Elkhart Lake Platform Silicon Initialization Code

Release Notes

March 2020

Revision 1.0.0

Intel Confidential

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

No product or component can be absolutely secure.

Contents

Revision History

Date	Revision	Description
March 2020	1.0.0	Alpha Release
December 2019	0.8.2	5th Pre-Alpha Release. Target for Elkhart Lake A0 ER#3 milestone.
November 2019	0.8.1	4th Pre-Alpha Release. Target for Elkhart Lake A0 ER#1 milestone.
October 2019	0.8.0	3rd Pre-Alpha Release. Target for Elkhart Lake A0 Silicon Power on milestone.
August 2019	0.5.2	2nd Pre-Alpha Release.
June 2019	0.5.1	Pre-Alpha Release. Target for Elkhart Lake PSS VP1.1 milestone.
March 2019	0.5.0	Initial Release.

§

1.0 Terminology

1.1 Terminology

Table 1. Terminology

Term	Description
ACPI	Advanced Configuration and Power Interface
ADSP	Audio Digital Signal Processor
BFX	Boot from X
BSOD	Blue Screen of Death
BtG	Boot Guard
CAN	Controller Area Network
CSRT	Core System Resources Table
DCI	Display Control Interface
DMA	Direct Memory Access
DOD	Development on Demand
EOI	End of Interrupt
FIA	Flexible I/O
GbE	Gigabit Ethernet
GCR	Global Control Registers
GPIO	General-Purpose I/O
HAE	Hardware Autonomous Enable
HDMI*	High-Definition Multimedia Interface
HECI	Host Embedded Controller Interface
HSIO	High-Speed I/O
IBECC	In-Band Error Checking and Correction
ID	Identity

Term	Description
IMR	Isolated Memory Region
Intel® CSE	Intel® Converged Security Engine
Intel® FSP	Intel® Firmware Support Package
Intel® PSE	Intel® Programmable Services Engine
JTAG	Joint Test Action Group
KM	Key Manifest
LPM	Low Power Mode
LPSS	Low-Power Subsystem
MMIO	Memory-Mapped I/O
ModPhy	Modular Physical Interface
MRC	Memory Reference Code
OTG	On The Go
PCD	Platform Configuration Database
PCH	Platform Controller Hub
PMC	Power Management Controller
PSMI	Periodic System Management Interrupt
PTCD	Platform Tuning Config Data
PSS	Pre-Silicon System
RVP	Reference Validation Platform
RTD3	Runtime D3
SATA*	Serial ATA
SDI	Serial Data In
SHA	Secure Hash Algorithm
SIIP	SoC Independent IP
SPB	Standard PCI* Controller B
SPC	Standard PCI Controller C
SPD	Standard PCI Controller D

Term	Description
SPI	Serial Peripheral Interface
SPx	Standard PCI Controller A to D
TCC	Time Coordinated Computing
TCO	Total Cost of Ownership
TCG	Trusted Computing Group
TGPIO	Time-aware GPIO
TC	Timed Channel
TSN	Time-Sensitive Networking
UART	Universal Asynchronous Receiver Transmitter
UFS	Universal File Store
UPIU	UFS* Protocol Interface Unit
VC	Virtual Channel
VP	Version Point
xHCI	eXtensible Host Controller Interface

2.0 Version Detail

2.1 Revision 0.5.0

Initial release.

Module	Version
Bailey Park Common Core	1.5.1.0.RP01
Client Silicon revision	0.2.0.13
Reference Code Version	8.7.1.10
Firmware Support Package	8.7.7.30
Memory Reference Code	0.0.4.18

2.1.1 Fixed Bugs

Not available as this is an initial release.

2.2 Revision 0.5.1

This release targets the Elkhart Lake PSS VP1.1 milestone.

Module	Version
Bailey Park Common Core	1.5.1.0.RP01
Client Silicon revision	0.2.0.13
Reference Code Version	8.7.1.10
Firmware Support Package	8.7.16.60
Memory Reference Code	0.0.4.18

2.2.1 Feature Updates

- Added SCI support
- Added support for PCIe* SPB, SPC and SPD
- Added support for SIIP Firmware Loading Intel® Firmware Support Package (Intel® FSP)

- Added Intel® PSE GPIO ownership settings
- Added support for PCIE2ND in FIA lane ownership
- Added _STA method for PCH PMC TGPIO

2.2.2 Fixed Bugs

- [1507178579] - Fixed RootPort 5 assertion
- [1507149509] - BIOS WA for RTL Loading Done Bug
- [1507188342] - Fixed Intel® PSE PWM ownership issue
- [1409299573] - Fixed Audio child devices enumeration
- [1506941917, 1507095442] - Fixed system unable to wake up from S3

2.3 Revision 0.5.2

Second Pre-Alpha Release

Module	Version
Bailey Park Common Core	1.6.1.0.RP01
Client Silicon revision	0.2.0.15
Reference Code Version	8.7.7.10
Firmware Support Package	8.7.7.40
Memory Reference Code	0.0.4.70

2.3.1 Feature Updates

- Updated Bailey Park common core to Bailey Park 1610
- Added support for Intel® PSE Log Channel Output
- Added Intel® Converged Security Engine (Intel® CSE) “get bootloader seed” message
- Updated the Device ID for I2C*6 and I2C7 devices
- Provided ability to set I/O Standby State operation for JTAG and DFx-related GPIO pads.
- Added Lane Reversal Support on FIA
- Modified related Intel® PSE MMIO to support 64-bit OS
- Enabled SHA384 hash algorithm for Intel® Boot Guard key manifest and boot policy manifest

2.3.2 Fixed Bugs

- [2207992925] - Fixed C-state latency values for ACPI tables
- [1507319345] - Fixed UFS Storage Proxy to Start Earlier
- [1607279461] - MCC: Wrong SB port ID mapping used for PMC-GPIO Tunneling feature
- [2204514993] - Heap Guard of Special Pool Feature doesn't work for flash read to get GbE UUID

2.4 Revision 0.8.0

This release targets the Elkhart Lake A0 silicon power-on milestone.

Module	Version
Bailey Park Common Core	1.6.1.0.RP01
Client Silicon revision	0.2.0.15
Reference Code Version	8.7.7.10
Firmware Support Package	8.7.7.40
Memory Reference Code	0.0.4.70

2.4.1 Feature Updates

- [1507308536] Implemented Intel® PSE DMA driver requirements
- [1507160626] Updated Elkhart Lake PEP device table
- [1507303757] 3 TSN sub-regions implementation
- [1607101675] CPU Program PL1 and PL2 power limits for EHL
- [1507308536] Modified Intel® PSE DMA0 for Zephyr* instead of DMA2
- [1507303757] Intel® PSE header and manifest handling for 3 GbE sub-regions
- [1409932397] Updated TSN Modphy configuration
- [1409989132] Updated UFS BIOS capsule support
- [1507303757] Changed Intel® PSE GBE TSN load address
- [1808161630] Program COMINIT and COMWAKE sampling registers based on sosc_clk frequency
- [1507308536] Appended Intel® PSE DMA MMIO to ACPI DSDT
- [1607289546] Moved HdAudio initialization to Pre-mem

- [14010081926] Removed RGMII GPIO in TsnInit
- Added support for USB* OTG via Device Subscription
- Changed ACPI ID for Intel® ECLite device
- Enabled DOD Support
- Enabled TCO timer for booting 4 Cores
- Enabled graphics with eDP*
- Updated eMMC* DLL
- Enabled HDMI* display
- Updated PCI* safe config
- Programmed TSN GCR link speed
- Added pin multiplexer for GbE and re-ordered the priorities
- Disabled CPU power states
- Put TsnInit after PseInit
- Disabled legacy devices reporting to the OS
- Refactored serial I/O IP block code
- Added Intel® PSEJTAG multiplexer and solved I2C0-1 issues and enabled Intel PSE secure fuse loading
- Moved programming IMR to after SIIP Loading
- Corrected Intel® PSE TSN address
- Added the PCIe hardware equalizer settings
- Provided the ability to enable or disable the SMBus dynamic power gating
- IBECC: Disabled the remap when the memory is 2 GB or less

2.4.2 Fixed Bugs

- [1507232750] - Fixed overwritten Sci BAR
- [1607549622] - SD Host Controller enumerating with yellow bang
- [1607585294] - Fixed TPM Page Error
- [1507360803] - System is unable to reset after enabling IFWI DNX setting in BIOS Menu
- [1409650905] - BIOS does not enable SMBus ROSC TCG, which blocks S0i3.4
- [1807623418] - Disabled USB 2-port reset messaging feature in PCH xHCI controller
- [1607662744] – Changed BIOS solution for UFS S0ix issues

- [1507375115] - Fix /dev/spidev not found
- [1507431253] - Removed IPU & ITBT DMAR table from publishing and return Base Address 0 to OS
- [1507434635] - iommu init failed due to "DMAR reported at address fed90000 returns all ones!"
- [1409645331] - BIOS does not enable GPIO PGCB PCG blocking S0i3.4 enabling
- [2209115322] – BIOS does not enable HD Audio power gating - blocks S0ix
- Fixed Windows* OS BSOD when the UFS* controller is not present or is disabled via the setup option
- Fixed the issue of HECI #2 not being hidden during BFX
- Fixed the hang at ExitBootService when the xHCI is not present
- Disabled D3_HOT_EN bit for xHCI temporarily to ungate Windows* boot.
- Fixed Multi-VC PCIe rootport function mapping
- Fixed the issue of "GPIO hangs because of UART and GbE"
- Fixed package C state limit setting
- Fixed interrupt routing for D29
- Fixed PCH TSN VC/TC programming bit manipulation
- Fixed UFS flag reading from Query Reap UPIU
- Fixed LPSS SPI interrupt programming
- Fixed Windows* BSOD after previous SPI interrupt changes
- Fixed HSIO table overflow
- Fixed blank screen while installing Windows* graphics driver
- Fixed HSIO overflow when three Ethernet TSN controllers are enabled
- Fixed sideband access assertion to SPx controller which is fused off
- Fixed the wrong Intel® PSE DMA ownership offset

2.5 Revision 0.8.1

4th Pre-Alpha Release. This release targets the Elkhart Lake A0 ER#1 milestone.

Module	Version
Bailey Park Common Core	1.6.1.0.RP01
Client Silicon revision	0.2.0.15

Module	Version
Reference Code Version	8.7.7.10
Firmware Support Package	8.7.7.40
Memory Reference Code	0.0.4.70

2.5.1 Feature Updates

- [1607101675] Suppressed Min Voltage Override option
- [14010268162] Enabled reg_bonuxcode_ovr_en when TSN is enabled
- Added master clock gating and power gating control for PCH devices
- Enabled IBECC support for DDR4
- Added SMBus support for DDR4 RVP2
- Added master clock gating and power gating control for PCH devices
- Added DEBUG_PG_WAC SAI for IBECC Error Injection
- Synced PMC and DCI IP block from Tiger Lake
- Removed re-active high for Intel® PSE UART
- Added TSN disabling flow
- Modified Intel® PSE CSRT
- Intel® PSE ownership setup menu changes
- Refactored Intel® PSE base address obtained in PseHeciHardwareInit
- Implemented the Boulder Island lite feature

2.5.2 Fixed Bugs

- [1507432103] Set default PMC Time-aware GPIO to disable and corrected MCC PCIe Grant Count Config
- [1507465139] Fixed PCIe Clock Gate PTOCGE register programming
- [1507478067] AC split lock are not enabled for all cores
- [1507478023] Fixed PCIe Rp2 ClkGate Issue and proper CRB Clock Mapping
- [1507447771] Disabled VCp and programme PXPEPBAR VC1RCTL TC/VC Map
- [1507511577] Fixed PCH-GBE not detected issue
- [1507515433] Changeed GPIO pad mode bits from 3-bit to 4-bit wide
- [1507458450] Fix edIntel® PSE SPI0 Chip Select Pin to native mode
- [1507515461] Linked the GBE VC TC mapping to TCC mode

- Provided a workaround to ungate the “interrupt not seen” issue
- Fixed EOI Programming
- Added a workaround to enable the eMMC device as a storage for Windows OS
- Fixed the SATA Clockreq asserted issue when the platform is in the S0i2.1 state
- Modified the Multi-VC configuration to make the PCIe port negotiate successfully
- Fixed the BIOS boot assert when master power and clock gating are set to default
- Fixed the CPU exception when the CPU trace is enabled
- Fixed the issue of system hang in the MRC when the disable page close idle timeout bit is set

2.6 Revision 0.8.2

5th Pre-Alpha Release

This release targets the Elkhart Lake A0 ER#3 milestone.

Module	Version
Bailey Park Common Core	1.6.1.0.RP01
Client Silicon revision	0.2.0.15
Reference Code Version	8.7.48.50
Firmware Support Package	8.7.48.50
Memory Reference Code	0.0.4.70

2.6.1 Feature Updates

- [1507501898] Updated Intel® PSE CAN ACPI property
- [1507515461] Programmed Intel® PSE GBE VC-TC Channels 8-15
- [1507435198] Updated Sd Card DLL setting
- [14010433495] Changed to use valid FSP-T UPD
- [1507520358] Updated UFS Boot features
- [1507441446] Hid Intel® PSE DMA1&2 devices
- [1608993645] Updated Elkhart Lake display configuration table
- [1507289605] Added USB3.1 Speed selection
- [1507577720] Programmed ASPM L0s, L1, L1ss enable registers
- Removed DEBUG_PG_WAC SAI for IBECC Error Injection

- Enabled PSMI and trace region
- Added pin mux configuration

2.6.2 Fixed Bugs

- [1608664346] Fixed Sideband lock up after SCI interaction
- [1507462048] Fixed expected data payload doesn't fill up mid level cache impacting cache efficiency
- [1507523371] Fixed C10 Exit Debug Latch MMIO Value
- [1507448249] Updated I2C Clock Speed Values
- [1608677836] Fixed Power button functionality is not working
- [14010456064] Fixed PCI extra Functions off Bus 0 Dev 0 that shouldn't exist
- [1507514905] Fixed PCIe VC1 traffic is not being generated

2.7 Revision 1.0.0

Alpha Release

Module	Version
Bailey Park Common Core	1.6.1.0.RP01
Client Silicon revision	0.2.0.15
Reference Code Version	9.02.08.30
Firmware Support Package	9.02.08.30
Memory Reference Code	0.0.4.70

2.7.1 Feature Updates

- [16010657986] Enabled all LPM state
- [1507529157] Updated TSN ModPhy lane C and D settings
- [1407858195] Updated TCC PTCD table and add tuning phases
- [2209869144] Added Sata Rx Polarity option
- [1507460600] Updated OPI/DMI register “T_SB_MIN” to 0x14
- [1507621272] Added Intel® PSE CS1 options
- Updated new FSP/RC versioning strategy

- Added Elkhart Lake B0 support
- Enabled FSP dispatch mode
- Enabled Chipset Init Sync
- Added support for SHA384 hashes for BtG event logs
- Updated UFS codes
- Added option for HDA SDI
- cAVS supports 8T-Mode
- Enabled TSN S0ix
- Redefined TCC MMIO64 base and address
- Updated MRC stepping info to Ice lake D1
- Added IBECC MRC task for S3
- Disabled IBECC Range 1 by default
- Added PCD to adjust memory type size
- Re-added USB OTG configuration support

2.7.2 Fixed Bugs

- [14010536004] Fixed Startup Locality and BtG Event logged twice in TCG Event log
- [16010657986] Fixed Sata not entering into RTD3
- [16010740661] Programmed TSN GCR register in S3 resume flow
- [16010761903] Assigned the Intel® PSE IOs ownership NONE, Intel® PSE or HOST-Owned
- [16010777438] UFS unable to power gate and enter S0ix
- [16010729064] Disabled ADSP bar by PSF and not by HD Audio subsystem logic
- [1507441446] Updated CSRT table when Intel® PSE DMA1/2 is enabled and owned by host
- [1608782199] Fixed Intel Management Engine Interface driver listed twice in device manage
- [1507342993] Configured GPIO pin to Intel® PSE when Intel® PSE JTAG pin mux is enabled
- [1507523997] Set HAE bit during HD Audio disable flow
- [1507508840] Fixed MultiVC not working with x1 setting mode

- [1609554084] Removed PSF IdleNak and Early Exit from Idle to fix long boot delays, reset issues, and missing sound card issue.
- [1507717249] Fixed GVT-d on ACRN that did not work
- [1507705134] PCIe VC1 lane traffic is not generated
- [1307077314] Fixing UFS RS3 Upstream does not work
- Avoid asserting when Intel® PSE DMA is not present
- Fixed for LPSS UART for S0ix validation
- Fixed CPU Strap Read/Write for BFX
- Added missing Elkhart Lake device id SKU

§

3.0 Known Issue

3.1 Revision 0.5.0

- 1507095442 - [EHL] [BIOS] [External Release]: System is unable to wake up from S3 in Windows* 10 environment.

3.2 Revision 0.5.1

- Not available.

3.3 Revision 0.5.2

- Not available.

3.4 Revision 0.8.0

- Not available.

3.5 Revision 0.8.1

- Not available.

3.6 Revision 0.8.2

- Not available

3.7 Revision 1.0.0

- 16010849327 - [EHL][A0] Delay observed during Sx/Boot

§

4.0 Reference Documents

Document	Document No./Location
Elkhart Lake Compute Die Intel® Architecture Firmware Specification Volume 1 of 2	RDC #605155
Elkhart Lake Compute Die Intel Architecture Firmware Specification Volume 2 of 2	RDC #610273
Elkhart Lake Platform - Firmware Architecture Specifications (FAS)	RDC #602632
Elkhart Lake External Design Specifications (EDS) - Volume 1	RDC #601458
Elkhart Lake External Design Specifications (EDS) - Volume 2	RDC #602633
Elkhart Lake External Design Specifications (EDS) - Volume 3	RDC #614110
Elkhart Lake External Design Specifications (EDS) - Volume 4	RDC #614111

§

5.0 Notes

5.1 Versioning Strategy

Starting with Alpha, the Elkhart Lake FSP binary and Silicon Init Code version will change to represent the code updates and platform support.

Version is represented in a 4 byte field with a new definition:
MajorVersion(255).MinorVersion(255).BuildWeek(255).BuildNumber(255)

Field	Description
Major Version	This number represents the code generation. *Example: '9' means 9th generation BIOS.*
Minor Version	This number will be used to identify the platform year supported by this code base. *Example: '01' is the first year of the platform.*
Build Week	This number represents the code work week and will change every time when code is released. *Example: '51' means WW51*
Build Number	This represents a build number based on BIOS build day and changes revision. Number is reset every time new BIOS version is built. [7:4]: Build Day [3:0]: Patch Revision *Example: '50' means 1st BIOS version built at Friday*

§