Kaby Lake CPU Initialization Code Version 3.7.6

Release Notes

August 2019

Revision 3.7.6

1 Introduction

- Product: Kaby Lake CPU Initialization Code

- Developed by: Intel Corporation

- Software version released date: <November, 2018>

Note: This document is cumulative and includes information on previous versions. The version information is presented with the newest release first and then regressing through earlier versions.

This program was developed by Intel Corporation. The 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 or any responsibility to update it.

Note: This sample code is to be used in accordance with the DCL document that came with the samples. Refer to the DCL for intended purpose of the sample and recommendations for testing that should not be performed with these samples.

Note: **Visual Studio 2013 Update 5 patch is needed**.
Update with release information can be obtained at following link:
https://support.microsoft.com/en-in/help/3021976/description-of-visual-studio-2013-update-5.

1.1 Purpose of CPU Initialization Code

This is sample Initialization Code for the initialization of Kaby Lake Processor. It complies with Processor BIOS Spec for all programming requirements.

The Processor Initialization Code is intended for use as part of Intel BIOS. An OEM may need to modify the code to meet specific platform designs, error handling features, platform specific BIOS features, or other local requirements.

1.2 Target Customers

The CPU Initialization Code is intended for use as part of Intel BIOS. The code is compatible with both mobile and desktop products.

1.3 Version Release History

Version	Description	Release Date
0.5.0	Initial external release	December 3, 2015
0.6.0	Alpha Update	January 8, 2016
0.6.1	Alpha Update	January 28, 2016
0.7	Beta U/Y	February 25, 2016
0.7.1	Beta U/Y Update	March 7, 2016
0.7.2	Beta U/Y Update	March 23, 2016
0.7.3	U/Y Beta Update DT with SPT Alpha Cons/Corp Halo Alpha Cons/Corp	April 5, 2016
0.8.0	U/Y Beta Update	April 25, 2016
0.8.1	U/Y Beta Update	May 6, 2016
0.9.0	U/Y PC Canidate, DT with SPT Alpha Update	May 17, 2016
0.9.1	U/Y PC, DT with SPT Alpha Update	June 2, 2016
1.0.0	U/Y PV, DT with SPT Alpha Update	June 7, 2016
1.0.1	U/Y PV update, DT with SPT Alpha Update	June 16, 2016
1.0.2	SR'17 S/H/Y/U Beta Consumer / Corporate*	July 1, 2016
1.0.3	SR'17 S/H/Y/U Beta Consumer / Corporate* Update	July 15, 2016
1.0.4	SR'17 S/H/Y/U Beta Consumer / Corporate* Update	August 12, 2016
1.0.5	Update U/Y HR'16 RS1 Update U23e RS1 Update SR'17 S/H/Y/U	August 28, 2016
1.1.0	PV U/Y HR'16 RS1 Update SR'17 S/H/Y/U Update U23e RS1	September 13, 2016
1.2.0	PV SR'17 S42 – consumer PCV SR'17 Y/U Update PCV SR'17 H/U32e/ all Corp SKUs	October 6, 2016
1.3.0	**PV SR'17 H – consumer** **PC/PV* SR'17 S42/H/ and Y/U22 – Corporate*** Beta SR'17 S22 with RS1	October 21,2016
1.4.0	**PV for SKL CPU on KBL boards with win 7/8.1** First Post SR'17 PV update BKC release (U32e and S22)	November 04, 2016
1.4.1	Update for all Kabylake platforms	November 17, 2016
1.5.0	PV SKL on KBL Platforms with Win7/Win8.1 Post SR'17 update – PR2 Update to U23e	December 02, 2016
1.6.0	PV U32e (both Consumer and Corporate)	January 24, 2017

	PR2 (both Consumer and Corporate)	
1.7.0	Update for all Kabylake platforms	February 06, 2017
1.8.0	Update for all Kabylake platforms	February 23, 2017
1.9.0	Update for all Kabylake platforms	March 09, 2017
2.0.0	Update for all Kabylake platforms	March 22, 2017
2.1.0	Update for all Kabylake platforms	April 10, 2017
2.2.0	Update for all Kabylake platforms	April 25, 2017
2.3.0	Update for all Kabylake platforms	May 17, 2017
2.4.0	Update for KBL-R/ KBL/ CFL	June 1, 2017
2.5.0	Update for KBL-R/ KBL/ CFL	June 22, 2017
2.5.1	Update for KBL-R/ KBL/ CFL	July 4, 2017
2.6.0	Update for KBL-R/ KBL/ CFL	July 18, 2017
2.6.1	Update for KBL-R/ KBL/ CFL	August 2, 2017
2.6.2	Update for KBL-R/ KBL/ CFL	August 08, 2017
2.7.0	Update for KBL-R/ KBL/ CFL	August 17, 2017
2.7.2	Update for KBL-R/ KBL/ CFL	September 5, 2017
2.8.0	Update for KBL-R/ KBL/ CFL	September 26, 2017
2.8.1	Update for KBL-R/ KBL/ CFL	October 11, 2017
2.9.0	Update for KBL-R/ KBL/ CFL	October 31, 2017
2.9.1	Update for KBL-R/ KBL/ CFL	November 22, 2017
3.0.0	Update for KBL-R/ KBL/ CFL	December 6, 2017
3.0.1	Update for KBL-R/ KBL	December 21, 2017
3.1.1	Update for CFL	February 9, 2018
3.1.2	Update for KBL-R/ KBL/ CFL	March 7, 2018
3.2.0	Update for KBL-R/ KBL/ CFL	April 11, 2018
3.2.1	Update for KBL-R/ KBL/ CFL	May 9, 2018
3.3.0	Update for KBL-R/ KBL/ CFL	May 23, 2018
3.4.0	Update for KBL-R/ KBL/ CFL	June 21, 2018
3.5.0	Update for KBL-R/ KBL/ CFL	June 21-2018
3.6.0	Update for KBL-R/ KBL/ CFL	June 29-2018
3.6.1	Update for KBL-R/ KBL/ CFL	July 20-2018
3.6.1.1	Update for KBL-R/ KBL/ CFL	August 01-2018
3.6.2	Update for KBL-R/ KBL/ CFL	August 01-2018
3.6.3	Update for KBL-R/ KBL/ CFL	September 12-2018
3.6.4	Update for KBL-R/ KBL/ CFL	September 28-2018
3.6.5	Update for KBL-R/ KBL/ CFL	October 22-2018

3.6.6	Update for KBL-R/ KBL/ CFL	November 15-2018
3.6.7	Update for KBL-R/ KBL/ CFL	November 20-2018
3.6.7.1	Update for KBL-R/ KBL/ CFL	December 20-2018
3.6.7.2	Update for KBL-R/ KBL/ CFL	January 25-2019
3.7.0	Update for KBL-R/ KBL/ CFL	March 5-2019
3.7.1	Update for KBL-R/ KBL/ CFL	March 29-2019
3.7.2	Update for KBL-R/ KBL/ CFL	April 24-2019
3.7.3	Update for KBL-R/ KBL/ CFL	May 6-2019
3.7.4	Update for KBL-R/ KBL/ CFL	June 6-2019
3.7.5	Update for KBL-R/ KBL/ CFL	June 10-2019
3.7.6	Update for KBL-R/ KBL/ CFL	August 30-2019

§

2 Version 3.7.6 Details

2.1 New Feature

None

2.2 Fixed Bugs

2.2.1 Bug 1

- **Description\Solution:**
  Improve error checking in BIOS Guard
- **Platform Affected:**
  KBL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.h
  KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c

3 Version 3.7.5 Details

3.1 New Feature

None

3.2 Fixed Bugs

None

4   Version 3.7.4 Details

4.1   New Feature

None

4.2   Fixed Bugs

4.2.1   Bug 1

- **Description\Solution:**
  KBL-S22 SKUs support is missing in the VR and PM override table.
- **Platform Affected:**
  KBL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

4.2.2   Bug 2

- **Description\Solution:**
  ACM_HEADER should be enclosed in a #pragma pack (1).
- **Platform Affected:**
  KBL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/Private/Library/TxtPeiLib.h

5 Version 3.7.3 Details

5.1 New Feature

None

5.2 Fixed Bugs

5.2.1 Bug 1

- **Description\Solution:**
  CPU Stepping showing as unknown for CFL-S-KBPH R0 config on BIOS Menu.
- **Platform Affected:**
  CFL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  KabylakeSiliconPkg/SystemAgent/MemoryInit/Include/MrcInterface.h
  KabylakeSiliconPkg/SystemAgent/MemoryInit/Library/Private/PeiMemoryInitLib/MemoryInit.c
  KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/Common/CpuRegs.h
  KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/MEMORY/MrcOemPlatform.c

5.2.2 Bug 2

- **Description\Solution:**
  Epid and PSE provisioning Failed
  -- Added logic check to ensure AML Y will use BIOS Guard Module 2.0.4285 (10BD)
  Added logic check to ensure AML Y will use BIOS Guard SE SVN 0x80.
- **Platform Affected:**
  KBL/CFL
- **Affected Files**
  KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c

6 Version 3.7.2 Details

6.1 New Feature

None

6.2 Fixed Bugs

6.2.1 Bug 1

- **Description\Solution:**
  PnP tests show performance degradation of about 8% on KBLY.
  --Incorrect CpuSkuIdentifier been detected. Fixed the logic to identify correct CPU Identifier.
- **Platform Affected:**
  KBL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

7 Version 3.7.1 Details

7.1 New Feature

None.

7.2 Fixed Bugs

None.

8   Version 3.7.0 Details

8.1   New Feature

None

8.2   Fixed Bugs

8.2.1   Bug 1

- **Description\Solution:**
  PL4 is always 0 when OC is disabled and VR PD Design is AUTO or selected
  --Added correct cTDP check to PL4 programming flow
- **Platform Affected:**
  CFL and KBL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

8.2.2   Bug 2

- **Description\Solution:**
  64-bit PCI MMIO Read/Write does not work
  -- 64-bit MMIO Read/Write does not work for PCI devices. This needs to be split into 2 DWORD Read/Writes.
- **Platform Affected:**
  KBL/CFL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuMailboxLib/MaiboxLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/IdleStates.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c
  KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/MiscFunctions.c
  KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PerformanceStates.c
  KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PowerLimits.c

9 Version 3.6.7.2 Details

9.1 New Feature

None.

9.2 Fixed Bugs

None.

10   Version 3.6.7.1 Details

10.1   New Feature

None

10.2   Fixed Bugs

None

11 Version 3.6.7 Details

11.1 New Feature

11.2 Fixed Bugs

11.2.1 Bug 1

- **Description\Solution:**
  No default AcLoadline/DcLoadline value set for Sklylake S 4+2/2+2 CPU on Kabylake RC
- **Platform Affected:**
  SKL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

11.2.2 Bug 2

- **Description\Solution:**
  Add W0/V0 CPUID Steppings to AML MRC
  - New CPUID must be added to MRC, so that any stepping related W/A or changes will be effective.
- **Platform Affected:**
  AML
- **Affected Files:**
  KabylakeSiliconPkg/SystemAgent/MemoryInit/Include/MrcInterface.h
  KabylakeSiliconPkg/SystemAgent/MemoryInit/Library/Private/PeiMemoryInitLib/MemoryInit.c
  KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/Common/CpuRegs.h
  KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/MEMORY/MrcOemPlatform.c

12   Version 3.6.6 Details

12.1   New Feature

12.1.1   Feature 1

- **Description\Solution:**
  BIOS Cpu detection logic doesn't detect AML-Y 4+2 properly
  -Loosened detection logic on AML-Y 4+2 to allow for all TDP's to be detected
- **Platform Affected:**
  AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

12.1.2   Feature 2

- **Description\Solution:**
  CFL-S 8+2 fully unlocked CPU change TjMax
  - BIOS code needs to include Tjmax offset programming in the S3 reset handling solution similar to Pll or BCLK resets.
- **Platform Affected:**
  CFL-S 8+2
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/PeiCpuOcInitLib.inf

12.1.3   Feature 3

- **Description\Solution:**
  Updated LL for 5W and 7W AML parts.
- **Platform Affected:**
  CFL-S 8+2
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

12.1.4   Feature 4

- **Description\Solution:**
  Disable Turbo when both EIST and HWP are disabled in KBL reference code.
- **Platform Affected:**
  CFL-S 8+2

- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c

12.2 Fixed Bugs

12.2.1 Bug 1

- **Description\Solution:**
  Update incorrect conditional logic to detect KBL-S skus correctly
- **Platform Affected:**
  KBL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

12.2.2 Bug 2

- **Description\Solution:**
  Iccmax, TDC, loadline values are programmed incorrectly in BIOS
  The CPU DID check for 2+2 and 4+2 wasn't correct. Hence the 4+2 part was getting
   identified as a 2+2 part
- **Platform Affected:**
  AML-Y42
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

13 Version 3.6.5 Details

13.1 New Feature

13.1.1 Feature 1

- **Description\Solution:**
  New AML-Y 4+2 Platform VR POR file WW38'18
    - Update power limits and VR config values for AML Y 4+2
- **Platform Affected:**
  AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

14   Version 3.6.4 Details

14.1   New Feature

14.1.1   Feature 1

- **Description\Solution:**
  Add Integrate AML-Y42 Microcode Patch
- **Platform Affected:**
  All
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuRegs.h

14.1.2   Feature 2

- **Description\Solution:**
  Integrate latest VBIOS V1060 and GOP V1081
- **Platform Affected:**
  KBL/AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

15   Version 3.6.3 Details

15.1   New Feature

15.1.1   Feature 1

- **Description\Solution:**
  Add additional BIOS related BIOS Guard debug data
    -Add additional BIOS Guard Module debug data
    -Update casting for BIOS Guard Module size
- **BiosGuardServices sPlatform Affected:**
  All
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  KabylakeSiliconPkg/Cpu/Include/BiosGuard.h

15.1.2   Feature 2

- **Description\Solution:**
  BIOS need to suport VrPowerDelivery , platform id not CPU ID , general request Per Product
- **Platform Affected:**
  All
- **Affected Files:**

  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

15.1.3   Feature 3

- **Description\Solution:**

TjMax Offset Overclocking feature on CFL-S 8+2 K SK   -Added range checking to prevent infinite warm reset cycle issue.

- **Platform Affected:**
  CFL-S 8+2 K
- **Affected Files:**

  KabylakeSiliconPkg/Cpu/Include/Library/CpuMailboxLib.h

  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

15.1.4 Feature 4

- **Description\Solution:**

Request to disable PECI reset on exit PKB-C10 by default on KBL/ KBL-R and AML platforms. Changed PeciC10Reset policy default to 'enabled'. THis will send MBX cmd 0x24 with data = 1 to pcode on every boot.

- **Platform Affected:**
  KBL, KBL-R, AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigLibPreMemConfig.h
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

15.2 Fixed bugs

15.2.1 Bug 1:

- **Description\Solution:**
  KBL-S RVP8 CPU Package Power can't up to max after adding workload
- **Platform Affected:**
  KBL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

15.2.2 Bug 2:

- **Description\Solution:**
  EnergyEfficientTurbo Default Setting on CFL-S 6+2 SKU with KBL It should be EnergyEfficientTurbo(CpuPowerMgmtTestConfig->EnergyEfficientTurbo) but not EnergyEfficentPState(CpuPowerMgmtTestConfig->EnergyEfficientPState)
- **Platform Affected:**
  CFL-S
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

15.2.3 Bug 3:

- **Description\Solution:**
  CFL ctdp override programming missing in KBL codebase mCflPpmCtdpOverrideTable is not applied for ctdp CFL SKUs.

- **Platform Affected:**
  CFL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

16 Version 3.6.2 Details

16.1 New Feature

16.1.1 Feature 1

- **Description\Solution:**
  PL2 limit is set to 8.7W instead of 24W in BIOS
- **Platform Affected:**
  AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

16.2 Fixed bugs

16.2.1 Bug 1:

None.

17   Version 3.6.1.1 Details

17.1   New Feature

17.1.1   Feature 1
None

17.2   Fixed bugs

17.2.1   Bug 1:
None.

18 Version 3.6.1 Details

18.1 New Feature

18.1.1 Feature 1

- **Description\Solution:**
  PL2 limit is set to 8.7W instead of 24W in BIOS
- **Platform Affected:**
  AML
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

18.1.2 Feature 2

- **Description\Solution:**
  Updated AML-Y 2+2 7W KC GT TDC from 14A to 18A.
- **Platform Affected:**
  KBL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

18.2 Fixed bugs

18.2.1 Bug 1:

- **Description/ Solution:**
  Incorrect boundary checks could potentially be exploited. Revised code to make safer use of memory.
- **Platform Affected**
  KBL
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c

19 Version 3.6.0 Details

19.1 New Feature

19.1.1 Feature 1

- **Description\Solution:**
  Disable EnergyEfficientTurbo for CFL S 6+2 and CFL S 8+2
- **Platform Affected:**
  CFL S 6+2 and CFL S 8+2
- **Affected Files:**
  KabylakePlatSamplePkg/Library/PeiPolicyDebugLib/PeiCpuPolicyDebugLib.c
  KabylakePlatSamplePkg/Library/PeiPolicyDebugLib/PeiPolicyDebugLib.inf
  KabylakePlatSamplePkg/Setup/CpuSetup.hfr
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

19.2 Fixed bugs

None.

20 Version 3.5.0 Details

20.1 New Feature

20.1.1 Feature 1

- **Description\Solution:**
  New CFL Platform VR POR file WW20'18
- **Platform Affected:**
  CFL- CNP-PCH, KBP
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

20.2 Fixed bugs

None.

21   Version 3.4.0 Details

21.1   New Feature

None.

21.2   Fixed bugs

21.2.1   Bug 1:
- **Description/ Solution:**
  5W power limit overrides are incorrect.
- **Platform Affected**
  KBL-YR
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

22   Version 3.3.0 Details

22.1   New Feature

22.1.1   Feature 1

- **Description\Solution:**
  Added TjMax Offset Overclocking feature on CFL-S 8+2 K SKU
- **Platform Affected:**
  CFL-S 8+2 K SKU
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  KabylakeSiliconPkg/Cpu/Include/Library/CpuMailboxLib.h
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

22.1.2   Feature 2

- **Description\Solution:**
  BIOS present Menu option list to support override platform VR parameters based on Platform ID.
- **Platform Affected:**
  All
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
  KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

22.2   Fixed bugs

22.2.1   Bug 1:

- **Description/ Solution:**
  Changed ratio limits to 255 max range entry.
- **Platform Affected**
  CFL-S 8+2 K SKU
- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtBasicConfig.h

23 Version 3.2.1 Details

23.1 New Feature

23.1.1 Feature 1

- **Description\Solution:**
  New KBL Platform VR POR file WW13'18
- **Platform Affected:**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

23.2 Fixed bugs

23.2.1 Bug 1:

- **Description/ Solution:**
  Fix TC MINTREE failure.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

24 Version 3.2.0 Details

24.1 New Feature

24.1.1 Feature 1

- **Description:**
  [CFL-S][KBP-H] CFL82/62/42 compatibility: BIOS should override platform VR parameters based on Platform ID and not CPU ID
- **Solution:**
  Added VR override table for CFL-S CPU skus and new VrPowerDeliveryDesign config block item to the VR config block.
- **Platform Affected:**
  CFL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPolicyCommon.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuPlatformLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

24.1.2 Feature 2

- **Description:**
  Single FRC for Kabylake and KabylakeG
- **Solution:**
  Single FRC for Kabylake and KabylakeG.
- **Platform Affected:**
  KBL, CFL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuPlatformLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

24.1.3   Feature 3

- **Description:**
  [CFL][KBP][OC]: Add Option to Disable Thermal Turbo Behavior for OC
- **Solution:**
  [CFL][KBP][OC]: Add Option to Disable Thermal Turbo Behavior for OC.
- **Platform Affected:**
  KBL, CFL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

24.2   Fixed bugs

None

25   Version 3.1.2 Details

25.1   New Feature

None

25.2   Fixed bugs

None

26   Version 3.1.1 Details

26.1   New Feature

26.1.1   Feature 1

- **Description:**
  Add support for CFL S 2+2/2+1 sku which are fused down version of 4+2
- **Solution:**
  Add SA and GT DID to BIOS to support these new skus
- **Platform Affected:**
  CFL
- **Affected Files:**
  /KabylakePlatSamplePkg/InternalOnly/Platform.ini
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  /KabylakeSiliconPkg/SystemAgent/Include/SaRegs.h

26.2   Fixed bugs

26.2.1   Bug 1:

- **Description/ Solution:**
  Loadline values are decremented by 1 every reboot. Fixed the math
  rounding error in fixed point arithmetic.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakePlatSamplePkg/Setup/CpuSetup.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

27 Version 3.0.1 Details

27.1 New Feature

None

27.2 Fixed bugs

None

28 Version 3.0.0 Details

28.1 New Feature

None

28.2 Fixed bugs

28.2.1 Bug 1:

- **Description/ Solution:**
  [KBL-R] BVT shows failure (not locked Power Limit 4) when Power Limit 4 Override is disabled.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

29   Version 2.9.2 Details

29.1   New Feature

None

29.2   Fixed bugs

None

30 Version 2.9.0 Details

30.1 New Feature

None

30.2 Fixed bugs

30.2.1 Bug 1:

- **Description/ Solution:**
  [CNL][BIOS Guard]BIOS Guard could hang when PcdCpuSmmEnableBspElection is set to TRUE. Index is not always 0 for SMM BSP. SMM BSP may be any CPU when PcdCpuSmmEnableBspElection is set to TRUE. Updated BIOS Guard code to account for System BSP not always being index 0.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c

30.2.2 Bug 2:

- **Description/ Solution:**
  [CFL][OC] VR menu needs to display actual values not zeros. Have the VR menu display the actual values programmed by BIOS instead of 0.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakePlatSamplePkg/Setup/CpuSetup.c
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h

30.2.3 Bug 3:

- **Description/ Solution:**
  [CFL-KBP-H & CNP-H][OC]: BIOS overrides are breaking OC.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakePlatSamplePkg/Library/PeiPolicyUpdateLib/PeiCpuPolicyUpdate.c
  /KabylakePlatSamplePkg/Library/PeiPolicyUpdateLib/PeiPolicyUpdateLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

31 Version 2.8.1 Details

31.1 New Feature

None

31.2 Fixed bugs

None

32 Version 2.8.0 Details

32.1 New Feature

32.1.1 Feature 1:

- **Description\Solution:**
  Need to add BiosGuard Module version number to Firmware Volume Information (FVI) table. Added dynamic updating of BIOS Guard MajorVersion, MinorVersion, and BuildNumber to FVI table. Updated TXT FVI logic.
- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h

32.2 Fixed bugs

32.2.1 Bug 1:

- **Description/ Solution:**
  Fix CPU demotion/un-demotion programming in Intel reference code. The Package C state Demotion and Undemotion should both be 0 on KBL. But the reference code only update PkgCStateDemotion. Found Intel reference code 2.7.0 demotion and un-demotion code is against spec.
- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtTestConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

32.2.2 Bug 2:

- **Description/ Solution:**
  V105_RVP3 and RVP7_PREF Cold boot time out of PV criteria.
- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

32.2.3 Bug 3:

- **Description/ Solution:**

PLL Trim settings causes an endless warm reset cycle with CFL42 (i3-8350K)

- **Platform Affected**

  All

- **Affected Files:**

  /KabylakePlatSamplePkg/Setup/SaSetup.h

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

33 Version 2.7.2 Details

33.1 New Feature

33.1.1 Feature 1:

- **Description\Solution:**
  Request new mailbox command in reference code for IMVP8 SVID VR Controller issue.
- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

33.2 Fixed bugs

33.2.1 Bug 1:

- **Description/ Solution:**
  BIOS can get stuck in an infinite S3 loop when EC failure occurs and BIOS Guard flow calls for cold reset
- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/PeiBiosGuardLib.inf

33.2.2 Bug 2:

- **Description/ Solution:**
  Reviewed debug_error usage and clean up incorrect use of debug_error. Change erroneous DEBUG_ERROR to DEBUG_WARN
- **Platform Affected**
  KBL-R
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/SoftwareGuard.c

33.2.3   Bug 3:

- **Description/ Solution:**
  Linker error for intrinsic function
- **Platform Affected**
  KBL-R
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

33.2.4   Bug 4:

- **Description/ Solution:**
  Fixed KlocWork error by clearing Mailboxdata, to make sure that it is initialized correctly.
- **Platform Affected**
  KBL-R
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

34 Version 2.7.0 Details

34.1 New Feature

34.1.1 Feature 1:

- **Description\Solution:**
  Add new CFL-S device IDs to check for CFL-S.
- **Platform Affected**
  CFL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

34.2 Fixed bugs

34.2.1 Bug 1:

- **Description/ Solution:**
  PL4 override error with KBL SiC v.2.5.0
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

35 Version 2.6.2 Details

35.1 New Feature

35.1.1 Feature 1:

- **Description\Solution:**
  Add new CFL-S device IDs to check for CFL-S.
- **Platform Affected**
  CFL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

35.2 Fixed bugs

35.2.1 Bug 1:

- **Description:**
  Change PL2 value to 122W to improve performance
- **Solution**:
  Updated PL2 values
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

36   Version 2.6.1 Details

36.1   New Feature

None

36.2   Fixed bugs

36.2.1   Bug 1:

- **Description:**
  In SGX functionality, EPID & PSE Provision part is failing. The SGX functionality is failing due to BIOS programming lower SE_SVN number than what CFL BIOS Buard binary module supports.
- **Solution**:
  Update the SE_SVN number for CFL to recommended value of 0x80. Also, had to add a runtime CPU detection check because the SE_SVN values are different between KBL & CFL.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c

37   Version 2.6.0 Details

37.1   New Feature

None

37.2   Fixed bugs

37.2.1   Bug 1:

- **Description:**
  PL4 override error with KBL SiC v.2.5.0.
- **Solution**:
  Fix PL4 override values which were off by 10x
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

37.2.2   Bug 2:

- **Description:**
  Add CPUID values for CFL 8 +2 P0.
- **Solution**:
  CFL new CPUID values. Add CPUID values for CFL 8 +2 P0.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakePlatSamplePkg/Setup/CpuSetup.c
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h

37.2.3   Bug 3:

- **Description:**
  Ring downbin is disabled by default.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

38 Version 2.5.1 Details

38.1 New Feature

None

38.2 Fixed bugs

38.2.1 Bug 1:

- **Description:**
  Update to Include production signed Bios Guard binary in CFL Bios.
- **Solution**:
  - Production signed BiG module compatible with KBL PCH.
  - Short term solution only for the CFL-S binary that is on KBL_PO to ungate Beta milestone.
  - BIOS will always load the production CFL BIOS Guard binary Module.
  - BIOS will dynamically detect CFL-S CPU and apply SVN 0x01.
  - BIOS will dynamically detect CFL-S CPU and disable PCH OC Watchdog timer prior to invoking BIOS Guard module and enable the time upon return from BIOS Guard module
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.inf
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuPlatformLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

39   Version 2.5.0 Details

39.1   New Feature

None

39.2   Fixed bugs

39.2.1   Bug 1:

- **Description:**
  Updates to KBL MRC from Latest Feedback
- **Solution**:
  Dq Pi Reserves Changes - ensuring that MRC algorithms reserve enough PI values to properly margin, and can accomodate a limited PI Range.
  Adding Read Voltage Centering during MrcReadODTTraining
  Increasing Write and Read DIMM ODT Duration by 1 for DDR4 on H/S SKUs
  Update CMD Loop Count for RMT, from 10 to 17
  Update MrcGetBERMarginByte() to check RcvEnaX for MrcCalcMaxRxMargin
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

39.2.2   Bug 2:

- **Description\Solution:**
  Fix ICCMAX #define units to 1/4A instead of 1/8A.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h

39.2.3   Bug 3:

- **Description\Solution:**
  Add CFL-S 4+2 support for VR overrides, CFL BIOS needs to sync to the latest CFL VR POR overrides.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommo n.h

39.2.4 Bug 4:

- **Description\Solution:**
  CPU MP driver not updating the PcdCpuApLoopMode based on Setup/UPD & must depend on MonitorMWaitEnable UPD/Setup.
- **Solution**
  Set PcdCpuApLoopMode according to setup policy
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf

40 Version 2.4.0 Details

40.1 New Feature

None

40.2 Fixed bugs

40.2.1 Bug 1:

- **Description:**
  Update to Include production signed Bios Guard binary in CFL Bios & more
- **Solution**:
  Production signed BiG module compatible with KBL PCH.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.inf
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuPlatformLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

41   Version 2.3.0 Details

41.1   New Feature

None

41.2   Fixed bugs

41.2.1   Bug 1:

- **Description:**
  BCLK Aware Adaptive voltage and DDR runtime OC feature are not enabled
- **Solution**:
  Enable both features.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

41.2.2   Bug 2:

- **Description:**
  Power limit 4 value is not overriding on KBL-R Board
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h

41.2.3   Bug 3:

- **Description:**
  Clean up unnecessary code for booting Windows for MinTree - Security features
- **Solution**:
  Updated SmmSpiFlashCommonlib to remove BIOS Guard related code in MinTree. Removed CpuSecurityPreMemConfig.h, CpuTxtPreMemConfig.h, BootGuardLib.h, TxtLib.h, SoftwareGuardLib.h, TxtPeiLib.h, BiosGuard.h, Txt.h, Txt.inc, TxtInfoHob.h files.
- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPolicyCommon.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibrary.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibPreMem.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/PeiDxeSmmCpuCommonLib.inf

41.2.4   Bug 4:

- **Description/Solution:**
  Merge 6 and 8 core support from KBL_GO_PO stream for Overclocking
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtBasicConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c

41.2.5   Bug 5:

- **Description/Solution:**
  Realtime Memory Timings enable/disable, Voltage PLL trim for all CPU domains, New PLL Trim option for Ring, GT, SA, Mc, Support for Ring down bin disable
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.c

42 Version 2.2.0 Details

42.1 New Feature

None

42.2 Fixed bugs

42.2.1 Bug 1:

- **Description:**
  System hang at PC:0036 while running Reboot cycle
- **Solution**:
  If GDT is in flash, copy to memory.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.c

42.2.2 Bug 2:

- **Description:**
  Processor Stepping shown as Unknown for KBL-R QS Samples
- **Solution**:
  Fix entry in CpuSetup.c table.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakePlatSamplePkg/Setup/CpuSetup.c
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h

42.2.3 Bug 3:

- **Description:**
  CpuMpPei driver uses - Non-Reserved Memory for S3 case & Doesn't update its memory usage to wrapper code for FSP
- **Solution**:
  Need to hardcode FSP memory used by FSP Wrapper.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.inf
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.c

43 Version 2.1.0 Details

43.1 New Feature

43.1.1 Feature 1:

- **Description\Solution:**
  Add support for optimized settings (hybrid graphics) on KBL.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuPlatformLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c

43.2 Fixed bugs

None

44   Version 2.0.0 Details

44.1   New Feature

None

44.2   Fixed bugs

44.2.1   Bug 1:

- **Description:**
  Use Feature or IP base flag to exclude unnecessary code for MinTree.
- **Solution:**
  There were too many MinTree flag used for multiple features/IPs. Used Feature or IP base flag instead so code can be more readable and modular.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c

45 Version 1.9.0 Details

45.1 New Feature

None

45.2 Fixed bugs

45.2.1 Bug 1:

- **Description:**
  PL1 and ICCMAX values for core, GT and SA are not set properly. This impacts platform power/performance.
- **Solution:**
  Remove code incorrectly overriding the default IccMax settings at power-on. Add a conditional check before configuring IccMax and VR parameters.
- **Platform Affected**
  KBL-R
- **Affected Files:**
  /KabylakeSiliconPkg/KabylakePlatSamplePkg/Library/PeiPolicyUpdateLib/PeiCpuPolicyUpdate.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

46 Version 1.8.0 Details

46.1 New Feature

None

46.2 Fixed bugs

46.2.1 Bug 1:

- **Description:**
  FSP overrides GDT causing S3 resume failure.
- **Solution:**
  After enlarging PcdS3AcpiReservedMemorySize from 0x1A0000 to 0x1C0000, we cannot reproduce S3 resume issue related to CpuMpPei BP1341 changes so added back the change to fix FSP GDT override issue.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.c
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.h
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/CpuMpPei.inf
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/Ia32/MpEqu.inc
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/Ia32/MpFuncs.asm
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/Ia32/MpFuncs.nasm
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/Microcode.c
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/Microcode.h
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/X64/MpEqu.inc
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/X64/MpFuncs.asm
  /KabylakeSiliconPkg/Override/UefiCpuPkg/CpuMpPei/X64/MpFuncs.nasm

46.2.2 Bug 2:

- **Description:**
  KBL-R BIOS: Power Management default overrides for KBL-R skus.
- **Solution:**
  KBL-R requires power management related default overrides in place for the new SKUs. Specifically for PL2, PL4, and VR TDC IA/GT.
- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

46.2.3   Bug 3:

- **Description:**
  Fixed a pointer bug in TXT save/restore of SMI enables.
- **Solution:**
  DisableSmiSources() routine corrupts the memory contents on the stack.
  "SavedSmiSourcesVariablesPointer + 8" must be
  "SavedSmiSourcesVariablesPointer + 1". "SavedSmiSourcesVariablesPointer +
  8" is equivalent to "&(SavedSmiSourcesVariablesPointer[8])".
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c

46.2.4   Bug 4:

- **Description:**
  Clean up CPU reference code that is not required for MinTree BIOS.
- **Solution:**
  Remove mailbox from mintree.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuMailboxLib.h

46.2.5   Bug 5:

- **Description/Solution:**
  Update policy comments and setting policy to minimize C6 DRAM Power
  Gating.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSecurityPreMemConfig.h

46.2.6   Bug 6:

- **Description/Solution:**

PECI May Not be Functional after Package C10 Resume.

- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc
  /KabylakeFspPkg/Library/PeiPolicyUpdatePreMemLib/PeiCpuPolicyUpdatePreMem.c
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigLibPreMemConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuMailboxLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c c

46.2.7   Bug 7:

- **Description/Solution:**
  CPU temperature cannot be read due to PECI communication fail.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc
  /KabylakeFspPkg/Library/PeiPolicyUpdatePreMemLib/PeiCpuPolicyUpdatePreMem.c
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigLibPreMemConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuMailboxLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

46.2.8   Bug 8:

- **Description/Solution:**
  System hang during post with OEM logo
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c
  /KabylakeSiliconPkg/Hsti/Dxe/MpServiceHelp.c

47 Version 1.7.0 Details

47.1 New Feature

None

47.2 Fixed bugs

None

48   Version 1.6.0 Details

48.1   New Feature

None

48.2   Fixed bugs

48.2.1   Bug 1:

- **Description:**
  Premem Code cache programming is incorrect in FSP wrapper build.
- **Solution:**
  Limit the CodeRegionSize to LLCSize-0.5MB (Reserved)-0.25MB (Data Cache), if requested is more than the available SKU LLC.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.asm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.nasm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.S

48.2.2   Bug 2:

- **Description:**
  Update CPU information for KBL-R.
- **Solution:**
  CPU Family/Model are the same as KBL. Only stepping information needs to be added KBL-R.
- **Platform Affected**
  KBL-R
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h

48.2.3   Bug 3:

- **Description:**
  Scrub undocumented register access - MMIO code in CPU.
- **Solution:**
  CPU Family/Model are the same as KBL. Only stepping information needs to be added KBL-R.
- **Platform Affected**

KBL-R

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuCommonLib.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c

48.2.4   Bug 4:

- **Description:**
  With FSP, Processor trace memory values are not maintained after S3 resume.
- **Solution:**
  Use HOB and PCDs to save and restore Processor Trace S3 resume data in FSP
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/Include/Private/CpuInitDataHob.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Pch/PchInit/Smm/PchInitSmm.h
  /KabylakeSiliconPkg/SiPkg.dec

48.2.5   Bug 5:

- **Description:**
  C7 % is low when HDMI/DP monitor is being used.
- **Solution:**
  For KBL, pkgc demotion so it should be disabled in bios.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc
  /KabylakeFspPkg/Library/PeiPolicyUpdateLib/PeiCpuPolicyUpdate.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

48.2.6   Bug 5:

- **Description:**
  Update KBL-R DID 0x5914 for CNL SKU.

- **Platform Affected**
  KBL
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/SystemAgent/Include/SaRegs.h

48.2.7 Bug 7:

- **Description:** Microcode load in SEC phase won't work if patches are not 2K aligned.
- **Solution:** Remove 2K alignment check
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.asm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.nasm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.S

48.2.8 Bug 8:

- **Description:** Update CPUID for KBL-R in MRC and MiniBIOS.
- **Solution:** Remove 2K alignment check
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/SystemAgent/MemoryInit/Include/MrcInterface.h
  /KabylakeSiliconPkg/SystemAgent/MemoryInit/Library/Private/PeiMemoryInitLib/MemoryInit.c
  /KabylakeSiliconPkg/SystemAgent/MemoryInit/Library/Private/PeiMemoryInitLib/Source/Include/MrcVersion.h
  /KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/Common/CpuRegs.h
  /KabylakeSiliconPkg/SystemAgent/MemoryInit/MiniBios/MEMORY/MrcOemPlatform.c

48.2.9 Bug 9:

- **Description:** Potential risk when scanning for microcode in PeiCpuPolicyLib.
- **Solution:** When PcdFlashMicrocodeFvBase or Size is 0, skip searching for microcode.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

49   Version 1.5.0 Details

49.1   New Feature

None

49.2   Fixed bugs

None

50　Version 1.4.1 Details

50.1　New Feature

None

50.2　Fixed bugs

50.2.1　Bug 1:

- **Description\Solution:**
  Fix KlocWork issues of KBL CPU RC.
- **Platform Affected**
  All
- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

50.2.2　Bug 2

- **Description:**
  Kabylake BIOS hangs at PC0x36 on PPV RVP10 after a fuse override

- **Solution:**
  All threads are not entering SMM when a SMI happens. But BIOS guard requires all threads to enter SMM, for any SMI generation. Because of this reason, system hangs in BiosGuard when SMI occurs and if one or more threads doesn't enter SMM.

  We have updated BiosGuard driver to skip NVRAM write and exit safely from SMM if any of the thread doesn't enter SMM.

- **Platform Affected:**
  All

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c

  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.h

  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.inf

50.2.3   Bug 3

- **Description:**
  Redefine ARRAY_SIZE macro considering compatibility issues with future EDK.

- **Solution:**
  SiliconPkg defined ARRAY_SIZE macro and it may be redefined in future EDK open source. To maintain compatibility, we need to redefine it with condition.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

50.2.4   Bug 5

- **Description/ Solution:**
  Store and restore each thread's memory address pointer in S3 resume.

- **Platform Affected**
  All

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.h

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.h

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MpCpu.c

  /KabylakeSiliconPkg/Cpu/Include/CpuDataStruct.h

  /KabylakeSiliconPkg/Cpu/Include/Private/CpuInitDataHob.h

  /KabylakeSiliconPkg/Cpu/Include/Private/CpuPrivateData.h

  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuS3Lib.h

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.h

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3Lib.inf

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3LibNull/CpuS3LibNull.c

51 Version 1.4.0 Details

51.1 New Feature

51.1.1 Feature 1:

51.1.1.1 Description/ Solution:

CpuRatioOverride needs to be disabled by default.

51.1.1.2 Platform Affected

All

51.1.1.3 Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigLibPreMemConfig.h

/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

51.2 Fixed bugs

51.2.1 Bug 1:

51.2.1.1 Description/ Solution:

Machine hung in EFI while running warm restarts

51.2.1.2 Platform Affected

All

51.2.1.3 Affected Files:

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

51.2.2   Bug 2:

51.2.2.1   Description/ Solution:

Intel Selftest tool reported failure on SKL i5-6500 CPU

51.2.2.2   Platform Affected

All

51.2.2.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/MiscFunctions.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/Thermal.c

51.2.3   Bug 3:

51.2.3.1   Description/ Solution:

Update PEI_MIN_MEMORY_SIZE to handle up to 2MB on a 4-core system. Update PEI_MIN_MEMORY_SIZE to handle up to 2MB on a 4-core system.

51.2.3.2   Platform Affected

All

51.2.3.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h

51.2.4   Bug 4:

51.2.4.1   Description/ Solution:

Description: Correcting the missed alignment, detected through the alignment check

Solution: Keep all FSP UPD in naturally aligned byte order

51.2.4.2   Platform Affected

All

51.2.4.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigFspData.h

51.2.5   Bug 5:

51.2.5.1   Description/ Solution:

Remove unused Global_remove_if_unreferenced variables in CPU code.

51.2.5.2   Platform Affected

All

51.2.5.3   Affected Files:

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c

51.2.6   Bug 6:

51.2.6.1   Description/ Solution:

MinTree Cleanup by removing dependency on BpCommonPkg, ClientCommonPkg and KabylakeFspPkg.

51.2.6.2   Platform Affected

All

51.2.6.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/PeiDxeSmmCpuPlatformLib .inf

51.2.7   Bug 7:

51.2.7.1   Description/ Solution:

Fix CPU RC Klockwork issues

51.2.7.2   Platform Affected

All

51.2.7.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

51.2.8   Bug 8:

51.2.8.1   Description/ Solution:

Description: Keep all UPD's naturally aligned

Solution: Keep all FSP UPD in naturally aligned byte order

51.2.8.2   Platform Affected

All

51.2.8.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigFspData.h

51.2.9   Bug 9:

51.2.9.1   Description/ Solution:

Update documentation for Overclocking config blocks and PCDs, and for
CpuPidTestConfig. Update documentation for Overclocking config blocks and PCDs, and
for CpuPidTestConfig.

51.2.9.2   Platform Affected

All

51.2.9.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPidTestConfig.h

51.2.10   Bug 11:

51.2.10.1   Description/ Solution:

ConfigBlock for PEI and DXE should be documented that if they are related

51.2.10.2   Platform Affected

All

51.2.10.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/BiosGuardConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSecurityPreMemConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSgxConfig.h

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTxtPreMemConfig.h

51.2.11   Bug 12:

51.2.11.1   Description/ Solution:

Description: Disabling thermal monitor also disables BIDIR_PROCHO

Solution: Decoupling PROCHOT and Thermal Monitor programming

51.2.11.2   Platform Affected

All

51.2.11.3   Affected Files:

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/Thermal.c

51.2.12   Bug 13:

51.2.12.1   Description/ Solution:

Description: Interrupt in cache code can trigger SW hang

Solution: Fix Interrupt cache code to resolve SW hang

51.2.12.2   Platform Affected

All

51.2.12.3   Affected Files:

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c

51.2.13   Bug 14:

51.2.13.1   Description/ Solution:

Description: SUT is hangs at Post code "0096" when CSM control is set to ON

Solution: Override the Fsp Hob for the CsmFlag for wrapper usage (thereby avoiding different check condition in rest of the place). CsmFlag is specific to BL, and should not be part of FSP

51.2.13.2   Platform Affected

All

51.2.13.3 Affected Files:

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

52 Version 1.3.0 Details

52.1 New Feature

None

52.2 Fixed Bugs

None

52.3 Known Issues

None

53   Version 1.2.0 Details

53.1   New Features

None

53.2   Fixed Bugs

None

53.3   Known Issues

None

54 Version 1.1.0 Details

54.1 New Feature

54.1.1 Feature1

- **Description/ Solution:**
  C6Dram disabling in BIOS by default.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSecurityPreMemConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

55   Version 1.0.5 Details

55.1   New Feature

55.1.1   Feature1

- **Description/ Solution:**
  Set HWPS maximum performance to 0xFF when enabling the over clocking menu.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

55.1.2   Feature2

- **Description/ Solution:**
  Integrate BIOS Guard Module 2.0.3683 to address irresponsible access to SBREG which may lead to limited data corruption.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h

55.1.3   Feature3

- **Description/ Solution:**
  Clean up FreePool usage in PEI Pch, Cpu, Core, SystemAgent, Csme and Security.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosType4.c

55.2   Fixed Bugs

55.2.1   Bug Name 1

- **Description:**
  Voltage Optimization setup default does not work properly.

- **Solution:**
  Set default value based on CPU SKU.

- **Platform Affected**
  ALL.

- **Affected Files:**

/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h

56   Version 1.0.4 Details

56.1   New Feature

56.1.1   Feature1

- **Description/ Solution:**
  Lock CPU soft straps on S3 Resume path.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c

56.1.2   Feature2

- **Description/ Solution:**
  Use PCD instead of Build flags in BIOS code base.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MemoryOperation.c

56.1.3   Feature3

- **Description/ Solution:**
  Correct ASSERT_EFI_ERROR usage.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/MiscFunctions.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtDts.c

56.1.4   Feature4

- **Description/ Solution:**
  Add CSM support for FSP Wrapper Build.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c

/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

56.2 Fixed Bugs

56.2.1 Bug Name 1

- **Description:**
  Voltage Optimization setup default does not work properly in HALO SKU's.

- **Solution:**
  Set default value based on CPU SKU.

- **Platform Affected**
  ALL.

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

56.2.2 Bug Name 2

- **Description:**
  If APs are reset immediately after locking, APs may not unlock spinlock.

- **Solution:**
  Re-inialize spinlock if AP times outs on StartupAllAps.

- **Platform Affected**
  ALL.

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

57 Version 1.0.3 Details

57.1 New Feature

57.1.1 Feature1

- **Description/ Solution:**
  CpuPrivateData needs to store address into structure before passing that to another structure.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/Include/CpuDataStruct.h

57.2 Fixed Bugs

57.2.1 Bug Name 1

- **Description:**
  Build error with Non-MS Complier.

- **Solution:**
  Fix multiple definition of "mCpuGlobalNvsAreaPtr" in KabylakeSiliconPkg CpuPowerManagementSmm module.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtDts.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHdc.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHwpLvt.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtSmm.

58 Version 1.0.2 Details

58.1 New Feature

58.1.1 Feature1

- **Description/ Solution:**
  After setting a core PLL VccTrim offset in OC->Processor menu, the PLL Trim values should be increased by that offset. This flow requires a warm reset to apply.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

58.1.2 Feature2

- **Description/ Solution:**
  Request policy for specific VR commands for KBL UEFI codebase - PS4 exit and VR decay BIOS mailbox commands.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

58.2 Fixed Bugs

58.2.1 Bug Name 1

- **Description:**

  Source level debug via UDK debugger not working once under BDS phase.

- **Solution:**
  Source level debug interrupts are being overwritten. If source level debug enabled, don't overwritten interrupts.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c

58.2.2 Bug Name 2

- **Description:**
  Not able to read PL3 values from [MSR 615(23:17)] as per PL3 bios option help text.

- **Solution:**
  Changed pl3 setup option to drop down menu and added input validation check to PL3.

- **Platform Affected**
  KBL-U/Y

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtBasicConfig.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

59   Version 1.0.1 Details

59.1   New Feature

59.1.1   Feature1

- **Description/ Solution:**
  Change all MCHBAR usage to UINT32 to compatible with 32bit/64bit build and clear upper 32bit to 0 for MCHBAR to make sure the MCHBAR is 32bit width.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuMailboxLib/MaiboxLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/IdleStates.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/MiscFunctions.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PerformanceStates.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PowerLimits.c

59.1.2   Feature2

- **Description/ Solution:**
  Add ACPI variable for DTS interrupt check.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl
  /KabylakeSiliconPkg/Cpu/Include/Private/PowerMgmtNvsStruct.h
  /KabylakeSiliconPkg/Cpu/Include/Protocol/CpuGlobalNvsArea.h
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtDts.c

59.1.3   Feature3

- **Description/ Solution:**
  Modify "CalculateTimeout" function to handle UINT64 timeout value properly.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

59.1.4   Feature4

- **Description/ Solution:**
  Create Boot Guard Null library and made sure function values made sense.

Kaby Lake CPU Initialization Code Version 3.7.6
Release Notes   2018
88   **Intel Restricted Secret**

- **Platform Affected**
  All

- **Affected Files:**

 Add:
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmBootGuardLibNull/BootGuardLibraryNull.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmBootGuardLibNull/PeiDxeSmmBootGuardLibNull.inf

59.1.5   Feature5

- **Description/ Solution:**
   Change logic to set max peformance to 0xFF when OC is enabled in the UI.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

59.1.6   Feature6

- **Description/ Solution:**
  Update MpService StartupThisAP() to follow PI definition of the function.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

59.1.7   Feature7

- **Description/ Solution:**
  Remove PchResetPpi usage as it is not compliant with PI 1.4 spec.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/PeiTxtLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c

59.1.8   Feature8

- **Description/ Solution:**
  Sync IntelFsp2pkg and IntelFsp2Wrapper pkg from EDK2 open source to KBL.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/SecCpuLibFsp.inf

59.1.9　Feature9

- **Description/ Solution:**
  Correct TPL for timer events in MpServices Protocol.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

59.1.10　Feature10

- **Description/ Solution:**
  Remove ACPI CPU comments-out code.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Cpu0Cst.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Cpu0Tst.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Ctdp.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/HwpLvt.asl

59.1.11　Feature11

- **Description/ Solution:**
   Rename MSRs from CpuRegs.h version to ArchitecturalMsr.h version.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MemoryAttribute.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MemoryOperation.c
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/MachineCheck.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHdc.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHwpLvt.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxe.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c

59.1.12　Feature12

- **Description/ Solution:**
  Move CPU strap, BCLK and over clocking mailbox programming to pre-memory
  phase to allow for higher BCLK frequency and stable OC flows.

- **Platform Affected**

All

- **Affected Files:**
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigLibPreMemConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingPreMemConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSecurityPreMemConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h
/KabylakeSiliconPkg/Cpu/Include/CpuPolicyCommon.h
/KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
/KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuPowerOnConfigLib.h
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibPreMem.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/PeiCpuOcInitLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/MiscFunctions.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c

59.1.13 Feature13

- **Description/ Solution:**
Implement FSP UPD new type: union.

- **Platform Affected**
All

- **Affected Files:**
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfigFspData.h
/KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtTestConfig.h

59.1.14 Feature14

- **Description/ Solution:**
 Load microcode update from CpuMpPei driver

- **Platform Affected**
All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

59.2 Fixed Bugs

59.2.1 Bug Name 1

- **Description:**
  After Disabling Intel Speed Shift Technology in bios SUT, is not booting to OS (BSOD is observed).

- **Solution:**
  Move OperationRegion creations out of Methods to meet ACPI best programming practices.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl

60 Version 1.0.0 Details

60.1 Fixed Bugs

60.1.1 Bug Name 1

- **Description:**
  BSOD observed with Multiprocessor_Configuration_Not_Support during Warm Reset.

- **Solution:**
  Ensure PRMRRs are programmed prior to enabling SGX across all threads.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

61 Version 0.9.1 Details

61.1 New Feature

61.1.1 Feature 1

- **Description/ Solution:**
  Move the Default initialization from SiliconPkg to PlatformPkg & Isolate the Setup updates to separate library along with Null instance.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

61.2 Fixed Bugs

61.2.1 Bug Name 1

- **Description:**
  The MMIO PL1 Tau value is not correct when DPTF enable.

- **Solution:**
  Fix mistake in code where custom value is copied to real value when custom value is 0.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

61.2.2 Bug Name 2

- **Description:**
  Systems hang with postcode 0092/0096 during Warm Reboot/S4 cycle.

- **Solution:**
  Increase timeout and retry times to make sure all APs execute BiosGuardModuleExecute function.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.h

61.2.3 Bug Name 3

- **Description:**
  BSOD observed with Multiprocessor_Configuration_Not_Support during Warm Reset.

- **Solution:**

If MSR 0x3A [18] (SGX enable bit) is out of sync, BIOS reset MSR 0x3A [0] lock bit by cold reset then re-program.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/BaseSoftwareGuardLibNull/BaseSoftwareGuardLibNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/SoftwareGuardLib.h

62   Version 0.9 Details

62.1   New Feature

62.1.1   Feature1

- **Description/ Solution:**
  Move the Default initialization from SiliconPkg to PlatformPkg and isolate the Setup updates to separate library along with Null instance.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

63 Version 0.8.1 Details

63.1 New Feature

63.1.1 Feature 1

- **Description/ Solution:**
  Enable FlashWearOutProtection by default in RC policy.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

63.1.2 Feature 2

- **Description/ Solution:**
  Use MSR definition from Cpuid.h and Msr .h files in UefiCpgPkg, and remove duplicated one from CpuRegs.h.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MemoryAttribute.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MemoryOperation.c
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/Thermal.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosCpu.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosType4.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtDts.h
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/IdleStates.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/MiscFunctions.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.inf

63.1.3　Feature 3

- **Description/ Solution:**
  Move the CPU Default initialization from SiliconPkg to PlatformPkg.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLibrary.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c

63.1.4　Feature 4

- **Description/ Solution:**
  KBL FSP expose Psys configuration policies to UPD.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/MiscFunctions.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

63.2　Fixed Bugs

63.2.1　Bug Name 1

- **Description:**
  FSP GCC TeamCity build error.

- **Solution:**
  Fix FSP GCC TeamCity Build error.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

63.2.2　Bug Name 2

- **Description:**
  Build error with enable /wall in VS2015.

- **Solution:**
  Fix the build error after enable /wall in VS2015.

- **Platform Affected**
  ALL

- **Affected Files:**

/KabylakeSiliconPkg/Cpu/Include/Private/Library/TxtPeiLib.h
/KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c

63.2.3 Bug Name 3

- **Description:**
  PRMRR Mask VALID BIT is not being set.

- **Solution:**
  Fix policy values on SGX Software Controlled Flow.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSgxRestrictedConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/CpuInitDataHob.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/SoftwareGuardLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/BaseSoftwareGuardLibNull/BaseSoftwareGuardLibNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c

64 Version 0.8.0 Details

64.1 New Feature

64.1.1 Feature1

- **Description/ Solution:**
  Fix ACPI compiler warnings

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Cpu0Hwp.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Cpu0Ist.asl
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl

64.1.2 Feature2

- **Description/ Solution:**
  Consolidate the number of calling APIs in SGX lib.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Private/CpuInitDataHob.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/SoftwareGuardLib.h
  /KabylakeSiliconPkg/Cpu/Library/Private/BaseSoftwareGuardLibNull/BaseSoftwareGuardLibNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.inf

64.1.3 Feature3

- **Description/ Solution:**
  Use Cpuid.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/Include/CpuAccess.h
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c

/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHwpLvt.c
/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.h
/KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibPreMem.inf
/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibrary.h
/KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.h
/KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/PeiDxeSmmCpuPlatformLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/MtrrSync.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3Lib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/PeiDxeSmmCpuCommonLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/PeiSmbiosCpuLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosCpu.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/PeiTxtLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtSmm.h
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtSmm.inf
/KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxe.inf
/KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.h

Delete:
/KabylakeSiliconPkg/Cpu/Include/Register/ArchitecturalMsr.h
/KabylakeSiliconPkg/Cpu/Include/Register/Cpuid.h
/KabylakeSiliconPkg/Cpu/Include/Register/Msr.h
/KabylakeSiliconPkg/Cpu/Include/Register/Msr/SkylakeMsr.h

64.1.4   Feature4

- **Description/ Solution:**
  Switch MCU patch loading from single thread to simultaneous mode.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

64.1.5   Feature5

- **Description/ Solution:**
  Disable HWP by default under Win8.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl

64.2 Fixed Bugs

64.2.1 Bug Name 1

- **Description:**
  KBL SGX random OWNER_EPOCH option locks system.

- **Solution:**
  Add proper variable to pass random 64bit value.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c

64.2.2 Bug Name 2

- **Description:**
  HWPS(Hardware P-State) maximum performance doesn't be set to 0xFF when enabling the Overclocking in BIOS menu.

- **Solution:**
  CPC table reports maximum frequency as 0xFF when a fully unlocked CPU is used.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Cpu0Hwp.asl
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c

65 Version 0.7.3 Details

65.1 New Feature

65.1.1 Feature1

- **Description/ Solution:**
  Align the IntelFspPkg and IntelFspWrapperPkg to FSP v2.0 Final Spec.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.asm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.inc
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.inc
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.S

65.1.2 Feature2

- **Description/ Solution:**
  Switch header files and remove use of CpuRegs redundant defines from
  KabylakeSiliconPkg.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/SoftwareGuard.c
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Include/Register/Cpuid.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon
  .h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.
  c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnC
  onfigLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLi
  b.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosType4.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtS3.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosType7.c

65.1.3　Feature3

- **Description/ Solution:**
  Add BIOS support for CPU V/F curves are aware of BCLK frequency when calculated.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.c

65.1.4　Feature4

- **Description/ Solution:**
  Use Cpuid.h and Msr .h files from UefiCpgPkg, and remove duplicated defines from CpuRegs.h.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/CpuAccess.h
  /KabylakeSiliconPkg/Cpu/Include/CpuRegs.h
  /KabylakeSiliconPkg/Cpu/Include/Register/Cpuid.h

65.2　Fixed Bugs

65.2.1　Bug Name 1

- **Description:**
  TXT return supported even when SMX or VMX is not supported.

- **Solution:**
  Remove return value in _PDC.

- **Platform Affected**
  ALL

- **Affected Files:**

- /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/CpuSsdt.asl

66 Version 0.7.2 Details

66.1 New Feature

66.1.1 Feature1

- **Description/ Solution:**
  Fix Doxygen warning messages for CPU RC.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtBasicConfig.h
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Library/BootGuardLib.h
  /KabylakeSiliconPkg/Cpu/Include/Private/CpuInitDataHob.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuCommonLib.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/TxtPeiLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmBootGuardLib/BootGuardLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLibNull/CpuOcLibraryNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c

66.1.2 Feature2

- **Description/ Solution:**
  Remove the "Include" path from #include <Include/Private...>.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/SoftwareGuard.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/Exception.c
  /KabylakeSiliconPkg/Cpu/Library/Private/BaseSoftwareGuardLibNull/BaseSoftwareGuardLibNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLibNull/BiosGuardInitNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Microcode.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLibNull/CpuOcInitNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLibNull/CpuOcLibraryNull.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtCommon
.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnC
onfigLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPo
werOnConfigLibDisable.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3LibNull/CpuS3LibNull.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSmmCpuCommonLib/CpuCommonLi
b.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareG
uardLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosCpu.h
/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPei.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLibNull/TxtPeiNull.c
/KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PowerMgmtInit.h
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtDts.h
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHdc.c
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtHwpLvt.c
/KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtSmm.h
/KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.h
/KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeOem.c

66.1.3   Feature3

- **Description/ Solution:**
  Build a HOB to preserve the Policy data which are need for both Pei and Dxe

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

66.1.4   Feature4

- **Description/ Solution:**
  Update CPU RC policy documentation

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c

66.1.5   Feature5

- **Description/ Solution:**
  Prevent to use any private file/protocol/ppi from SiliconPkg

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/BiosGuardConfig.h

/KabylakeSiliconPkg/Cpu/Include/Private/Library/BiosGuardInit.h

66.1.6   Feature6

- **Description/ Solution:**
  Execute DEBUG macro only on BSP, but not on APs.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.c

66.1.7   Feature7

- **Description/ Solution:**
  Clean up ASL warning messages.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/AcpiTables/CpuSsdt/Ctdp.asl

66.1.8   Feature8

- **Description/ Solution:**
  Put HW default values instead of zero for PSI cutoff in BIOS Setup.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

66.1.9   Feature9

- **Description/ Solution:**
  Clear the SPI_SYNC_SS bit before setting WPD in the BIOS CTRL register.

- **Platform Affected**

All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.inf

67   Version 0.7.1 Details

67.1   New Feature

67.1.1   Feature1

- **Description/ Solution:**
  During Monitor-Mwait flow it will check if any RUN AP SIGNAL wrote by BSP and valid, if yes, execute the AP function otherwise keep going on Mwait loop.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MpFuncs.asm
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MpFuncs.S

67.1.2   Feature2

- **Description/ Solution:**
  When SkipMpInit is enabled, exclude all MP programming.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

67.1.3   Feature3

- **Description/ Solution:**
  KBL Code Changes to handle new KBL Family IDs.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiDxeSmmCpuPlatformLib/CpuPlatformLibrary.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c

67.1.4   Feature4

- **Description/ Solution:**
  Enhance code to handle enable/disable of CSM properly.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

67.1.5   Feature5

- **Description/ Solution:**
  FSP UPD Structure modified to match version 2.0 Draft 5 spec.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

67.1.6   Feature6

- **Description/ Solution:**
  SkipMpInit UPD is enabled to Skip MP Initialization for Coreboot.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

67.1.7   Feature7

- **Description/ Solution:**
  List the API which is produced from core package in INF file.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf

67.1.8   Feature8

- **Description/ Solution:**
  Load microcode updates on APs if not loaded by FIT.

- **Platform Affected**
  All

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

67.2   Fixed Bugs

67.2.1   Bug Name 1

- **Description:**

When setting Ring Max OC ratio, Core voltage mode, voltage override, voltage offset in BIOS menu the changes doesn't be reflected to OC mailbox for CLR domain.

- **Solution:**
  Save core settings for ring domain.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c

67.2.2   Bug Name 2

- **Description:**
  If Mp Services Protocol StartupAllAps timeout occurs, processor will reset without executing other functions.

- **Solution:**
  If a AP Procedure is executing but time-outs, BSP will take back control of AP and execute same procedure again.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c

67.2.3   Bug Name 3

- **Description:**
  The value of MSR MSR_IA32_HWP_INTERRUPT and MSR MSR_PMG_CST_CONFIG_CONTROL on BSP are different than APs value if HT is not supported.

- **Solution:**
  The call of the procedure to setup the MSRs is added on BSP.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/IdleStates.c

68   Version 0.7 Details

68.1   New Features

68.1.1   Feature 1

- **Description/ Solution:**
  Sync CpuRng (Random Number Generator) library with the Open source version in MdePkg.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/Library/CpuRngLib.h
  /KabylakeSiliconPkg/Cpu/Library/BaseCpuRngLib/BaseCpuRngLib.inf
  /KabylakeSiliconPkg/Cpu/Library/BaseCpuRngLib/Ia32/CpuRng.asm
  /KabylakeSiliconPkg/Cpu/Library/BaseCpuRngLib/Ia32/CpuRng.S
  /KabylakeSiliconPkg/Cpu/Library/BaseCpuRngLib/x64/CpuRng.asm
  /KabylakeSiliconPkg/Cpu/Library/BaseCpuRngLib/x64/CpuRng.S
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/PeiBiosGuardLib.inf

68.1.2 Feature 2

- **Description/ Solution:**
  Change TDC Enable default to disabled to fix performance issues in OS timeframe.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

68.1.3 Feature 3

- **Description/ Solution:**
  Add GCC Support to Kabylake BIOS.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/Ia32/TxtPeiBspGccDummy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c

68.1.4 Feature 4

- **Description/ Solution:**
  Remove xxxFsp.inf in CPU RC, that are identical to regular xxx.inf.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  Delete:
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisableFsp.inf

68.1.5 Feature 5

- **Description/ Solution:**
  Use MtrrLib from UefiCpuPkg and stop producing PEI_CACHE_PPI.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLibFsp.inf
  Delete:
  /KabylakeSiliconPkg/Cpu/Include/Ppi/Cache.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CachePeim.c

68.1.6 Feature 6

- **Description/ Solution:**
  Update Bios guard driver to find Flash address dynamically instead of hardcoded address.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h

68.1.7 Feature 7

- **Description/ Solution:**
  Replace CpuPolicy.h with CpuPolicyCommon.h.

- **Platform Affected**
  ALL

- **Affected Files:**
  Add:
  /KabylakeSiliconPkg/Cpu/Include/CpuPolicyCommon.h
  Delete:
  /KabylakeSiliconPkg/Cpu/Include/Ppi/CpuPolicy.h#5

68.1.8 Feature 8

- **Description/ Solution:**
  Added VR specific mailbox commands to workaround customer VR issues.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

68.1.9 Feature 9

- **Description/ Solution:**
  Remove CPU S3 resume boot script and references. Use the same CPU initial for S3 resume as normal.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpService.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/x64/MpCpu.c
  /KabylakeSiliconPkg/Cpu/Include/CpuDataStruct.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuS3Lib.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/MachineCheck.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/Microcode.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/MtrrSync.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3Lib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf

68.1.10   Feature 10

- **Description/ Solution:**
  Change library instance PeiCpuPowerOnConfigLibNull to PeiCpuPowerOnConfigLibDisable.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeFspPkg/KabylakeFspPkg.dsc

  Add:
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisable.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibDisable/PeiCpuPowerOnConfigLibDisableFsp.inf
Delete:
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPowerOnConfigLibNull.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPowerOnConfigLibNull.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPowerOnConfigLibNullFsp.inf

68.1.11   Feature 11

- **Description/ Solution:**
  Use base address from TempRamInitApi for FSP.

- **Platform Affected**

  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.asm
  /KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.S

68.1.12   Feature 12

- **Description/ Solution:**
  Point out all API's usage (Produces/Consumes) on all INF files

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3Lib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareGuardLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/PeiTxtLib.inf
  /KabylakeSiliconPkg/Cpu/PowerManagement/Dxe/PowerMgmtDxe.inf
  /KabylakeSiliconPkg/Cpu/PowerManagement/Smm/PowerMgmtSmm.inf
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxe.inf

68.1.13   Feature 13

- **Description/ Solution:**
  Enable BIOS guard support in FSP wrapper build

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.c
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibrary.h
  /KabylakeSiliconPkg/Cpu/BiosGuard/Smm/BiosGuardServices.h
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.c
  /KabylakeSiliconPkg/Cpu/Include/BiosGuard.h
  /KabylakeSiliconPkg/Cpu/Include/BiosGuardDefinitions.h
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/BiosGuardConfig.h
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuBiosGuardConfig.h
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuSecurityPreMemConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Ppi/CpuPolicy.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/BiosGuardInit.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLibrary.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibrary.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/PeiBiosGuardLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLibFsp.inf

68.1.14   Feature 14

- **Description/ Solution:**
  Remove WDB WC region from SEC on Kabylake.

- **Platform Affected**
  ALL

- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.asm
  KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLib.inc
  KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.inc
  KabylakeSiliconPkg/Cpu/Library/SecCpuLib/Ia32/SecCpuLibGcc.S

68.1.15   Feature 15

- **Description/ Solution:**
  Create a PCD for ApWakeUpBuffer start address.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf
  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/MpCommon.c

68.1.16   Feature 16

- **Description/ Solution:**

BIOS Power Management overrides for KBL.

- **Platform Affected**
  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerLimits.c

68.1.17   Feature 17

- **Description/ Solution:**
  Update CPU RC policy documentation.

- **Platform Affected**
  ALL

- **Affected Files:**
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtBasicConfig.h

68.2   Fixed Bugs

68.2.1   Bug Name 1

- **Description**:
  Core ratio limits do not get set to manually set values. For example, Set 1-core ratio limit override to 25 and 2-core ratio limit override to 18. On the next reboot, 1-core ratio limit and 2-core ratio limit are not changing from the previous values.

- **Solution**:

  Fix 1-core ratio validity check to only compare to other active core's ratio limits.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PerformanceStates.c

68.2.2   Bug Name 2

- **Description**:
  S3 exit hangs at Post code 0x55 with FSP BIOS

- **Solution**:

  Remove dependencies on SMRAM. All required data is done either in FSP Wrapper (GDT, IDT setup) or passed in UPD (MTRR) and PEI MP Services AP wakeup is used instead of DXE.

- **Platform Affected**

  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf
  /KabylakeSiliconPkg/Pch/Library/Private/PeiPchInitLib/PchInit.c

68.2.3　Bug Name 3

- **Description**:
  Resolved boot failures with TXT when the Firmware Configuration Setup option was set to "Production".

- **Solution**:

  Moved the VmxEnable and SmxEnable bits from CPU Test Config structures into production CPU config structures.

- **Platform Affected**

  ALL

- **Affected Files:**
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuConfig.h
  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c

69   Version 0.6.1 Details

69.1   New Features

69.1.1 Feature 1

- **Description/ Solution:**
  Adding the support for the option to enable/disable TCO watchdog timer
- **Platform Affected**

  ALL
- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

69.1.2 Feature 2

- **Description/ Solution:**
  Adjusting the natural alignment in CpuBiosGuardConfig.h
- **Platform Affected**

  ALL
- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuBiosGuardConfig.h

69.2   Fixed Bugs

69.2.1   Bug Name 1

- **Description**:

  Can't perform S5 after resume from S3
- **Solution**:

  Restoring the PM_TMR_EMULATION_CFG MSR 0x121
- **Platform Affected**

  ALL
- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

69.2.2 Bug Name 2

- **Description**:

  Intermittent hang while stressing TXT by running SEnter/SExit/10s Wait/Cold Boot in efi mode

- **Solution**:

  Giving the APs time to enter wait-for-SIPI state

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c

70   Version 0.6.0 Details

70.1   New Features

70.1.1 Feature 1

- **Description/ Solution:**

   The following policies to determine the AP state in the DXE phase

      ApIdleManner

      ApHandoffManner

   The defaults are changed to Monitor/MWAIT state from HLT state, the intent is to comply with BWG rev2.0, #550049, and have performance and power savings benefits.

- **Platform Affected**

   ALL

- **Affected Files:**

   /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTestConfig.h
   /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c

70.1.2 Feature 2

- **Description/ Solution:**
   Removing the call of CollectProcessorFeature() across all thread before initialization, for client, it's be safely assumed there will be only one CPU, there is no need to run this module across all threads and have performance benefits.

- **Platform Affected**

   ALL

- **Affected Files:**

   /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

70.1.3 Feature 3

- **Description/ Solution:**
   Saving on the size of CPU_TXT_PREMEM_CONFIG by reducing some UINT64 elements to UINT32 and adjusting the order to achieve natural alignment.

- **Platform Affected**

   ALL

- **Affected Files:**

   /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTxtPreMemConfig.h

   /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
   /KabylakeSiliconPkg/SystemAgent/Library/Private/PeiSaInitLib/SaInitPreMem.c

70.1.4 Feature 4

- **Description/ Solution:**
  The SET_IMON_CONFIG VR sub-command 0x4 was updated and published in the BWG rev2.0, #550049 to allow for a finer resolution IMON offset to be programmed.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

70.1.5 Feature 5

- **Description/ Solution:**
  BIOS support for AVX ratio offset.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuOverclockingConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuOcLib.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.c

70.1.6 Feature 6

- **Description/ Solution:**
  PostCodes added for FSP.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/BiosGuardInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/CpuOcInit.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPowerOnConfigLibNull.c

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcLib/CpuOcLibrary.c

  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/PeiCpuPolicyLib.inf

/KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLibPreMem.in
f

/KabylakeSiliconPkg/Cpu/Library/Private/PeiBiosGuardLib/PeiBiosGuardLib.inf

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/PeiCpuInitLib.inf

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuOcInitLib/PeiCpuOcInitLib.inf

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3Lib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/PeiCpuS3LibFsp.inf

70.1.7 Feature 7

- **Description/ Solution:**
  Removing the McuUpdateDataAddr from TXT_CONFIG and the TXT HOB. TXT will
  now assume that the correct microcode has already been loaded and will simply
  verify that instead of reloading it.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuTxtPreMemConfig.h
  /KabylakeSiliconPkg/Cpu/Include/Private/Library/TxtPeiLib.h
  /KabylakeSiliconPkg/Cpu/Include/Txt.h /KabylakeSiliconPkg/Cpu/Include/Txt.inc
  /KabylakeSiliconPkg/Cpu/Include/TxtInfoHob.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLibPreMem/PeiCpuPolicyLib.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPeiLib.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/TxtDxeLib.c
  /KabylakeSiliconPkg/Cpu/TxtInit/Dxe/x64/TxtDxeAp.asm
  /KabylakeSiliconPkg/Cpu/TxtInit/Pei/Ia32/TxtPeiAp.asm16
  /KabylakeSiliconPkg/Cpu/TxtInit/Pei/Ia32/TxtPeiApGccDummy.c

70.1.8 Feature 8

- **Description/ Solution:**
  BIOS displays the calculated BCLK frequency in OC menu.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/cpu/Include/Library/CpuMailboxLib.h

70.1.9 Feature 9

- **Description/ Solution:**
  Removing the unnecessary FSP_FLAG build switch and corresponding code.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPeim.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PeiCpuPowerMgmtLi
  b.inf
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerMgmtLib/PowerMgmtInitPeim.

c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnC
onfigLib.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnC
onfigLib.inf
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPower
OnConfigLibNull.c
/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLibNull/PeiCpuPower
OnConfigLibNull.inf

70.2   Fixed Bugs

70.2.1   Bug Name 1

- **Description**:

  Got ASSERT with GCC debug build

- **Solution**:

  Use CopyMem() instead of AsciiStrnCpy() to fix missing one Null-terminated ASCII
  String.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiSmbiosCpuLib/SmbiosType4.c

70.2.2 Bug Name 2

- **Description**:

  The duplicated GUID found in the driver CpuInitDxe.inf

- **Solution**:

  Generating the new GUID.

- **Platform Affected**

  ALL

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/CpuInit/Dxe/CpuInitDxe.inf

70.2.3 Bug Name 3

- **Description**:

  S3 exit hangs at postcode 0055 on RVP8

- **Solution**:

  Adding some conditional capability check for C6Dram and SGX prior to restoring the
  MSR_PRMRR_PHYS_BASE and MSR_PRMRR_PHYS_MASK

- **Platform Affected**

Desktop

- **Affected Files:**

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

70.2.4 Bug Name 4

- **Description**:

Build error issue with VS2015

- **Solution**:

Fixing the source code build error issue with VS2015

- **Platform Affected**

All

- **Affected Files:**

/KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuS3Lib.hCpu/Library/Private/Pei cpuS3Lib/CpuS3Lib.c

70.2.5 Bug Name 5

- **Description**:

The value of SINIT and SCLEAN is 0x0 not expected 0xFF when silicon doesn't support TXT or if BIOS doesn't support TXT.

- **Solution**:

In the case, the value of SCLEAN SVN at MSR 0x302 BITS 31 to 24, should be 0xFF, and moves the code to program SCLEAN SVN to SGX library.

- **Platform Affected**

All

- **Affected Files:**

/KabylakeSiliconPkg/Cpu/Include/Private/Library/SoftwareGuardLib.h

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/Features.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuS3Lib/CpuS3Lib.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiDxeSoftwareGuardLib/PeiDxeSoftwareG uardLib.c

/KabylakeSiliconPkg/Cpu/Library/Private/PeiTxtLib/TxtPei.c

/KabylakeSiliconPkg/Cpu/Library/Private/BaseSoftwareGuardLibNull/BaseSoftwareG uardLibNull.c

70.2.6 Bug Name 6

- **Description**:

Missed FastSlew Enable/Disable implemetnation for GT and SA

- **Solution**:

Fast slew rate command is now sent for IA, GT, and SA domains

- **Platform Affected**

  All

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/ConfigBlock/CpuPowerMgmtVrConfig.h
  /KabylakeSiliconPkg/Cpu/Include/CpuPowerMgmt.h
  /KabylakeSiliconPkg/Cpu/Include/Ppi/CpuPolicy.h
  /KabylakeSiliconPkg/Cpu/Library/PeiCpuPolicyLib/CpuPrintPolicy.c
  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

70.2.7 Bug Name 7

- **Description**:

  The number of active Processor Core is not correct in BIOS during first reboot

- **Solution**:

  Fixing it caused by PCH reset type changed

- **Platform Affected**

  All

- **Affected Files:**

  /KabylakeSiliconPkg/Cpu/Include/Private/Library/CpuCommonLib.h

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuInitLib/CpuInitPreResetCpl.c

  /KabylakeSiliconPkg/Cpu/Library/Private/PeiCpuPowerOnConfigLib/PeiCpuPowerOnConfigLib.c

70.3   Known Issues

None

71 Version 0.5.0 Details

Initial Release

71.1 New Features

None

71.2 Fixed Bugs

None

71.3 Known Issues

None

§