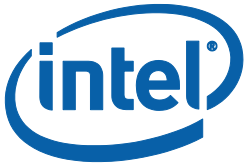

Gemini Lake Platform Silicon Initialization Code

Release Notes

January 2020 (WW02)

Contents

1 Revision History

Revision Number	Description	Revision Date
0.5	Initial Release	January 2017
0.6	Alpha Release	April 2017
0.6.5	Interim Bi-weekly release	May 2017
0.6.7	Interim Bi-weekly release	May 2017
0.7.0	Interim Bi-weekly release	June 2017
0.7.5	A1 Stepping WW30 BKC Release	July 2017
0.8.0	B0 POE SIC release	August 2017
0.8.5	B0 Bi-weekly BKC release	August 2017
0.9.0	B0 Bi-weekly BKC release	September 2017
0.9.5	B0 QS Milestone release	September 2017
1.0.0	B0 PV RC1 Release	October 2017
1.0.2	B0 RS3 Bi-weekly BKC release	October 2017
1.0.5	B0 RS2 PV BKC release	November 2017
1.2.0	B0 RS3 Bi-weekly BKC release – WW44	November 2017
1.4.0	B0 RS3 Bi-weekly BKC release – WW47	November 2017
2.0.0	B0 RS3 PV release	January 2018
2.0.1	B0 RS3 Bi-weekly BKC release – W09	February 2018
2.0.2	B0 RS4 BKC release – W15	April 2018
2.0.3.0	B0 RS4 Bi-weekly release	May 2018
2.0.4.0	B0 RS4 PV release	June 2018
2.0.4.1	B0 RS4 Bi-weekly release	June 2018
2.0.5.0	B0 RS4 Bi-weekly release	July 2018

2.0.6.0	B0 RS4 release	October 2018
2.0.7.0	B0 RS4 release	October 2018
2.0.7.1	B0 RS4 release	October 2018
2.0.8.0	B0 RS5 release	November 2018
2.0.9.0	B0 RS5 release	January 2019
2.1.0.0	B0 RS5 release	April 2019
2.2.0.0	Supports Both GLK & GLK-R Aligning with GLK-R 19H1, BKC WW28’2019	July 2019
2.2.1.0	R0 19H1 release Aligning with GLK-R PV Best Known Configuration (BKC) Software Package (Microsoft Windows*10 - 64 bit 19H1) WW40'2019	October 2019
2.2.1.1	GLK/GLK-R Independent Release, not aligned with any BKC	January 2020

§

2 Release Note

2.1 Revision 0.5.0

- Initial Release.

2.2 Revision 0.6.0

- Fix BIOS Settings Incorrect for LJ1PLL Register Values when CCP_FREF_SEL is set to 1
- Fix SUT is not entering into S0iX after S4/S5 on GLK RVP1/RVP2 .
- PSMI: Fix MOT register settings
- Fix CPU keep high performance (CPU loading always keep at 65-100%)
- UEFI Variable Attributes Should be Updated in the Recycle Flow
- Fix eMMC Command Queue Engine often gets stuck when HS400 is used
- Fix IA_UNTRUSTED bit should be set before any 3rd party code launched.
- Fix [GLK][SV] [SV BIOS] SV BIOS hangs after 466244 check-in
- Fix System hang after modify PCI B00:D13:F02 Reg0xDC, bit0 from 0 to 1 (SPI Write Protect Disable) if BIOS lock enabled
- Fix Attributes issue in SdHostDriverBindingStart
- Move IA_UNTRUSTED BIT setting from ExitBootService callback to End of PCIenumarationCallBack - Take2
- MRC 1.03 Update Set i_force_clkgateoff to 0 at beginning of lpddrgrp2m for all DRAM technologies & set i_force_clkgateoff to 0 in lpddrgrp2m instead of lpddrgrp1p5
- Fix [Flash debug IFWI on eMMC] SUT hangs at post code E8EA on eMMC boot
- Fix DispatchHandle issue in ScSmmCoreRegister
- SV Bios has garbage UART output. Corrects the problem where the code was incorrectly setting the UART to 5 bits instead of 8.
- Enable Marvell 9182 for PPV

- Fix hang on POST code "0095" when CSM always ON.
- Fix MSR 0x120 is not restored in S3 resume path
- Fix GLK A0/A1: Memory BW power measured on Reads is higher than pre-si expectations
- Fix - eMMC boot failure / BSOD (SDBUS_INTERNAL_ERRROR) observed while booting in RVP1 / I2S reworked RVP2a board.
- Fix - GLK A0/A1: Memory BW power measured on Reads is higher than pre-si expectations

2.3 Revision 0.6.5

- Added SVENTX Catalog messages for Release BIOS
- Resolved TCO_SMI is getting cleared after S3 resume in Geminilake platform.
- Added DLL 0x8 and 20mV bump - Vnn Changes for EMMC on S3 resume
- Add ExitBootServices callback for eMMC rev38 issue
- Optimize global variable usage from HECI driver.
- [Restructure] Set SGX Launch Control Enable bit by default
- Resolved : MMRC ver1.05 GLK FSP Profile values in comments in FspmUpd,h does not match MmrcProjectDefinitions.h
- Resolved : GLK BIOS: SUT hangs at PC 00E1 After waking from S3
- Added SV changes to stop UART from being initialized multiple times.
- MRC 1.06 Update: MRC using safe settings for lpmdtockedly (using safe settings)
- Enable Full Proxy Flow UEFI Variable Support
- Mask some additional bits in the MOT mask register
- Resolved : SD BUS INTERNAL ERROR" BSOD observed while booting and restarting OS through EMMC.

- Resolved :SMM_HECI_FUNCTION_READ_MESSAGE in HeciSmmHandler () Passes Wrong Arguments to EfiHeciReadMessage()
- MRC 1.07 Update: GLK A0/A1: Memory BW power measured on Reads is higher than pre-si expectations.
- Resolved : Win10 RS2 yellow bang ; HECI2 and HECI3 yellow bangs show up
- Resolved : EFI_OUT_OF_RESOURCES Assert in CseVariableStoragePei
- [Restructure] Add setup option to manually enroll SGX LE public key hash
- Resolved : Hibernate S4 resume fail at first time (Back out change-list 487812)
- After sending PME message vnn_req remains asserted.

2.4 Revision 0.6.7

- Setup/UPD & must depend on MonitorMWaitEnable UPD/Setup .
- GLK RAL Checker - additional registers not set according to documentation for LP4
- Update: Set the RT attribute on Setup for access in OS tools..
- Resolved : Assert error in FspInitPreMem
- Update: Overriden the CryptoPkg for BP1410 RC3 code merge.
- Resolved: System is stopping at Windows logo for about 40 seconds before proceeding to boot to OS.
- Resolved : S0ix entry is not happening.
- Resolved : After sending PME message vnn_req remains asserted
- Overriding CryptoPkg.

2.5 Revision 0.7.0

- MRC 1.09 Update: GLK MRC: Add algorithm to apply CTLE BIAS based on SKEW detection; set *rx*ctlecap =1

- Add setup option to manually enroll SGX LE public key hash
- Update : Dynamic SAR for WiFi
- Read IPN from PSS and update in SMBIOS table
- Use SSE4 copy in BpdtLib to improve boot responsiveness time.
- Assert error in FspInitPreMem
- Resolved : Intel audio got yellow bang in Windows 10 RS2 device manager after disabling DSP in BIOS setup menu.
- Resolved : PPV settings for PciClockRun = FALSE and PCIe SRL unlocked
- Implement the wifi power limit functions.
- Updated IBAS default address.
- Resolved : USB 3.0 port not working as SS deivce & Windbg debugging via USB3.0 port not working
- Resolved : [GLK] S0ix functionality failed, status LED is not ON
- Resolved : ScPciePmSwSmiCallback did not run at S3 resume
- Resolved : TrustedChannelSmm Should Not Reference BaseCryptLib in CryptoPkg
- Resolved : Siinit module debug logs shows junk data.
- Updated the PEIM graphics drivers to 13.10.1010
- Resolved : BayHub Card connected to RP03 does not enter into S0i3, WakePin Setting is corrected as per Apollo Lake Fix

  Resolved : When plugged in 3.5 mm audio Jack, internal wake event is not happening during s0ix

2.6 Revision 0.7.5

- Resolved : SMBIOS Memory Info Data HOB Structure name and parameters are not

  generic across platforms

- Implement split MRC data
- •Update : SGX need to be switched back to Software Controlled as default option
- Resolved: System not wake up from CS/S0i3 using PS2 mouse and Keyboard.
- Resolved : WOL is not working with WW23.1.2 IFWI
- Update : Preserving NV Storage in capsule update in SPI Boot
- Resolved : Energy report error on Autobot 1.0
- Update : CNVi W/A Force Active Clear should be applied for ES1/ES2, should not be applied for ES3
- Resolved : BIOS is not configuring CD clock appropriately in Gemini Lake
- Update : Need BIOS GPIO Configuration changes w.r.t IOS States and IOS Termination:: according to the PnP measurements for the SOC_Power numbers in CS
- Resolved: Number of Processor Cores showing wrong in Task manager & Device manager, after disabling core 2 option in BIOS.
- Update : No legacy USB support for DOS
- Update : Able to change CSM control mode, if Secure boot is enabled in BIOS

2.7 Revision 0.8.0

- PCIe CLKREQ pins from GPIO_120 to GPIO_123 are having pmode set to 0 on GLK B0 as reset default values (Back out changelists 508487 & 508485)
- Miss Board ID for RVP2C (0x9) & RVP2D (0xa) to all BKC images
- TNTE Wakes seen frequently in S0ix
- S0ix fails to enter in EPSI board because of LPC did not PG
- SoC xtal_clkreq not stopping on connected standby

2.8 Revision 0.8.5

- [Resolved] S0ix fail (Check S0ix Led)
- [Resolved] System get stuck during post because RxDqsDelay is over 0xFF
- [Resolved] The Variable Driver Should Return Successfully After Enumerating All Variable Storage Protocols

2.9 Revision 0.9.0

- Defeature 3.4 MHz mode on I2C 5,6 and 7 and ensure 1MHz mode configured correctly to prevent degradation
- SPIBAR+Bit11 WRSDIS changes
- GLK BIOS Code Writes UEFI Variable After End of Services is Sent.
- Connected Stand by hardware security test is failed with multiple errors
- Modphy settings added for USB SSIC - MBIST USBHost Showing High Fallout in Both Sort and Class
- SPI, TOUCH, SMUS, THERM, JTAG GPIO's are locked

2.10 Revision 0.9.5

- TPM 2.0 TCG Physical Presence Interface 1.3 Test is failing with multiple errors
- System get stuck during post because RxDqsDelay is over 0xFF (Clean debug prints added in earlier check-in)
- System get stuck during post because RxDqsDelay is over 0xFF Rcv Enable initial value fix

2.11 Revision 1.0.0

- System not able to enter S5 in EFI shell
- Dynamic Diffamp margin failures
- TPM 2.0 TCG Physical Presence Interface 1.3 Test is failing with multiple errors
- System get stuck during post because RxDqsDelay is over 0xFF (Clean debug prints added in earlier check-in)
- System get stuck during post because RxDqsDelay is over 0xFF Rcv Enable initial value fix

2.12 Revision 1.0.2

- [Resolved] Blank screen observed while booting to DOS with QMY6 A1 silicon / QNTL B0 Silicon on RVP1/RVP2.
- [Resolved] eMMC debug Boot fail
- [Resolved] The UEFI CSE Variable Storage Driver Should Not Process Windows Bugcheck Variables Due to Lack of OS Storage Proxy Driver Support
- [Update] SPLC Power limit for WiFi changed to default 2000
- [Resolved] DUT is not entering to shutdown when system reaches Critical trip point with DPTF disabled in BIOS in both RVP1 & RVP2 boards

2.13 Revision 1.0.5

- [Resolved] GLK Processor Frequency Mismatch in Windows 10 Properties

2.14 Revision 1.2.0

- [Resolved] PMC version shows incorrect under Platform Firmware information
- [Update] USB2/3 signal tuning configuration
- [Update] GLK B0 - I2c Configuration for RVP board
- [Resolved] MLK Running SGXFunctionalValidationTool get failure
- [Resolved] System stop at debug code number 7Fh when set MD=3.
- [Resolved] IPC1 IRQ related issue cause linux IPC timed out.
- [Resolved] CPU frequency keep low after disable SpeedStep in BIOS setup menu
- [Update]SV BIOS add setup option for SMM Code Check Enable
- [Resolved] S4 sleep fail at post code 0004
- [Update] Create UPD:SkipPunitInit to enable/disable P-unit initialization
- [Resolved] Hecidrv.c set boot script failed

2.15 Revision 1.4.0

- [Resolved] SDBUS_INTERNAL_ERROR Bug check observed across *Sx/S0ix/Warm reset cycling
- [Update] MRC Ver 1.28
- [Resolved] Not able to read Processor trace memory allocation size values using MSR [560 h]Bits[9:6].

- [Resolved] PCIe IRQ Routing is incorrect
- [Update] Making the SataController drive more Generic, to accomodate external Storage Cards
- [Resolved] Error 0x0006000A Platform Security Specification - CPU Security Configuration - Improper SMRR configuration when change Tseg size 0x800000 to 0x1000000.
- [Resolved] The OS Proxy Driver Stack May Not Be Loaded Before the OS Attempts to Write a UEFI Variable
- [Update] MRC Ver 1.29

2.16 Revision 2.0.0

- [Resolved] DCI Lock bit is not set with FSP BIN package build BIOS
- [Update] Implement the FSP policy use the wrapper setting
- [Update] MRC Ver 1.31 Update. Disable ECC CWL Fix Limitinig CWL fix to DDR4
- [Resolved] MRC: Unexpected training data change
- [Resolved] SPI Vendor Component Lock - SPIBAR + 0xC4 (Bit30 - VCL is not set)
- [Resolved] The OS Proxy Driver Stack May Not Be Loaded Before the OS Attempts to Write a UEFI Variable
- [Update] GLK bios must set GTTMADR + A194[5]=1 to avoid potential deadlocks between GPM cfg cycles and TLB invalidation flows
- [Resolved] :GELK - PCIE gen1 x1 audio and RAID card cannot be detected
- [Update]Update GLK CSE Variable Store Driver to Not Update In Memory Index Area If the NVM Transaction Fails
- [Resolved] Connected Standby Hardware Security Test failed with SPI Flash not write protected

2.17 Revision 2.0.1

- [Resolved] Update the memory index area and the variable cache in the CSE-assisted variable OS Runtime SMM flow.
- [Update] change use the PCIE root port setting to 4x1 enable the setup PCIE root port 4 to enable, PCIE devices 0x13 will gone.
- [Resolved] MRC code does not return control back to FSP Wrapperin case of MRC failures

- [Resolved] Windows *10 WDDM2 MS Hybrid Graphics Improvements, support for displays connected to the discrete GPU
- [Update] Intel® Software Guard Extensions (Intel® SGX) LCP Enabled
- [Resolved] Difference in maximum memory clock speed & configured memory clock speed between FSP scope tool log and system scope tool

2.18 Revision 2.0.2

- [Update] FSP UPD interface to enable/disable USB Port Disable Override
- [Resolved] Removing CryptoPkg from override in GLK
- [Resolved] GLK Copper Point Level 1 SMM Page Table
- [Resolved] eMMC Without Proxy driver set variable new variable, will get EFI_DEVICE_ERROR but read this variable can read the data.
- [Update] Support D3ColdAuxPowerAndTiming PCI ECN for CS enablement on Desktop
- [Update] HSTI 1.1a Changes
- [Update] Introduce a flag in the DMAR table flags field to communicate that DMA is only permitted into RMRR
- [Update] GLK+ R0 Stepping ID changes.
- [Update] NHLT table change needed for unifying the blobs for playback & capture
- [Update] GLK RS4 Include VT-d on/off BIOS switch in PCR[7] measurements

2.19 Revision 2.0.3.0

- [Resolved] Skip PCIe sequence initalization and PcieRootPort field in Fspm UPD
- [Resolved] GELK SGX devices are hidden after resume from S3
- [Resolved] GLK: BuildFsp.py should not use BaseTools Override
- [Resolved] system cannot boot with onboard memory in MRC V1.31
- [Update] Adapter Power Rating (ARTG) change for GLK

2.20 Revision 2.0.4.0

- [Resolved] GELK DTS changes does not sync with UeifCpuPkg\PismmCpuDxe
- [Resolved] GLK: BuildFsp.py should not use BaseTools Override
- [Update] GELK-Included latest PEIM driver in FSP

2.21 Revision 2.0.4.1

- [Resolved] Fix GCC 6.3 compilation issues
- [Resolved] SATA controller error behavior
- [Resolved] Vt-d protection check Added for HSTI

2.22 Revision 2.0.5.0

- [Update] Klocwork tool reported errors in GLK project
- [Update] Updated latest GraphicsPeim driver(version13.0.1017) in FSP
- [Update] Enabling CopperPoint Level1
- [Resolved] Fixed the new iasl.exe compiler version_20170831 build issues from BP_1420 changes
- [Resolved] LAN Isolate GPIO disable when RP5(LAN) disabled
- [Resolved] IPU Clean up

2.23 Revision 2.0.6.0

- [GLK BIOS][SCT]: Found 3 failures while running Self Certification Tests on RVP1 and RVP2 with SCT tool version v2.7
- [GLK] BIOS is not setting TCO_BASE_LOCK
- [GLK] Possible out-of-bounds memory writes
- [GLK] SCT fix causes dmpstore command failure so Backing out
- [GLK BIOS][SCT]: Found 3 failures while running Self Certification Tests on RVP1 and RVP2 with SCT tool version v2.7

2.24 Revision 2.0.7.0

- [GLK] When 2 SW SMI happen at the same time from different CPU thread, one of the SW SMI from one of the CPU thread is missed.
- GLK: Add ability to configure PMIC PCH_PWROK delay - build issue

2.25 Revision 2.0.7.1

- GLK FSP: xhci wake from S3, triggers multiple SMIs from within FSP Silicon Init resulting in a longer resume time

2.26 Revision 2.0.8.0

- [Resolved] Auto reboot issue during memory stress test or during idle(within 3 minutes)
- [Resolved] QQQA-2F SKU boot up issue with postcode 00F1
- [Resolved] Static MRC data changing on reboot

2.27 Revision 2.0.9.0

- [Implemented] Sensitive Data in MBP Must Not be exposed to Untrusted Code.
- [Resolved] USB Thumb drive disconnects from Type-A USB during chrome OS-install.
- [Resolved] Bump PMIC Vdd2 and MPHY LDO voltages to help with USB 3.0 enumeration for hotplugs.
- [Resolved] Bitlocker TPM and Recovery password tests for NONAOAC devices with PCR [7] HLK test item got failed if VT-d is disabled.

2.28 Revision 2.1.0.0

- [Resolved] System in dead loop if OEM verb table DWord size is larger than 256.
- [Resolved] MRC/MRRC v1.36 - MRC Fix for 2133mhz DLL Lock failure (F1).

2.29 Revision 2.2.0.0

- [Update] USB3 power control enable fix.
- [Update] MRC v1.37 (v1.36 + Improvement).
- [Fixed] SMM unmapped regions test is failing.
- [Update] Pmax platform control for Camera, display and audio BIOS requirements.
- [Regression] Debug build hangs at post code 0x0047, Processor Trace Mem Size issue. Please refer **CDI# 613769** for more details.

2.30 Revision 2.2.1.0

- [Implemented]GLK: XHCLKGTEN Register setting causes S0ix entry failure in less than 5 cycles when a USB2 Ethernet Dongle is connected. Refer GLK BIOS Spec Volume1 **CDI# 571118** under **chapter 7.20.6** for new Register settings.

2.31 Revision 2.2.1.1

- [Implemented] [GLK/GLK-R] DDR4 16Gb SDP Memory support for Gemini Lake/Gemini Lake – R
- [Update] MRC new version update to 1.38.
- [Fixed][GLK-R][WLAN] Removed the DSW function - Wake on LAN from S4 issue with latest Wifi driver.

3 Known issues

- None