Grantley/BDX-EP/EP4S Platform CPU/QPI/Memory Reference Code Release Notes

June 13th, 2016
CRB BIOS Revision: 276.R02 (276V12)
Reference Code Revision: 3.6.0

Contents

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.6.0 (276.R02/276V12) – Post Launch Release (PLR4) 4
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.5.0 (276.R01/276V07) – Post Launch Release (PLR3) 5
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.4.0 (276.R00/276V03) – Post Launch Release (PLR2) 6
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.3.0 (275.R03/275V19) – Post Launch Release (PLR1) 7
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.2.0 (275.R00/275V01) – Production Version (MR2) 8
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.1.0 (273.R00/273V02) – Production Version (MR1) 9
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.0.0 (272.R01/272V11) – Full Production Version (full PV) 10
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.5 (272.R00/272V04) – Early-Ship Production Version (esPV) 11
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.1 (271.R00/271V02) – Production Candidate (full PC) 12
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.0 (269.R02/269V10) – Pre-Production Candidate 1 (Pre-full PC) 13
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.4.0 (267.R00/267V04) – Early-ship Production Candidate 1 (esPC) 15
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.0.0 (261.V26) – Beta 5 16
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.9.0 (261.R05/D20) – Beta 4 18
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.5 (261.R01/D11) – Beta 3 19
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.1 (259.D09) – Beta 2 24
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.0 (255.R00) – Beta 1 32
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.3 (251.R01) – Alpha 4 40
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.2 (246.R01) – Alpha 3 44
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.1 (246.R00) – Alpha 2 45
Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.0 (242.R00) – Alpha 1 48


```
SUBTITLE – ReleaseNotes.txt
;------------------------------------------------------------------------------------------------------------------
;
; Intel Restricted Secret
;
; Grantley-EP/EP4S CPU/QPI/Memory Reference Code
;
; Copyright (c) 2013, 2016 Intel Corporation.
;
; This software and associated documentation (if any) is furnished
; under a license and may only be used or copied in accordance
; with the terms of the license. Except as permitted by such
; license, no part of this software or documentation may be
; reproduced, stored in a retrieval system, or transmitted in any
; form or by any means without the express written consent of
; Intel Corporation.
;
; This program has been developed by Intel Corporation.
; Licensee has Intel's permission to incorporate this source code
; into their product, royalty free. This source code may NOT be
; redistributed to anyone without Intel's written permission.
;
; Intel specifically disclaims all warranties, express or
; implied, and all liability, including consequential and other
; indirect damages, for the use of this code, including liability
; for infringement of any proprietary rights, and including the
; warranties of merchantability and fitness for a particular
; purpose. Intel does not assume any responsibility for any
; errors which may appear in this code nor any responsibility to
; update it.
;
;------------------------------------------------------------------------------------------------------------------
;
; PURPOSE:
;
; This is a revision history for the Grantley-EP/EP4S CPU/QPI/Memory
; Reference Code releases.
;
;------------------------------------------------------------------------------------------------------------------
```

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.6.0 (276.R02/276V12) – Post Launch Release (PLR4)

Release date: June 13th, 2016 (WW25.1)

Revision 3.6.0 - 276.R02 (276V12)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
1.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Fix in RC	Description
386166	NO	Updating Grangeville_Trunk BIOS IDs: 20160601_CP_GRANGEVILLE_GRANTLEY_REF_GNV_89_D12_GRT_REF_276_D12
386129	YES	5003434: Modify the Reference Code Revision for BDX-EP to 3.6.0.

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.5.0 (276.R01/276V07) – Post Launch Release (PLR3)

Release date: May 27th, 2016 (WW22.5)

Revision 3.5.0 - 276.R01 (276V07)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
2.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Fix in RC	Description
381283	NO	Updating Grangeville_Trunk BIOS IDs: 20160518_CP_GRANGEVILLE_GRANTLEY_REF_GNV_89_D07_GRT_REF_276_D07
381272	YES	5003421: Modify the Reference Code Revision for BDX-EP to 3.5.0.
381256	NO	5003405: Expose "NITROMFC" ACPI table for TB3.0 dynamically according populated CPU with the feature support.
380927	NO	5003420: Please update SPS ME FW to SPS_E5_03.01.03.036.0

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.4.0 (276.R00/276V03) – Post Launch Release (PLR2)

Release date: May 13th, 2016 (WW20.5)

Revision 3.4.0 - 276.R00 (276V03)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
3.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
375476	YES	NO HSD: Modify the Reference Code Revision for BDX-EP to 3.4.0.
375465	YES	5003347:[HSX-BDX] System hang at early memory initialization with 32 pieces of 128GB LRDIMM installed with EP4S Processors.
375458	YES	5003344: Shut off unused DDR Clocks on HSX
371236	YES	5003377: LRDIMM PPR failure: misinterpretation of Guard key by Data buffer, and 5003400: LRDIMM sPPR failure: misinterpretation of Guard key by Data buffer.

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.3.0 (275.R03/275V19) – Post Launch Release (PLR1)

Release date: April 29th, 2016 (WW18.5)

Revision 3.3.0 - 275.R03 (275V19)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
4.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
366764	YES	5003110: DDR4 host Coarse Write Leveling improvement for frequencies above 1866 MT/s
361836	YES	5003326: Perf: Request to update osb_config.loi2eadvnath to 1 for 4S EP default snoop mode and COD
361388	YES	5003364: Modify the Reference code revision for BDX- EP to 3.03.0.
359364	YES	5003315: [B] CATERR HOLD in case of certain NVDIMM Configuration in Interleaving mode
357886	YES	5003311: Encoded CS mode error (3DPC LRDIMM)
355199	YES	5003319: Change EP CoD Check to look for lcc chop rather than core count based (>10c): resubmitting the changelist 352591
353143	YES	5003296: BDX-EP sPPR operation error: resubmitting the changelists 351264 and 351297

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.2.0 (275.R00/275V01) – Production Version (MR2)

Release date: March 10th, 2016 (WW11.4)

Revision 3.2.0 - 275.R00 (275V01)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
5.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
352591	YES	5003319: Change EP CoD Check to look for lcc chop rather than core count based (>10c)
351297	YES	5003311: Encoded CS mode error (3DPC LRDIMM)
351264 345846	YES	5003296: BDX-EP sPPR operation error
350762 345848	YES	5003110: System would hang in MVL cycling test with 32GB 2400MHz LRDIMM
345853	YES	5003310: PPR Taget component error with RDIMM 8Gbx4
345745	YES	5003324: Modify the Reference code revision for BDX- EP to 3.02.0
345279	YES	5003277: [BDX-EP] System hangs up at 0xB1 while Enable options: Attempt Fast Boot, Attempt Fast Cold Boot and Multi-Threaded MRC
343355	YES	5003273: System would hang at post code 0xBF during DC cycle test after enabling WrCRC setup option
343282	YES	5003298: Incorrect DDR Frequency Check in MemXMP.c
341349	YES	5003312: Core Count missmatch with QKF0

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.1.0 (273.R00/273V02) – Production Version (MR1)

Release date: February 5th, 2016 (WW06.5)

Revision 3.1.0 - 273.R00 (273V02)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
6.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
337136	YES	5003303: Modify the Reference code revision for BDX- EP to 3.1.0
336841	YES	5003299: [Perf] 4S 22C BDX EP (QKSW) SKU hitting TOR Timeout
332075	YES	5003270: Debug Enable bit in C80h MSR is incorrectly getting set with TXT Enabled

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 3.0.0 (272.R01/272V11) – Full Production Version (full PV)

Release date: December 11th, 2015 (WW50.5)

Revision 3.0.0 - 272.R01 (272V11)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
7.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
315925	YES	5003249: Modify the Reference code revision for BDX- EP to 3.0.0
315388	YES	5003243: SMBus clock registers misconfiguration could cause SPD corruption
315308	YES	5003170: Need MRC option to force a SPD page switch on cold boots
315208	YES	5003217: [EP/DE] RxDq eye collapse when IOLat = 10 (maybe 8)
313298	YES	5003233: DDR4 BDX-EP S3 reboot at 2DPC 2133 speed - Specific to 20nm DIMMs

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.5 (272.R00/272V04) – Early-Ship Production Version (esPV)

Release date: November 30th, 2015 (WW49.1)

Revision 2.9.5 - 272.R00 (272V04)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
8.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
311494 307992	YES	5003212: BDX EP - BDX DE: Send B2P command SET_CORE_RING_RATIO for BDX-EP A1 onwards and avoid the same for BDX-DE - (2nd Check-in: Enhancements/optimization)
310833 310776	YES	5003223: Replace the fixed ratios while sending SET_CORE_RING_RATIO B2P Command (0xA4) with the actual P1 ratio
309129	YES	5003218: BDX-EP DMI Completion Timeout When Accessing Memory Below 4GB
308061	YES	5003187: RecEn failure found when Mapout specific DIMM at second processor
306753	YES	5003182: MapOut (Rank disable) causes MRC failure in RecEn Pi in certain topology

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.1 (271.R00/271V02) – Production Candidate (full PC)

Release date: November 12th, 2015 (WW46.3)

Revision 2.9.1 - 271.R00 (271V02)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
9.	None

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
300681 300617	YES	5003191: DDR4 BDX-EP S3 reboot at 2DPC 2133 speed - Specific to 20nm DIMMs
300539	YES	5003172: WrCRC causes uncorrectable memory errors on CPU1 when fast boot is enabled
297269	YES	5003116: DCN87/95 - DDR4 3DS RDIMM support in Grantley-R MRC has wrong ODT settings

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.9.0 (269.R02/269V10) – Pre-Production Candidate 1 (Pre-full PC)

Release date: October 30th, 2015 (WW44.5)

Revision 2.9.0 - 269.R02 (269V10)

Notes:

None.

Potential issues and enhancements (under investigation)**:**

No.	Description
10.	5003191: DDR4 BDX-EP S3 reboot at 2DPC 2133 speed - Specific to 20nm DIMMs
11.	5003172: WrCRC causes uncorrectable memory errors on CPU1 when fast boot is enabled

5003191: DDR4 BDX-EP S3 reboot at 2DPC 2133 speed - Specific to 20nm DIMMs

**description_repro*: With the latest BIOS 261.V11 and 261.V13, system rebooted ramdonly during S3 testing. The failure was seen with 20nm parts running 2DPC 2133. 1DPC worked fine.

1DPC 4CH ♦passed
2DPC 1CH even ♦passed
2DPC 1CH odd ♦passed
2DPC 4CH windows sleeper - failed
2DPC 2CH IMC0 ♦failed
2DPC 2CH IMC1 ♦failed
2DPC 2CH IMC0 (CH0) and IMC1 (CH2) ♦failed

The issue was seen with more than 700 S3 cycles.

5003172: WrCRC causes uncorrectable memory errors on CPU1 when fast boot is enabled

**description_repro:* intermittent uncorrectable memory errors were detected on CPU1 when wrCRC is enabled. Issue temporarily went away with B0h CPU and MCU 0x09, but now it is back. On warm boot (Ctrl+Alt_Del or itp.resettarget()), the 1st CPU generates uncorrectable memory errors. No error on the 1st CPU on a power cycle or itp.pulsepwrgood() boot. ITP log:

```
+-------------------------------------------------------------------+
+- Socket 0 -- Uncore MCA -------- HA0 -----------------------------+
+-------------------------------------------------------------------+
iA32_MC7_STATUS: 0xEC000000000400A0  * VALID *
iA32_MC7_ADDR: 0x000000007A085000  * VALID *
iA32_MC7_MISC: 0x0000000080368200  * VALID *
iA32_MC7_MISC2: 0x0000000000000000  * VALID *
HA0_STATUS_SHADOW: 0xEC000000000400A0  * VALID *
HA0_ADDR_SHADOW: 0x000000007A085000  * VALID *
HA0_MISC_SHADOW: 0x0000000080368200  * VALID *
+-------------------------------------------------------------------+
checking socket 0 uncore mca bank 8
checking socket 0 uncore mca bank 9
+-------------------------------------------------------------------+
+- Socket 0 -- Uncore MCA -------- iMC0 C0 -------------------------+
+-------------------------------------------------------------------+
iA32_MC9_STATUS: 0xC80015FF020000B0  * VALID *
iA32_MC9_MISC: 0x09002CC0C8F4BE00  * VALID *
```

```
iA32_MC9_MISC2: 0x0000000000000000  * VALID *
+--------------------------------------------------------------------------+
+--------------------------------------------------------------------------+
+- Socket 0 -- Core 00 MCA ------- MLC ------------------------------------+
+--------------------------------------------------------------------------+
iA32_MC3_STATUS: 0xF200000000300101  * VALID *
+--------------------------------------------------------------------------+
```

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
295590	YES	5003087: System hang when Multi threaded MRC is disabled and MemPwrSave
294362	YES	5003116: DCN87/95 - DDR4 3DS RDIMM support in Grantley-R MRC has wrong ODT settings
293715	YES	5003161: [BDX-EP] 3DS 128GB hang at postcode BF during S3 testing
293276	YES	5003145: Multi-threaded MRC fails to program Skt1
293116	YES	5003144: OS stress fails with tRRDD = 1, passes with tRRDD = 2
291318	YES	5003146: [BDX-EP]: Allow ISOC feature to be enabled for HSX- CPUs
290808	YES	5003133: Change in POR for 2133 RawCard 0 RDIMMs 2DPC to run at 1866 not 2133
290175	YES	5002983: [BDX-EP] RC 1.85 easy to stuck at Early CTL/CLK with certain configuration (QHV3 A1 x2, 16GB RDimm x16)
287226	YES	5003134: System hangs when mixing 2R and 4R LRDIMMs non-3DS on the same channel
287132	YES	5003120: [BDX] Apply "-8" offset to RxDQs after basic training for all DDR3 configs
286668	YES	5003117: PPR function cannot be set to ""PPR Disabled"" in BIOS setup utility
286450	YES	5003112: Need the WA (high_priority_wm=panic_wm+1) of sighing "5003013" be applied to 3DS RDIMMs also (3DS 3DPC RDIMM)
285810	YES	5002951: Memory Corruption on Mayancity with 3DPC (LRDIMM, Fedora20) while executing SSA API test content
285416	YES	5003119: POR Update: Add 1R RDIMM and UDIMM configs

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.4.0 (267.R00/267V04) – Early-ship Production Candidate 1 (esPC)

Release date: September 18th, 2015 (WW38.5)

Revision 2.4.0 - 267.R00 (267V04)

Notes:

Revision update only. No code change.

Potential issues and enhancements (under investigation)**:**

None.

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	RC	Description
280584	YES	5003070: Stepping down 2133 DIMM frequency to 1800 causes BIOS hang in MRC
280107	YES	5003093: Convert 3DS LRDimms stretch goals to run at same frequency as non-3DS LRdimms
278112	YES	5003080: cecc with 3DPC 64GB LRDIMMs @1867 and 1600
276359	YES	5002985: LLC Reservation with CRB Bios is not happening (failing)
275110	YES	5003040: BSSA: GetMarginParamLimits() and SetMarginParamOffset() didn't work for RxDqsBitDelay and TxDqBitDelay
274504	YES	5003004: MRC doesn't mask reserved bits when comparing KeyByte2
273992	YES	5003041: BSSA: margin group CtlGrp5 causes rc_assert error.
272895	YES	5003013: BTTO with thermal throttle content on 3DPC 3DS LRDIMM
271579	YES	5002989: Perf: tQS BIOS (261V13) and above causes DRAM performance throttling
270799	YES	5003014: BSSA chip functions needed for new CCMRC changes
269839	YES	5002908: Convert EP stretch goals configs to POR configs
269395	YES	5002840: MRC hang with VLP (Very Low Profile) memory DIMMs using newer baselines
268944	YES	5002618: RMT results no longer print with MIN debug level
268942	YES	5002911: BTTO with thermal throttle content on 3DPC 3DS LRDIMM
268941	YES	5002958: MRC will stuck at pipeinit (CP:0xA7) with Trace Message enabled when populated 2 CPUs
266059	YES	5002924: Perf: loi2eadvnath tuning for 4S EP NUMA
261953	YES	5002734: System hangs in MRC after SDDC with Intel CRB BIOS (broadwell EP BIOS) based on RC 1.8.0
258063	YES	5002915: Phase shedding Values not coming correct. Need to check the fix in in place

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 2.0.0 (261.V26) – Beta 5

Release date: September 4th, 2015 (WW36.5)

Revision 2.0.0 - 261.V26

Notes:

Revision update only. No code change.

Potential issues and enhancements (under investigation)**:**

5003080: CECC with 3DPC 64GB LRDIMMs @1867 and 1600

**description_repro:* cecc errors were seen running with 3DPC 64GB LRDIMMs at DDR freq 1866. Time to failure varies from platform to platform, minimum is 1 hour 20 mins.

1. The error is always coming from DIMM1 and rank 5
2. 32GB 3DPC LRDIMM so far no failure observed, run is IP so far 26 hours of run completed

This issue so far did not happen at 1600 frequency.

**affected_bios_collateral:* MRC

4987017: [BDX OEM Request] DDR3 and DDR4 OS Offset set up option

**description_repro:* Based on several customer experiences and the input from technical experts it was determined that a simple BIOS option to offset the final training results before entering the OS would facilitate customer debug.

**affected_bios_collateral:* MRC

5002985: LLC Reservation with CRB Bios is not happening (failing)

**description_repro:* enable the following in Bios - for IOT enablement (ATD etc.) .....Advanced ->Processor Configuration -> Pre-socket Configuration -> Cpu Socket 0 Configuration. IOT Cfg CBO Bitmap (HEX) from 0 -> FFFFFF ways to 4, and TOR id's to 12.

Expected behavior: sv.socket0.uncore0.cbo1_cbo_ocla_ctrl.ocla_min_way = 0x10

Actual behavior: sv.socket0.uncore0.cbo1_cbo_ocla_ctrl.ocla_min_way = 0x14

Outcome is that 'Abstract Trace Configuration' gets error: 'valueError: value of WaysReserved must be >= 0x0 and <= 0xC, got [5b] 0x18' leading to hindrance for IOT capture for debug The above is working with Internal Bios but not with CRB one

**affected_bios_collateral:* CPURC

5003040: BSSA: GetMarginParamLimits() and SetMarginParamOffset() didn't work for RxDqsBitDelay and TxDqBitDelay

**description_repro:* When ran EV test - marginparaminfo GetMarginParamLimits() and SetMarginParamOffset() did not handle per bit type margin parameter, they caused below assert error for the RxDqsBitDelay and TxDqBitDelay signals.

RC_ASSERT! ..\Library\ProcMemInit\Chip\Mem\MemIOControl.c: 2029 bit < 4

This is a bug in the BSSA margin parameter code. Without the fix, the EV can not margin RxDqsBitDelay and TxDqBitDelay signals.

**affected_bios_collateral*: MRC

5002784: Move InitADR() code to reduce ADR vulnerability window

**description_repro:* InitADR() function in the MRC is now an entry in the MRC call table which is called after we switch to normal mode. During ADR resume this would leave a big hole in time during which data is vulnerable to loss should a power failure occur. To reduce this vulnerability window to a minimum, ADR should be enabled just before calling ExitSelfRefresh().

**affected_bios_collateral:* MRC

5003009: Mismatch across resets with "dimmTypePresent"

**description_repro:* During formal BIOS log investigation, it is found that for the same version of BIOS, the "dimmTypePresent" prints different values across resets in Grantley-Refresh UEFI FW.
**affected_bios_collateral:* CPURC

5003025: OSC support for CPC

**description_repro*: OSC support for CPC. From Debug discussion/code, looks like the BIOS _OSC is based off UUID 4077A616-290C-47BE-9EBD-D87058713953 which enumerates vendor specific _OSC bits. Looks like BIOS needs to check platform _OSC bit (UUID 0811B06E-4A27-44F9-8D60-3CBBC22E7B48) as per ACPI specification 6.0
**affected_bios_collateral:* Binary ROM (External), Binary ROM (Internal), CPURC

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
271152	5002989: Perf: tQS BIOS (261V13) and above causes DRAM performance throttling **description_repro:* The calculated DRAM power with default settings of memory bandwidth is capped by RAPL. This is impacting peak performance and must be fixed. **bios_resolution_notes:* Phase shedding changes integrated **affected_bios_collateral:* MRC

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.9.0 (261.R05/D20) – Beta 4

Release date: August 11th, 2015 (WW33.2)

Revision 1.9.0 - 261.R05(D20)

Notes:

Revision update only. No code change.

Potential issues and enhancements (under investigation)**:**

5002734: System hangs in MRC after SDDC with Intel CRB BIOS (Broadwell EP BIOS) based on RC 1.8.0

**description_repro:* system hangs in MRC with Intel CRB BIOS (broadwell EP BIOS) based on RC 1.8.0 after SDDC.
System configuration: CPU: Broadwell A1*2, Memory: DDR4 16GB 2Rx4 *1 (socket 0, channel 2, dimm0) ITP Script's 551734_CScripts_BDX_Server.0.8.17231.495308, OS: Windows 2012 R2 Legacy
Steps to reproduce:

SystemEventLog -> System Errors - Enable/Disable Runtime Error Logging Support. Enabled all WHEA Setup options.
SystemEventLog ->Memory Error Enabling -> Memory Corrected Error - Enable/Disable the Correctable Error Logging support
SystemEventLog ->Memory Error Enabling -> Spare Interrupt [SMI]
Memory RAS configuration -> Correctable/Spare Threshold 2
Memory RAS configuration ->Device Tagging -> Enable

With this configuration, injected two correctable errors and device tagging is getting control. Used the ITP command ei.memDevs(dev0=3,dev0msk=0x8,dev1=4,dev1msk=0x10) to select the different Device number in DIMM Injected one more CE error and MCE happens and as expected windows blue screen occurred. After re-start system is hanging in MRC.

5002785: Clear ADR_STS register on NVDIMM resume

**description_repro*: ADR_STS register needs to be cleared during NvDIMM resume before doing NvDimmRestore. Without this the NVDIMM code thinks there is still a pending ADR and may corrupt the data.

5002873: DDR4 BDX-EP fail to boot LRDIMM with ECC Support disabled

**description_repro:* LRDIMM failed Rec En training when ECC Support disabled in the BIOS. RDIMM is working fine. Memory suppliers are using this option to debug failure in order to decode dq information.

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
267663	NO_HSD_Syncing Cl No-266077 from Grantley-R PV trunk to Grantley-R Release trunk 5002926:Modify the Reference code revision for BDX- EP to 1.9.0

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.5 (261.R01/D11) – Beta 3

Release date: July 24th, 2015 (WW30.5)

Revision 1.8.5 - 261.R01(D11)

Notes:

None

Potential issues and enhancements (under investigation)**:**

4988239: DDR3 MayaCity hangs up in MRC when Enable Fast Cold Boot with 2DPC QRx4 DDR3 RDIMM.

**description_repro*: SUT hang up on 2nd boot after enabling Fast Cold Boot. DDR3 MayaCity CRB hangs up at MRC, while enable Fast Cold Boot with 2DPC QRx4 DDR3 RDIMM.

Platform configuration: MayaCity DDR3 CRB BIOS V37.R05.RC105 DIMM configration: QRx4 DDR3 RDIMM 32GB DDR3 ECC RDIMM 1.35v 16pcs

Reproduce steps:

1. Install at least 2DPC in Socket 0 Channel 0 (or fully populated)
2. Go to BIOS setup menu.
3. Set "Fast Cold Boot" -> "Enable" (Default is Auto)
4. Save then exit.
5. Power down System by power button.
6. Cold boot system by power button.
7. Platform hangs up at postcode 0xB0.

5001646: HSX Clone: (BIOS only enable COD on parts with at least 10 cores) LCC derived from MCC is enabling COD and also imbalance configuration

**description_repro*: LCC parts derived from MCC have 2 HAs and hence COD could be enabled according to current BIOS checks. Intention was to only do COD on parts with 10C or more. Parts should have been fused with COD disabled but they weren't so BIOS w/a needed. Currently BIOS checks: If capid5.cod_enable =1 and 2 HAs are present, and if 2S then if 2 qpi links to enable COD. New requirement is to check if part has 10 cores or more before enabling COD.

5001665: HSX Clone: (MRC XMP DIMM discovery not MP safe) System stuck at CP: 0xB7 (Ddr4LrdimmBacksideTxCoarseWL) while mixing LRDimm vendor on CPU0,1

**description_repro*: system may stuck at LRDimm training phase - Ddr4LrdimmBacksideTxCoarseWL with below test configuration. Per serial log, found CPU1 LRDIMM MDQS Coarse WL - FAILED WRITE CYCLE. The issue occurs on Aztec City using non-RDIMM config. Failure due to XMP DIMM discovery code not being MP safe.

4988223: Some HSW CPU would CATERR during warm reset when PCIE hotplug and COD are enabled.

**description_repro*: If PCIE hotplug and COD are enabled, the system would CATERR and hang during warm reset.

Reproduce steps:

1. Boot to setup.
2. Change COD to 'Enabled' and change 'PCIE hotplug' to 'Enabled'
3. Save and reset system. CATERR would happen. Config: Board: MayanCity CPU: Haswell C1 stepping (QGN2), QGN1 can't reproduce BIOS: 37R05 According to current debug, this isssue is caused by another sighting 4166740 fix.

5001600: HSX Clone: (MRC: Disable DDR4 RCD SMBus interface for all vendors) SMBus SDA line getting stuck low during TSOD polling causing temperature data corruption

*description_repro: The root cause of the issue is the DDR4 register/RCD SMBus slave interface (which is on by default) gets into a bad state where it holds the SMBus SDA line low for some period of time (ms to sec). This can lead to faulty TSOD temperature values and even THERMTRIP if enabled. Issue will be avoided by disabling the RCD SMBus interface for all vendors as it is not necessary for BIOS to boot and is not used in any POR flows. It is for RCD debug only. BIOS workaround: Disable the SMBus slave interface on all DDR4 register/RCD devices.

5002783: Broadwell MRC code: Fast Warm Boot does not work with specific HSW processors

*description_repro: Haswell EP 2HA processors using the BDX-EP 1.8 reference code throws a CATERR when FastWarmBoot is enabled. 1HA processors don't appear to be impacted. This issue is about Broadwell MRC code and Haswell processors. We know that Broadwell MRC code is compatible with Haswell processors. However, Fast Warm Boot doesn't work with latest Broadwell MRC and specific Haswell processors. Broadwell MRC version used: 1.8.0 HSW processor E5-2640 v3 2.6GHz, R2 stepping, 8 core, 1HA - WarmFastBoot works fine with this processor. HSW processor E5-2683 v3 2.0GHz, C0 stepping, 14 core, 2HA - WarmFastBoot doesn't work. When ROM tries to switch stack from Cache to main memory, at that point CATERR Hold is asserted and system performs Warm reset. WarmFastBoot works fine with latest Haswell MRC 1.14 code drop with this processor.

5002785: Clear ADR_STS register on NVDIMM resume

*description_repro: ADR_STS register needs to be cleared during NvDIMM resume before doing NvDimmRestore. Without this the NVDIMM code thinks there is still a pending ADR and may corrupt the data.

5002893: RC1.80 caused certain BDX-EP (QHVB) hang at Early CTL/CLK training when doing warmboot cycle test

*description_repro: RC1.80 was found causing certain BDX-EP(QHVB) hang at Early CTL/CLK training when doing warmboot cycle test 1. TTF: RC-1.80 can reproduce <100 cycles, RC-1.73 has no this issue 2. Swap CPU0 and CPU1, the symptom would follow CPU MayanCity also can reproduce this issue with 255.R00 Reproduce steps 1. Set Attempt Fast Boot to [Disable]. 2. Save the setting. 3. Boot into OS and do warmboot

5002901: R0 fails to train memory in Ch 2 &3

*description_repro: QJRD and QJRK both fail to train memory on channel 2 and 3 on Mayan City platform. On Aztec system this works. Tried with several BIOSes. 260.V13 , 261.D02, 259.v13 The only bios that works is the one that was used in power on. 257.V15+DDR_ch2_ch3_fix_vccpq_ramp_patch

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
257389	Updating Grangeville_Trunk BIOS IDs: 20150720_CP_GRANGEVILLE_GRANTLEY_REF_GNV_74_D11_GRT_REF_261_D11
256865	5002911: BTTO with thermal throttle content on 3DPC 3DS LRDIMM *description_repro: Need the following WA for a 3DPC 3DS LRDIMM Memory configuration when throttle is enabled. WA per populated memory channel: sv.socket0.uncore0.imc0_c0_rowhammer_timer= 0x00000001 sv.socket0.uncore0.imc0_c0_rowhamconfig2 = 0x50800000 sv.socket0.uncore0.imc0_c0_rowhamconfig3 = 0x00000fff sv.socket0.uncore0.imc0_c0_rowhamconfig = 0x803f8032. This WA is already implemented in HSX BIOS (274174) *bios_resolution_notes: Row hammer WA is applied for 3DPC 3DS LRDIMM configuration for BDX EP. *affected_bios_collateral: MRC
256039	NO_HSD: Modify the Reference code revision for BDX- EP to 1.8.5
256034	5002314:Add Xover offsets/Silicon constants for HSX to Grantley Refresh BIOS *description_repro: We recently revamped some Xover offsets and silicon constants for BDX (5002244). Right now, the Xover BIOS

	code supports only one set of constants, and right now in the Grantley Refresh BIOS, those are for BDX specifically. We need to add a HSX-specific set of constants eventually, as the Grantley Refresh BIOS is supposed to support HSX as well as BDX. This sighting is a placeholder for now, we need to determine what this set of values will be for HSX prior to the point when the Grantley Refresh BIOS will be released for HSX use. **bios_resolution_notes:* Xover offsets constants for HSX are synced from Grantley to Grantley Refresh BIOS. **affected_bios_collateral:* MRC
254702	5002740: ECP_FLAG to be removed from BSSA code **description_repro:* Remove the stale ECP_FLAG from around the BSSA code. Medium. **bios_resolution_notes:* Core/Mem/MrcSsaServices.c CCMRC override done here; core should be updated. Other changes for this HSD are checked in via CCMRC s4757672. Changes checked in CL254702. **affected_bios_collateral:* MRC
254699	5001999: Fast Cold Boot is Broken on BDX DE and EP, Needs Validation **description_repro:* Fast Cold Boot does not work on LRDIMMs. From comparing RMT, it appears that Fast Cold Boot does not correctly restore the register and/or BIOS cache values for the LRDIMM backside. The frontside needs to be checked as well, I am not sure the Tx values are being restored correctly. The BIOS team needs to create a test BIOS which enables an MRC register dump with Fast Cold Boot and print out both the registers and the cache and make sure that after a Fast Cold Boot, everything is being properly restored to the expected values both in the cache and the registers. I have already run a comparison of the cache and the register on a normal boot, and they match, so we just need to prove they are correct following the Fast Cold Boot. Once we have this fixed, we also should test Fast Cold Boot on 3DS LRDIMMs and encoded mode LRDIMMs to ensure it handles the encoded mode cases correctly. **bios_resolution_notes:* 1. In DisplayTrainResults Backside LRDIMM values not restored on FCB and RMT_EN. Resolved. 2. In DisplayTrainResults MR6 values are not restored on FCB and hence not in RMT when Enabled. Partly resolved though some strobe values are mismatching. 3. In RMT CMD/CTL group values not restored/present in RMT on a FCB. For #3 we took register dumps made before cmd/ctl group values are populated in RMT regular_flow_reg_dump for the two flows: Regular flow and FastColdBoot +RMT_on. Reg dumps attached to the HSD. Also based on reg dump data tried calling CAParityRuntime in RMT; issue still remains. Being looked into. **affected_bios_collateral:* MRC
254580	4988057 : HEDT: XMP is not displayed correctly in Timing Override menu **description_repro:* When selecting "Profile 1" under Advanced->Memory->Timing Override all the values displayed are zeros. Afterwards, selecting "Manual" shows the correct values. The DIMM is a DDR4 UDIMM with XMP 2.0 data. High - this annoying behavior slows down work. Not everyone knows about the workaround. Should be a simple fix. **bios_resolution_notes:* **affected_bios_collateral:* <Unassigned>
254032	5002877 : Perf: iOSB tuning for 4S EP COD **description_repro:* Performance tuning found OSB settings that improve wcil and STREAM performance osb_config.loieadvnath=4 and osb_config.rmtadvnath=6 See over 10% performance improvement for Wcil traffic patters for local and remote BW **bios_resolution_notes:* Fix : When BDX- and 4S-COD- config is detected, set loieadvnath as 4. **affected_bios_collateral:* QPIRC
253953	5002879:BDX EP: 2/3DPC 3DS LRDIMM hits BTTO with PC6 content (OSR disabled, CKE= only APD) **description_repro:* This request is in addition to a previous request, with the setting from above bios request, we see that CKE mode is toggling between APD and CKE-off. We hit UC with the failing memory configs and root caused the issue to be because of this CKE toggling. In order to restrict CKE to only APD, we need below setting. We need to set one more filed in the same register (PCU_CR_DYNAMIC_PERF_POWER_CTL_CFG) for a failing memory config (3DPC LRDIMM or 3DS LRDIMM-any dpc). Bit field to set for the failing memory config: PCU_CR_DYNAMIC_PERF_POWER_CTL_CFG[10:10]=1. Same behavior is seen with 3DPC LRDIMM,

	sometimes I hit BTTO and some times just TOR TO. We have passes in our automation runs, as these runs are with MemPwrSave=User Defined. **bios_resolution_notes:* imc_apm_override_enable and sapm_osr_override bits of PCU_CR_DYNAMIC_PERF_POWER_CTL_CFG set to 1 for 3DPC/3DS LRDIMM configurations. **affected_bios_collateral:* MRC

253560	5002865, 5002002 : Delete all refererences to AltRtid2S in QPI Init Code, as it is dead code, and is causing confusion
	**description_repro:* Old variable is confusing customers. Please delete. Find all "AltRtid2S", Subfolders, "d:\Workspace\GrantleyBdxTrunk\GrantleySocketPkg", "*.*" File d:\Workspace\GrantleyBdxTrunk\GrantleySocketPkg\Include\Setup\IioCsiConfigData.h 73 25: UINT8 AltRtid2S; // 1 - Enable; 0 - Disable; Normally disabled, but if enabled can boost performance in some 2S environments File GrantleySocketPkg\Library\MemoryQpiInit\Chip\Include\QpiHost.h 785 23: UINT8 AltRtid2S; // 1 - Enable; 0 - Disable; Normally disabled, but if enabled can boost performance in some 2S environments File GrantleySocketPkg\Library\MemoryQpiInit\Chip\Qpi\QpiMain.c 744 49: QpiDebugPrintInfo1((host, QPI_DEBUG_INFO1, "\nAltRtid2S: %u", host->setup.qpi.AltRtid2S)); 744 81: QpiDebugPrintInfo1((host, QPI_DEBUG_INFO1, "\nAltRtid2S: %u", host->setup.qpi.AltRtid2S)); File GrantleySocketPkg\Library\MemoryQpiInit\Platform\Setup\QpiSetup.c 296 16: setup->qpi.AltRtid2S = FALSE; // Disable Alternate Rtid Scheme for 2S. Total found: 5 Matching files: 4 Total files searched: 118
	**bios_resolution_notes:* Fix: Removed references to AltRtid2S from all QPIRC except in QpiHost.h due to EP-EX- convergence constraint.
	**affected_bios_collateral:* QPIRC
	
	5002002: [HSX-BDX] [BDX] HandleDegraded4S() accesses SocketData->Cpu[QpiInternalGlobal->SbspSoc].LinkData out of bounds
	**description_repro:* In the function HandleDegraded4S() in the QpiMain.c file there is a call to invalidate the socket connected to the 3rd link of the legacy socket: SocketData->Cpu[QpiInternalGlobal->SbspSoc].LinkData[2].Valid=FALSE; This line contains a hard-coded 2 and LinkData is defined as LinkData[MAX_QPI_PORTS] which is 2. This means the line mentioned above indexes outside the array.
	**bios_resolution_notes:* Fix : The fragment of code where degradation for a degraded 4S to 3S ring/chain is valid only for EX-topologies. Nevertheless, using a hard-coded value of 2 is not right way of doing this. This is replaced by (MAX_QPI_PORTS - 1) as suggested. Since, this is applicable to EX- only which has 3 ports, this would mapped back to expected value of 2.
	**affected_bios_collateral:* QPIRC

252929	5002861:B0 - Uncorrectable Patrol Scrub Fatal Error on S3 Resume **description_repro:* Whenever Patrol Scrubbing is enabled in BIOS, doing an S3 cycle from the OS will cause a Fatal Error upon resume. Klaxon shows that an Uncorrectable Patrol Scrub Error has appeared. I have attached both Klaxon logs and serial output of the S3 resume, as well as serial output of the boot to OS before the S3 test executed. Testing has been reproduced on two separate Aztec Citys with B0 QJJ9 and QJJB SKUs and the latest V-label CRB BIOS, 259.V13. Critical, B0 is a production candidate and tPRQ is scheduled for WW36. This failure blocks all RAS testing with S3. **bios_resolution_notes:* PipeSync() in MemMain.c is modified to return correct status. **affected_bios_collateral:* MRC
251058	5002854: Support for DDR4 3DS RDIMM support in Grantley-R MRC **description_repro:* HSD to track the development of DDR4 3DS RDIMM support in the Grantley-R (BDX-EP) MRC. This is to support the DCN87/95 SOW **bios_resolution_notes:* The original 3DS implementation assumed LRDIMM. I modified the code to remove that assumption. **affected_bios_collateral:* MRC
250330	5002671: MRC: 3DS LRDIMMs are incorrectly overwriting CIDs when sending MRS commands **description_repro:* CIDs are used as MRS payload extension according to 3DS Jedec Spec. We see the overwrite occur in WriteCadbCmd in MemCpgc.c. By overwriting this field, you might send the dimm into an unintended state. **bios_resolution_notes:* We see the overwrite occur in WriteCadbCmd in MemCpgc.c. By overwriting this field, you might send the dimm into an unintended state. If ((host->nvram.mem.dramType == SPD_TYPE_DDR4) && ((*channelNvList)[ch].lrDimmPresent)

	&& ((*channelNvList)[ch].encodedCSMode)) { // here we are in encoded quad CS mode patCADBProg0.cid = (rank >> 1) | 0x6; } Change the check from encodedCSMode to encodedCSMode == 1. *affected_bios_collateral:* MRC
249587	5002786: BIOS Programs incorrect value for DRAM Phase Shedding *description_repro:* BIOS programs incorrect values to Phase shedding default registers. Bios Version = GRRFINT1.86B.0257.D04.XML_31.SV_31 *bios_resolution_notes:* corrected the DRAM Phase Shedding calculation *affected_bios_collateral:* MRC
249418	5002815 : BIOS 258.V10 does not allow ISOC to be enable on R0 (LCC) parts *description_repro:* During the BDX-E R0 PO checkout, we discovered that the BIOS we use up to 258.V10 does not enable ISOC on R0 silicon regardless of the setting. ISOC is a must for LCC SKU and must be enabled for validation. And the ISOC feature needs to be enabled for both EP and E (HEDT) segments. *bios_resolution_notes:* Fix: Permit the enabling of Isoc for all physical chops which are above BDX-A1 and above. *affected_bios_collateral:* QPIRC
249347	5002773, 5002811 : Perf: OSB tuning, DCA clusterid and PE bit for MEseg both overloaded on DNID bit 3 causing akrtidmiss due to dnid corruption *description_repro:* Performance tuning found OSB settings that improve wcil and STREAM performance. When osb_config.osbloi2e is set to 1 (local inval I to E OSB enabled): If COD is enabled, set osb_config.loieadvnath = 6 if COD is disabled, set osb_config.loieadvnath = 3 STREAM performance improves by 2-3 percent for non-COD, and 3-4 percent for COD. *bios_resolution_notes:* For 2S topologies in non-EX- configs, set osb_config.loieadvnath as 6 if COD is enabled and set osb_config.loieadvnath as 3 if COD is disabled. Override pe_mode as 0x2 (instead of 0x3) when COD- and MeSeg are both enabled (Applicable only for BDX-). *affected_bios_collateral:* QPIRC
248840	5002771: MRC displayed Out of range message when Tx piDelay was at its max limit. *description_repro:* During BIOS SSA EV test, a message of "TxDqDelay Out of range !! piDelay = 0x1e, maxLimit = 0x1e" was displayed in the serial console. Because the piDelay value was right at its limit, it should not print out this message. Suggest to modify the code in the GetSetTxDelay() of the \Chip\Mem\MemIOControl.c to fix the condition statement "if (piDelay >= maxLimit)". It should be changed to "if (piDelay > maxLimit)" just like other "GetSet" functions. *bios_resolution_notes:* implemented *affected_bios_collateral:* MRC

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.1 (259.D09) – Beta 2

Release date: Jule 1st, 2015 (WW28.1)

Revision 1.8.1 - 259.D09

Notes:

None

Potential issues and enhancements (under investigation)**:**

5001999: Fast Cold Boot is broken on BDX DE and EP, Needs Validation

*description_repro: Fast Cold Boot does not work on LRDIMMs. From comparing RMT, it appears that Fast Cold Boot does not correctly restore the register and/or BIOS cache values for the LRDIMM backside. The frontside needs to be checked as well.

5002528: SMI workaround needed for rank 1 patrol scrub of 12GB/24GB dual rank DDR4 RDIMM

*description_repro: a SMI workaround is needed to enable patrol scrub of rank 1. This sighting is being opened to track the SMI workaround request separately from the basic MRC support.

5002671: MRC: 3DS LRDIMMs are incorrectly overwriting CIDs when sending MRS commands

*description_repro: CIDs are used as MRS payload extension according to 3DS Jedec Spec. We see the overwrite occur in WriteCadbCmd in MemCpgc.c. By overwriting this field, the dimm might be sent into an unintended state.
Code:

```
if ((host->nvram.mem.dramType == SPD_TYPE_DDR4) && ((*channelNvList)[ch].lrDimmPresent) &&
((*channelNvList)[ch].encodedCSMode))
        {    // here we are in encoded quad CS mode
        patCADBProg0.cid     = (rank >> 1) | 0x6;
        }
```

Change the check from encodedCSMode to encodedCSMode == 1.

5002734: System hangs in MRC after SDDC with Intel CRB BIOS (Broadwell EP BIOS) based on RC 1.8.0

*description_repro: system hangs in MRC with Intel CRB BIOS (broadwell EP BIOS) based on RC 1.8.0 after SDDC.
System configuration: CPU: Broadwell A1*2, Memory: DDR4 16GB 2Rx4 *1 (socket 0, channel 2, dimm0) ITP Script's 551734_CScripts_BDX_Server.0.8.17231.495308, OS: Windows 2012 R2 Legacy
Steps to reproduce:

SystemEventLog -> System Errors - Enable/Disable Runtime Error Logging Support. Enabled all WHEA Setup options.
SystemEventLog ->Memory Error Enabling -> Memory Corrected Error - Enable/Disable the Correctable Error Logging support
SystemEventLog ->Memory Error Enabling -> Spare Interrupt [SMI]
Memory RAS configuration -> Correctable/Spare Threshold 2
Memory RAS configuration ->Device Tagging -> Enable

With this configuration, injected two correctable errors and device tagging is getting control. Used the ITP command ei.memDevs(dev0=3,dev0msk=0x8,dev1=4,dev1msk=0x10) to select the different Device number in DIMM Injected one more CE error and MCE happens and as expected windows blue screen occurred. After re-start system is hanging in MRC.

5002746: IERR observed during boot to Windows Server 2012 R2 on Matan City with 3DPC LRDIMM configuration

*description_repro: IERR was reported during system boot to Windows Server 2012 R2 on BDX EP platform with RC1.8.0, A1 stepping processor and 3DPC LRDIMM memory configuration. Issue ws duplicated on Mayan City with 255R00 (RC1.8.0) BIOS when any memory channel was populated with 3 LRDIMM.

Issue duplicate steps:

1. Update BIOS 255R00 to Mayan City.
2. Populate 2 A1 stepping BDX processors.
3. Plugged 3 LRDIMMs to any memory channel on socket 0 or 1.
4. Connect HDD with Windows Server 2012 R2 installed.
5. Boot system and system hangs during OS boot.
6. IERR found by sysError dump.

5002785: Clear ADR_STS register on NVDIMM resume

*description_repro: ADR_STS register needs to be cleared during NvDIMM resume before doing NvDimmRestore. Without this the NVDIMM code thinks there is still a pending ADR and may corrupt the data.

5002833: Spare Failover with lockstep enabled showing wrong dimm location in bios serial log.

*description_repro: with sparing and lockstep enabled, created a spare failover condition and BIOS serial output shows the wrong information. Should show socket 0 node 1 but it displays socket 1. Also missing the upper address information. This config is socket 0 ch 2 and 3 with 2DPC 2Rx4 DIMMs, socket 1 ch 0 and 1 with 2DPC 2Rx4 DIMMs.

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
248779	Updating Grangeville_Trunk BIOS IDs: 20150701_CP_GRANGEVILLE_GRANTLEY_REF_GNV_72_D09_GRT_REF_259_D09
248660	5002800: Set IMode to 0xF by default, IMode needs bug fixes. *description_repro*: The BDX DDR EVQT has decided to set IMode to 0xF by default on all channels/bytes. IMode training will continue to be disabled by default, but enabling it will switch from a constant setting of 0xF to running the IMode power training algorithm. TrainImode() in MemPowerTraining.C is the function that needs to be re-worked. Also, I found a bug in the GetSetImode() function in MemIOControl.C, where IMode can be disabled by a read-only call to the function. This bug was causing IMode to be disabled before RMT by the read-only calls in the training register dump, resulting in off-center RMT margins (this was also why RMT showed no benefit from IMode). This needs to be fixed as well. *bios_resolution_notes*: Set IMode to 0xF by default. Fixed the code bug related to RMT corruption *affected_bios_collateral*: MRC
248638	5002244: Fix RxEnable Offset in 2:2 mode *description_repro*: This bug was recently found on HSX by a PRT, and also applies to BDX DE and EP when operating in 2:2 mode. https://vthsd.fm.intel.com/hsd/bios_grantley/default.aspx#sighting/default.aspx?sighting_id=5002237 Summary (MemXoverCalib.C): Change this: #define X_OVER_OFFSET_2TO2_RCVEN 26 To this: #define X_OVER_OFFSET_2TO2_RCVEN 34 *bios_resolution_notes*: TX_PER_BIT_SETTLE_TIME, TxPerBitSetup2to2Offset, X_OVER_OFFSET_2TO2_RCVEN and X_OVER_OFFSET_2TO2_TXDQS offsets are changed. TxDqs and RcvEn offsets are changed as per the new values recommended. *affected_bios_collateral*: MRC
247504	5002764: B0 Cpu stepping detected as Unknown at Setup menu *description_repro*: B0 CPUs are detected as Unknown at the Main menu. Serial log show the correct CPU stepping. How to reproduce: Boot system to setup menu, go to EDKII -> Main -> Processor BSP Revision, verify system reports the Revision as B0 *bios_resolution_notes*: the BIOS setup now correctly shows "Broadwell B0" instead of "Unknown" for BDX B0 CPU. *affected_bios_collateral*: CPURC

246618	5002752: MRC: Receive-enable, Early CTL/CLK and/or Early CMD/CLK training failures when IO latency= 4 at 2666 **description_repro*: Depending on the DIMMs being used, one or more of several training failures may be present when the resulting IO latency for a given rank is 4 during operation at 2666 MT/s. With RE8 DIMMs the failure occurred during receive-enable PI, with multiple strobes having no passing region. With RC8 DIMMs training actually proceeded all the way through MRC, but no eye was found for CTL group 0 during early CTL/CLK, and early CMD/CLK failed to find an eye for multiple signals when it subsequently ran. Only one BDX part training to an IO latency of 4 on one particular channel so it is unknown if HSX would similarly fail were MRC to settle on a value of 4. EV's recommendation is that a minimum of 6 be used across both HSX and BDX out of caution, but it is BIOS's prerogative to perform formal testing on HSX HEDT if required. 2666 MT/s DDR is not POR on HSX or BDX but is useful for pathfinding and necessary for overclocking support on HEDT. **bios_resolution_notes*: Fixed as requested **affected_bios_collateral*: MRC
245997	5002729: MRC: Idle time change in s5002509 causing failures during Tx Eq training at 2400 **description_repro*: EV has observed failures in BIOS change from 252.D06 to 252.D07 where training fails during Tx Eq due to no margin. This failure has thus far been observed only with RDIMMs and LRDIMMs. The issue was narrowed down by changing imcX_cX_idletime.idle_page_rst_val back to 8 after it was being set to 0x3F in Early Config, and observing the failure go away. **bios_resolution_notes*: Removed the deselect and prevented running CPGC on non-target channels during JEDEC init. **affected_bios_collateral*: MRC 5002509: CPGC Idle Time needs update for 2400 to enable back-to-back writes **description_repro*: CPGC is not able to correctly perform back-to-back writes at 2400 due to the register imcX_cX_idletime.idle_page_rst_val not being set to 0x3F. This value is currently defined to be 0x8 for all speeds in MemDefaults.H: #define IDLE_PAGE_RST_VAL 8 **bios_resolution_notes*: CPGC Idle Time is set to 0x3F for 2400 to enable back-to-back writes **affected_bios_collateral*: MRC
245829	5002730: keyword replacement **description_repro*: request to use appropriate terminology **bios_resolution_notes*: fixed **affected_bios_collateral*: MRC
245350	5002782, 5002781 : QPI Kahuna Tuning Values: Tx EQ and CTLE Peaking, QPI Inca City Tuning Values: Tx EQ and CTLE Peaking **description_repro*: We have an attached spreadsheet (Arandas_QPI_EQ.xlsx) that has the new Tx EQ and CTLE values for all of the QPI ports. These values need to be programmed for all speeds. **bios_resolution_notes*: Fix: Update the TxEQ and CTLEp for Kahuna platforms for BDX-B0 and above only. **affected_bios_collateral*: QPIRC 5002781: QPI Inca City Tuning Values: Tx EQ and CTLE Peaking **description_repro*: We have an attached spreadsheet (INCA_QPI_EQ.xlsx) that has the new Tx EQ and CTLE values for all of the QPI ports. These values need to be programmed for all speeds. **bios_resolution_notes*: Fix: Update the TxEQ and CTLEp for Inca City platforms for BDX-B0 and above only. **affected_bios_collateral*: QPIRC
245349	5002793 : [BDX-ML] : QPIRC EP-EX- code base sync [22062015] **description_repro*: [BDX-ML] : QPIRC EP-EX- code base sync **bios_resolution_notes*: **affected_bios_collateral*: <Unassigned>
245171	5002693:MRC seeing random bad Rx/Tx Margins **description_repro*: We are seeing bad Rx Margins on some systems under certain configurations, and random 0 margins in RMT. These issues have been seen at 2400 and 2133. This bug(s) are likely going to impede BDX EP broad-scale testing, as we are seeing training failures and random 0 RMT margins that appear for no discernible reason. Checked to see if there is a register/cache mismatch problem when we see bad RxVref margins, but nothing showed up. It seems neither the registers nor the BIOS cache is corrupted. Bad RxVref margins can be seen in Python script and in MRC training, but if running RMT via scratchpad 5, it never shows bad RxVref margins. Then if I run Python RxVref margins again after running RMT, bad RxVref margins are no longer ocurring. It's possible this is a memory corruption failure caused by pointer overflow, as it has many of the same characteristics of

	previous bugs that were root caused to that. **bios_resolution_notes*: RfOn made 0 during MRC training. **affected_bios_collateral*: MRC
244777	5002719 : BDX QPI: Need hvm_mode = 0x10 for LBC 46 WA enhancent on A & L - Step BDX Si **description_repro*: 1. Need hvm_mode = 0x10 with the A-step LBC 46 Work-Around enabled 2. The clear CRC sequence needs to be removed. This is a copy over from BDX EX. This helped to stop the reoccuring Tx DCC cals causing errors during the fast OC WA for A&L-step BDX Si. This is critical. Need this for L0 samples. **bios_resolution_notes*: Fix: Implemented the LBC46WA enhancements by setting hvm_mode=0x10 before the in-band phy resets. **affected_bios_collateral*: QPIRC
244112	5002729: MRC: Idle time change in s5002509 causing failures during Tx Eq training at 2400 with RCD02 **description_repro*: EV has observed failures in BIOS change from 252.D06 to 252.D07 where training fails during Tx Eq due to no margin. This failure has thus far been observed only with RCD02 (Gen 2) RDIMMs and LRDIMMs. The issue was narrowed down by changing imcX_cX_idletime.idle_page_rst_val back to 8 after it was being set to 0x3F in Early Config, and observing the failure go away. Proposed Severity with Justification: High because this has been observed to cause training failures at 2400. **bios_resolution_notes*: Removed the deselect and prevented running CPGC on non-target channels during JEDEC init. **affected_bios_collateral*: MRC 5002509: CPGC Idle Time needs update for 2400 to enable back-to-back writes **description_repro*: CPGC is not able to correctly perform back-to-back writes at 2400 due to the register imcX_cX_idletime.idle_page_rst_val not being set to 0x3F. This value is currently defined to be 0x8 for all speeds in MemDefaults.H: #define IDLE_PAGE_RST_VAL 8 **bios_resolution_notes*: CPGC Idle Time is set to 0x3F for 2400 to enable back-to-back writes **affected_bios_collateral*: MRC
243887	5002726, 5002750 : BDX EP QPI: New Aztec City EQ values for R93 Si, QPI Arandas Tuning Values: Tx EQ and CTLE Peaking **description_repro*: These are the newly optimized settings for QPI. The Tx EQ values should be set this way at all speeds on Aztec City. The Rx CTLE peaking settings apply to 9.6Gb/s only. The settings are in the attachment: QPI_TxEQ_values.xlsx (Aztec City worksheet). The EV to BIOS file: AztecCity_EVtoBIOS_R93_QPI-uniPhyRecipe_v6.00.xls **bios_resolution_notes*: Fix: Update the TxEQ and CTLEp for Aztec City platforms for BDX-B0 and above only. **affected_bios_collateral*: QPIRC 5002750: QPI Arandas Tuning Values: Tx EQ and CTLE Peaking **description_repro*: We have an attached spreadsheet (Arandas_QPI_EQ.xlsx) that has the new Tx EQ and CTLE values for all of the QPI ports. These values need to be programmed for all speeds. **bios_resolution_notes*: Fix: Update the TxEQ and CTLE values for Arandas plaforms for BDX-EP-B0 and onwards. **affected_bios_collateral*: QPIRC
243865	5002694 : QPI MayanCity Tuning Values: Tx EQ and CTLE Peaking **description_repro*: We have an attached spreadsheet (MayanCity_QPI_EQ.xlsx) that has the new Tx EQ and CTLE values for all of the QPI ports. These values need to be programmed for all speeds. **bios_resolution_notes*: Fix: Update the TxEQ and CTLEp for Mayan City platforms for BDX-B0 and above only. **affected_bios_collateral*: QPIRC
243851	5002699 : [Isoc]BDX EP MCC Isoc enable in BIOS **description_repro*: Isoc has been disabled in bios for MCC due to a sighting. Only HCC isoc is enabled. Test bios was provided by Ram to check MCC isoc on the WW15TP parts which had the bug fix. Feedback has been provided and we can enable MCC Isoc in bios now. **bios_resolution_notes*: Fix: Open up isoc configuration for BDX-MCC- chops **affected_bios_collateral*: QPIRC
243431	4988122: MRC to implement maximum (relaxed) latency value support and BIOS setup to expose programmability **description_repro*: MRC to support full range for ALL memory timings (e.g. RAS, CAS...). Please do not limit this artificially. We rely on this for overclocking. **bios_resolution_notes*: found and fixed one place where tCL was being limited to 24.

	affected_bios_collateral: MRC

241471	4988525: BIOS not clearing high memory on a surprise reset
	description_repro: Using a TXT enabled platform, OS, Tboot, boot system Trusted. Using the e820 memory map, write to usable low and high memory range. Perform a surprise reset. Reboot back to Trusted environment and verify both low and high memory ranges are clear. High memory range is not clear:
	>>> itp.threads[0].memdump("0x8e800p",20,4) 0x000000000008E800P: 00000000 00000000 00000000 00000000 0x000000000008E810P: 00000000 00000000 00000000 00000000 0x000000000008E820P: 00000000 00000000 00000000 00000000 0x000000000008E830P: 00000000 00000000 00000000 00000000 0x000000000008E840P: 00000000 00000000 00000000 00000000
	>>> itp.threads[0].memdump("0x380000000p",20,4)
	>>> itp.threads[0].memdump("0x380000000p",20,4) 0x0000000380000000P: deadbeef 00000000 00000000 00000000 0x0000000380000010P: 00000000 00000000 00000000 00000000 0x0000000380000020P: 00000000 00000000 00000000 00000000 0x0000000380000030P: 00000000 00000000 00000000 00000000 0x0000000380000040P: 00000000 00000000 00000000 00000000
	1. From TXT Bios Spec: The Intel TXT for Servers flow when the platform is reset or power cycled with secrets in memory is as follows: 1. Memory Controllers detect this condition and lock memory
	2. The Startup AC Function is invoked before the BIOS reset vector
	3. The Startup AC Function invokes the BIOS Policy Engine. The BIOS Policy Engine will verify if the Startup BIOS Code can be trusted with secrets. See Section 6.7.1.1 for the algorithm.
	4. If Startup BIOS can be trusted, the AC module will unlock memory before the BIOS reset vector gets control. a. BIOS will detect whether memory needs to be scrubbed or not by reading the WAKE-ERROR.STS flag from TXT.ESTS register (Table 6- 2). b. If this bit is set, BIOS must initialize memory and clear all secrets from memory. Prior to checking this bit, BIOS must confirm whether the processor and the chipsets supports Intel TXT.
	bios_resolution_notes: MemInit was being skipped because of the variable host->var.mem.skipMemoryInit. I added code to ignore it if memory needs to be cleared because of secrets.
	affected_bios_collateral: MRC

241270	5002730: keyword replacement *description_repro*: request to use appropriate terminology *bios_resolution_notes*: fixed *affected_bios_collateral*: MRC
241224	5002686: Need to update Ron/ODT for DQ based on volume HVM data *description_repro*: Change following registers for all channels-pairs for DE EP imc_c01_ddrcrcompctl0.dqdrvpupvref = 43 (30 Ohms) imc_c01_ddrcrcompctl0.dqodtpupvref = 38 (50 Ohms) *bios_resolution_notes*: updated Ron/ODT for DQ based on volume HVM data *affected_bios_collateral*: MRC
240880	5002709: oppSR=Disable is not taking effect *description_repro*: Setting the oppSR=Disable is not taking effect. In a 3DPC LRDIMM on socket0 and a 2DPC LRDIMM on a socket1 Memory configuration, with oppSR=Disable, socket0 is coming up with osr disabled and socket1 is coming up as osr enabled. Bios knob is not taking affect on both socket. If we specify oppSR=Disable, all sockets should have OSR disable. Attaching the dimminfo, bios boot log and pull.gbt. *bios_resolution_notes*: The self refresh control field was being overwritten based on an LRDIMM related check. *affected_bios_collateral*: MRC
240305	5002592: BIOS SSA: Need additional margin parameters added to BIOS SSA API *description_repro*: BIOS SSA API does not currently support the following margin parameters: Backside CMD Backside CTL Backside CMD Vref Proposed Severity with Justification: High. These items are needed to test backside Cmd margin for the rev.2 RDIMM/LRDIMM dim. *bios_resolution_notes*: During the process of implementing and testing the backside Cmd/Ctl/CmdVref, found and fixed below list of issues: 1. RxDqs margin test sometimes sent “out of range”message. RxDqs margin parameter limits should be calculated based on both teh ranges of both RxDqsP and RxDqsN. 2. LRDIMM TxVref margin test failed at nominal: DQ margin parameters get/set functions should use GSM_FORCE_WRITE

	| GSM_WRITE_OFFSET 3. CmdVref margin test didn't work: fixed the front side CmdVref margin parameter. 4. ReCEn margin test showed no failure: Increased the range limit to +/-64 5. JedecReset: disable debug message print to not display "N0.C2.D0.R0: Write RC00 = 0x00" message 6. InitParam: Changed the algorithm to match to that was used by the legacy RMT. In particular the order of Setup/Cleanup. Also added a hack to support backside Cmd/Ctl/CmdVref. 7. Fixed memory leakage in the ITP download agent. **affected_bios_collateral*: MRC
238222	5002712: BDAT_Support flag to surround all BSSA related BDAT code plus Spec entry conformity **description_repro*: Schema entry in BDAT_SCHEMA_LIST_STRUCTURE does not conform with the BDAT 4.0 spec entry for the same. //AcpiPlatformLibLocal.h PurleyPcPkg and PurleyRpPkg. BDAT_SUPPORT should surround all BSSA related BDAT code. Proposed Severity with Justification: Medium **bios_resolution_notes*: Schema entry in BDAT_SCHEMA_LIST_STRUCTURE does not conform with the BDAT 4.0 spec entry for the same. //AcpiPlatformLibLocal.h PurleyPcPkg and PurleyRpPkg. BDAT_SUPPORT should surround all BSSA related BDAT code. **affected_bios_collateral*: MRC
238126	5002672: Change patterns from AA to A5 for Basic RxDQS training- Changes reverted for DDR3 DIMMS **description_repro*: Some systems are failing during advance training in MRC. Basic training passes. 2DPC failures need to be addresses. 1DPC is not POR at 2400. BDC system was failing for Ch0. Both of CDC systems fail for Ch1. Failing dimms pass when moved to Ch0. For the first failing system, DQ28 is suspect as it has lowest margin than all other lanes and stands out. Also, DDQ28 has low margin for all 4 ranks. **bios_resolution_notes*: Clock pattern and MPR patterns are changed from AA to A5 for Basic RxDQS training **affected_bios_collateral*: MRC
237580	5002592: BIOS SSA: Need additional margin parameters added to BIOS SSA API **description_repro*: BIOS SSA API does not currently support the following margin parameters: Backside CMD Backside CTL Backside CMD Vref Proposed Severity with Justification: High. These items are needed to test backside Cmd margin for the rev.2 RDIMM/LRDIMM dim. **bios_resolution_notes*: During the process of implementing and testing the backside Cmd/Ctl/CmdVref, found and fixed below list of issues: 1. RxDqs margin test sometimes sent “out of range”message. RxDqs margin parameter limits should be calculated based on both teh ranges of both RxDqsP and RxDqsN. 2. LRDIMM TxVref margin test failed at nominal: DQ margin parameters get/set functions should use GSM_FORCE_WRITE | GSM_WRITE_OFFSET 3. CmdVref margin test didn't work: fixed the front side CmdVref margin parameter. 4. ReCEn margin test showed no failure: Increased the range limit to +/-64 5. JedecReset: disable debug message print to not display "N0.C2.D0.R0: Write RC00 = 0x00" message 6. InitParam: Changed the algorithm to match to that was used by the legacy RMT. In particular the order of Setup/Cleanup. Also added a hack to support backside Cmd/Ctl/CmdVref. 7. Fixed memory leakage in the ITP download agent. **affected_bios_collateral*: MRC
237558	5002633: Need to increase tRFC by 1 cycle at 3200 in order to meet JEDEC spec with t_xsoffset = 0xF **description_repro*: Per t_xsoffset only has 4 bit definition [15:12] in tcsrftp register, the current MRC does not enforce the t_xsoffset limit 0xf, so this could be a problem for overclocking. So the recommendation for BIOS workaround is to cap tXSoffset at 15 and increase tRFC by 1 cycle at 3200 MT/s. Attached discuss mail for reference. Proposed Severity with Justification: Med **bios_resolution_notes*: Added code to max out t_xsoffset at 15 and add 1 to tRFC when running >= 3200. **affected_bios_collateral*: MRC
236601	5002703: ADR related fixes in the latest code **description_repro*: There are a few redundant code in the MRC that needs to be removed for proper ADR resume functionality. **bios_resolution_notes*: Fixed the code in ResetAllDDRChannels() for adr resume. **affected_bios_collateral*: MRC
236094	5002672: Change patterns from AA to A5 for Basic RxDQS training- Changes reverted for DDR3 DIMMS **description_repro*: Some systems are failing during advance training in MRC. Basic training passes. 2DPC failures need to be

	addresses. 1DPC is not POR at 2400. BDC system was failing for Ch0. Both of CDC systems fail for Ch1. Failing dimms pass when moved to Ch0. For the first failing system, DQ28 is suspect as it has lowest margin than all other lanes and stands out. Also, DDQ28 has low margin for all 4 ranks. **bios_resolution_notes*: Clock pattern and MPR patterns are changed from AA to A5 for Basic RxDQS training **affected_bios_collateral*: MRC
235828	5002614: BDX bugeco 282988 Si WA removal is not applicable for BDX-DE V0 stepping **description_repro*: During the ratification of the BDX bugeco 282988 (original HSX bugeco 283282), which is required to be removed for BDX ML B0 and greater stepping only; is actually removed for BDX-DE V0 stepping wrongly. This was introduce with the BIOS HSD 4988208. Proposed Severity with Justification: Critical - This Si WA should not be removed for BDX-DE. Customers may face issue with Grangeville RDIMM platforms. **bios_resolution_notes*: -- WA to be applied for all stepping of DE and HSX. -- WA to be applied for A0 BDX ML only (Reverese WA for B0 and above) **affected_bios_collateral*: MRC
235821	5002651: R0 PKG Delay Tables needed for R0 HEDT power-on **description_repro*: request to check the BIOS to see if these tables were properly integrated **bios_resolution_notes*: Added pkg delay table for R0 **affected_bios_collateral*: MRC
235584	5002678 : [BDX-EP]: 4S COD POR Change : Disable IODC, HitMe$ and 1+ hops DCA accesses for 4S-COD- EP configs **description_repro*: Given the flux of changes around sighting am capturing the final BIOS configuration for clarity. 1. NO changes for non-4SCOD configs 2. For 4S COD: a. IODC disable b. HITME disable c. IVT style OSB enabled d. DCA: 2hop+ disable **bios_resolution_notes*: Fix: When 4S-COD configuration is detected, i] disable HitMe$ (already done by previous HSD), ii] enable IVT- Style OSB (already done by previous HSD), iii] disable DCA for > 1 hops away sockets (addressed here), iv] disable IODC- for EP-SKU only (addressed here) **affected_bios_collateral*: QPIRC
235567	5002459, 5002673 : Need BDX EP BIOS with QPI LBC 56 = 0x2A5C + LBC 59= 0x3F1C, Need BIOS with LBC 57 = 0x28 **description_repro*: We want LBC 56 = 0x2A5C and LBC 59 = 0x3F1C for all speeds. This goes on top of all of the best known test BIOS versions from the QPI task force. Proposed Severity with Justification: This is high severity as we need the validation community to work with these settings. **bios_resolution_notes*: Fix: For BDX-EP- B0 and above, set LBC56 as 0x2A5C and LBC59 as 0x3F1C. This setting is not applied for BDX-A0/A1 which have older values of LBC56 = 0x5C and LBC 59 = 0x3E00 **affected_bios_collateral*: QPIRC 5002673: Need BIOS with LBC 57 = 0x28 **description_repro*: This will turn on the QPI DLL fix for phy resets. This should be included in the same BIOS as LBC 56 = 0x2A5C + LBC 59= 0x3F1C. This is for all QPI speeds. **bios_resolution_notes*: Fix: Set the LBC 57 for BDX-B0- and above to enable the BDX- delta of QPI DLL logic. **affected_bios_collateral*: QPIRC
234796	5002681: Add CL Information related to CCMRC sync **description_repro*: Add CCMRC CL number to the serial console to keep track of the sync information. Proposed Severity with Justification: High **bios_resolution_notes*: Added CL Information related to CCMRC sync. **affected_bios_collateral*: MRC
234793	5002587: BIOS changes are required for enabling CA Parity DIMM isolation on error **description_repro*: The HSD 5002134 talks about the enabling of CADB workaround in BIOS, but here we are not asking for CADB WA. To enable the CA Parity DIMM isolation in hardware, we need certain programming in the MC register (ERF_CMD) and RC5x programming in DIMM. If these are not programmed we would not be getting the correct information from the DIMM in RTL flow. **bios_resolution_notes*: CAP Error isolation implemented **affected_bios_collateral*: MRC
234058	5002579: OEM hook as a means to enable the BIOS SSA Loader **description_repro*: OEM hook meant to be used by customers where they can use it to write their own jumper detection code

	and have it return FALSE when no jumper is present, thereby, blocking calling of the BSSA loader; else have it return TRUE if the concerned jumper is physically present. This check ensures that someone will have to be physically present by the platform to enable the BSSA Loader. Only if this jumper is enabled will the BIOS execute the SSA loader functionality. To enable the 'Jumper' someone will have to be physically be present by the platform to perform this operation. This mechanism prevents the security hole by the loader to a certain extent as physical presence is required for enabling the loader. Proposed Severity with Justification: High. **bios_resolution_notes*: Code changes made to make the SSA loader execute only if the MFG Jumper is present on the platform. Changes Tested on Grantley with the jumper present and absent. It behaves as expected in both cases. Logs attached to the HSD. As of today we have one setup option for BIOS SSA called - BSSA Loader - since loading test content is the only approach to run API content on Broadwell servers this change will disable executing the loader (i.e. in turn the API itself) unless the MFG Jumper is present on the board. **affected_bios_collateral*: MRC
233466	5002570: Seperate build flag for the BIOS SSA Loader **description_repro*: request to have a separate build flag for just the SSA loader (Host and Target) so that this new flag can be used by customers to strip out the SSA loader code if necessary. With this new flag added customers can use it to exclude the SSA loader while continue on including the 'Stitched Mode SSA'. This will also help improve the SSA security feature aspect and block a security hole. As of today the 'SSA_FLAG' build flag surrounds most of the SSA code. The default for the 'loader flag' will be enabled; OEMs can use the flag to strip out loader code as they deem fit. Proposed Severity with Justification: High **bios_resolution_notes*: Changes tested on a Grantley platform. Local minibios, full bios and rc sim builds work fine with the 'SSA_LAODER_FLAG' on and off. GrantleyRefresh full BIOS tree CL229809. **affected_bios_collateral*: MRC

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.8.0 (255.R00) – Beta 1

Release date: May 29th, 2015 (WW22.5)

Revision 1.8.0 - 255.R00

Notes:

None

Potential issues and enhancements (under investigation)**:**

5001999: Fast Cold Boot is broken on BDX DE and EP, Needs Validation

description_repro: Fast Cold Boot does not work on LRDIMMs. From comparing RMT, it appears that Fast Cold Boot does not correctly restore the register and/or BIOS cache values for the LRDIMM backside. The frontside needs to be checked as well.

5002300: [BDX] System asserts when changing QPI link speed from Fast to Slow

description_repro: System asserts when changing QPI link speed from Fast to Slow. It is asserting at check point 0xA7 after printing below debug messages. Issue can be reproduced with Intel Binary based on RC 1.7.0.

Debug Messages:

;******* Check for QPI Topology Degradation - START *******

CPU0 Port1 has inconsistent LEP with Peer socket. Topology Not Supported

z:\a5\broadwell\lb08\lb08_ss\GrantleySocketPkg\Library\MemoryQpiInit\Chip\Qpi\QpiLib.c: 1511 FALSE

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
232536	Updating Grangeville_Trunk BIOS IDs: 20150525_CP_GRANGEVILLE_GRANTLEY_REF_GNV_68_D06_GRT_REF_255_D06
232519	5002622: 3DPC LRDIMM + OSR harasser hits TOR TO and RPQ Entry is stuck *bios_resolution_notes:* OSR is disabled and PPD is forced to APD for 3DPC/3DS LRDIMM Memory config. *affected_bios_collateral:* MRC
232478	5002613: Uncore frequency MSR 620h not restored during S3 resume for BDX B0 or greater stepping *bios_resolution_notes:* BIOS flow for S3 is such that if manual mode is enabled then uncore frequency can be programmed for all CPU stepping's based on uncore knob value provided by user. Where as in AUTO mode, its as per fuse values. Uncore programming for S3 flow is same as what we have in normal BIOS flow. *affected_bios_collateral:* CPURC
232312	5002113: Grantley BIOS incorrectly determine DDR4 8Gb technology capability *bios_resolution_notes:* removed condition to check for DDR3 8Gbit *affected_bios_collateral:* MRC
231726	5002631:Enable CAP DIMM isolation by default *bios_resolution_notes:* CAP DIMM isolation is enabled by default for BDX-EP. *affected_bios_collateral:* MRC
231328	5002649 : [BDX-EP-] : Update QPIRC- to QpiRcSimGtlRf21052015 [EX->EP] *bios_resolution_notes:* Fix: Performed the sync of code base from EX -> EP for general development activity. This need not need to release notes though there are code changes associated. *affected_bios_collateral:* QPIRC

229809	5002570: Seperate build flag for the BIOS SSA Loader *bios_resolution_notes:* new SSA_LOADER_FLAG was added *affected_bios_collateral:* MRC
229536	5002584: BIOS needs to set bit 25 in MSR 0x1FC when enabling HWP autonomous out of band mode *bios_resolution_notes:* BIOS needs to set bit 25 in MSR 0x1FC when enabling HWP autonomous out of band mode (OOB mode). BIOS has existing knob PwrPerfTuning knob to change bit25 in 0x1FC. BIOS needs to set bit 25 in MSR 0x1FC when enabling HWP autonomous out of band mode (OOB mode) irrespective of PwrPerfTuning setting by user. *affected_bios_collateral:* CPURC
228748	5002522: BDX B0 PO: Request for test BIOS with DDR clock gating & Vccpq ramp down disabled during PC6 *bios_resolution_notes:* ddrcrclkranksused.disablepc6fix bit made 0 for all B0 SKUs of BDX EP in InitDdrioInterface() *affected_bios_collateral:* MRC
227637	5002028: Enable BIOS SSA as a runtime BIOS option instead of a build option *bios_resolution_notes:* Changes checked in CL 227637. New SSA_LOADER_FLAG was added. *affected_bios_collateral:* MRC
226293	4987134 [HSX-BDX] ENHANCE: CPUCSRACCESS RUNTIME DRIVER *bios_resolution_notes:* driver function "GetCpuCsrAddress", previously only returns 32-bit address. It was modified to return 64-bit address to satisfy the 64-bit virtual mode addressing *affected_bios_collateral:* CPURC
226218	5002567: Memory frequency 2933 incorrectly listed as 2993 in setup menu *bios_resolution_notes:* Fixed Memory frequency 2933 incorrectly listed as 2993 in setup menu *affected_bios_collateral:* MRC
226207	5002587: BIOS changes are required for enabling CA Parity DIMM isolation on error *bios_resolution_notes:* CAP Error isolation implemented *affected_bios_collateral:* MRC
226190	5002572: RxDqs Backside Training printing out fake errors *bios_resolution_notes:* Fixed RxDqs Backside Training printing fake errors *affected_bios_collateral:* MRC
226189	5002228: Parallel MRC Init disabled by default; Enable parallel MRC and fix any related issues *bios_resolution_notes:* Enabled multithreaded MRC *affected_bios_collateral:* MRC
225718	5002499: TCSTAGGER_REF_MCDDC bits being accessed in MemTiming are missing the LRDIMM flag *bios_resolution_notes:* this WA is needed only until B0 silicon. Changes checked in CL225718. *affected_bios_collateral:* MRC
225072	5002579: Manufacturing Jumper as a requirement to enable the BIOS SSA Loader *bios_resolution_notes:* Code changes made to make the SSA loader execute only if the MFG Jumper is present on the platform. Changes Tested on Grantley with the jumper present and absent. It behaves as expected in both cases. Logs attached to the HSD. As of today we have one setup option for BIOS SSA called - BSSA Loader - since loading test content is the only approach to run API content on Broadwell servers this change will disable executing the loader (i.e. in turn the API itself) unless the MFG Jumper is present on the board. *affected_bios_collateral:* MRC

223776	5001675 [HSX-BDX] - Update RC to use new P1 pcode feature *bios_resolution_notes:* BIOS sends b2p mailbox command, SET_CORE_RING_RATIO, code 0xa4. This logically shares some functionality with the enhanced adr flow, so Parameters are bits 7:0 are core ratio, bits 15:8 are the uncore ratio. The ratios commanded through this command only hold until we hit CPL3, when the normal PM control mechanisms wake up. BIOS sends the mailbox to command core/uncore ratios to 0x20 sv.socket0.uncore0.pcu_cr_bios_mailbox_interface=0x802020a during SEC phase which is very early BIOS phase just after loading micro code on BSPs. BIOS support is added A1 CPU onwards as CLR issue encountered on previous BDX stepping's. *affected_bios_collateral:* CPURC
223624	5002509:CPGC Idle Time needs update for 2400 to enable back-to-back writes *bios_resolution_notes:* CPGC Idle Time is set to 0x3F for 2400 to enable back-to-back writes *affected_bios_collateral:* MRC
223416	5002238: Implement LRDIMM Rx/Tx Skew Reduction Changes *bios_resolution_notes:* Implement LRDIMM Rx/Tx Skew Reduction Changes *affected_bios_collateral:* MRC
223157	5002577: Integrate production ucode patch 0x10 in to Grantley Refresh BIOS trunk *bios_resolution_notes:* Integrated production microcode patch 0x10 for BDX-EP A0/A1. *affected_bios_collateral:* CPURC
222987	5002451: ADDENDUM: Upgrade the CSR Header files with B0 TO model ConfigDb (Compatibility changes for V0/V1) *bios_resolution_notes:* The CL 213831 covers the new CSR header merge for BDX mainline B0 and beyond. The CL 222987 covers the compatibility of this CSR header merge for BDX-DE V0/V1. *affected_bios_collateral:* CPURC,MRC,QPIRC
222596	5002539: Sync Latest CCMRC tree(15ww17) into the BDX-EP/DE source tree *bios_resolution_notes:* CCMRC sync completed *affected_bios_collateral:* MRC
222167	5002415 : [4S-EP]: HITME Enable causing COD-4S boot fail with TOR TO in DXE phase *bios_resolution_notes:* Enforce the new POR mode (Home Snoop with Directory and OSB, HitMe is disabled and IVT- Style OSB-settings) when 4S-COD configuration is detected. *affected_bios_collateral:* QPIRC
221722	5002482: CRB BIOS randomly erasing MRC BIOS cache, probably due to pointer overflow *bios_resolution_notes:* a pointer overflow was located in BIOS. The array 'rankList' to be 4 cells long, and then write 8 values to it. Fix was checked-in. *affected_bios_collateral:* MRC
221527	5002524 : BDX-EP QPI Agent DEVHIDE not matching with HSX *bios_resolution_notes:* Fix: Unhidden all the QPIDEVHIDEs in line with Grantley-HSX- leaving the IioMiscHide() to have full control on QPI related DEVHIDEs. *affected_bios_collateral:* QPIRC

219311	5002488: MemStart update to setup change check list *bios_resolution_notes:* 'iotMemBufferRsvtn' and 'enableBiosSsaLoader' are missing from the setup menu changes check list in MemStart. These need to be added in. Also move defining the 'EV_STITCHED_CONTENT_ENBL' macro from MrcSsaServices.c to BiosSsaChipFunc.h to enable its usage across multiple C files as is the case after the core merge. SsaStichedModeRMTChip requires this macro for conditional compilation. SsaStichedModeRMTChip will exist as an empty function on BDX while on SKX its functionality is present. *affected_bios_collateral:* MRC
219309	5002519: Persitent memory changes in the BIOS for Core Package 3.2.0 *bios_resolution_notes:* *affected_bios_collateral:* <Unassigned>
219002	5002293: [HSX] DDR3 UDIMM CLK RComp Values Incorrect *bios_resolution_notes:* DDR3 UDIMM CLK RComp values modified with correct values for HSX BIOS. *affected_bios_collateral:* MRC
218561	5001933: ACC x S3 causing GP *bios_resolution_notes:* We use APIs S3BootScriptSaveMemWrite for saving CSRs and WriteRegisterTable for MSRs writes during S3 resume. MSRs write is done before CSRs during S3 resume. So implementing Si Workaround which programs ACC bit after RST_CPL4 needs EDK2 support. Waiting for EDK2 support to try out this workaround,solution implemented as follows- (1) Do not save the MSR ACC bit in S3 boot script (2) Write a post S3 resume callback routine which gets invoked once all the S3 boot script execution is completed during S3 resume flow (3) In that callback routine enable the ACC bit in MSR *affected_bios_collateral:* CPURC
218108	5002414 : Unable to boot with A0 using 247V11 - Addendum v1 *bios_resolution_notes:* Enhanced the workaround algorithm to have phy-resets back to back so that delays can be reduced instead of issuing one phy-reset and assert when the links fail to train back. *affected_bios_collateral:* QPIRC
217604	5001795 : [HSX-BDX] Requesting COD mode with concurrent support for ME traffic (VCM) *bios_resolution_notes:* Fix: Permit the configuration of MeSeg with COD- feature for 1S - 2SEP configs. When isoc is disabled, set vc1_pri_en is zero and priority as zero. *affected_bios_collateral:* QPIRC
217559	5002358: [QPI-EP]: For all EP Grantely BIOS Only & for Latest WW07 TP Parts Onwards QPI speed should be moved to 9.6GT/s *bios_resolution_notes:* Fix: Remove the override which caps the QpiLinkSpeed to 8.0 GT/s for Aztec City. This will boot with 9.6 GT/s as default (POR- config as in HSX-). Implication: Users are advised to use WW07TP parts without which BIOS 250.D07 and future BIOS will not boot. *affected_bios_collateral:* Other Chipset Ref Code 5002464: [Isoc] Enable isoc knob by default on HEDT and WS SKUs *bios_resolution_notes:* Fix: Removed the override which disabled Isoc on Aztec City and HEDT- (in both of these platforms, enabling Isoc is POR- config). Implication: Users must use BDX-HCC-A1 or later parts to see isoc getting enabled. Also, for BDX-MCC- parts, isoc is disabled due to requirement of PIF- applied parts. *affected_bios_collateral:* Other Chipset Ref Code,QPIRC 5002465: [Isoc]: Isoc support restricted to <=20 CBOs *bios_resolution_notes:* Fix: Disabled isoc when SKUs are populated which has more than 20 Cbos. *affected_bios_collateral:* QPIRC

217015	5002414 : Unable to boot with A0 using 247V11 *bios_resolution_notes:* Enhanced the workaround algorithm to have phy-resets back to back so that delays can be reduced instead of issuing one phy-reset and assert when the links fail to train back. *affected_bios_collateral:* QPIRC
216360	5001954: BIOS not restoring RAS features on S3 resume *bios_resolution_notes:* Runtime access is enabled for the Memconfig variables in MemRasS3Save.c and S3NvramSave.c which makes proper S3 restoration. *affected_bios_collateral:* MRC
214727	5002448:SDP: PCI Express Slot become Non-functional with BIOS 246R01 *bios_resolution_notes:* The changes done here was backing out inclusion of TPM1.asi file in PchLpc.asi that was added for a new feature support for RHEL and this was done only for SDP. Since that check-in was the reason for other windows driver issues for SDP, it was determined by SDP team to backout the TPM1.asi changes for now, till we get windows support for the same feature. *affected_bios_collateral:* Binary ROM (External),Binary ROM (Internal)
214636	4987872: [HSX-BDX] eMCA review - Fatal error floe should check MCA_SRC_ERR_LOG.msmi_ierr_internal(bit 19) on all sockets *bios_resolution_notes:* checking the msmi_ierr_internal(bit 19) in MCA_SRC_ERR_LOG register *affected_bios_collateral:* BIOS Core Issue
214347	5001637: [CCB] Extend Intel® ASA1.0 support to Broadwell server 2S and 4S EP SKUs *bios_resolution_notes:* The DEBUG_INTERFACE knob has been enabled by default. This will make BIT0 of the IA32_DEBUG_INTERFACE MSR (0xC80) to be set if it is not set already. This is required for supporting Intel's ASA feature. *affected_bios_collateral:* CPURC
213866	5002451: Upgrade the CSR Header files with B0 TO model ConfigDb (code indentationm fix) *bios_resolution_notes:* The CL 213831 covers the new CSR header merge for BDX mainline B0 and beyond. The CL 222987 covers the compatibility of this CSR header merge for BDX-DE V0/V1. *affected_bios_collateral:* CPURC,MRC,QPIRC
213831	5002451: Upgrade the CSR Header files with B0 TI ConfigDb *bios_resolution_notes:* The CL 213831 covers the new CSR header merge for BDX mainline B0 and beyond. The CL 222987 covers the compatibility of this CSR header merge for BDX-DE V0/V1. *affected_bios_collateral:* CPURC,MRC,QPIRC
213734	5002241: Set final CMD Stretch in CMD Vref Training for better robustness if training in 2n/3n *bios_resolution_notes:* Set final CMD Stretch in CMD Vref Training for better robustness *affected_bios_collateral:* MRC
213187	5002471: [BDX EP] - PPR flow always fails on slot1 with 1ch 2dpc cfg *bios_resolution_notes:* Bug in handling rankid for PPR CPGC patterns resulting in DIMM1 PPR failures fixed. Minor display bug causing invalid row addr to be printed is also fixed with this change. *affected_bios_collateral:* MRC
212629	5002353: tcrwp.t_rwsr getting set incorrectly for DDR4 LRDIMMs, degrading backside Rx eye on ranks 2/3 *bios_resolution_notes:* tcrwp.t_rwsr getting set incorrectly for DDR4 LRDIMMs, *affected_bios_collateral:* MRC

212614	5002240: Advanced Backside Training does not support encoded mode *bios_resolution_notes:* added support in Advanced Backside Training in encoded mode *affected_bios_collateral:* MRC
212573	5002468: BDX-EP -patch integration production version mef406f0_0000000d *bios_resolution_notes:* Included the ucode revision mef406f0_0000000d *affected_bios_collateral:* CPURC
212034	5002446:[BDX EP] - CH2/3 errors are logged on CH0/1 for PPR *bios_resolution_notes:* There was a mismatch in the CH id interpretation in error handler and the MRC. RAS Error handler reports the CHID in MC view, i.e., CH0/1. MRC interpreted the CHID in SKT view CH0/1/2/3. So injecting error in CH2/3 would be logged as CH0/1 in Error handler. The fix is to add the MCID to the PPR error structure and update MRC to use MCID and CHID to get the SKT CHID. *affected_bios_collateral:* MRC
211846	5002424: BIOS SSA setup option renaming to BiosSsaLoader *bios_resolution_notes:* BIOS SSA setup option name was renamed *affected_bios_collateral:* MRC
211597	5002315: DisplayMRS() only prints out results for 9 DRAMs on LRDIMMS *bios_resolution_notes:* DisplayMRS() is modified to print results for 18 DRAMs. *affected_bios_collateral:* MRC
211581	5002151: BDX-EP : OCLA IOT ways enabling needs NEM ways vs Slice count table for ML (Design Input) *bios_resolution_notes:* Added Slice Count vs NEM way usage table for BDX for 24 CBO slice count *affected_bios_collateral:* CPURC
211580	5002255: Power Training, Per-bit Deskew, Per-bit RMT, and Backside Training Register Dump do not work correctly in encoded mode *bios_resolution_notes:* Training Register Dump print issues fixed. *affected_bios_collateral:* MRC
211579	5002412:[BDX_EP] - WR_CRC option handling is buggy - mem.options used in some place and mem.optionsExt used in some *bios_resolution_notes:* setup.mem.options is replaced with setup.mem.optionsExt while using WR_CRC option. *affected_bios_collateral:* MRC
209972	5002440:Integrate BDX -EP Debug patch mef406f0_8000200d to BIOS *bios_resolution_notes:* Debug patch mef406f0_8000200d included into BIOS *affected_bios_collateral:* CPURC
209653	5002276: System stuck in MRC when enable Fast Cold Boot and disable Multi-thread MRC - Grantley MRC v1.12 *bios_resolution_notes:* The BDX EP parts under test are not PPIN capable as from the data received from 'MSR_PLATFORM_INFO, BIT23', hence, the 'fast cold boot option' path cannot be followed. Fixed was checked-in. *affected_bios_collateral:* MRC
208941	5002386: QPI CRC errors and incorrect uniphy recipe on EP4S station with ES2 parts *bios_resolution_notes:* Fix: Verify ep_2s bit OR ep_4s bit for applying the EP- UniPhy recipe instead of checking only ep_2s. Pre-ES2 CAPID0[3:0]=0xC is incorrect and this was fixed in ES2 parts as CAPID0[3:0]=0x8. This is the reason this failure was not seen during PO- activities until now. *affected_bios_collateral:* QPIRC

208940	5002377: EP-ES2 QHU0 SKU - QPI speed for this SKU should be clipped at 6.4GTS since OC is enabled *bios_resolution_notes:* Fix: Whenever a part with CAPID4[28] oc_enabled is observed by the BIOS, clip the QPI link speed to 6.4 GT/s. *affected_bios_collateral:* QPIRC
208938	5002387: QPI Drift buffer overrun errors with PkgC6 sensitive to LBC 56 0x2A5C fix on certain SKU's *bios_resolution_notes:* Fix:- 1. Updated LBC 56 to 0x5C for EP- and 0x2A5C for EX 2. Updated the uniPhy sheet to v5.0 - lcampen is set to 1 for all QPI speeds for EP-. *affected_bios_collateral:* QPIRC
207547	5002295: Per-bit RMT results do not match per-rank RMT *bios_resolution_notes:* CCMRC code changes are synced to BDX trunk for this fix. *affected_bios_collateral:* MRC
207036	5002385: PackageCState/C6Enable/C3Enable/ProcessorC1eEnable should be as per POR values *bios_resolution_notes:* PackageCState/C6Enable/C3Enable/ProcessorC1eEnable is as per POR values PackageCState-->c6 retention C3Enable->disabled C6Enable-->Enabled ProcessorC1eEnable -->Enabled *affected_bios_collateral:* CPURC
206291	5001677:HSX-BDX] - BIOS programming value too large for .t_xpdll *bios_resolution_notes:* .t_xpdll value limited to 31(5 bits) if the value is greater than 31 *affected_bios_collateral:* MRC
206276	5002247: Changes to CTLEP Values for QPI *bios_resolution_notes:* We need the value of 0x1E03 in Uniphy Load Bus address 46. This is to enable stage 1 CTLE peaking to the correct values for full speed, CFO (1/2 speed), and slow mode. LBC 46 gets cleared in warm-reset. To WA this, BIOS sets this register in warm-reset path and does a reset on all links to get this LBC 46 value re-applied again. This would be done in all warm-reset paths. *affected_bios_collateral:* QPIRC
206228	5001936: CPGC Row Hammer tool modification to deliver 33% more hammers *bios_resolution_notes:* CPGC Row Hammer tool modification to enhance hammering *affected_bios_collateral:* MRC
205739	5002348: Set en_pgta2=0 for 2DPC 3DS systems. *bios_resolution_notes:* en_pgta2 set to 0 for all 3DS LRDIMM configurations *affected_bios_collateral:* MRC
205738	5002340: Imode is not running after enabling in Bios setup *bios_resolution_notes:* Fixed bug in iMODE setup option handling; IMODE enable/disable setup option now enables/disables IMODE training step. *affected_bios_collateral:* MRC
205594	5002317: Power Training only setting rank 0 registers on LRDIMMs *bios_resolution_notes:* fixed Power Training only setting rank 0 registers on LRDIMMs *affected_bios_collateral:* MRC

205301	5002380: SODIMM support broken in MRC. *bios_resolution_notes:* incorrect SPD byte decoding fixed *affected_bios_collateral:* MRC
205154	4988335: [BDX-EP] - Add PPR (Post Package Repair) support *bios_resolution_notes:* Support for Soft and Hard PPR implemented. Two new options have been added pprType (Disabled / Hard / Soft PPR) and pprErrInjTest (Enable / Disable). To test PPR, enable the following options in BIOS setup; save and reboot to EFI shell / OS: System Errors = Enabled EMCA Logging Support = Enabled EMCA CMCI-SMI Morphing = Enabled PPR Type = Hard PPR or Soft PPR PPR Error Injection test = Enabled *affected_bios_collateral:* MRC
205136	5002355: Sync CCMRC to Grantley refresh trunk *bios_resolution_notes:* MRC sync with CCMRC A *affected_bios_collateral:* MRC
205015	5002370: HSX Synch Grantley 46R00 merge to BDX *bios_resolution_notes:* HSX to BDX merge for CR_17579 *affected_bios_collateral:* CPURC
204662	5002118 : Switch default 2s snoop mode to Dir + ivt style OSB (no CoD) *bios_resolution_notes:* Implemented IVT- Style OSB w/o HitMe but w/ osbrmt and osblord set as the default POR- mode for non-isoc based 2S- configs *affected_bios_collateral:* QPIRC
204070	5002355: Sync CCMRC to Grantley refresh trunk *bios_resolution_notes:* MRC sync with CCMRC A *affected_bios_collateral:* MRC

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.3 (251.R01) – Alpha 4

Release date: May 5th, 2015 (WW19.2)

Revision 1.7.3 - 251.R01

Notes:

None

Potential issues and enhancements (under investigation)**:**

Log.ID	Description
4988239	DDR3 MayaCity hangs up in MRC when Enable Fast Cold Boot with 2DPC QRx4 DDR3 RDIMM.
5001646	(BIOS only enable COD on parts with at least 10 cores) LCC derived from MCC is enabling COD and also imbalance configuration
5001665	(MRC XMP DIMM discovery not MP safe) System stuck at CP:0xB7(Ddr4LrdimmBacksideTxCoarseWL) while mixing LRDimm vendor on CPU0 1
5001670	BDX: (MemRAS.c SyncronizeTimings) 32GB LRDIMM DIMM lost during DC power cycling with Advance ECC mode and mirror mode
5001922	[QPI]: All Full speeds PhyReset produces Drift Buffer Uncorrectable Errors at all
5001946	SBE on LRDIMM cause system hang
5002420	SDP: BDW does not boot with 32GB dimm part

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
222010	5002566: Modify the Reference code revision for EP to 1.73 bios_resolution_notes: affected_bios_collateral: <Unassigned>
220992	5002426 : SDP: Request to expose Snoop options in all future BIOS release bios_resolution_notes: Fix: Exposed the SnoopMode, IoDcEn and HitMe as SDP knobs and modified the QPIRC- to consume these values. These knobs are now available under "Advanced -> QPI Configuration -> QPI General Configuration" for SDP- images. affected_bios_collateral: Other Chipset Ref Code,QPIRC
220355	5001868 : Add VccU voltage control to enable higher Ring freq OC on BDX-E bios_resolution_notes: affected_bios_collateral: <Unassigned> 4988124: Combine IOA/IOD,SA voltage into one option and clarify help text. bios_resolution_notes: affected_bios_collateral: <Unassigned> 4987885: VCO PLL PDIV vCode support to mitigate BCKL issue bios_resolution_notes: affected_bios_collateral: <Unassigned> 4987305: VCCIN override not working properly. Actual voltage does not reflect request bios_resolution_notes: affected_bios_collateral: <Unassigned>

219311	5002488: MemStart update to setup change check list bios_resolution_notes: 'iotMemBufferRsvtn' and 'enableBiosSsaLoader' are missing from the setup menu changes check list in MemStart. These need to be added in. Also move defining the 'EV_STITCHED_CONTENT_ENBL' macro from MrcSsaServices.c to BiosSsaChipFunc.h to enable its usage across multiple C files as is the case after the core merge. SsaStichedModeRMTChip requires this macro for conditional compilation. SsaStichedModeRMTChip will exist as an empty function on BDX while on SKX its functionality is present. affected_bios_collateral: MRC
219309	5002519: Persitent memory changes in the BIOS for Core Package 3.2.0 bios_resolution_notes: affected_bios_collateral: <Unassigned>
219002	5002293:[HSX] DDR3 UDIMM CLK RComp Values Incorrect bios_resolution_notes: DDR3 UDIMM CLK RComp values modified with correct values for HSX BIOS. affected_bios_collateral: MRC
218737	5002526: ADR failing during memory writes bios_resolution_notes: affected_bios_collateral: <Unassigned>
218561	5001933: ACC x S3 causing GP bios_resolution_notes: We use APIs S3BootScriptSaveMemWrite for saving CSRs and WriteRegisterTable for MSRs writes during S3 resume. MSRs write is done before CSRs during S3 resume. So implementing Si Workaround which programs ACC bit after RST_CPL4 needs EDK2 support. Waiting for EDK2 support to try out this workaround,solution implemented as follows- (1) Do not save the MSR ACC bit in S3 boot script (2) Write a post S3 resume callback routine which gets invoked once all the S3 boot script execution is completed during S3 resume flow (3) In that callback routine enable the ACC bit in MSR affected_bios_collateral: CPURC
218108	5002414 : Unable to boot with A0 using 247V11 - Addendum v1 bios_resolution_notes: Enhanced the workaround algorithm to have phy-resets back to back so that delays can be reduced instead of issuing one phy-reset and assert when the links fail to train back. affected_bios_collateral: QPIRC
217604	5001795 : [HSX-BDX] Requesting COD mode with concurrent support for ME traffic (VCM) bios_resolution_notes: Fix: Permit the configuration of MeSeg with COD- feature for 1S - 2SEP configs. When isoc is disabled, set vc1_pri_en is zero and priority as zero. affected_bios_collateral: QPIRC
217559	5002358, 5002464, 5002465 : [QPI-EP]: For all EP Grantely BIOS Only & for Latest WW07 TP Parts Onwards QPI speed should be move to 9.6GT/s, [Isoc] Enable isoc knob by default on HEDT and WS SKUs, [Isoc]: Isoc support restricted to <=20 CBOs bios_resolution_notes: Fix: Remove the override which caps the QpiLinkSpeed to 8.0 GT/s for Aztec City. This will boot with 9.6 GT/s as default (POR- config as in HSX-). Implication: Users are advised to use WW07TP parts without which BIOS 250.D07 and future BIOS will not boot. affected_bios_collateral: Other Chipset Ref Code 5002464: [Isoc] Enable isoc knob by default on HEDT and WS SKUs bios_resolution_notes: Fix: Removed the override which disabled Isoc on Aztec City and HEDT- (in both of these platforms, enabling Isoc is POR- config). Implication: Users must use BDX-HCC-A1 or later parts to see isoc getting enabled. Also, for BDX-MCC- parts, isoc is disabled due to requirement of PIF- applied parts. affected_bios_collateral: Other Chipset Ref Code,QPIRC 5002465: [Isoc]: Isoc support restricted to <=20 CBOs bios_resolution_notes: Fix: Disabled isoc when SKUs are populated which has more than 20 Cbos. affected_bios_collateral: QPIRC

217015	5002414 : Unable to boot with A0 using 247V11 bios_resolution_notes: Enhanced the workaround algorithm to have phy-resets back to back so that delays can be reduced instead of issuing one phy-reset and assert when the links fail to train back. affected_bios_collateral: QPIRC
216360	5001954:Clone from BDX Sighting:BIOS not restoring RAS features on S3 resume bios_resolution_notes: Runtime access is enabled for the Memconfig variables in MemRasS3Save.c and S3NvramSave.c which makes proper S3 restoration. affected_bios_collateral: MRC
215157	5002477:Integrate BDX-ML-B0 Debug signed Patch mef406f1_b0000001 bios_resolution_notes: Inclusion on B0 stepping PO patch into BIOS. affected_bios_collateral: Binary ROM (External),Binary ROM (Internal),CPURC
214347	5001637: [CCB] Extend Intel? ASA1.0 support to Broadwell server 2S and 4S EP SKUs bios_resolution_notes: The default value of DEBUG_INTERFACE knob has been set to "Enabled" to support Intel's ASA feature. affected_bios_collateral: CPURC
213866	5002451: Upgrade the CSR Header files with B0 TO model ConfigDb (code indentationm fix) bios_resolution_notes: The CL 213831 covers the new CSR header merge for BDX mainline B0 and beyond. The CL 222987 covers the compatibility of this CSR header merge for BDX-DE V0/V1. affected_bios_collateral: CPURC,MRC,QPIRC
213831	5002451: Upgrade the CSR Header files with B0 TI ConfigDb bios_resolution_notes: The CL 213831 covers the new CSR header merge for BDX mainline B0 and beyond. The CL 222987 covers the compatibility of this CSR header merge for BDX-DE V0/V1. affected_bios_collateral: CPURC,MRC,QPIRC
213734	5002241: Set final CMD Stretch in CMD Vref Training for better robustness if training in 2n/3n bios_resolution_notes: Set final CMD Stretch in CMD Vref Training for better robustness affected_bios_collateral: MRC
213187	5002471:[BDX EP] - PPR flow always fails on slot1 with 1ch 2dpc cfg bios_resolution_notes: Bug in handling rankid for PPR CPGC patterns resulting in DIMM1 PPR failures fixed. Minor display bug causing invalid row addr to be printed is also fixed with this change. affected_bios_collateral: MRC
212635	5002383: After latest CCMRC sync, one-line code changes needed bios_resolution_notes: Correction to use the right API in MRC affected_bios_collateral: MRC
212629	5002353: tcrwp.t_rwsr getting set incorrectly for DDR4 LRDIMMs, degrading backside Rx eye on ranks 2/3 bios_resolution_notes: tcrwp.t_rwsr getting set incorrectly for DDR4 LRDIMMs, affected_bios_collateral: MRC
212614	5002240: Advanced Backside Training does not support encoded mode bios_resolution_notes: added support in Advanced Backside Training in encoded mode affected_bios_collateral: MRC
212034	5002446: [BDX EP] - CH2/3 errors are logged on CH0/1 for PPR
211846	5002424: BIOS SSA setup option renaming to BiosSsaLoader
211597	5002315: DisplayMRS() only prints out results for 9 DRAMs on LRDIMMS
211581	5002151 : BDX-EP : OCLA IOT ways enabling needs NEM ways vs Slice count table for ML (Design Input)
211580	5002255: Power Training, Per-bit Deskew, Per-bit RMT, and Backside Training Register Dump do not work correctly in encoded mode
211579	5002412: [BDX_EP] - WR_CRC option handling is buggy - mem.options used in some place and mem.optionsExt used in some
210887	5002407: ppd.bar45_32bit is getting set without even enabling the NTB mode
210473	5002110: WHEA Error Injection is disabling Patrol scrubbing
209653	5002276: System stuck in MRC when enable Fast Cold Boot and disable Multi-thread MRC - Grantley MRC v1.12

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.2 (246.R01) – Alpha 3

Release date: April 1st, 2015 (WW14.3)

Revision 1.7.2 - 246.R01

Notes:

None

Potential issues and enhancements (under investigation)**:**

Log.ID	Description
4988239	DDR3 MayaCity hangs up in MRC when Enable Fast Cold Boot with 2DPC QRx4 DDR3 RDIMM.
4988572	BDX CRB bios fails MRC when setting to 2400
5001646	(BIOS only enable COD on parts with at least 10 cores) LCC derived from MCC is enabling COD and also imbalance configuration
5001665	(MRC XMP DIMM discovery not MP safe) System stuck at CP:0xB7 (Ddr4LrdimmBacksideTxCoarseWL) while mixing LRDimm vendor on CPU0 1
5001670	(MemRAS.c SyncronizeTimings) 32GB LRDIMM DIMM lost during DC power cycling with Advance ECC mode and mirror mode
5001903	[H] MemRas.c indexes out of bounds on the mMemRas->SystemMemInfo->MemSetup.imc array
5001922	[QPI]: All Full speeds PhyReset produces Drift Buffer Uncorrectable Errors at all
5001946	SBE on LRDIMM cause system hang

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
208919	5002416: TOR Timeout with C-states enabled on ES2 SKUs QHUY and QHUZ bios_resolution_notes: code added to CpuInit.c to program the uncore ratio based on processor SKU. affected_bios_collateral: <Unassigned>

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.1 (246.R00) – Alpha 2

Release date: Mar 20th, 2015 (WW12.5)

Revision 1.7.1 - 246.R00

Notes:

- Package C6 is disabled by default in the BIOS.
-

Potential issues and enhancements (under investigation)**:**

Log.ID	Description
4988239	DDR3 MayaCity hangs up in MRC when Enable Fast Cold Boot with 2DPC QRx4 DDR3 RDIMM.
4988572	BDX CRB bios fails MRC when setting to 2400
5001646	(BIOS only enable COD on parts with at least 10 cores) LCC derived from MCC is enabling COD and also imbalance configuration
5001665	(MRC XMP DIMM discovery not MP safe) System stuck at CP:0xB7 (Ddr4LrdimmBacksideTxCoarseWL) while mixing LRDimm vendor on CPU0 1
5001670	(MemRAS.c SyncronizeTimings) 32GB LRDIMM DIMM lost during DC power cycling with Advance ECC mode and mirror mode
5001903	[H] MemRas.c indexes out of bounds on the mMemRas->SystemMemInfo->MemSetup.imc array
5001922	[QPI]: All Full speeds PhyReset produces Drift Buffer Uncorrectable Errors at all
5001946	SBE on LRDIMM cause system hang

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
203878	Updating Grangeville_Trunk BIOS IDs: 20150318_CP_GRANGEVILLE_GRANTLEY_REF_GNV_59_D13_GRT_REF_246_D13
202944	5002305: Add new BIOS/MRC setup option to disable backside RMT by default bios_resolution_notes: Changes checked in for CL 202944. Changes made to have a setup option for backside RMT. By default backside RMT is disabled from the INT and EXT BIOS. affected_bios_collateral: MRC
202821	5002062: Grangeville- CCMRC - Disable/Enabling the Debug message in MRC code. bios_resolution_notes: Build issues related to SERIAL_DBG_MSG are fixed. affected_bios_collateral: MRC
202112	5002316: Caching bug preventing CLKs from being disabled bios_resolution_notes: Caching bug in InitDdrioInterface() of MemIOCOntrol.C affected_bios_collateral: MRC
201803	5002331: Enable different modes of serial debug message level via a scratchpad for the PPV BIOS bios_resolution_notes: Changes made and tested for BDX EP on a Mayan. Setting scratchpad6 bits 0&1 to the desired debug message level works as expected. 00 - DIS, 01 - MIN, 10 - NOR, 11 - MAX affected_bios_collateral: MRC
201576	5002104: BIOS MRC Print Fixes for N-ECC mode bios_resolution_notes: Training Register Dump print fixes are done for N-ECC DIMMS. affected_bios_collateral: MRC

201232	5001676: WA s5097785 QPI Drift Buffer Overrun UC bios_resolution_notes: Enable pkg C6 state by Default in BIOS. Earlier We had seen Klaxcon errors after enabling C6 and windows boot had issues so BIOS had disabled C6 by default. Since its working now with Latest pcode. We enabled it by default. We have added BIOS WA to enable C6 by default to QPI Link speed 9.6 issue with C6 enabled, as below: 1. QpiLinkL1En to 0x0 2. PkgCstEntryValCtl, clear BIT25, 26, 27 from where QPI L1 criteria is taken out. 3. C6Enable knob is set 0x1 affected_bios_collateral: <Unassigned>
201013	5002335: Update the syshost.h with latest BDX-EP collateral revision i.e. 1.71 bios_resolution_notes: affected_bios_collateral: <Unassigned>
199935	5002244: Fix RxEnable Offset in 2:2 mode bios_resolution_notes: TX_PER_BIT_SETTLE_TIME, TxPerBitSetup2to2Offset, X_OVER_OFFSET_2TO2_RCVEN and X_OVER_OFFSET_2TO2_TXDQS offsets are changed affected_bios_collateral: MRC
199290	5002259: Eliminate Rx per-bit re-training in RMT bios_resolution_notes: RxPerBitDeskew() is eliminated from RMT in MemMargins.c affected_bios_collateral: MRC
198043	Moving to Production Patch 8 for R label
197471	5002235: Memory requests only sent to 2 channels with 4 channels populated bios_resolution_notes: Added the missing snippet during porting. affected_bios_collateral: MRC
196942	5001905: REQ to integrate the new Memory weight table for SODIMM into BDX-DE BIOS bios_resolution_notes: Integrated the new power weights affected_bios_collateral: MRC
196099	5002258: [BDX-EP] Sync QPIRC : From Grantley 46.R00 to Grantley Refresh Stream (26022015) bios_resolution_notes: Synced the QPIRC code from Grantley 46.R00 to latest Grantley Refresh tree for BDX-. affected_bios_collateral: QPIRC
195689	5002256: Memory frequency setup additions for the XMP menu bios_resolution_notes: The Memory frequency setup in the XMP menu is missing values greater that 2667. This causes a setup hang if a freq. > 2667 is set from the Mem Config menu for freq and then a change in the XMP Menu made. Also code that prints out the XMP profile numbers needs to be incremented by 1 to indicate the correct naming. affected_bios_collateral: MRC
194996	5002236 : [BDX-ML] : Cross sync QPIRC code bases from EX- to EP- bios_resolution_notes: QPIRC codebase synced from EX stream to EP. affected_bios_collateral: QPIRC
194993	5002236 : [BDX-ML] : Cross sync QPIRC code bases from EX- to EP- bios_resolution_notes: QPIRC codebase synced from EX stream to EP. affected_bios_collateral: QPIRC
194950	5002049: [HEDT] Support all memory speeds for HEDT in 2D Strobe Centering bios_resolution_notes: Memory speeds are changed to ranges instead of specific speeds in AdvancedCentering() affected_bios_collateral: MRC
193405	5002227: Checkpoint additions for BIOS SSA bios_resolution_notes: Changes for this HSD checked in CL - 193405. Tested on a BDX Grantley system that the postcodes behave as expected. 0Xbe01 0000 - will halt (SSA API Start) 0Xbe02 0000 - won't halt (we provide this checkpoint only to enter the SSA EV loader; otherwise it has no other use) 0Xbe02 0f00 - will halt (SSA EV loader); we assume an opcode == 0 means to carry on and not halt; added code in to check for opcode =0 affected_bios_collateral: MRC

192835	5002066: BDX EP A0 - 3DS LRDIMMS not booting with the latest core MRC bios bios_resolution_notes: MemJedec.c - DoRegisterInitDDR4() updated to set RC08 for 3DS LRDIMMs to 0x8 to always include C[2:0] in parity computation regardless of # of signals used affected_bios_collateral: MRC
192424	5002170: NVDIMMs are not working in the Grangevile tree bios_resolution_notes: MRC functions related to NVDIMMs were broken with common core mrc which has been fixed. affected_bios_collateral: MRC
192330	5002224: BDX MCC-L0 PO: HA UC data read error hit if Package C6 is enabled in conjunction with RDIMMs bios_resolution_notes: MRC sets ddrcrclkranksused.disablepc6fix = 0 only for BDX MCC L0 SKU in InitDdrioInterface() and enable C6 by default. affected_bios_collateral: MRC
191871	5002024 : BDX EP 4S QPI 9.6 link fails with detect.fwdclk during PkgC L1 exit or Phy reset bios_resolution_notes: Implemented the qpi[0,1]_fwdc_spare as 0x08 as per the QPI uniPhy recipe v4.0 integration. affected_bios_collateral: QPIRC
191738	5002131: BIOS 38 R00 - not working with BCV-S nodes (SODIMM) - booting failure bios_resolution_notes: SPD Byte 3 Definition scope to be increased. affected_bios_collateral: MRC

Grantley_BDX-EP/EP4S CPU/QPI/Memory Reference Code - Revision 1.7.0 (242.R00) – Alpha 1

Release date: Feb 13th, 2015 (WW07.5)

Revision 1.7.0 - 242.R00

Notes:

- C6 is currently disabled in the BIOS. Enabling C6 on specific QDFs (QHPM) causes OS hangs.
- Some BDX-EP QDFs experienced QPI failures at 9.6GT/s. This can be worked around by limitting QPI speed to 8.0GT/s and bootting in a 1P configuration.
- Capsule update from BIOS earlier than 224R00 will not work due to Setup structure changes done on 224R00. If a capsule update is done, a CMOS clear is required to enable booting.

Potential issues and enhancements (under investigation)**:**

Log.ID	Description
4988567	[BDX] Provide OEM hook for CR_14079 (4986275: Fast Boot Paths need 3 month timeout)
5001598	CLONE from broadwell_server: PUSH from haswell_server: ZQCal won't be issued to all ranks when running LRDIMM encoded CS mode
5001668	[Haswell EP - Broadwell EP][Mayan City]Rank margin data in BDAT is ZERO when booting with release BIOS image
5001708	BDX - disabling cores in DP MC in BIOS setup fails with PNP BSOD in Windows 2012 R2
5001710	[CC-MRC] System fail to boot using 213.C03
5001711	HSX-Clone: BDX: E5-2650 v3 fail warm reset testing with LRDIMMs
5001718	Backside Cmd Ctl timing and Vref margining via BIOS RMT
5001740	[CC-MRC] Inca fail to reset from Windows and RedHat
5001766	rip out all refererncs to SETVID_DECAY_DISABLE as it is no longer supported
5001771	[BDX EP] LRDIMM RxVref Margins are much better on rank 0
5001877	Mayan City hang when memory is set at 1333Mhz
5001879	Update Uniphy QPI Recipe and Tuning Settings
5001890	[BDX EP][BDX DE][CCMRC] In RMT all the values are shifted from the headers columns are not lined up on the least significant digit
5001898	[BDX EP][CCMRC] GetMargins() is broken for LRDIMMs in encoded mode LRDIMM RxVref Margins are much better on rank 0
5001951	System fail with HA UC when Wr CRC enabled on BIOS > 219V02
5001961	Clone from BDX Sighting:3DPC/2DPC + WrCRC enabled + CAP error inj = SDC
5001980	Kahuna Platform QPI Tx EQ and CTLE peaking Updates
5001999	Fast Cold Boot is Broken on BDX DE and EP Needs Validation
5002009	Integrate BDX-ML-A0 Debug signed Patch mef406f0_80000008
5002024	Clone from BDX Sighting: BDX EP 4S QPI 9.6 link fails with detect.fwdclk during PkgC L1 exit or Phy reset
5002028	Enable BIOS SSA as a runtime BIOS option instead of a build option
5002039	Integrate BDX EP Debug signed Patch mef406f0_80001008
5002046	Integrate BDX-ML-A0 Production Patch mef406f0_00000008
5002058	BSSA: err_pntr bits need to be removed from SV_HOOKS
5002095	CLONE from broadwell_server: Refile 282988: S3/Warm Reset exit failures due to violating JEDEC spec by floating DDR clock above VIL(static) before sending valid clock
5002107	ConvergedMRC to GrantleyRefresh Sync - 2
5002127	Clone from BDX Sighting:HA data read error & Patrol scrub error with PkgC6 on DDR3-UDIMM system

5002156	BSSA: New Chip layer function required to move a part of SsaBiosInitialize

Sighting fixes and enhancements: (fixes and enhancements since last RC release)

Log.ID	Description
190702	5002158:[BDX-EP/DE] - DDRCRSPDCFG2 setting for 1 HA sku should be changed for DIMM detection to work on CH2/3 - bios_resolution_notes: Set crspdcfg2 = 0x56B0 for CH0/1 and0x16B0 for CH2/3 for all BDX SKUs regardless of 1HA / 2HA - affected_bios_collateral: MRC
190136	5002156: BSSA: New Chip layer function required to move a part of SsaBiosInitialize - bios_resolution_notes: Changes checked in CL 190136 As this is a strcutural change to the SSA structs I tested the changes on a BDX Grantley platform; built a BIOS which called 2 of the API functions from within BIOS code and printed out results in the log. They work as expected. Peter Tan also tested the test BIOS also by running Margin 1D tests on a on a Grantley platform; he confirmed the BIOS behaves as expected. - affected_bios_collateral: MRC
190099	5002189:CLK Gating needs to be enabled on L0, B0, R0 - bios_resolution_notes: Updated InitDdrioInterface() to keep rxpion = 1 regardless of BDX-EP stepping. Updated SwitchToNormalMode() to keep rxpion = 1 only for BDX-DE, and EP A0 HCC SKU. For all other Stepping/SKU combinations, rxpion = 0 to enable clock gating. - affected_bios_collateral: MRC
189595	5002175 : Latest Build GRT_229_D01 failing to boot after FAST boot disabled (False scrambling check is issuing POWER GOOD) - bios_resolution_notes: Misplaced scrambling check was causing the COLD reset during fast boot disabled path , removed buggy code - affected_bios_collateral: MRC
188148	5002154: SSAInit() CallTable mpFlag change - bios_resolution_notes: Code checked - CL188148. - affected_bios_collateral: MRC
188063	5002074: BCV-R/S nodes - U0 CPU Failures on Warm Reboot (sometimes resets > 5 minutes) - bios_resolution_notes: Disabled warm fast boot. - affected_bios_collateral: MRC
188040	5002127:Clone from BDX Sighting:HA data read error & Patrol scrub error with PkgC6 on DDR3-UDIMM system - bios_resolution_notes: Set DDRCRCLKCOMP.rcompdrvup = 60 and DDRCRCLKCOMP.rcompdrvdown = 63 DDRCRCLKCOMP (same setting as DDR4 UDIMM) for DDR3 UDIMMS on BDX - affected_bios_collateral: MRC
187959	5002114: CLONE from broadwell_server: Clone from BDX Sighting:os uncore ring ratio reg : min_clr_ratio > max_clr_ratio does not follow os_ring_min = min(os_ring_min, os_ring_max) - bios_resolution_notes: As per bugeco 286790, BIOS should provide a check not to overwrite the max_clr_ratio less than min_clr_ratio at all times. This check has been provided in the BIOS. - affected_bios_collateral: CPURC
187909	5002104:BIOS MRC Print Fixes for N-ECC mode - bios_resolution_notes: Training Register Dump print fixes are done for N-ECC DIMMS. - affected_bios_collateral: MRC
187490	5001750:[CC-MRC] Low Voltage DDR3 UDIMMs are detected as 1.5V - bios_resolution_notes: Issue was because of initializing DDR3 voltages before initializing host->nvram.mem.dramType variable which was causing DDR3 voltages always set to 1.5. InitDDRVolatgeDDR4() and InitDDRVolatgeDDR3() are invoking from to DetectSpdTypeDIMMConfig(), after the initialization of host->nvram.mem.dramType - affected_bios_collateral: MRC
187457	5001997 : BDX-DE V0 :setting IOT OCLA ways to 4 do not change number of ways (for IOT enablement) - bios_resolution_notes: Algorithim calculate OCLA ways in BDX-DE ocla ways = total ways (12) - non-isoch(1) - NEM_ways (based slice count) - affected_bios_collateral: CPURC

187369	5002029:[Grangeville] MiniBIOS 36V07 CRB not booting on platform - bios_resolution_notes: IioEarlyPreDataLinkInit () was missed in procMemInit(). Added this change to initialize serial logs for minibios. - affected_bios_collateral: MRC
186848	5002095: CLONE from broadwell_server: Refile 282988: S3/Warm Reset exit failures due to violating JEDEC spec by floating DDR clock above VIL(static) before sending valid clock - bios_resolution_notes: To account for the RTL fix that forces ddrcrclkranksused.drvpupdis = 1, MRC sets ddrcrclkranksused.drvpupdis = 0 in InitDdrioInterface() before xover training. - affected_bios_collateral: MRC
186374	5002107: ConvergedMRC to GrantleyRefresh Sync - 2 - bios_resolution_notes: Checked in - CL 186374. a.) GrantleyRefresh stream: CL 172783 (first CCMRC integration). b.) GrantleyRefresh stream: CL 183105 (GrantleyRefresh CL used for this integration). c.) ConvergedMRC CL 183130 is being used to be merged. - affected_bios_collateral: MRC
183612	5001752: [HSX-BDX] 4S HSX ACPI NUMA distance tables getting wrongly populated in certain non-fully connected cases - bios_resolution_notes: Modified the SLIT tables as below case. Fix has been committed through CL 183612 4S- NON-COD Node 0 1 2 3 0: 10 21 31 21 1: 21 10 21 31 2: 31 21 10 21 3: 21 31 21 10 4S-COD Node 0 1 2 3 4 5 6 7 0: 10 11 21 21 31 31 21 21 1: 11 10 21 21 31 31 21 21 2: 21 21 10 11 21 21 31 31 3: 21 21 11 10 21 21 31 31 4: 31 31 21 21 10 11 21 21 5: 31 31 21 21 11 10 21 21 6: 21 21 31 31 21 21 10 11 7: 21 21 31 31 21 21 11 10 - affected_bios_collateral: <Unassigned>
183590	Updating Grangeville_Trunk BIOS IDs: 20150127_CP_GRANGEVILLE_GRANTLEY_REF_GNV_39_D01_GRT_REF_226_D01
183585	GNV Release 39 GRT REF 226 BIOSID Update
183144	Updating Grangeville_Trunk BIOS IDs: 20150127_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D18_GRT_REF_225_D18
183129	5002088: Disable IMODE and enable Per-bit Deskew and Per-bit Margins by default on BDX DE - bios_resolution_notes: Checked in CL 183129. Yes, for IMODE there is only one option shared by DE and EP. Have disabled it. Enabled Per-bit Deskew and Per-bit Margins by default on BDX DE. - affected_bios_collateral: MRC
183105	5002063 : [BDX-EP] : Sync QPIRC from Grantley 43.R00 to Grantley Refresh Tree - bios_resolution_notes: Fix: Synced the QPIRC codebase from 43.R00 to 225.D09 (approx). Only 1 trivial CL need to be synced - logging of a warning message. - affected_bios_collateral: QPIRC
183095	5002055 : Clone from BDX Sighting:[QPI-EP]: Changes for BIOS LBC writes as - bios_resolution_notes: Implemented the LBC 56 change to 0x2A5C instead of 0x5C and removed the changes done to LBC 57 as requested from Design/EV. - affected_bios_collateral: QPIRC
182726	5002081:Old code in common core MRC has creeped in breaking ADR - bios_resolution_notes: Fixed the issue in OemIioInit.c wrt to retime initialization. - affected_bios_collateral: Binary ROM (Internal)
182362	Updating Grangeville_Trunk BIOS IDs: 20150124_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D17_GRT_REF_225_D17

182126	5002077: [BDX_EP] - Pkg delay entries for LCC/MCC SKUs is not available; may result in training failure - bios_resolution_notes: PKG delay table for MCC SKU included - affected_bios_collateral: MRC
182027	Updating Grangeville_Trunk BIOS IDs: 20150123_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D16_GRT_REF_225_D16
181937	5002069: Set MCMAIN_CHKN_BITS_0_19_0_CFG.defeature_10 to 1 for all MCs for BDX DE/EP (Irrepective of the stepping) - bios_resolution_notes: sv.socket0.uncore0.imc0_mcmain_chkn_bits.defeature_10 bit made 1 for all stepings for both DE and EP in MemLate() and verified. - affected_bios_collateral: MRC
181922	5001885 - Failed ranks are being scrubbed after Mirror failover - bios_resolution_notes: Disable scrubbing of failed channels using AMAP registers - affected_bios_collateral: BIOS Core Issue
181547	5001796:Add new b2p mailbox command for DE to enable pcode to block PCIe / SC traffic during ADR - bios_resolution_notes: Implemented the feature by providing a setup option - affected_bios_collateral: Binary ROM (Internal)
181516	5002080:NTB to RP configuration is not working between 2 TBC systems - bios_resolution_notes: Retimer is held in reset and never released in NTB to RP mode. - affected_bios_collateral: Binary ROM (Internal)
181360	Updating Grangeville_Trunk BIOS IDs: 20150122_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D15_GRT_REF_225_D15
181282	5002077: [BDX_EP] - Pkg delay entries for LCC/MCC SKUs is not available; may result in training failure - bios_resolution_notes: PKG delay table for MCC SKU included - affected_bios_collateral: MRC
181225	4988101: [HSX-BDX] HEDT/OC: Copy latest HSW-E HEDT BIOS Sandbox overclocking fixes - bios_resolution_notes: - affected_bios_collateral: <Unassigned>
180743	4987220: [BDX-EP] Support the BIOS Guard Anti flash wearout feature. - bios_resolution_notes: BIOS Guard Anti flash wearout feature has been implemented, validated and checked-in. - affected_bios_collateral: Binary ROM (Internal)
180714	5001680: [BDX EP] Enable Backside Training for RxDq/TxDq/RxVRef - bios_resolution_notes: LRDIMM backside training steps added to MRC - affected_bios_collateral: MRC
180708	Updating Grangeville_Trunk BIOS IDs: 20150121_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D14_GRT_REF_225_D14
180705	5002072: DE V1 pre-ES2 w/a - Disable ACC by default through BIOS] - bios_resolution_notes: BIOS changes added to disable ACC bit msr 0xe2 when ACC knob is disabled. - affected_bios_collateral: CPURC

180578	5001684: CLONE from broadwell_server: PUSH from haswell_server: Clone from HSX Sighting:IERR TOR Timeout while running linux memory stress at EFI with C1, 32G 3DPC configuration - bios_resolution_notes: 07/09/2014 - Fatal from customer demand for DDR4. HSX working on a patch to use row hammer machine to break the starvation deadlock. It is not fully proven on Customer silicon yet. BE effort is 4days - 1 EW (mcmnts fub) with current fub. Sambaran to provide the fix with de-feature bit so we can use HSX workaround. Pre-silicon validation effort is 4 days (Kausik). DCCB_AR ======= Sambaran to close with BE on the effort. 07/10/2014 - AR completed. Chicken bit implementation provided and ok with BE. Approved for MCC. - affected_bios_collateral: MRC 5002010: Test BIOS with ERF_DDR4_CMD_REGX programming for DDR CRC / CA Parity on L0 - bios_resolution_notes: Added knobs for CRC and CAP error flow. - affected_bios_collateral: MRC 5002011: Request 2 new BIOS knobs to enable ERF flow for WrCRC and CAP - bios_resolution_notes: Added master knobs for Error Flow (CAP and CRC) - affected_bios_collateral: MRC 5002031: Working back the SDDC workaround (to address CECC sighting) on MCC and subsequent silicon - bios_resolution_notes: Added master knob for Cecc WA - affected_bios_collateral: MRC
180560	5001802: [BDX DE][BDX EP] TxEq/CTLE/IMODE sweep changes - bios_resolution_notes: new sweep range for CTLE /TXEQ. - affected_bios_collateral: MRC
180128	4988477: [BDX DE][BDX EP] Fix BIOS Caching for C/A Vref, CMD, DDR3 TxVref - bios_resolution_notes: Change made to cache the C/A Vref training value (dimmVrefControl1) per channel. Please verify test BIOS attached. - affected_bios_collateral: MRC
180074	5002061:PERF: wmm_enter should be reverted to 0x24 for DDR4 2133 - bios_resolution_notes: Updated MemTimingChip.c - ProgramTimings() to set wdbwm.wmm_enter = 0x24 - affected_bios_collateral: MRC
179621	5002012: WrCRC breaking the S3 flows - bios_resolution_notes: restored MC registers in S3 path. - affected_bios_collateral: MRC
178934	5001680: Enable Backside Training for RxDq/TxDq/RxVRef - bios_resolution_notes: LRDIMM backside training steps added to MRC - affected_bios_collateral: MRC
178887	5001808: change the default value of MpllOffEna to Enable in BDX DE V0 and ML A0 onwards - bios_resolution_notes: Modified the default value of MpllOffEna to Enable(0x1) in BDX DE V0 and ML A0 onwards. - affected_bios_collateral: CPURC
178824	4988477:[BDX DE][BDX EP] Fix BIOS Caching for C/A Vref, CMD, DDR3 TxVref - bios_resolution_notes: Change made to cache the C/A Vref training value (dimmVrefControl1) per channel. Please verify test BIOS attached. - affected_bios_collateral: MRC
178770	5001853:[BDX EP][BDX DE] Print out R-COMP, S-COMP, and ODT COMP in BIOS serial logs(Moving changes from Core to Chip) - bios_resolution_notes: Added DisplayCompRegResults() function in MemDisplay.c which prints the COMP register contents. - affected_bios_collateral: MRC
178406	Updating Grangeville_Trunk BIOS IDs: 20150115_CP_GRANGEVILLE_GRANTLEY_REF_GNV_38_D05_GRT_REF_225_D05
177692	5001975: 2 DPC 1600 DDR3 has bad dq margins - bios_resolution_notes: Fix for 2DPC DDR3 margin degradation. - affected_bios_collateral: MRC

177194	5002022:In the training register dump, BIOS is printing out only the RxDqsP per-bit results - bios_resolution_notes: Added separate per-bit RxDqsP and RxDqsN debug print messages in training register dump. - affected_bios_collateral: MRC
177183	5001976: Initial CMD/CTL delays are off for DDR3 and DDR4 - bios_resolution_notes: Adjusted the initial delays to center CTL and CMD - affected_bios_collateral: MRC
177097	5001802: TxEq/CTLE/IMODE sweep changes - bios_resolution_notes: new sweep range for CTLE /TXEQ. - affected_bios_collateral: MRC
176661	5002001:Per-bit Deskew disabled in CRB BIOS for BDX ML - bios_resolution_notes: per-bit skew changes made available for CRB BIOS also by removing VFR_CRB_FLAG in MemorySetup.hfr - affected_bios_collateral: MRC
176656	5001853:[BDX EP][BDX DE] Print out R-COMP, S-COMP, and ODT COMP in BIOS serial logs - bios_resolution_notes: Added DisplayCompRegResults() function in MemDisplay.c which prints the COMP register contents. - affected_bios_collateral: MRC

END OF DOCUMENT