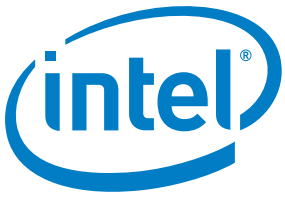

Brickland Platform/Broadwell-EX Reference and Sample Code Release Note

Legal Information

Disclaimer

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

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

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

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

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

Release Notes

Version History/Revision History

Date	Revision	Description
21 November 2019	4.0.0	Central Park UEFI FW (Full Source)
1 June 2018	3.9.1	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
16 June 2017	3.9.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
5 April 2017	3.8.0	CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
25 February 2017	3.7.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
17 October 2016	3.6.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
2 September 2016	3.5.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
5 August 2016	3.4.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
17 June 2016	3.3.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
13 May 2016	3.2.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
29 April 2016	3.1.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
21 March 2016	3.0.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
9 March 2016	2.9.1	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
5 February 2016	2.9.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
8 January 2016	2.8.4	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
1 December 2015	2.8.3	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code

		RAS/IIO/CPUPM Sample Code
6 November 2015	2.8.2	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
18 September 2015	2.8.1	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
4 September 2015	2.8.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
7 August 2015	2.7.2	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
15 July 2015	2.7.1	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
29 May 2015	2.7.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
11 May 2015	2.6.1	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
2 April 2015	2.6.0	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
17 March, 2015	2.5.8	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
2 February 2015	2.5.7	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
26 November 2014	2.5.6	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code
24 October 2014	2.5.5	Central Park UEFI FW (Full Source) CPU/QPI/Memory Reference Code RAS/IIO/CPUPM Sample Code

Intended Audience

This documented is intended for UEFI FW and BIOS developers who integrate Intel Reference/Sample Code.

Customer Support

For technical support, including answers to questions not addressed in this document, please create an IPS issue.

Contents:

1 Introduction

This is Brickland Platform/Broadwell-EX reference/sample code source release. This document provides system requirements, build instructions, issues and limitations, and legal information.

To learn more about this product, see:

- New features and fixes listed in the New in this Release section below.
- Reference documentation listed in the Related Documentation section below

2 New in This Release

To see a list of all changes to the source use the History facility of the Git repository. You may use git log from a command prompt or if you have a graphical interface installed for Git, you may use the gitk Git History equivalent.

A sample snapshot of the change lists is provided below for reference.

3 Known Issues/Limitation

General Note

1. Before updating any image first makes sure that your board is booting fine with HSX image or previous BDX image.
2. Please make sure the platform BIST enable strap is enabled. Otherwise BIST engine in the CPU will not run and BIOS BIST check will be always pass.
3. Capsule update image includes ACM, hence Capsule Update from any version before 332, has to be first updated to 332.R00.
4. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.

RC 3.9.1/3.9.0

1. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.8.0

1. BDX-EX B0 Production Patch version mef406f1_0b000021 is included in this release.
2. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.7.0

1. BDX-EX B0 Production Patch version mef406f1_0b000020 is included in this release.
2. HSX-EX E0 Production Patch version m80306f4_0000000f is included in this release.
3. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.6.0

1. BDX-EX B0 Production Patch version mef406f1_0b00001f is included in this release.
2. HSX-EX E0 Production Patch version m80306f4_0000000e is included in this release.
3. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't

known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.5.0

1. BDX-EX B0 Production Patch version mef406f1_0b00001e is included in this release.
2. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash

RC 3.4.0

1. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.3.0

1. BDX-EX B0 Production Patch version mef406f1_0b00001d is included in this release.
2. HSX-EX E0 Production Patch version m80306f4_0000000d is included in this release.
3. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.2.0

1. BDX-EX B0 Production Patch version mef406f1_0b00001b is included in this release.
2. HSX-EX E0 Production Patch version m80306f4_0000000c is included in this release.
3. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.1.0

1. Code Sync to HSX-EX stream up to 70R (RC 1.70). HSX-EX RC version is 1.70.00.01
2. A0 Production Patch mef406f0_00000014 is included in this release
3. B0 Production patch version mef406f1_0b00001A is included in this release
4. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 3.0.0

1. Code Sync to HSX-EX stream up to 69R (RC 1.60). HSX-EX RC version is 1.60.00.01
2. A0 Production Patch mef406f0_00000014 is included in this release
3. B0 Production patch version mef406f1_0b000019 is included in this release
4. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 2.9.1

1. Code Sync to HSX-EX stream up to 69R (RC 1.60). HSX-EX RC version is 1.60.00.01
2. A0 Production Patch mef406f0_00000014 is included in this release
3. B0 Production patch version mef406f1_0b000015 is validated for this release
4. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash.

RC 2.9.0

1. Code Sync to HSX-EX stream up to 69R (RC 1.60). HSX-EX RC version is 1.60.00.01
2. A0 Production Patch mef406f0_00000014 included in this release
3. B0 Production patch version mef406f1_0b000014 included in this release
4. Before updating any image first makes sure that your board is booting fine with HSX image or previous BDX image.
5. Please make sure the platform BIST enable strap is enabled. Otherwise BIST engine in the CPU will not run and BIOS BIST check will be always pass.
6. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.
7. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.
8. Capsule update image includes ACM, hence Capsule Update from any version before 332, has to be first updated to 332.R00

RC 2.8.4

1. Code Sync to HSX-EX stream up to 69R (RC 1.60). HSX-EX RC version is 1.60.00.01
2. A0 Production Patch mef406f0_00000014 included in this release
3. B0 Production patch version mef406f1_0b000011 included in this release

4. Before updating any image first makes sure that your board is booting fine with HSX image or previous BDX image.
5. Please make sure the platform BIST enable strap is enabled. Otherwise BIST engine in the CPU will not run and BIOS BIST check will be always pass.
6. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.
7. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.
8. Capsule update image includes ACM, hence Capsule Update from any version before 332, has to be first updated to 332.R00.

RC 2.8.3

1. Code Sync to HSX-EX stream up to 69R (RC 1.60). HSX-EX RC version is 1.60.00.01
2. A0 Production Patch mef406f0_00000014 included in this release
3. B0 Production patch version mef406f1_0b00000f included in this release
4. Before updating any image first makes sure that your board is booting fine with HSX image or previous BDX image.
5. Please make sure the platform BIST enable strap is enabled. Otherwise BIST engine in the CPU will not run and BIOS BIST check will be always pass.
6. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.
7. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.

RC 2.8.2

1. Code Sync to HSX-EX stream up to 67R02. HSX-EX RC version is 01.40.00.03
2. A0 Production Patch mef406f0_00000014 included in this release
3. B0 Production patch version mef406f1_0b00000b included in this release
4. Before updating any image first makes sure that your board is booting fine with HSX image or previous BDX image.
5. Please make sure the platform BIST enable strap is enabled. Otherwise BIST engine in the CPU will not run and BIOS BIST check will be always pass.
6. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors

are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.

7. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.

RC 2.8.1

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available.
2. Enable BIST check by default for B0 Silicon for CRB BIOS. If you are not using ES2 parts you may see BIST check failure. If you are seeing BIST errors with CRB BIOS you need to change your CPUs to ES2 parts, or disable BIST check through setup option.
3. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.
   SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW

RC 2.8.0

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available.
2. Default QPI link speed changed from 8.0 GT/s to Auto made in line with POR-configuration. There might be noticeable CRC- errors (correctable in nature and doesn't known to impact the OS boot) seen as a result of this change at EFI- Shell. The errors are known to happen only during the first boot after the BIOS flash. This is a known issue and debug is WIP.
3. SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.

RC 2.7.2:

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available.
2. Need to change the Interleave Mode in MRC to 1_WAY when ClusterOnDieEn is enabled.
   SPS ME FW cannot limit power in certain 1DPC and minimum riser configurations. This is a limitation of SPS ME FW.

RC 2.7.1:

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available
2. Need to change the Interleave Mode in MRC to 1_WAY when ClusterOnDieEn is enabled
3. Windows doesn’t report all sockets if CPU Online settings are set with QDF: QHWJ
4. System hangs at boot with BDX A0 QDFs: QHWJ and QH9L

RC 2.7.0:

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available
2. Need to change the Interleave Mode in MRC to 1_WAY when ClusterOnDieEn is enabled
3. Can't flash BIOS with capsule app tool in EFI Shell

RC 2.6.1:

1. Image supports HSX-EX & BDX-EX only. IVT-EX unary image support is not yet available
2. BDX CPU Online failed (with 2 or 4 processors), after to remove 1th jumper the system is restart
3. [BDX BIOS] Memory online DDR3/DDR4 Failed to add memory raiser
4. Can't flash BIOS with capsule app tool in EFI Shell

RC 2.5.7:

MiniBIOS build fails with the following message: NMAKE : fatal error U1073: don't know how to make 'OUT32\memxmp.obj'

Non-Intel Issues

.

4 Related Documentation

5 Where to Find the Release

These releases can be downloaded from Validation Internet Portal (VIP) at https://platformsw.intel.com

How to Install and Build this Release

Downloaded .zip files: main source tree; contains a bare git repo.

Must have git installed to proceed. Can be obtained from http://git-scm.com/downloads

Extract .zip files (e.g., extract to C:\repo\Brickland*File_name*.git)

First Time Use:

- Create new working directory for the sample, e.g., c:\CODE\SAMPLE\Brickland
- Clone the repository to working area (e.g., "cd C:\CODE\SAMPLE\Brickland; git clone C:\repo\Brickland*File_name*.git)

Your working copy (e.g., C:\CODE\SAMPLE\Brickland*File_name*) represents the tip of the repository and is the most recent state of the Intel source.

You can see the history using the "git log" command in a command line or using a GUI's "Git History" function.

To build the source as delivered,

1. For Central Park UEFI FW (Full Source), run "BricklandPkg\bbk release bdx"
2. For CPU/QPI/Memory Reference Code, run “ExternalBuildMiniBIOS”
    a. rc.bin is created at the root directory.
    b. Legacy MiniBIOS folder BricklandSocketPkg\MiniBIOS\EXT_RC_RELEASE is generated for backward compatibility.

    Note: some necessary executables (such as EXE2BIN.EXE, h2inc.exe, link.exe, unifdef.exe) are not included in the release package. Users need to set up the appropriate build environment.
3. For RAS/IIO/CPUPM Sample Code, legacy RAS/IIO/CPUPM folders can be generated by running “ExternalRas”.

6 Best Known Configuration (BKC)

Brickland Broadwell-EX Best Known Configuration (BKC) is available on platformsw.intel.com. Please search description “Brickland Broadwell-EX BKC” for latest update.