU exception at BMC force update mode
403754:EPSD100033895: PTU driver is not loaded after ME updated.
403753:EPSD100030812: SUT got some error and warning test items after finish selftest(7.0.19) under W2K12R2-64
403748: Back out changelist 397172

BIOS revision: 95D12

No change

BIOS revision: 95D11

403447:5371781: [4s, SIMICS] SUT and Simulation Simics hangs with Assert message
403444:5371750: ME error types update in EINJ OEM defined structure
403340:5371750: ME error types update in EINJ OEM defined structure.
403339:5371638: SVL failing on supercollider w/CECC
403315:5371256: GB Alignment for SNC 1 cluster on systems with only 1 iMC populated and 3way ddr4 chn interleaving

BIOS revision: 95D10

403298:5371771: Platform goes to WARM RESET after resume from S3 (Back out changelist 401771)
403274:5370521: [Security VT] GPIO Pad locks should be in place by EndOfDxe
403266:5371677: PCH DMI ASPM setup option is under Restricted Flags
403243:5371705: PchSmmCore.c code cleanup
403236:EPSD100034032: ACPI TMP2 table revision field value incorrect.

BIOS revision: 95D09

No change

BIOS revision: 95D08

No change

BIOS revision: 95D07

403020:5371138: TSC synch issues on LR Platforms (CPUPWRGD Routing)
403014:5371654: L0 Remote BW lower than expected (IRQ threshold required for L0 step)
402963:5371416: Minor code improvements. Replace use of magic numbers with macros already available.
402899:5371612: Request to Enable Multithreading call on TxtDxe driver

BIOS revision: 95D06

402867:5371749: Bios is using a deprecated B2P DDR_RANKS_PRESENT (0x92)
402853:

> 5371688: Disable Poison in setup, inject Memory UCE, next boot, system will get assert in LastBootErrorLog driver
> 5371635: patrolScrub_cecc fails with BIOS SMI Assert (SynchronizationMsc.c (161): Total < Timeout)

402842:5371683: Request to Enable Multithreading call on SocketSetup driver
402836:5371244: Boot time not matching Landing Zone (Timeout reduction)
402819:5371538: Pcie/Pch Test Content spec compliance modification
402789:5371707: Eliminate all remnants of EFI_SMM_RUNTIME_PROTOCOL code and usage in platform and silicon layer
402782:NO_SIGHTING: Submit Build Failure (Back out changelist 402772)
402772:5370664: BIOS print out buffer gen, FM controller and Stepping

BIOS revision: 95D05

402611:5370948: Failed to allocate IRQ to I350 Network card if connecting it to Slot 2 of CPU0
402599:[EPSD100033854, EPSD100033952]: The FRB2 timer is not suspended when waiting for entering Power On Password or the System Boot Timeout is waiting to continue.
402526:5331734: FPGA-specific RAS flows
402497:5371676: InitDdrioInterfaceLate routine causes excess csr writes, failures in emulation
402419:5371038: RC8/RD4 DIMM combination failing with CECCs
402367:5370432: BIOS issuing B2P commands not support by pcode and not checking for error codes.

BIOS revision: 95D04

402297:5371679: NTB not working in latest BIOS 91.D18
402296:5371746: After +1 condition, bios gets stuck in smi storm from memory ECC error
402295:5371608: BIOS should train DMI before DID/MRC

BIOS revision: 95D03

402233:5370918: Eliminate PCH_SPT macro in Purley code base - merge fix

BIOS revision: 95D02

402219:5370918: Eliminate PCH_SPT macro in Purley code base

BIOS revision: 95D01

402215:5371495: Change the Dynamic L1 default setting to enable
402211:5371354: [Klocwork] Issues in PurleyPlatPkg\Cpu\Dxe\GetCpuInfo
402205:5371247: NVMDIMM: namespace label area writes are mishandled
402161:5371649: AdrEn and ADREn are duplicate bios knob names

BIOS revision: 94D29

402080:5345142: Purley Patch: Release Version of 0x80000025 for SKYLAKE B0
402077:5371743: [SKX-P FPGA] GPIO table is not programmed for NC FPGA and OC FPGA board after the UBA change CL400307
402020:5371583: Multi-channel ADDDC test case fails with UC spare error
402006:5371561: KTI RC: mask KTI csr accesses on DE parts where functions do not exist
401921:5371725: Update PPI-x to version 0.04 in IFWI
401867:5371518: CL 381632 in the file CrystalRidge.c was reverted when submitted CL 390777.
401845:5371418: Handling of Processor Core and Uncore Errors inm case of Poison Enabled
401806:5371642: MRC Training algorithms Component Level Validation
401779:5371008: Isolate RC_REVISION into it's own header file Rc_Revision.h
401771:5333028: Violation to the PCH BWG - section 3.6 Flash Security Recommendation
401751:5371262: ME test menu cleanup (implementation of SPS_HW_CHANGE_PROTOCOL)

BIOS revision: 94D28

401667:EPSD100032817: The type 17/19 structure still report the disabled DIMM when populated the DIMMs that are different rank

BIOS revision: 94D27

401566:5371239: BIOS is not correctly configuring registers when stop and scream is enabled
401501:5371690: Hang at "Invalid Socket Id 0" with 94.D18
401498:5371735: NC Boot failed with PEI ASSERT (Back out changelist 400953)
401481:5370818: Server BIOS requires implementation of RAS flow notification to CSME
401408:5371593: Advanced Error Reporting options not available on some PCIe root ports
401404:5370818: Server BIOS requires implementation of RAS flow notification to CSME
401365:5371673: Missing ACPI0012 device (92D09+)
401352:5371685: PCIE: Enable bug fix for Phase2 EQ
401340:5371498: Register settings are set differently on SKT1 of 2S system
401334:5371689: System slowdown (possible TOR_TO) with large Snoop Response Hold Off Timer

BIOS revision: 94D26

401326:5371515: DXE ASSERT when attempting to enable BIOS Guard with 91.D04 and newer
401308:5332397: UBA (Unified Board Architecture) on Purley not fully implemented:IIO - Part2.
401298:EPSD100032463: Backup BIOS can't be flash when online flash BIOS via "UpdateBackupBios+UpdateNvram" parameter

BIOS revision: 94D25

401103:5370722: The memory information in BIOS setup menu is wrong when Mirror mode.
401068:5370957: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal. Part 3 of 3. Move MRC chip headers to chip folder.
400953:5371698: APs not meant to access the EWL HOB; to be accessed by only the BSP
400895:5371681: Clear HECI circular buffer before new transaction
400883:5371546: Receiver errors detected at GEN2 in two slots of Lighting ridge

BIOS revision: 94D24

400749:EPSD100033962: Win2012 R2 UEFI Device Manager has a yellow bang for FTPM

BIOS revision: 94D23

No change

BIOS revision: 94D22

400577:5371350: Request to set the proper default for MRC related settings on release build for boot performance enhancement
400573:5371651: AttempFastBoot and AttempFastColdBoot are not re training after new dimms are added

BIOS revision: 94D21

400549:5370303: MdeModulePkg\Library\PiDxeS3BootScriptLib is missing destructor and may cause SMM exception
400548:5371366: [Klocwork] Issues in PurleyPlatPkg\Platform\Pei\PlatformInit
400547:5345123: Purley Patch: Release Versions of 0x80000024 for SKYLAKE B0
400546:5371161: Remove/Update code for "All CPU Information Page"
400545:5371529: BIOS overrides Prochot Assertion Ratio which was set by ME
400543:5371369: [Klocwork] Issues in PurleyRpPkg\Library\AcpiPlatformTableLib

400542:5371364: [Klocwork] Issues in PurleyPlatPkg\Platform\Dxe\MemorySubClass
400541:5371367: [Klocwork] Issues in PurleyPlatPkg\Platform\SpiFvbServices

BIOS revision: 94D20

400510:5332702: MRC: add the HOB structure to pass this data forward (EWL) (Back out changelist 399221)
400506:5371641: SEC OEM Hooks cannot be overridden using library
400501:5371637: Incorrect pointer in KtiHooks.c
400472:5371570: [CLV] IIO Core Error setup option has no purpose in Purley code
400469:5371533: System Exception (Machine-Check) when use the B0 CPU (QL1K 1.80 GHz) and "disable" PCIE error;
400468:5371638: SVL failing on supercollider w/CECC
400467:5371452: Cloned from Brickland/IVT - Poisoned Memory Write Packet That Triggers LER Is Not Dropped
400466:5371640: Mirror x +1 Sparing Failures
400459:5371633: Persistent CAP errors causes Windows BSOD when in channel mirror mode
400457:5371480: SKX-F and SKX-SP combination will not boot on BIOS 89.D08 (Same fix valid for 5371609).
400451:5371070: PCI-E Port will be enabled when the port has support of Hot-plug [addemdum].
400434:5370371: GPE0 offset is not correct in ASL
400433:5345116: Integrate Intel Apache Pass UEFI driver 01.00.00.1697
400431:5371606: Cannot clear TPM in windows 2012R2 and PPI-X Ver 0.0.2
400430:5370950: SP8C intermittent cat error on boot with SKX B0
400428:5371358: [Klocwork] Issues in PurleyPlatPkg\Library\PeiPolicyUpdateLib

BIOS revision: 94D19

400307:5332397: UBA (Unified Board Architecture) on Purley not fully implemented:GPIO
399958:5371639: PlatformEwlInit called incorrectly in the master/slave tables
399938:5371243: ME capsule cannot be flashed using iFlash
399914:5371631: sSATA ports 4 and 5 not enabled in ECB

BIOS revision: 94D18

No change

BIOS revision: 94D17

399395:EPSD100251790: SUT is not able to boot in legacy mode when RMS3JC080 is populated.
399384: Back out changelist 398903 to restore the code change in CL#398899.

BIOS revision: 94D16

399223:5371114: Multithread MRC EN Fails after 85 D15
399221:5371659: Fatal error message on memory training (Back out changelist 396324)
399220:NO_SIGHTING: Broke MTMRC (Back out changelist 398547)
399209:5371656: Spare ranks are getting wrongly initialized in DXE MemRas driver

BIOS revision: 94D15

399182:5371661: Bios can't boot because DXE_ASSERT (Back out changelist 398965)
399048:5371656: Spare ranks are getting wrongly initialized in DXE MemRas driver (Back out changelist 398549)
399046:5370632: ACPI 6.1: Update ARS to ACPI 6.1
399040:5370314: Function BiosGuardInit() in PurleyPlatPkg cause system hang
399036:5370934: Force boot from local HDD - doesn't work (part II)
399010:5371630: Build BIOS fails when setting amt or sps enable on false

398965:5332397: UBA (Unified Board Architecture) on Purley not fully implemented:GPIO
398915:Back out changelist 398905
398905:5332397: UBA (Unified Board Architecture) on Purley not fully implemented:GPIO
398903:Back out changelist 398899 as no CCB approval for check-in yet.
398899:5371567: Rank is 0 in SMBIOS Type 17 when memory install in channel D,E,F only
398848:5371603: Build error with RAS_CPU_ONLINE_OFFLINE_ENABLE as False

BIOS revision: 94D14

398822:5371057: BIOS PCIe mPHY Duplication in ME
398700:5371560: Remove the Pl2SafetyNetEnable from the Adv PM-CPU Pstate Ctrl menu

BIOS revision: 94D13

398646:5370729: BIOS assumes SPD reserved bits=0
398641:5345101: Integrate Intel Apache Pass UEFI driver 01.00.00.1693
398608:5371342: Fails to inject patrol scrub error on BIOS 88D09
398606:5371180: Modify Default For ViralEn to be Enable
398593:5371554: NVMCTLR access mode changed from C/A bus to SMBUS which removes some MRS commands from CoEmu
398589:5371424: Incorrect bit masking for IIO uncorrectable errors;
398588:5371425: Request to Optimize <PurleyPlatPkg\Cpu\Dxe\GetCpuInfo\GetCpuInfo.inf > performance
398583:5332760: The serial port issue in Linux OS for Purley.
398568:5371375: [Klocwork] Issues in PurleySktPkg\Library\emcaplatformhookslib
398557:5371070: PCIE-Port capabilities Knobs will be available when PCI-E Port is "AUTO" (addendum)

BIOS revision: 94D12

398549:5371114: Multithread MRC EN Fails after 85 D15

BIOS revision: 94D11

398547:5371639: PlatformEwlInit called incorrectly in the master/slave tables
398539:5345100: Purley Patch: Release Versions of 0x80000023 for SKYLAKE B0 (Back out changelist 398331)

BIOS revision: 94D10

398501:5371582: Intermittent boot failure (machine check) with 92.D09 (Back out changelist 395144)

BIOS revision: 94D09

No change

BIOS revision: 94D08

398358:5370842: NVMDIMM Sample Code Package missing some files

BIOS revision: 94D07

398331:NO_SIGHTING: Back out changelist 398328, need to generate PO label
398328:5345100: Purley Patch: Release Versions of 0x80000023 for SKYLAKE B0
398234:5371622: SuperC hits UC Last-level memory Errors

BIOS revision: 94D06

398179:5371632: [8S Simics] System does not boot, simulation hangs at "TSC Sync - START" (Back out changelist 397213)

BIOS revision: 94D05

398138:5371632: [8S Simics] System does not boot, simulation hangs at "TSC Sync - START" (Back out changelist 397213)

BIOS revision: 94D04

398067:5371359: [Klocwork] Issues in PurleyPlatPkg\Library\PlatformBootManagerLib
398066:5371361: [Klocwork] Issues in PurleyPlatPkg\Library\UbaPlatLib
398065:5332397: UBA (Unified Board Architecture) on Purley not fully implemented:IIO.
398049:5371063: USRA Enhancements to move from bit-manipulation to struct/union format.
398048:5371504: Follow up to s5371016: NM ASL doesnt report HWP state properly
398044:5371602: ME State option value displayed wrongly in BIOS menu
398043:5371601: Wrong ME Firmware Type
397999:EPSD100253951: [WFP] System Assert on POST

BIOS revision: 94D03

397983:5371182: [SKX-P FPGA]: there is no FPGA device (deviceId: 0xbcbc) in the device manager of Windows
397981:5371363: [FPGA Klocwork] Issues in PurleyPlatPkg\Platform
397969:5371406: [SKX-P FPGA] IPS 1208464396 Large FgpaLoader PEIM size causes out of space in Boot block firmware volume.

BIOS revision: 94D02

397868:5371329: Need to enable LER x16 specific data containment related fixes from IVT B0 step onwards
397859:5370755: BIOS clocking knobs need to be modified
397803:5371510: PPR does not work as expected with current Purley BIOS
397799:5371362: [Klocwork] Issues in PurleyPlatPkg\Pci\Dxe\PciPlatform
397785:5332853: ACPI and PCI conflict when loading watchdog device
397723:5371216: Weak password encoding
397718:5371499: 2DPC 1CH 1MC 2SKT config does not boot with SNC Disabled or Auto at 2400
397703:Backing out CL 397634 HSD 5371621: [Simics] System does not boot, BIOS get freezed at message Initialize Enhanced Warning Log
397649:5370376: CR Spec Update - ACPI V6.1 - Move SW to the ACPI V6.1 specification - NFIT changes only compliant w/ ACPI 6.1

BIOS revision: 94D01

397634:5371114: Multithread MRC EN Fails after 85 D15

BIOS revision: 93D12

397565:5371591: Disable C6 for PO1 (power on stage1) BIOS
397549:5371174: String name change for MMIO High Granularity Size

BIOS revision: 93D11

No change

BIOS revision: 93D10

397494:Back out changelist 397337 - SKX-F and SKX-SP combination will not boot on BIOS 89.D08
397394:5371377: Issues while connecting switches (backplane, Futondale x8) into slots connected to 2'nd CPU on Neon City

BIOS revision: 93D09

397350:Back out changelist 396971 (5371281 Violation to BWG - SMI_LOCK (B0:D31:F0:Offset A0h Bit[4]='1')
397337:5371480 : SKX-F and SKX-SP combination will not boot on BIOS 89.D08
397297:5371536: BIOS restarts continously during Nfit programming.
397252:5371536: BIOS restarts continously during Nfit programming.
397244:5371484: SDDC +1, Patrol Scrub and Memory Mirroring validation libraries correction
397239:5332943: PCIe M.2 NVMe drive enumeration fails on the M.2 PCIE/SATA Slot
397232:5371202: PCIE: BIOS-ME disables SSC after links have being enabled to train (breaks SRNS model) - 1405120647: [RESET DUNGEON GATE] DMI Link going down around the time clock setup happens for SSC
397227:5371327: Unexpected ColdReset (0E) on execution of WarmReboot (06) from EFI shell
397213:5371138: TSC synch issues on LR Platforms (CPUPWRGD Routing)
397179:5370948: Failed to allocate IRQ to I350 Network card if connecting it to Slot 2 of CPU0

BIOS revision: 93D08

397172:EPSD100031353: No display output from addin VGA under 2012R2 UEFI mode if set both onboard VGA and AddinVideo adapter to enabled with one VGA on Socket 1. (Legacy passed)

BIOS revision: 93D07 – BKC WW29, BKC WW30

397137:5371604: [Simics] System does not boot, Assert is shown (back out changelist 397087)

BIOS revision: 93D06

397104:5371483: Fix Pcie Test Content to include changes of 5333024

BIOS revision: 93D05

397092:5371371: [Klocwork] Issues in PurleyRpPkg\Platform\Dxe\Setup
397087:5371202: PCIE: BIOS-ME disables SSC after links have being enabled to train (breaks SRNS model) - 1405120647: [RESET DUNGEON GATE] DMI Link going down around the time clock setup happens for SSC
397086:5371400: PS/2 KB can't work after s3/s4 resume
397083:5371537: Request to remove BIOS knob EdpcRepEn
397081:5371202: PCIE: BIOS-ME disables SSC after links have being enabled to train (breaks SRNS model) (HECI Transport)

BIOS revision: 93D04

396972:5370833: Add the support for PMTT table in Purley Reference Code
396971:5371281: Violation to BWG - SMI_LOCK (B0:D31:F0:Offset A0h Bit[4]='1'
396948:5371471: WMP B0 RC31 Test BIOS
396945:5371506: HSIO_TX_DWORD6 for sSATA is not programmed correctly
396924:EPSD100032846: The A6A0 error code is show a lot of in Error Manager Page.

BIOS revision: 93D03

396875:EPSD100030812: SUT got some error and warning test items after finish selftest (7.0.19) under W2K12R2-64

BIOS revision: 93D02

396865:[EPSD100033480, EPSD100033728]: DIMM Size show logical memory size but not physical size after enable rank sparing.
396846:5371375: [Klocwork] Issues in PurleySktPkg\Library\emcaplatformhookslib
396844:5370957: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal. Split MRC chip-specific header contents between CpRcPkg and PurleySktPkg and move MRC header files from CpRcPkg to PurleySktPkg. Isolate Chip function prototypes called by the MRC Core into BiosSsaChipFunc.h, KtiApi.h and MemApiSkx.h. Modify code where necessary to abstract MRC Chip data from MRC Core files.
396838:5370957: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal. Wrap all calls from BaseMemoryCoreLib to ProcMemInit in a macro. Macro does nothing in the Purley tree. It is required in the 10nm tree.
396836:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL 363084: Support for Headless MRC Host executable
396834:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL 359979: Update turnaround timing registers for 10nm
396827:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL's 370507 and 377979
396814:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL's 370424, 369398, and 364214
396812:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL's 371125, 379000, 373292 and 379071
396811:5371304: Port 10nm MRC core changes to Purley MRC - 10nm CL's 361541 and 374702

BIOS revision: 93D01

396746:5371368: [Klocwork] Issues in PurleyPlatPkg\Ras\Library\mpsyncdatalib;
396726:5371452: Poisoned Memory Write Packet That Triggers LER Is Not Dropped
396688:5371446: MRC: FC Emulation not initializing ddrio
396630:5371404: SVL Error Logging Continually Logging Errors w/ Patrol
396629:5371102: ADDDC : Buddy_cs_en is not cleared for non +1 spares & reversing from Bank to Rank with multi-channel regions is incorrect.
396628:5370722: The memory information in BIOS setup menu is wrong when Mirror mode.
396621:5371008: Isolate RC_REVISION into it's own header file Rc_Revision.h
396620:5371576: 394788 introduced a bug in the rasdebug serial print

BIOS revision: 92D10

396426:5371296: KW Builds Targets Failing
396422:5371575: Extend WA 5371341
396346:5371260: FD Disks are not hidden in EDKII Menu when VMD is enabled on Socket1 (Addendum)
396324:5332702: MRC: add the HOB structure to pass this data forward (EWL) (Put Back Initial Changes of 395253)

BIOS revision: 92D09 – BKC WW28

396277:

5371545: Need to set link_cfg_read[12]=1 to disable byte enable parity check
5371551: Need to set .mccbgfd_en_3ch=1 for MCs with 3 channels populated.
5371571: Need to extend WA for SKX s5353086

396240:5345060: Purley Patch: Release Versions of 0x80000022 for SKYLAKE B0
396223:5371556: SUT does not resume from S3 (Back out changelist 395145)
395848:5371070: PCIe port can't be disabled from setup if the slot is populated with a device (Device Hide logic in IioLateInitilaize.c)
395843:5371539: Supercollider split lock hanging with outstanding Ubox lock to IIO
395798:5371116: Enable Parallel Mode for Cold Reset using multithread in MRC
395796:5370733: B2B Turnaround Optimization Fixes Causes Training Failures on B-step
395788:5371429: Request to Optimize <PurleyPlatPkg\Legacy\Dxe\LegacyBiosPlatform\LegacyBiosPlatform.inf > performance
395787:5371470: Investigate optimization of making PatchSratTable() StartupThisAP call run in parallel
395773:5370553: Kernel panic occurs during system S4 reboot/hibernation in RHEL 7.1 on Neon city
395745:5371170: Enable NFIT/DSM to support OEMs
395720:5371289: Violation to BWG - PACKAGE_POWER_LIMIT MSR 610h LOCK (bit 63)
395712:5371287: Violation to BWG - PACKAGE_RAPL_LIMIT B1:D30:F0 Offset E8h PKG_PWR_LIM_LOCK (bit 63)

395711:5371290: Violation to BWG - CONFIG_TDP_CONTROL B1:D30:F3 Offset 60h CONFIG_TDP_LOCK(bit 31)
395709:5371294: Violation to BWG - LTDPR B0:D5:F0 Offset 290h LOCK (bit 0)
395704:5371039: Incorrect initialization of decoding the port80 by LPC at SEC phase
395702:5371420: Make PchIoApic24119Entries setup option available in External BIOS

BIOS revision: 92D08

395665:5371556: SUT does not resume from S3 (Back out changelist 395253)
395652:5371037: Implement KT interrupt configuration for ME and IE
395621:5371448: Option /setting in BIOS menu to enable ME is not shown, after disabling ME using BIOS menu
395532:5331255: [SKX-P FPGA] program LLPR (protection registers) for FPGA

BIOS revision: 92D07

No change

BIOS revision: 92D06

395253:5332702: MRC: add the HOB structure to pass this data forward (EWL)
395201:5371316: Enhanced Log for Gen 1 does not contain corrected memory error record with 88d09 bios - 5371401 | Memory corrected error causes hang in SMM loop
395183:5371261: Build flag option to select EWL and Legacy Warning Log
395161:5370648: MRC: 2 DPC NVMCTLR mixed with RDIMM fails backside write Corase
395160:5332889: [NVDIMM] Require LBG PM_CFG3.HOST_MISC_RTC_CFG set to non-default value (longer) to meet NVDIMM ADR timing requirements
395145:5371479: Acpidump in Linux throws error
395144:5371495: Change the Dynamic L1 default setting to enable
395143:5371517: PPM code is writing MSR 0x1aa when HWP_EN fuse disabled
395084:5371385: LBG: FW Status Read Fails w/FDO enabled

BIOS revision: 92D05

No change

BIOS revision: 92D04

394807:5371522: Wrong Code Version - BP shown in BIOS Release notes
394788:5332688: Request for TRUE Release mode BIOS builds for Purley
394777:5371452: Poisoned Memory Write Packet That Triggers LER Is Not Dropped
394775:5371380: Unable to query TPM1.2 module / TCSD service wont start
394762:5371411: Unable to handle any severity error form PCH Root Ports;
394757: ADDDC : Buddy_cs_en is not cleared for non +1 spares & reversing from Bank to Rank with multi-channel regions is incorrect.
394751:5371516: SDDC is disabled when mirroring capability is supported.
394730:5371246: Change in recommended value of starve count
394727:5371114: Multithread MRC EN Fails after 85 D15 and 5371165: [Purley][Simics]RC_ASSERT break the boot sequence related with Smbus.c
394726:5370778: [LRDIMM] 2DPC failing w/ data miscompare (PGT Alias x PPD)

BIOS revision: 92D03

394670:5345045: Purley Patch: Release Versions of 0x80000021 for SKYLAKE B0

BIOS revision: 92D02

394511:EPSD100253097: iFlash32_v14_1_Build3: it will show error "wrong command string to get BIOS boot info by SW SMI(0x26)" when run cmd "iflash32 -ccs".

BIOS revision: 92D01

394242:5370724: System hang at early memory initialization with 32 pieces of 128GB LRDIMM installed with EP4S Processors
394238:5370910: Memic + cap fails w/ M2M TO after traffic stops
394237:5371419: Purley Bios implementation of Physical Presence Interface extensions (PPI-x)
394234:5371315: System is not able to boot after TXT has been enabled.

BIOS revision: 91D18

393733:5371502: S3 broken due x64 Exception (Back out changelist 393244)

BIOS revision: 91D17

393560:5345000: Integrate Intel Apache Pass UEFI driver 01.00.00.1680
393545:5371266: [SKX-P] Inbound transaction on UPI from FPGA gets no response

BIOS revision: 91D16

393317:5345033: Purley Patch: Release Version 0x80000020 for SKYLAKE

BIOS revision: 91D15

393247:5371349: ICV (Integrity Check) failure to UMA (MESEG) with SPS FW
393244:5371289: Violation to BWG - PACKAGE_POWER_LIMIT MSR 610h LOCK (bit 63)
393242:5371285: Violation to BWG - SAPMCTL B1:D30:F1 Offset B0h LOCK (bit 31)
393241:5371282: Violation to BWG - MSR_POWER_CTL MSR 1FCh PROCHOT_LOCK (bit 27)
393215:5371184: Correct the type of CL386858 of s5371184
393214:5371258: Apparently vestigial part of the KtiLib.c, CalculateBusResources() function that could be removed if no plan to use it.
393201:5371413: SMB_TSOD_CONFIG_CFG registers are not updated when TSOD is disabled
393105:5371003: Update UEFI Shell for RP

BIOS revision: 91D14

393064:5371243: ME capsule cannot be flashed using iFlash
393060:5371011: AMAP.dimmX_pat_rank_disable not being updated correctly after rank failover with mapped out ranks
392930:5371343: BL Egress Credit Mismatch / TOR TO.
392927:5371173: CommonCore: PipeInit.c should be moved to Chip to eliminate file ScratchpadRegHack.h.
392905:5370672: Investigate optimization of making all StartupAllAPs calls run in parallel

BIOS revision: 91D13

No change

BIOS revision: 91D12

392850:5345030: Lighting Ridge don't make transition to Cstates (Back out changelist 392066)

BIOS revision: 91D11

392730:5371472: NC Boot failed with PEI ASSERT (Back out changelist 392080)
392664:EPSD100030777: There is no screen displayed in remote terminal after SUT boot to DOS.
392662:EPSD100110744: PCH temp sensor does not appear to be working

BIOS revision: 91D10

392606:EPSD100032424: No PTU Driver loaded in shell after 'PTUHWChange' variable changed. (Add one more patch)
392555:5371317: IIO: PCIE - Correctable errors with DLW/ASPM L1 and Laguna/PLX
392499:5371142: System reset on injecting SRAR error if eMCA and LMCE are enabled in BIOS
392497:5371387: BIOS is not correctly configuring LER_CTRLSTS register when LER is enabled
392491:5371275: ADR setup: values written to ADRTIMERCTRL:ADR_MULT are not correct
392399:5371175: Memmap does not reflect NFIT table PersistentMemory Map for multisocket systems

BIOS revision: 91D09

392376:5371260: FD Disks are not hidden in EDKII Menu when VMD is enabled on Socket1
392338:5371344: NVMe SSD's don't show up in BIOS setup
392286:5371052: ADDDC x Mirroring SMI Handler Code Is Incorrect
392262:5371404: SVL Error Logging Continually Logging Errors w/ Patrol
392250:5370953: [10nm] Modify Purley OEM Hook from statically link to dynamically link.
392247:5371253: Clear xpdfxsparereg1[dis_msk_uncerrsts_cto_in_ler] to keep synthetic CTO from getting logged during LER
392239:5370942: Memhot bits not set for low, mid, high and oem throt when MEMHOT enabled in BIOS
392238:5345017: Purley Patch: Release Version 0x80000020 for SKYLAKE

BIOS revision: 91D08

392220:5370204: Platform is signaling ExitPmAuth instead of EndOfDxe, too late, not signaling SMM event

BIOS revision: 91D07

392213:5331307: FatalError after nvdimm configuration Persistent1Setting=ByOne Persistent2Setting=ByOne
392210:5371447: SKX Patch Initial Integration
392206:5371303: SP7D CatErr with 89.D08 (Back out changelist 386394)
392200:5371204: MRC handling of SKX/ICX SKU capability vs. detected memory on the platform
392193:5371077: Request to review and change SATA EQ code within the SATA/sSATA Test mode setup options
392117:5371208: [SKX-P FPGA] Cold reset is required when BBS index or FPGA enable bitmap is changed in setup menu

BIOS revision: 91D06

392080:5332397: UBA (Unified Board Architecture) on Purley not fully implemented.
392070:5370971: Device type 19 & Device Type 20 (extended address), not supported in RC.
392069:5371091: FPGA: Need BIOS to disable TSOD polling during BBS load
392066:5370602: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal (configure MAX_SOCKET via PCD).

BIOS revision: 91D05

No change

BIOS revision: 91D04

391689:5371434: S3 does not complete 10 cycles (Back out changelist 389706)

391678:5332397: UBA (Unified Board Architecture) on Purley not fully implemented: BMC_PCIE_PORT, OEMID, external clkgen.

BIOS revision: 91D03

No change

BIOS revision: 91D02

391329:5332511: Platform Reset function does not honour Pch Platform Reset Policy in Purley

BIOS revision: 91D01

391204:5371308: BIOS not restoring the xover training registers before enabling the clock during S3 resume
391201:5370223: MRC: Need Get function for GNT2ERID delay for use by BSSA ERID margining
391159:5371248: KTIRC: Add back the H0 step support for RRQ threshold - loack definition of RRQ_IRQ_THRESHOLD_DIS
391141:5371248: KTIRC: Add back the H0 step support for RRQ threshold
391121:5370540: [ME] Split ME configuraion into separate screens for ME11 and SPS to make it easier to maintain
391085:5371087: [ME] ME Storage Services Library for Physical Presence Interface extensions (PPI-x)
391056:5371348: Wrong length of SPS_GET_ME_BIOS_INTERFACE response

BIOS revision: 90D14

390869:5370996: PCIe Gen 3 Alternate TxEq
390867:5370815: Core sync in december backleveled multiple purley overrides
390824:5370235: Need hook after address maps configured

BIOS revision: 90D13

390786:5333024: CheckForIioErrors should support both IoMCA and EMca2 are enabled case
390777:5370187: Skylake memory mapping. Use of arrays to get channel interleave bit maps per IMC in socket SAD table.

BIOS revision: 90D12

390373:EPSD100253542: PCIe correctable errors not logged in BMC (WFT board)
390273:5371249: Injecting corrected errors corrupts target location in memory

BIOS revision: 90D11

390179:5371298: MRC: BSSA RMT CMD Margining Broken with 89.D01 + (Back out changelist 386434)

BIOS revision: 90D10

390150:5371332: PCIE: PHY recipe v3.0
390140:5371388: LightingRidge does not boot due PpmInitialize.pdb error
390130:5371199: <ResetDungeon>UMA Integrity check failures with SPS FW
390057:5371335: [SKX H0 TI] UCECC causes SDC
390055:5371341: [SKX H0 TI] (4S Only) Silent Data Corruption (SDC) in presence of Core C6
390042:5371397: [SKX H0 TI] Disable SSC by default. SSC causing issues with Reset testing

BIOS revision: 90D09

390029:5371140: chn_temp_cfg.bw_limit_tf changes unexpectedly when adding memory to different channel
389984:5371086: Move ADR enablement code out of PurleySvRestrictedPkg for OEM use

389979:5371378: The maximal pad number definition of GPIO GPP I and K are wrong.
389966:5371135: Cleanup ME_TESTMENU options impact for customers
389960:5370509: Reserve more than 64MB of memory from BIOS TraceHub menu causes assertion
389952:5370595: CD-ROM not being detected when set PCH SATA to RSTe RAID mode and legacy boot mode
389939:5371210: [SKX-P FPGA] SKX-P FPGA B4D02F0 is forced to Hot Reset
389934:5371092: Adapt CLV simulation layer to use MmPciLib instead of PciExpressLib
389930:5371209: [SKX-P FPGA] GPP_E_0_FM_CPU0_RC_EN need to be set to low when FPGA is disabled on Opal City FPGA board

BIOS revision: 90D08

389806: Back out changelist 389803
389803:5371092: Adapt CLV simulation layer to use MmPciLib instead of PciExpressLib

BIOS revision: 90D07

389768:5371332: PCIE: PHY recipe v3.0 (Back out changelist 389724)

BIOS revision: 90D06

389724:5371332: PCIE: PHY recipe v3.0
389723:5371307: Wrong DMI Gen and Link Speed traces
389706:5370672: Investigate optimization of making all StartupAllAPs calls run in parallel
389653:5370986: PCR1 value doesn’t change when add a RAM on Neon City
389575:EPSD100033090: There is a fail message in Setup after use F9 to load default when SAS module OpROM is disabled.
389479:5370298: [SKX-P FPGA] Enable capsule support to update FPGA BBS firmware volume only

BIOS revision: 90D05

389473:5371214: FPGA BIOS knob doesn't synced to the Setup structure correctly
389469:5371166: SKX-FPGA BIOS for Opal City FPGA may be configuring GPP_E_4 (RC_ERROR) as output low

BIOS revision: 90D04

389296:5370703: Enhance Mtrr programming when using default type=UC

BIOS revision: 90D03 – BKC WW26

389260:5371315: System is not able to boot after TXT has been enabled (Back out changelist 386463)
389226:5370972: MC Link Fail Setup
389182:5371239: BIOS is not correctly configuring registers when stop and scream is enabled
389181:5371236: Default value of snp_rsp_count knob in IIO.
389180:5371201: PCIE: Request. Change default Downstream Tx Preset to P7
389172:5371131: Remove unused SV code
389159:5370699: Not possible to build single binary for both 4 and 8 socket. Intel to remove if/endif for MAX_SOCKET
389096:5371071: ME11: With GeForce 210 card, S3 -> S0 transition results in BSOD
389089:5371185: ME11: BIOS detection of ME11 can fail after reset
388947:NO_SIGHTING: Build failure (Back out changelist 388931).
388932:5370735: [10nm] Silicon init code should be contained to a firmware volume with ABI.
388931:5371173: CommonCore: PipeInit.c should be moved to Chip to eliminate file ScratchpadRegHack.h.
388912:5370675: Page Break Management Bug Causes Hang for Some DIF INSERT Operations
388902:5370834: Need NVDIMM enabled binary builds as a build target in BKC releases
388894:5371101: On ADR Resume, memory error threshold registers are not restored]
388892:5370357: On Linux host, transition to S4 is treated like S5

388880:5344972: Integrate Intel Apache Pass UEFI driver 01.00.00.1676

BIOS revision: 90D02

388875:5371212: Modify IMC Viral Change in 5332578 To Apply To All Steppings
388872:5371337: System is not able to boot to Setup (Back out changelist 388750)
388871:5371227: Usage of AllocateZeroPool without Runtime check before dereference
388870:5370446: IIO does not log Advisory Non-Fatal error in correrrsts when Poison is enabled
388869:5371213: BIOS does not seem to enable partial mirroring for efibootmgr on RHEL 7.2

BIOS revision: 90D01

388754:5371274: MeDeviceControl() for HECI enable operation uses wrong definitions
388750:5371246: Change in recommended value of starve count
388748:5371038: RC8/RD4 DIMM combination failing with CECCs
388747:5371222: Newly-added CPU could execute untrusted code while being inserted in a running system
388745:5330673: RC has insufficient PCU mailbox communication error handling (Fix Typo)
388743:5371016: NM ASL doesnt report HWP state properly
388736:5371299: Need to change Register revision for memory vendor in BIOS
388717:5370934: Force boot from local HDD - doesn't work
388713:5370472: S3 resume fails with DXE Assert (MemRasS3Save.c) with Bios Guard Enabled
388712:5371190: Despite of disabling hmrfpo Lock in Bios menu this message is still sent during booting

BIOS revision: 89D10

388684:5371120: [NVDIMM] ADREn setup option is dependent on other setup option which is not part of MRC data structure
388683:5333044: SMART DDR4 NVDIMMs fails to train

BIOS revision: 89D09

388343:5371276: [Simics] Assert after returning from S3 in SVOS (Back out changelist 386786)
388338:EPSD100033396: HDD connect to SATA controller can?t be detected. sSATA controller without this issue.
388327:NO_SIGHTING: Unapproved content (Back out changelist 388291)
388291:5370735: [10nm] silicon init code should be contained to a firmware volume with ABI.
388267:5371087: [ME] ME Storage Services Library for Physical Presence Interface extensions (PPI-x)

BIOS revision: 89D08

387749:5371267: Blue Screen is shown on system when try to boot to Windows (Backout of CL#386508)
387737:5371271: Cpu GP exception at LastBootErrorLog driver (Back out changelist 387559)
387717:5370699: Not possible to build single binary for both 4 and 8 socket. Intel to remove if/endif for MAX_SOCKET. Revert WheaSiliconHooksLib changes.
387580:5371136: BIOS to update for SKX CAPID changes - CPU
387575:5370392: Cannot PXE boot Neon City with SKX-F parts

BIOS revision: 89D07

387559:5370699: Not possible to build single binary for both 4 and 8 socket. Intel to remove if/endif for MAX_SOCKET
387515:5370783: Infinite looping SMM error handler when Emcagen2 enabled and system recoverying from IERR
387449:5371065: RasModesSupported don't expose right value for mirror
387436:5371102: ADDDC : Buddy_cs_en is not cleared for non +1 spares & reversing from Bank to Rank with multi-channel regions is incorrect.

BIOS revision: 89D06

No change

BIOS revision: 89D05

No change

BIOS revision: 89D04

387002:5332382: [Part 4] PurleyPlatPkg and PurleySktPkg should not depend on PurleyRpPkg KTI code fix

386911:EPSD100253437: SPS FW E5.04.00.02.053 support A0&B0 PCH for PCSD projects

BIOS revision: 89D03

386858:5371184: KTIRC: Index of StackBus array is programmed incorrect in FillEarlySystemInfo

386843:5371105: Change V_PCH_RST_CNT_FULLRESET when ColdReset

386840:5371186: SVOS is not booting properly. Revert "5332760: The serial port issue in Linux OS for Purley."

386800:5332714: Remove BIOS w/a for Pilot 4 BMC lack of L1 support Revert "5331967: [LBG Val Critical] Set PCIEDBG.DMIL1EDM for BMC on Non City Boards"

386794:5371034: PurleySktPkg is depending on PurleyPlatPkg in ME module

386786:5371039: Incorrect initialization of decoding the port80 by LPC at SEC phase

386780:5370683: PurleyNeon City CRB: Remote Boot from USBr UEFI CD does not work.

386767:EPSD100032225: Change serial port A and B IRQ/Address to the same value, OS not take effect

386765:EPSD100032921: in socket 2 is not list on W2K12 R2 OS device manager.

386745:EPSD100031739: The iSCSI OPROM has enable, BIOS disk order have iSCSI & sSATA HDD option,it should have iSCSI & sSATA & SATA HDD option.

386697:EPSD100253200: Use "ASPPED_ENABLE" to replace "PC_HOOK" for ASPPED related code in if any.

386685:5371081: The definition of variable “ReserveMemFlag” violates UEFI Specification.

BIOS revision: 89D02

386654:5371153: [SKX-P FPGA] System hang during program bus number for FPGA after CL382561

386536:5371101: https://vthsd.intel.com/hsd/bios_purley/default.aspx#sighting/default.aspx?sighting_id=5371101&hsdmsgstr=3

386532:5370542: BIOS support for FIS 1.2 Release

386515:5371151: BIOS 86D01 and above failed to train PCIe uplink up to x8 Gen3

386510:5371109: ADDDC failover on socket 1 causes system hang

386508:5371212: Modify IMC Viral Change in 5332578 To Apply To All Steppings

386506:5370843: Second failure with ADDDC on STD Sku B0 parts cause M2Mem TO and TOR TO

BIOS revision: 89D01

386476:5371132: KTIRC: Ignore m3kti mismatch when when -P present

386463:5371180: Modify Default For ViralEn to be Enable

386438:5371144: RcSIM instances don't stop executing and their logs don't stop growing.

386434:5371181: MRC: BiosSetMarginParamOffset should not cache Cmd/Ctl/Erid group offsets

386433:5370645: IIO Additional error reporting and XPGLBERRSTS should be checked separately

386423:5370963: ”String not found on command” error in SSC test suites for CLVR bios

386420:5370650: PciErrLibIsRootPortErrReportingEnabled implementation is incomplete

386419:5332663: HSBP U.2 SSD LED Acitivity Not working as Expected on NeonCity 2S

386417:5371179: Modify Default For UboxToPcuMcaEn to be Enable

386414:5370152: TOR TO/ECC w/ Retries on No Data Packets

386412:5333073: Purley PCI-E Multi-segment support is not fully implemented in some drivers [RAS]

386394:5370733: B2B Turnaround Optimization Fixes Causes Training Failures on B-step

386280: Build Failure / Unapproved Submit (Back out changelist 386247)
386250:5371160: Add the Pl2SafetyNetEnable knob back to the Adv PM-CPU Pstate Ctrl menu
386247:5370602: [10nm] CpRcPkg/Library/MemoryCoreLib chip/platform dependency removal (configure MAX_SOCKET via PCD).
386244:5370992: Xover Margin Offsets, EV update part2

BIOS revision: 88D09 – BKC WW24

385873:5370775: RAS Error Handler causing URs on PCIe Endpoints
385864:5371211: BSOD when trying ot boot to Winows (Back out changelist 385406)

BIOS revision: 88D08

385700:5371191: Not able to complete 10 S3 cycles, DMI training hang
385429:5370910: memic + cap fails w/ M2M TO after traffic stops
385406:5370910: memic + cap fails w/ M2M TO after traffic stops
385361:EPSD100252527: High Definition Audio Controller Unknown USB Device.
385273:5371167: CL383168 will cause system hang at 0xE8 (Back out CL383168)

BIOS revision: 88D07

385245:5370844: Update to IASL compiler in BpCommonPkg\Tools directory to make our RC ACPI 6.0 compliant
385242:5371066: Memory VDD setting doesn't work with 5mv steps in Purley BIOS

BIOS revision: 88D06

385075:EPSD100030812: SUT got some error and warning test items after finish selftest (7.0.19) under W2K12R2-64

BIOS revision: 88D05

No change

BIOS revision: 88D04

No change

BIOS revision: 88D03

384890:5370775: RAS Error Handler causing URs on PCIe Endpoints
384820:5333091: Purley ddr4 reverse address traslation support-- re-opened.
384819:5330179: [Security VT][SDL S2] ACPI Parameter Block used as OSPM/SMI mailbox needs security analysis
384808:5371051: BIOS should be able to inject error into ME UMA test page
384796:5370133: Blue screen in Windows 2012 when mmcfg base set to 3G
384746:5370826: EWL: numerous "EWL warning size mismatch" in serial log (Re-enable warning promotion)
384731:5370110: <ResetDungeon>CATERR observed during Warm Reset testing. - Program the mini-sad before enabling the Prefetch
384726:NO_SIGHTING: Back out changelist 384449 (Not approved)
384687:5371046: Update USB ACPI tables for PC BIOS
384651:5344912: Integrate Intel Apache Pass UEFI driver 01.00.00.1671

BIOS revision: 88D02

384629:5370954: [10nm] phase 1 transition Ia32CpuFamilyPkg to UefiCpuPkg]
384524:5332396: PRD/CCB: BIOS should display Security ACM firmware version

384500:5370773: Check for SNC disable before NUMA interleaving between IMCs within socket.
384449:5370834: Need NVDIMM enabled binary builds as a build target in BKC releases
384433:5370813: Faststrings inconsistently enabled across sockets
384432:5370855: No code is updating CoreCount2

BIOS revision: 88D01

384340:5370883: SRIS Recipe Mismatches on BIOS 83D06
384333:5370812: [BP 1.3.3.0] msr61 bit0 incorrect and inconsistent across sockets
384282:5370835: Merge to latest code with one more #include "CpuCsrAccessDefine.h"
384267:5371095: PCI Express ECRC Errors Not Being Properly Escalated When Enabled
384260:5371169: System hang during MRC training (Back out revision 9 from //CP_Server_BIOS/Skylake_Trunk/CpRcPkg/Library/BaseMemoryCoreLib/Platform/Purley/Include/MemDefaults.h)
384188:5371075: PCD: Multisocket configuration returning DIMM interleave information table change status 0xA
384138:5371074: WMP B0 RC6 Test BIOS
384065:5332093: [SKX-P FPGA] BIOS to provide thermal configuration of FPGA

BIOS revision: 87D11

383931:5371133: KTIRC:GetCpuType incorrectly identifies -P as -F
383928:5370207: BIOS to update for SKX CAPID changes - RAS
383868:5371019: SetGpioPadMode Parameter passed correction
383866:5370536: It takes too much to run <of MpService->StartupAllAPs ( ) service > on Purley tree
383856:5370993: RAS: RMCA Content Hangs with No Error Info

BIOS revision: 87D10

383816:5371137: BIOS to update for SKX CAPID changes - MRC
383814:5370841: EMCA logs are not generated by BIOS when memory corrected error is injected in EMCA GEN 1 mode
383807:5371114: Multithread MRC EN Fails after 85 D15
383805:5371009: KTI RC: BIOS should not use host setup structure as local variable and modify it in SelectSupportedKtiLinkSpeed
383803:5370583: Viral not containing writes to PMEM when not in link fail]
383794:5371139: *BL Egress Credit Mismatch / TOR TO
383792:5371029: Training failure with NVMCTLR dimm buffers running at 1866 -part2
383790:5370779: NVMCTLR DQ Sqizzle should not be changing with Write CRC Enabled
383786:5370704: PWR prescrub on hitting uncorrectable doesnt poison the line which could eventually lead to data corruption
383656:5371129: LD64 LRDIMM failing when in Ch2/Ch5
383654:5370987: CPU1 frequency cannot down in the min frequency when idle or add loading in the Max frequency when stress it
383647:5370318: MRC: Min messages fixes including training register dump and module information
383644:5371134: Request to disable DWR by default for LBG B0
383633:5371130: Support for LBG B1 - add revision ID for stepping B1

BIOS revision: 87D09

383343:5371049: MESEG not required to be set as UC memory region using MTRRs
383297:5370895: [Security VT][SDL S3] ChipSec failures - Cpu
383277:5333006: Modify Default for PoisonEn to be enabled
383236:5370916: Inconsistent WARN_PMIRROR_DISABLE_MINOR_RAS_DISABLED definition is defined in MRC and document “RAS Technology Integration and Validation Guide”
383235:5370901: S3 resume issue with multi threaded MRC
383208:

    5371029: Training failure with NVMCTLR dimm buffers running at 1866
    5370635: DDR-T: MRC hangs during CMD normalization in Late CMD/CLK with RDIMM/DDR-T

383195:5370474: Please use different minor error code for each instance of fatal errors with major code 0xF2

BIOS revision: 87D08 – BKC WW23

383169:5370732: Seeing advanced read training failures on RDIMMs at 2667
383168:5370221: MRC: DDR4 host Coarse Write Leveling improvement for frequencies above 1866 MT/s
383084:5371068: DXE_ASSERT during platform boot after HECI-3 disable
383001:5370321: [10nm]: Move IIO Late Configuration to PEI phase
382890:5370835: [BP 1.3.3.0] Core update broke csr access routines when changing mmcfgbase
382879:5371056: SncEn default value requests 2 cluster when default BIOS will setup 1 cluster
382822:5371110: <ResetDungeon>CATERR observed during Warm Reset testing.
382815:5371090: KTIRC: mmioh rules in IIO are misprogrammed when -P present and fpga active

BIOS revision: 87D07

382633:5370568: DDR4 Cap Logged on 2DPC RDIMM+ Config
382568:5370714: (*channelNvList)[ch].lrdimmpresent opens up unnecessary code for RDIMM, when RDIMM/ dimms are present in one channel
382561:5333031: CSR access function overhead increased by 1600% compared to HSX

BIOS revision: 87D06

382467:5370804: FM_MEM_THERM_EVENT_CPU0_LVT3_N and FM_MEM_THERM_EVENT_CPU1_LVT3_N cannot be asserted when the temp of DIMM overheat used the heat gun to heat up.
382464: Rollback CL382460
382460:5371003: Update UEFI Shell for RP

BIOS revision: 87D05

382406:5370120: Purley source unable to buid using VS 2008 SP1 Compiler Part2
382397:5370120: Purley source unable to buid using VS 2008 SP1 Compiler

BIOS revision: 87D04

382195:5370304: Program DRAM_RULEs and INTERLEAVE_LISTs for FPGA
382187:5370528: NVMCTLR cmd parity error seen on 79D13 BIOS on SKX B0 when system idle

BIOS revision: 87D03

382153:5371083: CLK swap WA needs to be default
382151:5330609: Share SMBus mailbox with use of SYSTEMSEMAPHORE0_UBOX_MISC_REG with other agents after END_OF_POST
382121:5370728: CORE_WB_MISS_LLC from XmlCliDxe during bios boot when using knob dfxHighAddressStartBitPosition
382119:5371084: SKX-FPGA Bios for Opal City PPV Board has RC_EN signal as low

BIOS revision: 87D02

382030:5371061: Hitting fatal error blocking 2 socket boot to SVOS with SKX L0 NVMDIMM
382026:5371089: KTIRC: Missing a param in PrepareDiscEngData cause the data cannot return correctly, it may cause the system hang in some topologies
381975:5371024: Disabling AMT_SUPPORT causes build failure in RC 82.D04

BIOS revision: 87D01

381887:5371060: FPGA:KTIRC: Fpga cannot support L0p or failover bios needs to disable on the fpga link
381884:5371032: System hangs at first mmcfg cycle going to FPGA through KTI
381769:5370421: SelectLfpAsBsp() function is broken, changing BSP on single socket
381707:5371031: Change the FPGA_PARAM structure version and Payload version
381699:5370914: Remove Setup ApicId Tag Mapping (ApicIdTagMapping)
381694:5371036: KTIRC: OutRrqThreshold would not be inited if Init_IRQ_Threshold is not called
381693:5370891: [Security VT][SDL S3] ChipSec failures - Iio

BIOS revision: 86D11

381632:5370380: PCD returns incorrect status on second reboot after applying goal
381611:5371028: BIOS issues warm reset on every boot with video card installed
381556:5370437: BIOS needs to enable SMI & ERR pin signaling on NVMDIMM interrupts by programming MC_RRD_CRNODE_CH0_MC0_CR_NVMDIMM_FNV_INTR_CTL register
381503:5371035: Request to fix BIOS Supplied Mask for PMC Generated G2H s5370771

BIOS revision: 86D10

No change

BIOS revision: 86D09

381150:5371027: Hide PKGC ENTRY CRITERIA BIOS Knobs for all SKX steppings

BIOS revision: 86D08

380989:5370911: Pmax Offset Correction Codes Issues
380974:5370436: Eliminate #define CONFIG_DP

BIOS revision: 86D07

380966:5370273: Uplink port is currenlty hard-coded to port #5, socket #0
380964:NO_SIGHTING: Default PCH is LBG in build
380951:5370937: Add EWL Spec to the CpRcPkg\Documentation directory in Purley Stream
380938:5370774: EWL: initialized after first use
380914:4929882: Scrub the list of routines that are part of CR protocol.
380798:5344884: Integrate Intel Apache Pass UEFI driver 01.00.00.1669
380788:5370932: Eliminate IA32 macro in IIO_OUT_DATA structure
380778:5370983: PCIe: TCRH cal enable causing dual polling pass after warm reset

BIOS revision: 86D06

No change

BIOS revision: 86D05

380690:5333073: Purley PCI-E Multi-segment support is not fully implemented in some drivers [RAS]

BIOS revision: 86D04

380616:5370759: Full/Partial Memory Mirroring Validation Library

380589:5371033: MCP PCIe1 Max Payload not setup correctly
380588:5370772: Opal City STHI FPGA - BIOS creation (Kti part)
380580:5370826: EWL: numerous "EWL warning size mismatch" in serial log

BIOS revision: 86D03

380548:5371005: Enabling HPWM = Native Mode on Windows 10 / WS2016 results in Max freq of 800Mhz under Balanced/Power Saving Mode
380545:5370970: PKGC - Need to set all of the entry criteria masks as default
380543:5370960: Change the default HWP BIOS settings.
380522:5370903: Stepping incorrectly reported as B0 -remove chop
380521:5371023: SKX-FPGA: CL#378504 break NeonCity FPGA BIOS Post
380519:5370899: IioPciePortEWL function logs manyType 8 and Type 9 warnings as fatal
380518:5370941: Change protocol dependency in CrystalRidgeSMM.inf

BIOS revision: 86D02

380356:5370990: Add device IDs for new LBG SKUs
380354:5370956: Disable "PTU Load Override" knob for server PCH where MROM is implemented
380353:5370992: Xover Margin Offsets
380351:5370717: MRC: BDX-EP sPPR operation error
380350:5333083: (Validate Inputs) Implement use of VarCheckHiiLib for Setup variables
380349:5370976: WMP B0 RC3 Test BIOS
380348:5370973: BSSA SetCadbPattern function bug
380347:5370923: Divide by 0 bug in Power TrendLine Calculation
380342:5370969: ASSERT_EFI_ERROR Dxe\Setup\MeSetup.c(195) when entering BIOS menu
380341:
    5370399: PCD - status is changed to error after 3 reboots on one dimm config
    5333043: PCD - Persistent Mem Mapped into SPA is changed after reboot
380340:5370767: Potential memory leak in SaveS3StructToNvram() routine
380339:5371021: One of the FPGA MCP EPs is not discoverable
380338:5371008: Isolate RC_REVISION into it's own header file Rc_Revision.h
380287:EPSD100252527: BKC WFP - High Definition Audio Controller Unknown USB Device.
380249:EPSD100253146: Resolve VGA resource reset problem in MFG mode.

BIOS revision: 86D01

380188:EPSD100032302: Failed to update primary bios under recovery mode when primary BIOS image corruption.
379823:
    5332402: [SKX-P FPGA]: Disable IIO IOMMU engine for MCP stack supporting FPGA
    5331519: [SKX-P FPGA]: Initialize VT-d / IOMMU for SKX-P
379808:5370839: IIO0 LTSSM enters POLLING/L0_EXT.COMP_G1/POL_COMPLIANCE causing PKGC faliures
379765: base://CP_Server_BIOS/Skylake_Trunk add ScratchPadList.xls

BIOS revision: 85D17 – BKC WW22, BKC WW21

379550:5371010: SKX CPUs Fails to enter C-states with Latest Collateral

BIOS revision: 85D16

No change

BIOS revision: 85D15

378861:5332067: Hide MCP0 root port(s) on SKX-P with associated ACPI table changes (1. CL376031 fixed reset broken issue, re-checkin 2. Use UsraLib instead of PciExpressLib)
378786:5332988: Bios for Neon City FPGA Board (PCI-E Multi-segment support in UBA)

BIOS revision: 85D14

378760:5370772: [SKX-P FPGA]: Opal City STHI FPGA - BIOS creation (UBA part)
378759:5370979: Serial Port function check is failed.
378745:5370772: [SKX-P FPGA]: Opal City STHI FPGA - BIOS creation
378744:5370933: EWS -> System -> DIMM Information showing two CPU1_DIMM_A1]

BIOS revision: 85D13

378676:5370731: Bifurcation (IOU2 (IIO PCIe Br1)) sets to x16 don?t work as expected

BIOS revision: 85D12

378550:5370927: adddc_err_inj register is not writable when ERR_INJ_LOCK (MSR 0x790) is cleared
378504:5370958: BIOS RAS Level detection WA for Current LIRA Mappings
378503:5344827: Integrate Intel Apache Pass UEFI driver 01.00.00.1663
378468:5370795: Occasionally System got hang at POST 00 with SKX B0 during reboot cycle tests on Neon City

BIOS revision: 85D11

378464:5370984: Enable FPGA feature by enabling the feature pcd
378463:5370998: [SKX-P FPGA BU] Tip BIOS cannot boot OS
378460:5371000: [SKX-P FPGA] : Incorporate BBS Package in BIOS Image
378457:5370663: LRDIMM Asymmetric Tx margined centered when backside training is enabled

BIOS revision: 85D10

378245:5370573: FPGA:KTI:Connect Fpga hob as input to KtiRc, and KtiRc output back to Fpga hob
378072:
    5370967: RankSpare + eccHarasser failing w/UC TOR TO
    5370903: Stepping incorrectly reported as B0

BIOS revision: 85D09

377952:5370822: SPD CRC Check needs optimization to avoid incurring extra boot time
377950:5370881: Remove/Cleanup all MRC OEM function in CallTableMaster and CallTableSlave
377893:5370771: BIOS Supplied Mask for PMC Generated G2H (Global Reset Demotion) Requires Changes
377878:5370818: Server BIOS requires implementation of RAS flow notification to CSME (Add HECI3 transport)
377868:5370850: Combination of BIOS CRB (83D07) and SVFW not booting on NeonCity nor DVP(CLK as Hybrid).
377772:5370200: Minimize VN0 credits for UPI FPGA Link - 5370201: Maximize VNA credits for UPI FPGA Link

BIOS revision: 85D08

377706:5370886: PCH Root Port Error Handler does not check all root ports for errors

BIOS revision: 85D07

377668:5370808: [Platform PO] Proof of Concept - Proper LER configuration for Purley BIOS
377631:5370639: Inconsistent implementation and/or commenting of EnableDisableGlobalSMIGeneration
377604:5370807: PCH PCI/PCIe RAS Test Content
377602:5370637: Function EnableCorrectedErrRep is calling EnableUboxError and EnableElogKTI - FIX COMMENT
377590:5370944: Address translation errors while injecting nonfatal memory errors with EINJ
377541:5370346: Always stuck at postcode 06 on Barker Peak platform with bios 74D15

BIOS revision: 85D06

377539:5370880: Eliminate usued macro LT_STRUCT in memVar structure in MRC
377537:5370925: tCCD Register Overflow
377536:5370849: Eliminate GROVEPORT_FLAG macro in memSetup in MRC
377535:5332986: Memory mapping code should check ddrt_disable fuse bit
377534:5332863: BIOS MRC should remove workaround for Simics HSD 5167507
377533:5370873: Update Memory POR Tables to reflect 2666 2DPC and RDIMM 3DS
377531:5370865: [BP 1.3.3.0] L1/L2 cache size is incorrect with BIOS.
377530:5370938: Remove unused code from xover calibration algortihm
377529:5370828: BIOS Setup Menu shows zero values in Processor 0 Max Ratio and Min Ratio
377521:5370535: ADDDC-MR failed - system hang after 3rd strike -> reverse bit set unexpectedly thus triggering sparing copy flow causing hang (corrected behavior should have been SDDC+1)
377461:5370718: gSmmMeHeci3ProtocolGuid is not installed during the boot - part 3
377447:5370981: Windows 2012R2/RHEL 7.1 boot broken
377412:5370718: gSmmMeHeci3ProtocolGuid is not installed during the boot - part 2
377373:5370377: CR Spec Update - DSM V1.2 - Updates for all child device DSM return status values

BIOS revision: 85D05

No change

BIOS revision: 85D04

No change

BIOS revision: 85D03

376911:5370749: Wrong setup of SLTCAP register
376908:5370928: not getting b2b gnts during receive enable training
376904:5370831: IIO_PCIE: Fix request for BIOS HSD 4930200 (Disable MSGD length check should be set to match BDX handling of VDM > 16DW)

BIOS revision: 85D02

376867:5370692: D7:F4 could still be discovered if Dfx disable
376843:5370696: Correct PPI flow to meet security requirements; implement onboard video enumeration with PPI request
376838:5370820: BIOS does not program AER registers/IIO error escalation for non-DMI ports
376829:5370930: System gets CAT error on all boards when running stress/S4/warm reset tests on Neon city
376804:5370751: Mirror 4GB option does not set correct size - FIX HELP STR
376784:5370191: Replace instances of direct IO Write to 0xCF9 port for system reset with PchResetPpi->Reset call.
376777:5370718: Install HECI-3 driver regardless of current ME ready state
376751:5370159: Purely: After S3 -> S0 transition, platform gets BSOD.

BIOS revision: 85D01

376627:4930554: Bifurcate MCP PCIe port for -P (FPGA) - Bifurcation only need be done when SKX-P is present and this is per-socket
376597:5370322: Uclk < dclk WA only happening for systems configured for 2LM
376582:5331742: MemMap: Cannot enable SNC with 1GB, 2GB, 3GB TOLM using 3/6way ddr4 chn interleaving
376565:5370921: BIOS/SMM not recognizing x8 SVL config when error is injected on STD SKU
376563:5370936: MMX P5E3-MP4 Config Failing with IDI_C2U_REQ_WCiLF and M2M AK Egress Overflow
376561:5370780: EMCA logs not reported in RHEL when SRAO patrol scrub error is injected in EMCA GEN1 mode using EINJ
376557:5370488: Mirror Failover MC bank registers are not being handled correctly
376553:5370661: Bimodal CMD margins
376544:5370716: BGF Overflow at some U:D Ratios w/ CH2 Populated.
376516: Build Error (Back out changelist 376501)
376507:5332737: Make BTG a buildable option in the external IPClean Collateral release
376501:5370191: Replace instances of direct IO Write to 0xCF9 port for system reset with PchResetPpi->Reset call.
376449:5370823: KTIRC: SlowModeRxDccOverride is incorrectly programming IOVB registers via csr routines and results is CHA registers programmed
376441:5370737: Set boot script outside SMM after SmmReadyToLock!!!
376433:5370238: Incomplete EnableElogFnv error signal implementation for NVMDIMM alert packet interrupt;

BIOS revision: 84D15

No change

BIOS revision: 84D14

376212:5330524: [SKX-P FPGA]: FPGA power off flow when user want to disable or error occur.
376188:5370935: IDER not disabled on Purley AMT
376186:5370848: LBG B0 Differential Disconnect for USB2 ports as POR indicates
376178:5370829: Add option to enable all Root Ports

BIOS revision: 84D13

376031:5370920: FPGA Falsely Detected in Warm Reset flow
376024:EPSD100031533: SUT cannot boot to EFI payload directly after use IPMI command to force payload boot.

BIOS revision: 84D12

375805:5344818: Windows reset broken on SKX B0/LBG A0 -0 (Back out changelist 374118)

BIOS revision: 84D11

375559:5332988: Bios for Neon City FPGA Board - Update GPP_E3 to Native1. it is the pin connected to CPLD that need be set to native.

BIOS revision: 84D10

375189:5370821: Add missing STP cases in switches in PurleyPlatPkg

BIOS revision: 84D09

375072:5331844: KTIRC: Enhance CheckForOemResourceUpdate()
374812:5370906: EXCEPTION rebooting BIOS (Back out changelist 374552)
374791:5370907: FVSECPEI running out of space after CL 374346

374668:5370785: Purley 12GB/24GB dual rank DDR4 RDIMM Support

374664:5370752: MRC: Upload HCC package delay table

374660:5370339: Newer Windows OSes need support added in ACPI tables (Os.asi)

BIOS revision: 84D08

374552:5370321: [10nm]: Move IIO Late Configuration to PEI phase

BIOS revision: 84D07

374533:5332988: Bios for Neon City FPGA Board

BIOS revision: 84D06

374458:5370637: Function EnableCorrectedErrRep is calling EnableUboxError and EnableElogKTI

374397:5370751: Mirror 4GB option does not set correct size

374393:5370846: SX2 hw config hits PEI_ASSERT with 83.D10

BIOS revision: 84D05

374346:5370757: Bios Version 82D03 causing MC errors.

374345:5331210: EWL structures for CPU BIST (Legacy fix)

BIOS revision: 84D04

No change

BIOS revision: 84D03

374290:5370861: S3 does not resume: Offline

374276:5370203: Remove (SystemRAS Type != 1 / 2) dependency on PcieCorErrCntr knob;

374260:5370824: Appears to be an illegal math operation in KtiFinalBusCfgKti()

374248:5370529: Exiting SMM after ADDDC 2nd strike (SDDC spare) using std RAS part causes system to caterr

374231:5370538: Both Windows Server 2012R2 and 2016 Log Event ID #55 when HWPM Out of Band mode is enabled in BIOS

374229:5370537: Purley BIOS (BKC#19) doesn't set IA32_PM_ENABLE[0] when HWPM Native mode with No Legacy Support is Selected in BIOS setup menu

374189:5332760: The serial port issue in Linux OS for Purley.

374154:5333068: Purley PCI-E Multi-segment support is not fully implemented in some drivers [ME]

374118:5332067: Hide MCP0 root port(s) on SKX-P with associated ACPI table changes

BIOS revision: 84D02

373907:5370684: [ADDDC x Partial Mirroring] System sees CECC's when doing device sparing

373891:5370614: VPP_SMBUS controller sends incorrect AttnLed encoding for slots 8-11 - due to legacy typo

373858:5370429: System gets caterr due to CTO fatal error (along with UR) when LER is enabled in BIOS

373780:5370832: Fix index-off-by-1 bug in PciHostBridge algorithm

BIOS revision: 84D01

373695:5370854: [Simics] RC_Assert raised related with Smbus.c (Back out changelist 373169)

373687:5370198: MRC: NVMCTLR SenseAmp/ODT Delay/Duration calculations need to account for illegal settings

373685:5370762: KTILib.c has likely incorrect check when checking CAPID5.spare

BIOS revision: 83D13

373670:5370677: Boot hang with DDR4 and NVMDIMM in same channel
373529:5333071: Purley PCI-E Multi-segment support is not fully implemented in some drivers [Uba]
373498:5332988: Bios for Neon City FPGA Board (UBA code part)
373469:5332187 [SKX-P FPGA]: Enabled FPGA setup menu

BIOS revision: 83D12

373434:5330610: Eliminate RAS Dependency on legacy Framework interfaces by aligning to Native EDKII interfaces
373370: Back out changelist 373236. 5370187: Skylake memory mapping. Use of arrays to get channel interleave bit maps per IMC in socket SAD table.

BIOS revision: 83D11

373263:5370676: [Emu] MRC: When enabling CAP, BIOS sends read/write NVMDIMM command in 3N command timing
373253:5370379: MRC: NVMDIMM Use NVMCTLR CA Vref instead of overriding CA Vref (FW 2871)
373236:5370187: Skylake memory mapping. Use of arrays to get channel interleave bit maps per IMC in socket SAD table.
373220:5370534: BIOS should disable imcx_cx_chn_temp_cfg.thrt_allow_isoch in B0 to allow DRAM RAPL throttling
373216:5370740: MRC: BSSA backside CMD margining dependency on BIOS RMT setup knobs
373169:5332863: BIOS MRC should remove workaround for Simics HSD 5167507
373148:5332804: MRC: Enable multi-threaded MRC

BIOS revision: 83D10

373028:5370655: ME SPS not response while booting in ipclean build
373027:5370793: Need BIOS to enable SX_ENT_TO_EN
373018:5331746: [SKX-P FPGA]: Add Blue Bitstream Loader PEIM
373006:5333072: Purley PCI-E Multi-segment support is not fully implemented in some drivers [CR]
372938:5332094: [SKX-P FPGA] Add Platform PEIM to pass the platform decision of bbs GuidIndex to loader

BIOS revision: 83D09

No change

BIOS revision: 83D08

372739:5370796: Coding error found on PciHostBridge driver of PurleyPlatPkg
372725:5370781: KTI COR PHY RESETS constantly occurring in OS
372723:5370750: Prefetch enabled on socket 0 and disabled on socket 1
372715:5370727: Modify Default for EmcaCsmiEn to be Enable.
372595:5331063: Support "chain" topology for SKX-P et al

BIOS revision: 83D07

372536:5370317: (Remove banned function) Enable build flag DISABLE_NEW_DEPRECATED_INTERFACES (Part 2 - Enable build flag and correct last-second platform code)
372445:5370799: CRB BIOS+SV ME Firmware NOT BOOTING on Opal City SKX B0+LBG B0 SKU-T and 4
372397:5333068: Purley PCI-E Multi-segment support is not fully implemented in some drivers [PCH]
372341:5370819: 8SKT not booting on SIMICS (Back out changelist 371357)
372194:5370157: Isolate NUMA interleave code for volatile and non- volatile memory.
372164:5370682: LNKCAP2 programmed incorrectly to 0x1C instead of 0xE

BIOS revision: 83D06

372156:5370764: RC:FPGA:Create csr access routine for fpga upi csr block
372139:5344799: Integrate Intel Apache Pass UEFI driver 01.00.00.1660

BIOS revision: 83D05

372100:5370811: FortPark devices not being detected (Back out changelist 370828)
371990:5370548: Fix intrinsic functions are used in the code
371919:5370297: IFWI generation for SKX-P(FPGA)

BIOS revision: 83D04

371841:5330524: [SKX-P FPGA] Update the CL#362520 define per-socket knob(s) to disable FPGA for SKX-P
371840:5370768: BP 1330.420: Wrong config space (same for different devices)

BIOS revision: 83D03

No change

BIOS revision: 83D02

371573:5370667: IIO/PCIe Relax Ordering override incorrectly programmed by BIOS
371519:5370426: Remove the MIERRST and related misc error status from BIOS code
371411:5370531: ProcMemErrReporting.c using SKX A0 only registers
371357:5332382: [Part 4] 6000138750: PurleyPlatPkg and PurleySktPkg should not depend on PurleyRpPkg KTI code fix

BIOS revision: 83D01

371296:5370753: 82D02 breaks PTT implementation. (CL_368471 - 5332931;[Client Sync] Sync driver and add client...)
371271:EPSD100252177: External video card is losing video before BIOS Splash.
371012:5370734: Logic for PowerCycleReset based on Mirror and Lockstep setting always evaluates to 0
371010:NO_SIGHTING: merge BP packages down from EDKII_BP_MAIN to update resolved status (this only updates perforce bookkeeping, there is no effective change)
370965:5370640: Take 10nm WriteCHACSRs() changes into Skylake for code compatibility.
370916:5370258: IoMcaEn knob Default was Reverted back to Disable
370907:5370641: Remove use of redundant define "THREE_WAY_BITMAP". Replace use of MAX_SAD_RULES with a new variable.
370870:5370619: Page fault in routine ClearDMIErrors (in the module SbErrorHandler) during post.
370837:5331221: EWL structures for IIO root port link error types
370828:5370273: Uplink port is currenlty hard-coded to port #5, socket #0
370825:5370455: Remove Unvalidated Interleave Settings from BIOS Setup and PCAT Tables
370815:5333057: BIOS needs to add NTB registers new names to the BIOS setup help menu.
370799:5370720: Need BIOS to unlock Thermal registers

BIOS revision: 82D08

370794:5370761: PCIE: PHY recipe v2.75
370787:5333070: Purley PCI-E Multi-segment support is not fully implemented in some drivers [CPU_PPM]
370775:5333069: Purley PCI-E Multi-segment support is not fully implemented in some drivers [Platform]
370718:5332700: Purley] In-correctly initialize R_PCH_PCIE_LCAP[11:10] APMS in PchRootPorts.c
370686:5370626: Support for External Clock Mode MPHY Table
370650:5332424: Support for disabling global reset on 2nd ME and IE watchdog expiration - Hide DWR config menu for LBG A0
370644:5370522: PchLpcIoDecodeRangesSet() and PchLpcIoEnableDecodingSet() for CS#1 support - fix

BIOS revision: 82D07

No change

BIOS revision: 82D06

370476:5333026: Incomplete and inconsistent IIO error processing function implementations
370200:5333026: Incomplete and inconsistent IIO error processing function implementations
370199:5370470: When NTB mode is enabled, max payload size bit is locked
370198:5370478: SVL not setup by BIOS
370191:5370243: MemTest86 Hits SAD_ERR_NON_CORRUPTING_OTHER with Channel Interleaving Set to 3-Way (Auto)
370148:5370389: RRQ/IRQ throttle settings, build error fix
370113:5370688: BIOS need to set GPP_H_8 and GPP_H_6 pins to GPIO mode to train PCIe slot 4 in ECB platform
370112:5370558: VMD MemBar access can be falsely detected as CfgBar hit
370111:5370389: RRQ/IRQ throttle settings
370100:5370513: KTI: RxDCC Override (SLOW mode only)

BIOS revision: 82D05

370095:5370428: Diable Serial Debug Message Level option doesn't work for the first boot after LBG part being replaced (Opal City)
370093:5370705: KTIRC: SNC_EN knob enable should enable the SNC_FULL(2-clusters) only and disable cannot block the SNC_IND programming-Disable Snc when Numa is disabled
370091:5370317: Enable build flag DISABLE_NEW_DEPRECATED_INTERFACES (Part 1 - Fix Platform Code ; Chapter 3 - The Socket Package)
370090:5370317: Enable build flag DISABLE_NEW_DEPRECATED_INTERFACES (Part 1 - Fix Platform Code ; Chapter 2 - The Plat Package)
370089:5370317: Enable build flag DISABLE_NEW_DEPRECATED_INTERFACES (Part 1 - Fix Platform Code ; Chapter 1 - The Rp Package)
370086:5370750: Prefetch enabled on socket 0 and disabled on socket 1
370085:5370195: Remove multiple definitions of PCI_DEVICE_NUMBER_PCH_PCIE_ROOT_PORTS
370084:5370145: Merge VFR_CRB_FLAG and CRB_FLAG into CRB_FLAG

BIOS revision: 82D04 – BKC WW18

369696:5370712: S3 entry CATERRs on LBG B0
369623:5370763: OS reboot not working on SIMICS
369573:5370766: S3 not functional on SKX A1/LBG A0 (Back out changelist 367789)
369200: BP 1330.420 - remove Max_socket.h

BIOS revision: 82D03

368691: BP 1330.420 - Fix build error
368679: BP 1330.420 core update done by Copying //CP_Server_BIOS/Skylake_Devpipe to Skylake_Trunk (//CP_Server_BIOS/Skylake_Trunk)

BIOS revision: 82D02

368471:5332931: [Client Sync] Sync drivers and add Client's AMT & ME Policy
368332:5370166: Fix postbuild been invoked twice on IPClean Code.
368183:5333039: Assert when KNL connected to platform
368146:5332382: [Part 3] PurleyPlatPkg and PurleySktPkg should not depend on PurleyRpPkg Implementing PCI_BMC_Port_Selection_WA and PCI_SATA_Port_Selection_WA

BIOS revision: 82D01

368126:5333012: VNA Credit config programming by incorrect definition
368102:5370700: Change the Dynamic L1 default setting to disable
368096:5332382: [Part 2] PurleyPlatPkg and PurleySktPkg should not depend on PurleyRpPkg Implementing UpdateOemTableIdXhci
368061:5370270: RAS/S3: use of wrong register definitions and structures in memras.c and memrass3save.c can cause S3 entry/resume failure.
368060:5370698: BSSA stitching RMT produced incorrect Cmd margin results
368054:5370466: SDP: Add help strings to explain purpose of 'Auto' option in BIOS knobs related to KTI
368051:5370477: BIOS Workaround for SKX Sighting 5352995 (M2M EMCA2 Incorrectly Defaults to a Thresholded CSMI)
368048:5332382: [Part 1] PurleyPlatPkg and PurleySktPkg should not depend on PurleyRpPkg Implementing BoardTypes.h
368040:5331408: Add new method to write out sockets/ports at each stage for Topology changes (Resubmit of CL 367467)
368021:5332845: DimmIsolationFlow.c Prints To Serial With serialDebugMsgLvl=Disable FIX

Purley SKX change list (post-PV)

Changes from PV MR5 to PLR1

Fixed issues:

Log.ID	Fix in RC	Description
518007	YES	5385766: Hard PPR Failure after Memory CE injection
517977	YES	5385651: MRC: BIOS configures illegal MC mode when ADDDC mode=en and pagepolicy=adaptive page mode
517644	NO	5385977: Finalize code that sets Bit 11 in SPIBAR+0x04
514071	YES	5385635: BIOSSCRATCHPAD7[27] is used for two purposes
513660	NO	5385736: DCU SRAR hangs in bios under windows 2016 with Gen1 mode enabled, no opt-in
513654	NO	5385724: Hot Plug PCIe late Device Present Detection and command complete interrupt
513625	NO	5385534: ADDDC Bank to Rank upgrade doesnt take effect on Region 1
513605	YES	5385365: MAILBOX_BIOS_CMD_WRITE_PCU_MISC_CONFIG (0x6), Bit[28] UFS Disable was to be removed

Sighting desctiption:

5385766: Hard PPR Failure after Memory CE injection

Issue description:

PPR fails after memory CE injection.

Reproduction steps:

1. Boot to OS and inject Memory CE using ITP C-Scripts
2. Reset the system from Windows and observe the PPR failure log

Resolution:

Skip PPR on S3 resume or WarmBootFast

Status:

Fix was provided in Purley PLR1 Reference Code release (142R08)

5385651: MRC: BIOS configures illegal MC mode when ADDDC mode=en and pagepolicy=adaptive page mode

Issue description:

ADDDC workaround is to set "Page Policy" = "Closed" in the presence of ADDDC. BIOS does not check restrict page policy programming when in ADDDC. This allows user to select adaptive page mode.

Resolution:

Force close-page mode in ADDDC

Status:

Fix was provided in Purley PLR1 Reference Code release (142R08)

5385977: Finalize code that sets Bit 11 in SPIBAR+0x04

Note: related sighting 5385619

Issue description:

Platform should set bit 11 in SPIBAR+0x04

Resolution:

Set bit WRSDIS (bit11) before FLOCKDN (bit 15)

Status:

Fix was provided in Purley PLR1 CRB BIOS release (142R08)

5385635: BIOSSCRATCHPAD7[27] is used for two purposes

Issue description:

BIOSSCRATCHPAD7[27] is used for two purposes:

- Debug Interface MSR Enable
- Cold Fast Boot

From a DCI/debug perspective, when Cold Fast Boot is disabled (bit27=0), the Debug Interface MSR is not enabled again after a warm reset.

Reproduction steps:

1. Boot to setup menu
2. Enable DEBUG INTERFACE:
   Socket Configuration -> Processor Configuration -> DEBUG INTERFACE: (default is <Disabled>)
3. Observe that ColdBootFast will be disabled during subsequent boots.
4. This message will appear in the serial log:
   ```
   ColdBootFast disabled, clearing the MRC NVRAM structure for ColdBoot.
   bootMode = NormalBoot
   subBootMode = ColdBoot
   ```

Other than this defect, ColdBootFast works as expected.

Resolution:

Removed references to BIOSSCRATCHPAD7[27] from ColdBootFast flow.

Status:

Fix was provided in Purley PLR1 Reference Code release (142R08)

5385736: DCU SRAR hangs in bios under windows 2016 with Gen1 mode enabled, no opt-in

Issue description:

Running under Win2016 with Gen 1 enabled (CSMI and MSMI morphing to Gen1), the system hung in BIOS after the following:

SMM space when halted

```
[SKX_C0_T0]  Halt Command break at 0x38:0000000077AD03A2 in task 0x0040
[Break Summary] 95 other thread(s) took a sympathetic break.
```

Allocate page with OS application.
Inject UC Patrol Scrub error on that page. (SRAO)
then consume that same address with DCU read.

This happens with a single DRx4 memory dimm installed on Ch2 of both sockets.
This works with memory in ch0!!!

Resolution:

The issue here is when handling SRAR on the demand Read by DCU on already poisioned data location, BIOS is trying to look for the non-existing poisoned record, and on failure falling through another function which has a bug in getting the McId, which doesn't work for non-zero ChId.

So to support this test case, added the code to create the poison record during SRAO handling. (Currently, the poison record would be created for UCNA only). So that the poison record would be avaialbe in the SRAR caused by DCU demand read. Also fixed the bug in CheckM2MUCNA() in getting the McId.

The rootcause for this issue uncovered a gap in the code for handling this test case, and it is independent of memory configs.

Status:

Fix was provided in Purley PLR1 CRB BIOS release (142R08)

5385724: Hot Plug PCIe late Device Present Detection and command complete interrupt

Issue description:

Few PCIe cards experienced a receiver detect on some lanes even when powered off. Here is the sequence of events leading to the anomalous hot add:

1. Card is in L0.
2. OS removes device, puts card in power off mode.
    a. Link goes down. PDC and DLLSC get set. Interrupt is generated and handled. (everything ok so far).
3. Card provides receiver detect on some lanes.
    a. Link goes to Pol.Compl.
    b. PDC is set due to s5353435 (known issue).
    c. Interrupt handler of unrelated interrupt sees PDC=1, PDS=1 and OS decides to do hot add.

Resolution:

Disabling PDS polling (IioPortInit.c) for cards with hot-plug capable and power controller present.

Status:

Fix was provided in Purley PLR1 CRB BIOS release (142R08)

5385534: ADDDC Bank to Rank upgrade doesnt take effect on Region 1

Issue description:

With second bank failure in the device, BIOS keeps region 0 in Bank VLS, and brings the rest of the banks to +1 state. The design intend is to reverse the Bank VLS, then establish Rank VLS.

The BIOS flow works as expected when making use of region 0, but with region 1, Bank VLS doesn't get upgraded. This misbehavior results in false call to repair DIMM.

The corrected algorithm will keep the DIMM in service, prevents un-necessary service call.

Resolution:

Extended number of strikes to 4 to allow more ADDDC operations (upto 4 strikes).

Status:

Fix was provided in Purley PLR1 CRB BIOS release (142R08)

5385365: MAILBOX_BIOS_CMD_WRITE_PCU_MISC_CONFIG (0x6), Bit[28] UFS Disable was to be removed

Issue description:

Turbo encountered a mismatched uncore ratio limit issue when using the PCU mailbox command.

Resolution:

Fixed UFS Disable logic when set to TRUE by matching MIN CLM Ratio to MAX CLM Ratio.
Removed an incorrect tie in for UFSDisable setup question to disabling SAPM control.
Removed the B2P usage of MAILBOX_BIOS_CMD_WRITE_PCU_MISC_CONFIG (0x6), Bit[28].

Status:

Fix was provided in Purley PLR1 Reference Code release (142R08)

Changes from PV MR4 to MR5

Fixed issues:

Log.ID	Fix in RC	Description
510495	YES	5385886: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed
510309	NO	5385887: A core 3-strike event may be seen under certain test conditions (Disable XPT in MR5)
509695	YES	5385863: Windows 2016 CATERRs when trying to boot in non-NUMA mode with 128GB DIMMs
507254	NO	5346277: [2S-SKX] Ctrl+P menu is not displayed at splash screen with ME11 BIOS

Sighting desctiption:

5385886: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

Issue description:

Correctable and Uncorrectable errors are observed across RDIMM/NVDIMM when mixing in the same channel.
System configuration:

12 RDIMMs and 12 NVDIMMs in total, with RDIMMs on slot 0 and NVDIMMs on slot 1 of each mem channel.
16GB 2Rx8 16GB 1Rx4 2667 Fail
16GB 2Rx8 16GB 1Rx4 2400 Fail
16GB 2Rx8 16GB 1Rx4 2400 Fail
32GB 2Rx4 16GB 1Rx4 (vendors were not mixed) 2667 Pass

The issue was seen when either PTU was run or heavy read/writes were being done into the NVDIMM logical volumes at the OS. The failures were reported on RDIMMs and not the NVDIMMs and started with correctable errors, followed by uncorrecble errors. There was a consistency in the failures when x8 RDIMM were mixed with the x4 NVDIMMs.
No errors were seen when x4 RDIMMs were mixed with x4 NVDIMMs.

Resolution:

Implemented t_rrdd and t_rrdr with a floor of 2, for all configurations, to provide sufficient margin on these turnaround times.

Status:

Fix was provided in Purley MR5 Reference Code release (140R10)

5385887: A core 3-strike event may be seen under certain test conditions (Disable XPT in MR5)

Issue description:

When running some stress tests and/or related applications, a core 3-strike event may be seen. This similar 3-strike event may also occur when system is at idle.

Resolution:

Under investigation. Disabling XPT Pre-fetch is recommended as a temporary workaround. BIOS release MR5 is configured with XPT Pre-fetch disabled by default.

GenerationCsiSetup.hfr:

```
oneof varid = PC_GENERATION_VARIABLE.XptPrefetchEn,
        prompt  = STRING_TOKEN(STR_XPT_PREFETCH),
        help    = STRING_TOKEN(STR_XPT_PREFETCH_HELP),
        option text = STRING_TOKEN(STR_DISABLE), value = KTI_DISABLE, flags = RESET_REQUIRED |
        MANUFACTURING | DEFAULT;
        option text = STRING_TOKEN(STR_ENABLE), value = KTI_ENABLE,  flags = RESET_REQUIRED;
endoneof;
```

KtiSetup.hfr:

```
oneof varid = SOCKET_MP_LINK_CONFIGURATION.XptPrefetchEn,
        prompt  = STRING_TOKEN(STR_XPT_PREFETCH),
        help    = STRING_TOKEN(STR_XPT_PREFETCH_HELP),
        option text = STRING_TOKEN(STR_DISABLE), value = KTI_DISABLE, flags = RESET_REQUIRED |
        MANUFACTURING | DEFAULT;
        option text = STRING_TOKEN(STR_ENABLE), value = KTI_ENABLE,  flags = RESET_REQUIRED;
endoneof;
```

UPI Prefetch remains ‘enabled’:

```
oneof varid = SOCKET_MP_LINK_CONFIGURATION.KtiPrefetchEn,
            prompt  = STRING_TOKEN(STR_KTI_PREFETCH),
            help    = STRING_TOKEN(STR_KTI_PREFETCH_HELP),
            option text = STRING_TOKEN(STR_DISABLE),            value = KTI_DISABLE, flags = RESET_REQUIRED;
            option text = STRING_TOKEN(STR_ENABLE),             value = KTI_ENABLE,  flags = RESET_REQUIRED |
            MANUFACTURING | DEFAULT;
    endoneof;
```

Status:

Temoporary fix was provided in Purley MR5 CRB BIOS release (140R10)

5385863: Windows 2016 CATERRs when trying to boot in non-NUMA mode with 128GB DIMMs

Issue description:

8S system with fully populated processors fails to boot to Windows 2016 with 128GB LRDIMMs in non-NUMA mode. If processor count is reduced 6S or 4S or NUMA mode is enabled, the system successfully boots.
ITP dumps showed that all CPUs fired CATERRs and there was a 3strike TOR timeout.

Resolution:

Changed 16-bit TotalInterleaveSize to a 32-bit variable so that overflow will not occur in this (and other) configurations.

Status:

Fix was provided in Purley MR5 Reference Code release (140R10)

5346277: [2S-SKX] Ctrl+P menu is not displayed at splash screen with ME11 BIOS

Note: this issue is specific to Intel CRBBIOS only.

Issue description:

During POST, CTRL+P key is not present in splash screen

Expected Behavior:

Splash screen should show the option to boot ME with CTRL+P key

Resolution:

Fixed in Intel CBR BIOS build. Custom BIOS is not impacted.

Status:

Fix was provided in Purley MR5 CRB BIOS release (140R10)

Changes from PV MR3 to MR4

Fixed issues:

Log.ID	Fix in RC	Description
505845	YES	5385840: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed
505416	NO	5385825: [2S] FW Eval lost PCIe Error Injection capabilities
505067	YES	5385787: [NVDIMM] JedecNvDimm Security issue
504786	NO	5385697: AcpiIoApic incorrect for 8S
504192	NO	5385491: BuildImage.sh files Restricted Tags in PurleyRpPkg and BakervillePkg do not match
503682	NO	5385796: Request to integrate WMP B0_RC47 and S0_RC8 recipes into the IFWI official release
503024	NO	5385789: [FPGA] Caterr and POST code displaying 72 when boot from S5 with FPGA disabled

Sighting desctiption:

5385840: Memory configs with NVDIMMs installed are showing SBE and MBE when stressed

Issue description:

Request BIOS to implement a change for t_rrdd where, for all configurations, t_rrdd has a floor of 2.

Resolution:

Floor trrdd to 2.

Status:

Fix was provided in Purley MR4 Reference Code release (139R08)

5385825: [2S] FW Eval lost PCIe Error Injection capabilities

Issue description:

Error injection capabilities were lost after 137_R08.

Resolution:

Adding a setup option to condition Error Injection Disable bit.

Status:

Fix was provided in Purley MR4 CRB BIOS release (139R08)

5385787: [NVDIMM] JedecNvDimm security issue

Issue description:

Uninitialized variable in JedecNvDimm driver (/PurleySktPkg/Dxe/JedecNvDimm/JedecNvDimm.c):
In the routine ServeNgnCommandsFromOS() the variable Data is not initialized before it is used. The address(&) of Data passed to WriteSmb() without Data content initialized.
This is a potential security issue.

Resolution:

Initialize variable to 0 before use it

Status:

Fix was provided in Purley MR4 Reference Code release (139R08)

5385697: AcpiIoApic incorrect for 8S

Issue description:

As mPlatformInfo->SysData.SysIoApicEnable is only UINT32, Intel RC assumes 32 IoApics max and adjusts the meaning of bits based on MAX_SOCKET.

```
#if MAX_SOCKET >4
        #define PCH_IOAPIC0
#else
        #define PCH_IOAPIC (1<<0)
#endif
```

However, it's not accounting for while determining CurrSkt and CurrStack.
Need to add #ifMAX_SOCKET >4 case below:

\PurleyRpPkg\Library\AcpiPlatformTableLib\AcpiPlatformLibApic.c

```
#if MAX_SOCKET >4
        CurrSkt = (ApicPtr->AcpiIoApic.IoApicId - PC00_IOAPIC_ID) /4;
        CurrStack = (ApicPtr->AcpiIoApic.IoApicId - PC00_IOAPIC_ID) %4;
#else
        CurrSkt = (ApicPtr->AcpiIoApic.IoApicId - PC00_IOAPIC_ID) / MAX_IIO_STACK;
        CurrStack = (ApicPtr->AcpiIoApic.IoApicId - PC00_IOAPIC_ID) % MAX_IIO_STACK;
#endif
```

Resolution:

8S SKUs have max 4 IIO stacks per socket.

Status:

Fix was provided in Purley MR4 CRB BIOS release (139R08)

5385491: BuildImage.sh files Restricted Tags in PurleyRpPkg and BakervillePkg do not match

Issue description:

Code clean up (no failure or functional changes)

Resolution:

N/A

Status:

N/A

5385796: Request to integrate WMP B0_RC47 and S0_RC8 recipes into the IFWI official release

Issue description:

Request to integrate WMP RC47 recipe as the POR recipe across all Purley platforms.
Intermittent occurrences of failures due to CorErr, UncorErr and RcvrErr are coming from the PCIe Gen3 x16 and x8 Uplink on the LBG NS die when running the Concurrency Tests.

Resolution:

Integrate new HSIO tables: Bx RC47 and Sx RC8.

Status:

Fix was provided in Purley MR4 CRB BIOS release (139R08)

5385789: [FPGA] Caterr and POST code displaying 72 when boot from S5 with FPGA disabled

Issue description:

System will CATERR and post code display "72" when boot up system from S5 with FPGA disabled in BIOS.
Expected Behavior:

System should boot from S5 with FPGA disabled in BIOS setup.

Reproduction Steps:

1. Enter BIOS setup
2. Disable FPGA in BIOS setup:
   EDKII Menu -> FPGA Configuration -> Sockets Enable Bitmap(Hex)" to "0" ("0" means disable FPGA in all sockets)
3. Save the configuration and reboot to OS
4. Shutdown the system in OS
5. Press the power button to boot up system

Resolution:

Set RC_EN signal reset type to normal, it reset when enter to S5.

Status:

Fix was provided in Purley MR4 CRB BIOS release (139R08)

Changes from PV MR2 to MR3

Fixed issues:

Log.ID	Fix in RC	Description
501674	NO	5385744: ERRINJCON.ERRINJDIS should be set by BIOS in every boot to disable error injection
501573	YES	5385685: Hitting 768G limitation with Mirror mode enabled + MMCFG base set to 1 + 768G DDR4 installed
501434	NO	5385764: Set_Strap_Lock is not set after resume from S3
499551	NO	5385285: [NVDIMM] NVDIMM marked as "?" in windows 2016 Device Manager
498574	NO	5385708: [FPGA] RSA cannot add SMBIOS type198 as FPGA FV HOB init is skipped on subsequent boot

497796	YES	5385686: [NVDIMM] System hangs with exception 0x0 at PC 0xD4, when ADR Batterybacked mode is enabled
497327	NO	5385644: IOU2 PCIe bifurcation incorrect on Kyanite boards
497273	NO	5385667: [FPGA] Request to add a setup option to control HSSI EQ tuning as DFX hooks
497119	YES	5385666: s5372912 Needs to be extended for H0 and CLX

Sighting desciption:

5385744: ERRINJCON.ERRINJDIS should be set by BIOS in every boot to disable error injection

Issue description:

ERRINJCON.ERRINJDIS should be set by BIOS on every boot to disable error injection. Current BIOS only set these in B0.D0.F0 and B(3).D0-3.F0 but did not set for PCIe root ports.

```
>>? sv.socket0.uncore0.showsearch("ERRINJDIS","f")
pxp_b0d00f0_errinjcon.errinjdis = 0x1
pxp_b1d00f0_errinjcon.errinjdis = 0x0
pxp_b1d01f0_errinjcon.errinjdis = 0x0
pxp_b1d02f0_errinjcon.errinjdis = 0x0
pxp_b1d03f0_errinjcon.errinjdis = 0x0
pxp_b2d00f0_errinjcon.errinjdis = 0x0
pxp_b2d01f0_errinjcon.errinjdis = 0x0
pxp_b2d02f0_errinjcon.errinjdis = 0x0
pxp_b2d03f0_errinjcon.errinjdis = 0x0
pxp_b3d00f0_errinjcon.errinjdis = 0x0
pxp_b3d01f0_errinjcon.errinjdis = 0x0
pxp_b3d02f0_errinjcon.errinjdis = 0x0
pxp_b3d03f0_errinjcon.errinjdis = 0x0
```

Resolution:

Set Error Injection Disable bit on Error Injection control Registers for all root ports.

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385685: Hitting 768G limitation with Mirror mode enabled + MMCFG base set to 1 + 768G DDR4 installed

Issue description:

Reproduction steps:

1. QS CPUs x 2. MRC: 128R08 and later
2. Install DIMM 64GB*12=768GB on socket0.
3. Boot to setup and modify the settings as:

   Memory RAS Configuration -> Enable Partial Mirror = Partial Mirror mode 1LM
   Common RefCode Configuration -> MMCFG Base = 1G

   Or:

   Memory RAS Configuration -> Mirror mode 1LM
   Common RefCode Configuration -> MMCFG Base = 1G
4. Save and exist.

System halts on next MEMORY MAPPING:

```
FatalError: BSP - SocketId = 0 registered Major Code = 0xFA, Minor Code = 0x1
ERROR: AP detected error on SocketId = 0 registered Major Code = 0xFA,Minor Code = 1
ERROR: BSP has an error Reported to SocketId = 1 registered Major Code = 0xFA, Minor Code = 1
```

Resolution:

Updated DoChannelInterleave(), DoThreeWayInterleave(), DoTwoWayInterleave(), and DoOneWayInterleave() to report the correct size when calling IsSkuLimitViolation() for the memory allocated below 4GB.

Status:

Fix was provided in Purley MR3 Reference Code release (137R08)

5385764: Set_Strap_Lock is not set after resume from S3

Issue description:

Per Lewisburg BIOS specification, BIOS needs to set "Set_Strap_Lock", SPI_BAR0 + F0h [0] to 1b.
This bit has been set in normal boot mode but missed in S3 resume path.

Resolution:

Added SPI_SSML register to boot script.

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385285: [NVDIMM] NVDIMM marked as "?" in windows 2016 Device Manager.

Issue description:

Populate a system with NVDIMM and few RDIMMs. Boot to Windows 2016, the Device manager shows NVDIMM device marked with "?".

Resolution:

Fixed with modified ACPI code.

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385708: [FPGA] RSA cannot add SMBIOS type198 as FPGA FV HOB init is skipped on subsequent boot

Issue description:

BIOS skips building FPGA FV HOB if FPGA BBS has previously been loaded (or disabled). During POST, just before OS hand-off, RSA driver is dispatched to add SMBIOS type 198 info (FPGA) which failed as it cannot get the FPGA FV. Reproduced with BIOS 133R02.

Resolution:

Fixed.

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385686: [NVDIMM] System hangs with exception 0x0 at PC 0xD4, when ADR Batterybacked mode is enabled

Issue description:

System hangs at PC 0xD4, when ADR Batterybacked mode is enabled.
Reproduction steps:

1. Boot to Setup and enable ADR "Baterybacked" mode and "check_pm_sts"
2. Reboot
3. System will hang at PC 0xD4 with exception 0x0

Symptom:

```
SAD[1] ChInterBitmap = 4
SAD[1] imcInterBitmap = 1
!!!! X64 Exception Type - 00(#DE - Divide Error) CPU Apic ID - 00000000 !!!!
RIP - 00000000630AAE61, CS - 0000000000000038, RFLAGS - 0000000000010246
RAX - 0000000180000000, RCX - 0000000100000000, RDX - 0000000000000000
```

```
RBX - 000000006F24E2C0, RSP - 000000006F24D840, RBP - 000000004F98F8AC
RSI - 000000004F9A6480, RDI - 00000000FFC117A3
R8 - 0000000000000020, R9 - 0000000000000000, R10 - 00000000000000C0
R11 - 0000000000000000, R12 - 0000000000000000, R13 - 0000000000000000
R14 - 0000000000000000, R15 - 0000000000000000
DS - 0000000000000030, ES - 0000000000000030, FS - 0000000000000030
GS - 0000000000000030, SS - 0000000000000030
CR0 - 0000000080000013, CR2 - 0000000000000000, CR3 - 000000006F0CD000
CR4 - 0000000000000668, CR8 - 0000000000000000
DR0 - 0000000000000000, DR1 - 0000000000000000, DR2 - 0000000000000000
DR3 - 0000000000000000, DR6 - 00000000FFFF0FF0, DR7 - 0000000000000400
GDTR - 000000006AAB1580 0000000000000047, LDTR - 0000000000000000
IDTR - 0000000069505018 0000000000000FFF, TR - 0000000000000000
FXSAVE_STATE - 000000006F24D4A0
!!!! Find PE image f:\src\ami\neoncity\lb73b_ss_adrwa0_dbg\Build\NeonCity\DEBUG_MYTOOLS\X64\PurleySktPkg\Dxe\JedecNvDimm\JedecNvDimm\DEBUG\JedecNvDimm.pdb (ImageBase=00000000630A9000, EntryPoint=00000000630A92E0) !!!!
```

Hardware config:

Neon City PBA 300 board
2x QMXL M0-QS 14 Core CPU
2x 8GB DDR4 memory
RC 130.R06 BIOS /r10373 BMC/5D22 CPLD

Resolution:

Fixed an issue wherein if the ADRDataSaveMode is set to Battery backed mode, zero size of the NVDIMM regions was not comprehended, which resulted in assert.

Status:

Fix was provided in Purley MR3 Reference Code release (137R08)

5385644: IOU2 pcie bifurcation incorrect on Kyanite boards

Issue description:

Note: only applies to Kyanite board. No impact to Neon City and Lightning City.

On Kyanite boards, the IOU2 PCIe bifurcation is not properly set by BIOS. The default should be x8x8. It is being set to x16 and does not match the board layout. The issue was found when Florine cards were not training properly when placed in slot 7.

This issue was able to WA by changing the bifurcation manually. EDKII Menu -> Socket Configuration -> IIO Configuration -> Socket1 Configuration -> IOU2 (IIO PCIe Br3) <x8x8>

Resolution:

The Board definition table for Kyanite Board has been updated according with the Purley Kyanite Architecture Block Diagram.

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385667: [FPGA] Request to add a setup option to control HSSI EQ tuning as DFX hooks

Issue description:

The newly added support for HSSI EQ tuning is being enabled everytime system cold boot before OS boot.
There might be a need to disable it so that EQ tuning can be done manually for comparison.
Propose to add a set up option to disable/enable EQ tuning as DFX hooks. Enabled should be the default value.

Resolution:

A setup option was added to control HSSI EQ tuning as DFX hooks

Status:

Fix was provided in Purley MR3 CRB BIOS release (137R08)

5385666: s5372912 Needs to be extended for H0 and CLX

Issue description:

It was discovered that the fix for sref_idle_timer in s5372912 wasn't included for H0 steppings. This needs to be included in H0 and CLX. From the original HSD:
BIOS needs to use the formula trfc + tzqcs + 100 to set sref_idle_timer. Additionally, BIOS should remove the setup option to allow customers to change this to something that doesn't match this formula.

Resolution:

Integrated

Status:

Fix was provided in Purley MR3 Reference Code release (137R08)

Changes from PV MR1 to MR2

Fixed issues:

Log.ID	Fix in RC	Description
496519 496517	NO	5385619: Set Bit 11 in SPIBAR+0x04
495797	YES	5385623: Add checks in RC to automatically disable SNC when proc with less than 12 slices
495078	YES	5385583: MRC: Incorrect programming of TxEq setting post TxEQ training
494492	NO	5385633: [FPGA] add HSSI 4x10 EQ table to BIOS
494485	NO	5385564: [FPGA] Request to add BBS version in Setup menu and bios serial log

Sighting desctiption:

5385619: Set Bit 11 in SPIBAR+0x04

Issue description:

Platform should set bit 11 in SPIBAR+0x04.

Resolution:

Integrated

Status:

Fix was provided in Purley MR2 CRB BIOS release (135R03)

5385623: Add checks in RC to automatically disable SNC when proc with less than 12 slices

Issue description:

A NEM eviction/CATERR occurred in POST doing reboot testing if SNC is enabled on low core count/small LLC processors such as QM80/QMRQ (4 core/16MB LLC).
Reference Code does not automatically disable SNC if installed processor(s) in the system doesn't meet the minimum (12 slice) criteria.

Resolution:

Fixed in Reference Code

Status:

Fix was provided in Purley MR2 Reference Code release (135R03)

5385583: MRC: Incorrect programming of TxEq setting post TxEQ training

Issue description:

Note: only affects LRDIMMs

TxEq training is happening correctly, but BIOS does not update the trained setting correctly which might cause the TxV margins to go down. If the margin loss is high, it can lead to unexpected memory errors. No report of any such errors due to this as of now.

Resolution:

Fixed in Reference Code

Status:

Fix was provided in Purley MR2 Reference Code release (135R03)

5385633: [FPGA] add HSSI 4x10 EQ table to BIOS

Issue description:

Set HSSI retimer card jumper to 4x10 mode. BIOS does not set Go To mode, or apply HSSI EQ. Request to apply "e40mode1" EQ if RC_CARD_ID is 6.

Resolution:

Fixed in CRB BIOS

Status:

Fix was provided in Purley MR2 CRB BIOS release (135R03)

5385564: [FPGA] Request to add BBS version in Setup menu and bios serial log

Issue description:

Request BIOS to retrieve the version info and display it in FPGA bios setup menu and bios serial log. This is for debug purpose only.

Resolution:

Fixed in CRB BIOS

Status:

Fix was provided in Purley MR2 CRB BIOS release (135R03)

Changes from PV to PV MR1

Fixed issues:

Log.ID	Fix in RC	Description
493238	NO	5385488: TXT is currently limited to 255 threads, not functional in 8S
492981	YES	5385643: MRC: BIOS does not cache capIDs correctly for single-threaded mode. Can lead to training failures with control and command signals.
492193	YES	5385509: t_stagger_ref change 1/2 tRFC -> 1/3 tRFC
492174	YES	5385178: CNFG_500_NANOSEC in PCU (D30,F5,RD8[9:0]) is incorrectly programmed based on DDR Freq

Sighting desctiption:

5385488: TXT is currently limited to 255 threads, not functional in 8S

Issue description:

InitializeLtDxeLib in PurleyPlatPkg/Override/ServerCommonPkg/Universal/GetSec/Dxe/TxtDxeLib.c is not compatible with more than 256 threads in a system. This blocks TXT from functioning in an >4S system with Skylake Server CPUs.

LockConfig is unable to execute for sockets greater than 4S (socket 4-7) because 'ApCount' in 'LT_DXE_LIB_CONTEXT' structure is defined as UINT8. It needs to be defined as UINT16 because 8S system has more then 256 threads. InitializeLtDxeLib() procedure should be modified to use 16-bit APCount instead of casting the (CpuCount - 1) to (UNIT8).

PurleyPlatPkg/Override/ServerCommonPkg/Universal/GetSec/Dxe/TxtDxeLib.c:

```
        LtDxeCtx->ApCount = (UINT8)(CpuCount - 1);
needs to change to:
        LtDxeCtx->ApCount = (UINT16)(CpuCount - 1);

PurleyPlatPkg/Override/ServerCommonPkg/Universal/GetSec/Dxe/TxtDxeLib.h:
        UINT8                     ApCount;
needs to change to:
        UINT16                    ApCount;
```

Resolution:

Fixed in CRB BIOS

Status:

Fix was provided in CRB BIOS (133R12)

5385643: MRC: BIOS does not cache capIDs correctly for single-threaded mode. Can lead to training failures with control and command signals

Issue description:

SetStartingCCC uses cached CAPID4 to determine SKX SKU. In single threaded-mode, BIOS does not cache CAPID4 for socket > 0. This will lead BIOS to always program LCC delays and may lead to training failure.

Resolution:

Fixed

Status:

Fix was provided in Reference Code (133R12)

5385509: t_stagger_ref change 1/2 tRFC -> 1/3 tRFC

Issue description:

For performance reasons, BIOS needs to change the default t_stagger_ref value to be 1/3 tRFC for all configurations. This is a low risk change, and we've verified from the board team that the board can handle the 1/3 tRFC change.

Resolution:

Fixed

Status:

Fix was provided in Reference Code (133R12)

5385178: CNFG_500_NANOSEC in PCU (D30,F5,RD8[9:0]) is incorrectly programmed based on DDR Freq

Issue description:

MemHot registers were moved from iMC on HSX to PCU on SKX. HSX programmed MemHot 500ns counter based on DDR frequency. PCU uses a different clock, that is fixed except in cases it is being overclocked. The result is that the MemHot registers are being programmed incorrectly. This affects SPD SMBus and MCP SMBus poll rate timing.

D30, F5, RD8[9:0] and D30, F5, RDCh[9:0] are impacted, but others may be as well. Below is there RD8h is programmed.

```
PurleyProductionTrunk\PurleySktPkg\Library\ProcMemInit\Chip\Mem\MemThrot.c:
        mhSense500nsReg.Data = ReadCpuPciCfgEx (host, socket, PCU_INSTANCE_0,
        MH_SENSE_500NS_PCU_FUN5_REG);
```

Resolution:

Fixed

Status:

Fix was provided in Reference Code (133R12)

CRB BIOS errata

This section lists permanent errata for Intel CRB BIOS

No.	Description
1.	5371666: USB keyboard does not work in DOS in eSPI mode
2.	5345499:5372639: WOL function is still working when disabled in BIOS
3.	5344902:5371080: The USB Stack mode can't save in BIOS boot option
4.	5385513: CRB BIOS is not triggering NMI under Red Hat Linux
5.	5372699: Missing Server RAS for PCH - GIC register SERM and SDPS bits need to be set
6.	5372794: UCE PPR support is missign from the RAS sample code
7.	5372945: (Purley) Kernel Panic during reading any EFIvars after S4 Power cycle (RHEL 7.3 GA)
8.	5373090: SMBIOS Type 4 Processor Upgrade field is not correct for Purley Socket-P (LGA3647)
9.	5373102: ACPI SLIT doesn't scale to support 8SG
10.	5373103: IIO sysmap configuration is not aligned per architecture
11.	5385159: Reduce the CpuSmmApSyncTimeout from 10ms to 1ms
12.	5385209: Incomplete C/A parity RAS feature implementation
13.	5385364: BIOS may hang during Warm Resets with non-default MMCFG_BASE

5371666: USB keyboard does not work in DOS in eSPI mode

Issue description:

USB keyboard in eSPI mode does not work under DOS. Keyboard is fully functional during POST, EFI-Shell and under POR operating systems. Issue is not seen in LPC mode.

Steps to reproduce:

1. Setup options to boot DOS
2. Boot Maintenance Manager → UEFI Optimized Boot → Uncheck UEFI 2.Optimized Boot → Commit changes and Exit
3. EDKII Menu → Boot Options → USB Stack change to "Legacy Stack"
4. Boot to DOS and check KB functionality

Resolution:

No fix. DOS is not a Purley POR operating system.

Status:

No fix in Intel Purley CRB BIOS.

5345499:5372639 WOL function is still working when disabled in BIOS

Issue description:

When disabled WOL in Intel CRB BIOS, system still can wake up on LAN.

Resolution:

CRB BIOS improperly ignores WOL setup setting. May not apply to custom BIOS.

Status:

No fix in Intel Purley CRB BIOS.

5344902:5371080 The USB Stack mode can't save in BIOS boot option

Issue description:

The USB Stack mode can't be saved in BIOS setup

Reproduction Steps:

1. Boot to BIOS setup: EDKII Menu ->Boot Options -> USB Stack
2. Click and change the mode (for example: UEFI Stack change to Legacy Stack) and save it (F10 ->Y)

3. Go back to the EDKII Menu and select to enter another path (for example: Platform Configuration -> PCH Configuration -> PCH SATA Configuration).
4. Go back to the USB Stack option and find that the mode still shows UEFI Stack mode. The selected Lagacy Stack mode wasn't saved correctly.

Resolution:

CRB BIOS improperly handled this option. May not apply to custom BIOS.

Status:

No fix in Intel Purley CRB BIOS.

5385513: CRB BIOS is not triggering NMI under Red Hat Linux

Issue description:

CRB BIOS does not generate NMI if IOMCA is disabled.
When PCIe error is signaled through legacy IIO reporting (IOMCA = off). IIO error handler tries to identify error source. It searches down stream device AER registers before probe int RP's AER regs. If a lesser severity error is found in the down stream device, CRB BIOS skips the deep check for RP.

In the case, an ANFE (Advisory Non-Fatal Error) was found in down stream device. BIOS then skips the check on RP and ignore the CTO injected on it. As a result, only corrected error is reported to signaling phase and NMI is not trigger as BIOS only triggers NMI for uncorrectable case (NFE and FE).

Resolution:

This is Intel CRB BIOS RAS runtime specific issue. No fix.

Status:

No fix in Intel Purley CRB BIOS.

5372699: Missing Server RAS for PCH - GIC register SERM and SDPS bits need to be set

Issue description:

System encountered instances where CPU took an INIT interrupt and UEFI Firmware just hang in early PEI code after reset vector. The debug reveal that both of the SERM and SDPS bits are not been set in Intel UEFI Firmware with the Neon City Reference Platform (WW40 BKC). These two bits need to be set for Purley server platforms:

Below is these two bits definition:

16 - Shutdown Policy Select (SDPS): When cleared (default), the PCH will update INIT# in response to the shutdown Vendor Defined Message (VDM). When set to 1, PCH will treat the shutdown VDM similar to receiving a CF9 I/O write, and will drive PLTRST# active.

8 - Server Error Reporting Mode (SERM): when set, the CPU complex is the final target of all host space errors. In this mode, if the PCH detects a fatal, non-fatal, or correctable error on DMI or downstream functions from DMI, it sends one of the ERR_FATAL, ERR_NONFATAL, or ERR_CORR to cpu complex. When cleared, the PCH is the final target of all host space errors.

Resolution:

Need investigation in Purley Refresh.

Status:

No fix in Intel Purley CRB BIOS.

5372794: Purley RAS sample code does not include UCE PPR

Issue description:

SKX-SP Sample RAS Code doesn't include the UCE PPR support.

Resolution:

This is Intel CRB BIOS RAS code. No fix.

Status:

No fix in Intel Purley CRB BIOS.

5372945: (Purley) Kernel Panic during reading any EFIvars after S4 Power cycle (RHEL 7.3 GA)

Issue description:

Attempt to read EFI var after S4 causing kernel panic:

```
[   93.199091] BUG: unable to handle kernel NULL pointer dereference at 0000000000000280
[   93.207869] IP: [<0000000000000280>] 0x27f
[   93.212462] PGD 1f9e067 PUD 1f9f067 PMD 1fa0067 PTE 8000000000000163
[   93.219618] Oops: 0011 [#1] SMP
[   93.223232] Modules linked in: vfat fat intel_powerclamp coretemp intel_rapl iosf_mbi kvm_intel kvm irqbypass
crc32_pclmul ghash_clmulni_intel aesni_intel lrw gf128mul glue_helper ablk_helper cryptd iTCO_wdt
iTCO_vendor_support ipmi_devintf snd_hda_codec_realtek snd_hda_codec_generic pcspkr snd_hda_intel
snd_hda_codec snd_hda_core snd_hwdep snd_seq snd_seq_device snd_pcm snd_timer sg snd i2c_i801 lpc_ich
soundcore shpchp wmi ipmi_ssif ipmi_si ipmi_msghandler nfit tpm_crb libnvdimm acpi_power_meter acpi_pad
nfsd auth_rpcgss nfs_acl lockd grace sunrpc ip_tables xfs libcrc32c sr_mod cdrom sd_mod crc_t10dif
crct10dif_generic crct10dif_pclmul crct10dif_common crc32c_intel mgag200 i2c_algo_bit drm_kms_helper
syscopyarea sysfillrect sysimgblt fb_sys_fops ttm i40e e1000e ahci libahci drm ptp nvme r8169 libata pps_core
i2c_core mii fjes uas usb_storage dm_mirror dm_region_hash dm_log dm_mod vmd_update(OE) md_rste(OE)
[   93.314258] CPU: 33 PID: 2930 Comm: hexdump Tainted: G           OE  ------------   3.10.0-514.el7.x86_64 #1
[   93.325230] Hardware name: Intel Corporation PURLEY/PURLEY, BIOS PLYDCRB1.86B.0102.D12.1609232341
09/23/2016
[   93.336195] task: ffff88015e69edd0 ti: ffff88006b930000 task.ti: ffff88006b930000
[   93.344550] RIP: 0010:[<0000000000000280>]  [<0000000000000280>] 0x27f
[   93.351854] RSP: 0018:ffff88006b933da8  EFLAGS: 00010002
[   93.357785] RAX: ffff880169c97000 RBX: ffff880169c97000 RCX: ffff880169c97000
[   93.365752] RDX: ffff880169c97400 RSI: ffff880169c97000 RDI: 0000000000000280
[   93.466972] RBP: ffff88006b933e80 R08: 0000000000000000 R09: ffff88006b933ec0
[   93.474939] R10: 0000000000000022 R11: 0000000000000246 R12: ffff880169c97400
[   93.482906] R13: 0000000000000000 R14: ffff88006b933ec0 R15: 0000000000099000
[   93.490873] FS:  00007f199d5e8740(0000) GS:ffff880175240000(0000) knlGS:0000000000000000
[   93.499907] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[   93.506324] CR2: 0000000000000280 CR3: 0000000000099000 CR4: 00000000003407e0
[   93.514295] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[   93.615529] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
[   93.623498] Stack:
[   93.625745]  ffffffff8107a2fe 00007f199d5f7000 ffff88006ea8b398 0000000000000000
[   93.634059]  ffff88006b933e50 0000000000000000 ffff880169c97000 ffff88006b933e50
[   93.642373]  0000000080050033 0000000000000000 0000000000000000 0000000000000000
[   93.650682] Call Trace:
[   93.653416]  [<ffffffff8107a2fe>] ? efi_call+0x7e/0x100
[   93.659251]  [<ffffffff81078b3b>] ? virt_efi_get_variable+0x4b/0x60
[   93.666274]  [<ffffffff81518d61>] efivar_entry_size+0x41/0xb0
[   93.672683]  [<ffffffff8128e969>] efivarfs_file_read+0x49/0x100
[   93.679286]  [<ffffffff811fdf9e>] vfs_read+0x9e/0x170
[   93.684928]  [<ffffffff811feb6f>] SyS_read+0x7f/0xe0
[   93.690477]  [<ffffffff816964c9>] system_call_fastpath+0x16/0x1b
[   93.790509] Code:  Bad RIP value.
[   93.794238] RIP  [<0000000000000280>] 0x27f
[   93.798927]  RSP <ffff88006b933da8>
[   93.802821] CR2: 0000000000000280
[   93.806513] ---[ end trace aca41ee64a96875f ]---
[   93.910206] Kernel panic - not syncing: Fatal exception
[   93.921242] Rebooting in 10 seconds..
```

How to reproduce:

1. Install RHEL 7.3 GA on single SATA drive
2. Perform S4 power cycle
   - #echo 0 > /sys/power/pm_async
   - #echo disk > /sys/power/state
   - (After that - resume platform from S4)
3. After resuming try to read any efi-variable:

   hexdump -C /sys/firmware/efi/efivars/*

Expected Results:

Efi variable is read without an error

Actual Results:

Attempt to read EFI variable cause kernel panic (Logs attached)

Resolution:

This is Intel CRB BIOS isuse. No fix.

Status:

No fix in Intel Purley CRB BIOS.

5373090: SMBIOS Type 4 Processor Upgrade field is not correct for Purley Socket-P (LGA3647)

Issue description:

Purley BIOS reports "Processor Upgrade" as "Socket LGA2011-3(02Bh)". SMBIOS Specification - Version 3.1 have value "36h" for Socket "LGA3647-1".
https://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.1.0.pdf, page#54.

Resolution:

This is Intel CRB BIOS issue. No fix.

Status:

No fix in Intel Purley CRB BIOS.

5373102: ACPI SLIT doesn't scale to support 8SG

Issue description:

Intel CRB BIOS ACPI SLIT table doesn't scale to 8SG. EFI_ACPI_SYSTEM_LOCALITIES_ENTRY_COUNT should not be hardcoded and should base on the MAX_SOCKET count.

\PurleyPlatPkg\Include\Acpi\Slit.h:

```
        #define EFI_ACPI_SYSTEM_LOCALITIES_ENTRY_COUNT 64
    Should be:
        #define EFI_ACPI_SYSTEM_LOCALITIES_ENTRY_COUNT ((MAX_SOCKET*2)*(MAX_SOCKET*2))
```

\PurleyRpPkg\Library\AcpiPlatformTableLib\AcpiPlatformLibSlit.c:

```
        UINT8 Index;
    Should be
        UINTN Index;
```

Resolution:

This is Intel CRB BIOS issue. No fix.

Status:

No fix in Intel Purley CRB BIOS.

5373103: IIO sysmap configuration is not aligned per architecture

Issue description:

Case of IOMCA=OFF:

Local sysmap is configured to 0x50 = generate SMI for SEV 1, and NMI for SEV 2.
Global sysmap in Ubox is configured to also trigger SMI for SEV 0, and SEV 1, and NMI for SEV 2.

Above setting when IOMCA is OFF is not aligned with the architect intend and may result in a storm of SMIs and multiple NMIs. System needs local stack to only trigger NMI, and SMIs from global sysmap in Ubox.

Resolution:

Need investigation in Purley Refresh.

Status:

No fix in Intel Purley CRB BIOS.

5385159: Reduce the CpuSmmApSyncTimeout from 10ms to 1ms

Issue description:

Amount of time spent in SMM error handling may cause VMWare PSOD and Windows BSOD.

Resolution:

Reduce the setting for PcdCpuSmmApSyncTimeout from 10ms to 1ms.

Status:

No fix in Intel Purley CRB BIOS.

5385209: Incomplete C/A parity RAS feature implementation

Issue description:

Intel RAS sample code didn't implement MEM_DDR_PARITY_ERROR type. SMI is not getting generated when injecting DDR4 command and Address parity error.

Resolution:

Need investigation in Purley Refresh.

Status:

No fix in Intel Purley CRB BIOS.

5385364: BIOS may hang during Warm Resets with non-default MMCFG_BASE

Issue description:

In TxTDxeLib.h, PcdPciExpressBaseAddress is hard coded to 0x8000000

```
"#define PcdPciExpressBaseAddress          0x80000000"
```

If the Uncore MMCFG_BASE is programmed with a different value, below function that checks for ME UMA size may look at a wrong location:

```
 // ME UMA Size outside of a 0MB-64MB range is not defined or if BDF 0:22:0 is not present, exit.
if ((host->var.common.meRequestedSize > ME_UMA_SIZE_UPPER_LIMIT) || (host->var.common.meRequestedSize
== 0) ||
             (PchD22PciCfg32 (0x10) == 0xffffffff) ) {
            DEBUG ((EFI_D_INFO, "UMA: Invalid ME UMA Size requested.\n"));
            InitStat = 0x01;
```

Resolution:

Need investigation in Purley Refresh.

Status:

No fix in Intel Purley CRB BIOS.

END OF DOCUMENT