Intel Atom® x6000E Series, and Intel® Pentium® and Celeron® N and J Series Processors for Internet of Things (IoT) Applications

Specification Update - Public

January 2023

Revision 2.0

Document Number: 636674-1.9

Contents

§

January 2023
Document Number: 636674-2.0

Revision History

Date	Revision	Description
January 2023	2.0	Added: 1) EHL32.
December 2022	1.9	Updated: Table 2 to add Performance Update (PU) SKUs.
July 2022	1.8	Added: 1) EHL29, EHL30 and EHL31. 2) Documentation Changes 1: Datasheet Vol2 Book2 update.
May 2022	1.7	Added: 1) EHL28. Removed: 1) Specification Clarifications: Debug access of Intel® PSE and Intel® Safety Island (Intel® SI) since Section 28.4.3 in the Datasheet Volume 1 has been updated.
March 2022	1.6	Added: 2) EHL26. 3) EHL27.
January 2022	1.5	Added: 1) EHL25.
November 2021	1.4	Added: 1) EHL24. 2) Specification Clarification 1.
October 2021	1.3	Added: 4) EHL22. 5) EHL23.
July 2021	1.2	Added: 3) EHL21.
June 2021	1.1	Added: 1) EHL19, EHL20. Updated: 1) Table 2 package size updated.
March 2021	1.0	Initial release.

§

Preface

This document is an update to the specifications contained in the documents listed in the following Affected Documents table. It is a compilation of device and document errata and specification clarifications and changes. This document is intended for hardware system manufacturers and for software developers of applications, operating system, and tools.

Information types defined in the Nomenclature section of this document are consolidated into this document and are no longer published in other documents. This document may also contain information that has not been previously published.

Errata listed in this document apply to all product SKUs unless otherwise indicated.

Affected Documents

Document Title	Document Number
Intel Atom® x6000E Series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications Datasheet, Volume 1	636112
Intel Atom® x6000E Series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications Datasheet, Volume 2 (Book 1 of 3) Compute Die	635255
Intel Atom® x6000E Series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications Datasheet, Volume 2 (Book 2 of 3) Mule Creek Canyon (MCC)	636722
Intel Atom® x6000E Series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications Datasheet, Volume 2 (Book 3 of 3) Intel® Programmable Service Engine (Intel® PSE)	636723

Nomenclature

Errata are design defects or errors. These may cause the Product's behavior to deviate from published specifications. Hardware and software designed to be used with any given stepping must assume that all errata documented for that stepping are present on all devices.

S-Spec Number is a five-digit code used to identify products. Products are differentiated by their unique characteristics, that is, core speed, L2 cache size, and package type as described in the processor identification information table. Read all notes associated with each S-Spec number.

Specification Changes are modifications to the current published specifications. These changes will be incorporated in any new release of the specification.

Specification Clarifications describe a specification in greater detail or further highlight a specification's impact to a complex design situation. These clarifications will be incorporated in any new release of the specification.

Documentation Changes include typos, errors, or omissions from the current published specifications. These will be incorporated in any new release of the specification.

Note: Errata remain in the specification update throughout the product's lifecycle, or until a particular stepping is no longer commercially available. Under these circumstances, errata removed from the specification update are archived and available upon request. Specification changes, specification clarifications, and documentation changes are removed from the specification update when the appropriate changes are made to the appropriate product specification or user documentation (datasheets, manuals, so on.).

§

Identification Information

The Processor can be identified by the register contents in Table 1.

When EAX is initialized to a value of 1, the CPUID instruction returns the Extended Family, Extended Model, Type, Family, Model, and Stepping value in the EAX register.

Note: EDX Processor signature value after reset is equivalent to the Processor signature output value in the EAX register.

Table 1. Component Identification via Programming Interface

Reserved	Extended Family[1]	Extended Model[2]	Reserved	Processor Type[3]	Family Code[4]	Model Number[5]	Stepping ID[6]
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
0x0	0x0	0x9	0x0	0x0	0x6	0x6	B1: 0x1

NOTES:

1. The Extended Family, bits [27:20] are used in conjunction with the Family Code, specified in bits [11:8], to indicate whether the Processor belongs to the Intel 386, Intel 486, Pentium®, Pentium® Pro, Pentium® 4, or Intel® Core™ processor family.
2. The Extended Model, bits [19:16] in conjunction with the model number, specified in bits [7:4], are used to identify the model of the Processor within the Processor family.
3. The Processor Type, specified in bits [13:12] indicates whether the Processor is an original OEM Processor, an OverDrive Processor, or a dual Processor (capable of being used in a dual Processor system).
4. The Family Code corresponds to bits [11:8] of the EDX register after RESET, bits [11:8] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
5. The Model Number corresponds to bits [7:4] of the EDX register after RESET, bits [7:4] of the EAX register after the CPUID instruction is executed with 1 in the EAX register, and the model field of the Device ID register accessible through Boundary Scan.
6. The Stepping ID in bits [3:0] indicates the revision number of that model. Refer to Table 2 for the Processor stepping ID number in the CPUID information.

§

Table 2. Identification Table

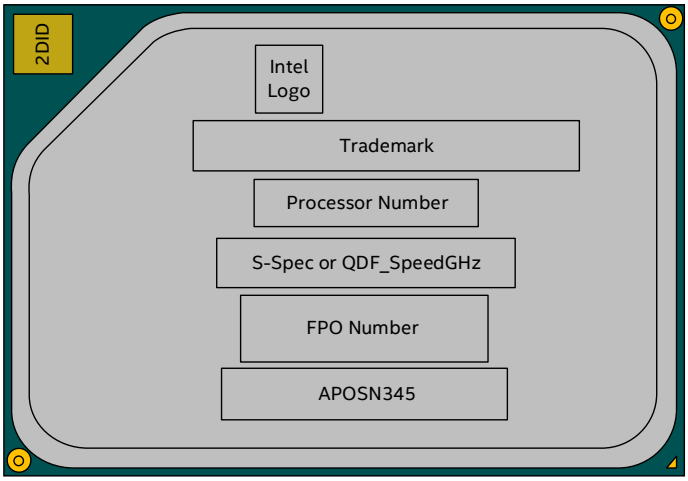
S-Spec Number	SKU Number	Processor Number	CPUID	Stepping	Package
RKL7	1	J6413	90661	B1	FCBGA1493, 35x24mm
RKUA	1A	J6412	90661	B1	FCBGA1493, 35x24mm
RKUB	2	J6426	90661	B1	FCBGA1493, 35x24mm
RKL9	3	N6211	90661	B1	FCBGA1493, 35x24mm
RKUC	3A	N6210	90661	B1	FCBGA1493, 35x24mm
RKLA	4	N6415	90661	B1	FCBGA1493, 35x24mm
RKUD	5	x6211E	90661	B1	FCBGA1493, 35x24mm
RKLC	6	x6413E	90661	B1	FCBGA1493, 35x24mm
RKUE	7	x6425E	90661	B1	FCBGA1493, 35x24mm
RKLE	8	x6212RE	90661	B1	FCBGA1493, 35x24mm
TBD	8PU	x6214RE	90661	B1	FCBGA1493, 35x24mm
RKLF	9	x6414RE	90661	B1	FCBGA1493, 35x24mm
TBD	9PU	x6414RE	90661	B1	FCBGA1493, 35x24mm
RKLG	10	x6425RE	90661	B1	FCBGA1493, 35x24mm
RKLH	11	x6427FE	90661	B1	FCBGA1493, 35x24mm
RKST	12	x6200FE	90661	B1	FCBGA1493, 35x24mm

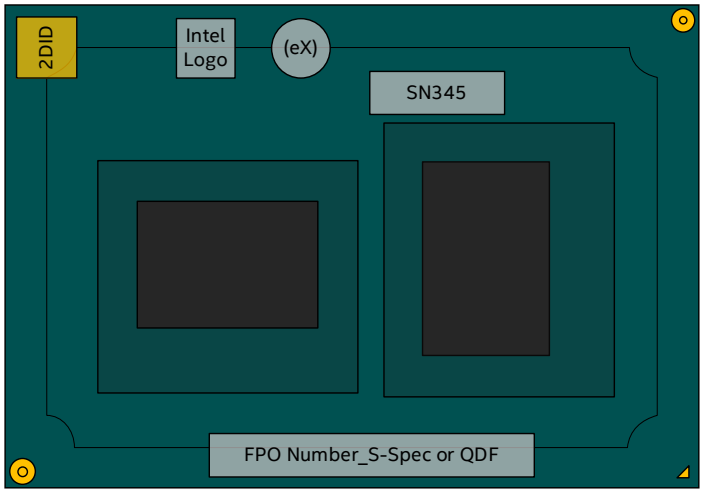
Note: Refer to Section 1.6 of Datasheet – Volume 1 (RDC#636112) for SKU-specific specifications.

Component Marking Information

The IHS (Integrated Heat Spreader) and bare die package processors are identified by the following component markings.

Figure 1. Processor Markings





§

Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes that apply to the product. Intel may fix some of the errata in a future stepping of the component and account for the other outstanding issues through documentation or specification changes as noted. These tables use the following notations:

Codes Used in Summary Table

Stepping

X:	Erratum exists in the stepping indicated. Specification Change that applies to the stepping indicated.
Blank (No mark):	This erratum is fixed in listed stepping or specification change does not apply to list stepping.

Status

Doc:	Document change or update will be implemented.
Plan Fix:	This erratum may be fixed in a future stepping of the product.
Fixed:	This erratum has been previously fixed in Intel hardware, firmware, or software.
No Fix:	There are no plans to fix this erratum.

Area

PCH	Platform Controller Hub
CD	Compute Die
PKG	Processor Package
NA	Not Applicable

Row

Shaded:	This item is either new or modified from the previous version of the document.

Table 3. Errata Summary

ID	Status	Impacted Area	Stepping Impacted	Erratum Description
			B1	
EHL1	No Fix	CD	X	Intel® PT CYC Packet May Follow a TNT Packet That it Should Precede
EHL2	No Fix	CD	X	Intel® PT CR3 Filtering Compares Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH outside of PAE Paging Mode
EHL3	No Fix	CD	X	PEBS DLA May Report Incorrect Value
EHL4	No Fix	CD	X	Performance Monitoring Event Demand Data Read Offcore Response May Overcount
EHL5	No Fix	CD	X	Intel® PT CYC Packet May Follow a TNT Packet That it Should Precede
EHL6	No Fix	CD	X	GPA reports only page base on VM exit due to Intel® PT output
EHL7	No Fix	CD	X	Performance Monitoring Event Mem Load Uops Retired HitM will include DRAM and MMIO Hit Counts
EHL8	No Fix	CD	X	Performance Monitoring Event OFFCORE_RESPONSE may Undercount Outstanding Uncacheable Reads
EHL9	No Fix	CD	X	Intel® PT ToPA Stop May Occur Early When ToPA Region is Comprised of Multiple EPT Pages
EHL10	No Fix	PCH	X	xHCI Serial Bus Release Number Version
EHL11	No Fix	PCH	X	SPI SFDP Program Suspend and Program Resume Instruction Fields Not Used
EHL12	No Fix	PCH	X	USB DbC or Device Mode Port when Resuming from S3, S4, S5, or G3 State
EHL13	No Fix	PCH	X	Intel® Trace Hub Pipe Line Empty
EHL14	No Fix	PCH	X	eSPI SBLCL Register Bit Not Cleared by PMC_PLTRST_N
EHL15	No Fix	PCH	X	xHCI USB 2.0 ISOCH Device Missed Service Interval
EHL16	No Fix	PCH	X	xHCI Protocol Speed ID Count Field
EHL17	No Fix	PCH	X	xHCI Short Packet Event Using Non-Event Data TRB
EHL18	No Fix	PCH	X	S0ix Entry When Connecting a USB-C* Power Adapter
EHL19	No Fix	PCH	X	PCIe Clock Maximum Rising/Falling Edge Rate and VCROSS
EHL20	No Fix	PCH	X	USB VTIO Device Capabilities Field Length
EHL21	Fixed	PCH	X	PCH Thermal Subsystem Not Updated After S0ix Exit

ID	Status	Impacted Area	Stepping Impacted	Erratum Description
			B1	
EHL22	No Fix	PCH	X	Intel® PSE GbE Controllers Incorrectly Advertised RX & TX FIFO Size
EHL23	Fixed	PCH	X	Processor Unable to Enter DnX Mode
EHL24	No Fix	PCH	X	No S0i3.0 State when Device is Connected to DDI2 Interface
EHL25	No Fix	PCH	X	xHCI Force Header Command Incorrect Return Code
EHL26	No Fix	PCH	X	Leakage Current from VCC_1P8A Power Rail
EHL27	Fixed	PCH	X	USB 2.0 Device Interrupt IN Endpoint Split Transaction Error
EHL28	Fixed	CD	X	Processor May Not Wake From TPAUSE/UMWAIT in Limited Situations
EHL29	No Fix	PCH	X	Processor C-States with USB Full-speed or Low-speed Device Hotplug
EHL30	No Fix	PCH	X	USB 3.2 Gen 1x1 Port Does Not Send 16 Polling LFPS Burst
EHL31	No Fix	PCH	X	PMC_TGPIO Event May Have a Mismatched Time Stamp
EHL32	Fixed	PCH	X	EPT-based Address Translation May Not Operate Correctly After Posted-interrupt Processing

Table 4. Specification Changes

Number	Stepping	Specification Changes
		No specification changes in this revision of the Specification Update

Table 5. Specification Clarifications

Number	Stepping	Specification Clarifications
		No specification clarifications in this revision of the Specification Update

Table 6. Documentation Changes

Number	Stepping	Documentation Changes
1	All	Datasheet updates

§

Errata

EHL1 Intel® PT CYC Packet May Follow a TNT Packet That it Should Precede

Problem:	In cases where Intel® PT (Intel® Processor Trace) is enabled and a partial TNT (Taken/Not Taken) packet is forced out by a following packet that is not a TIP (Target IP) packet, if the first branch in the TNT retired in the same cycle that the following packet was generated then any CYC (Cycle Count) packet will come after the TNT instead of before it.
Implication:	The first branch in the TNT will appear to an Intel® PT decoder to have retired earlier than it did.
Workaround:	If cycle packets are enabled with a threshold of 0, such that CycEn[bit 1]=1 and CycThresh[bits 22:19]=0 in IA32_RTIT_CTL (MSR 570H), then if a TNT is found without a preceding CYC the decoder can apply the time of the next CYC to the first branch in the TNT.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL2 Intel® PT CR3 Filtering Compares Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH outside of PAE Paging Mode

Problem:	CR3[11:5] are used to locate the page-directory-pointer table only in PAE paging mode. When using Intel® PT (Intel® Processor Trace), those bits of CR3 are compared to IA32_RTIT_CR3_MATCH (MSR 572H) when IA32_RTIT_CTL.CR3Filter (MSR 570H, bit 7) is set, independent of paging mode.
Implication:	Any value written to the ignored CR3[11:5] bits, which can only be non-zero outside of PAE paging mode, must also be written to IA32_RTIT_CR3_MATCH[11:5] in order to result in a CR3 filtering match.
Workaround:	None identified
Status:	For the steppings affected, refer Summary Table of Changes.

EHL3 PEBS DLA May Report Incorrect Value

Problem:	Due to a rare microarchitectural condition, a PEBS (Processor Event-Based Sampling) record taken on a load instruction may report an incorrect value in the DLA (Data Linear Address) field.
Implication:	A software profiler may be confused by a PEBS record suggesting that the associated load accessed an address that it did not.
Workaround:	None Identified
Status:	For the steppings affected, refer Summary Table of Changes.

EHL4 Performance Monitoring Event Demand Data Read Offcore Response May Overcount

Problem:	If using performance monitoring events OFFCORE_RESP.MSR_OFFCORE_RESP0 (Event: B7H, UMask: 01H) or OFFCORE_RESP.MSR_OFFCORE_RESP1 (Event: B7H, UMask: 02H) and Demand Data Read Request Types are enabled, by setting DEMAND_DATA_RD [bit 0] in MSR_OFFCORE_RESP0 (MSR 01A6H) or MSR_OFFCORE_RSP_1 (MSR 01A7H), L1 Software Prefetches will be counted in addition to Demand Data Reads.
Implication:	Software counting Demand Data Reads may observe inaccurate event counts.
Workaround:	None identified
Status:	For the steppings affected, refer Summary Table of Changes.

EHL5 Intel® PT CYC Packet May Follow a TNT Packet That it Should Precede

Problem:	In cases where a partial TNT (Taken/Not Taken) packet is forced out by a following packet that is not a TIP (Target IP) packet, if the first branch in the TNT retired in the same cycle that the following packet was generated then any CYC (Cycle Count) packet will come after the TNT instead of before it.
Implication:	The first branch in the TNT will appear to an Intel® PT (Intel® Processor Trace) decoder to have retired earlier than it did.
Workaround:	For maximum timing precision, if cycle packets are enabled with a threshold of 0, such that CycEn[bit 1]=1 and CycThresh[bits 22:19]=0 in IA32_RTIT_CTL (MSR 570H), then if a TNT is found without a preceding CYC the decoder can apply the time of the next CYC to the first branch in the TNT.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL6 GPA reports only page base on VM exit due to Intel® PT output

Problem:	If the EPT (Extended Page Tables) translation for an Intel® PT (Intel® Processor Trace) output address causes a VM exit, the GPA (Guest Physical Address) field will hold 0 in the page offset bits.
Implication:	A hypervisor will not be able to discern the precise address that was accessed, only the page.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL7 Performance Monitoring Event Mem Load Uops Retired HitM will include DRAM and MMIO Hit Counts

Problem:	If using the performance monitoring events MEM_LOAD_UOPS_RETIRED.HITM(Event: D1H, UMask: 20H), the event will also count any load uops retired with a hit type of DRAM or MMIO.
Implication:	Due to this erratum, software monitoring events for Mem Load Uops Retired HitM may overcount.
Workaround:	Subtracting MEM_LOAD_UOPS_RETIRED.DRAM count from this event will provide the true Mem Load Uops Retired HitM count.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL8 Performance Monitoring Event OFFCORE_RESPONSE may Undercount Outstanding Uncacheable Reads

Problem:	If using performance monitoring event OFFCORE_RESP.MSR_OFFCORE_RESP0 (Event: B7H, UMask: 01H) and Outstanding Uncacheable Read of Offcore Response events are enabled, by setting OUTSTANDING [bit 63] as well as UC_RD [bit 44] in MSR_OFFCORE_RESP0 (MSR 01A6H), the event may undercount.
Implication:	Due to this erratum, software monitoring Outstanding Uncacheable Read requests may observe inaccurate counts.
Workaround:	Non-available.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL9 Intel® PT ToPA Stop May Occur Early When ToPA Region is Comprised of Multiple EPT Pages

Problem:	If Intel® Processor Trace (Intel® PT) is enabled by setting IA32_RTIT_CTL.TraceEn[0] (MSR 0570H) to 1 while executing in a Virtual Machine Extensions (VMX) guest with the "Intel® PT uses guest physical addresses" VM-execution control set to 1, and Intel® PT is writing to a ToPA (Table of Physical Addresses) region configured for ToPA stop, such that the ToPA region size is greater than the size of the underlying Extended Page Table (EPT) pages and the IA32_RTIT_OUTPUT_MASK_PTRS.OutputOffset[63:32] (MSR 0561H) value indicates that the next trace byte should be written to the last EPT page in the ToPA region, IA32_RTIT_STATUS.STOPPED[5] (MSR 0571H) will be set immediately rather than when the region is filled.
Implication:	ToPA stop may occur before the last page of the associated ToPA region is filled. Intel has only observed this erratum in synthetic test conditions. Intel has not observed this erratum in any commercially available software.
Workaround:	Non-available.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL10 xHCI Serial Bus Release Number Version

Problem:	The xHCI Host Controller reports the value of 31h for the Serial Bus Release Number (SBRN) register (offset 60h), which does not meet the xHCI specification revision 1.2.
Implication:	USB-IF xHCI CV TD 1.1 may report a failure. Intel has obtained a waiver for TD 1.1. ***Note:*** There are no known functional failures due to this erratum.
Workaround:	Non-available.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL11 SPI SFDP Program Suspend and Program Resume Instruction Fields Not Used

Problem:	For flash device suspend / resume opcodes, the SPI controller does not use JEDEC SFDP's 13th DWORD bits [15:0], Program Suspend Instruction and Program Resume Instruction fields. The controller only uses bits [31:16], Suspend Instruction and Resume Instruction fields, to obtain the suspend / resume opcodes.
Implication:	If the SPI flash requires bits [15:0] to be different than bits [31:16], then the suspend / resume feature is not functional. In this case, system behavior varies depending on what the suspend / resume instruction is and when it is generated. ***Note:*** Major flash vendors have been using the same value for bits [31:16] and bits [15:0].
Workaround:	If a device requires bits [15:0] to be different than bits [31:16], then disable the device suspend / resume via the SPI Suspend / Resume Enable soft strap.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL12 USB DbC or Device Mode Port when Resuming from S3, S4, S5, or G3 State

Problem:	If a PCH USB Type-C* port is configured in Device Mode (or in DbC mode) and connected to an external USB 3.1 host controller, it may cause the USB port to go into a non-functional state in the following scenarios: 1. The PCH resumes from S3, S4, or S5 state, the port may remain in U2. 2. The port is connected to a USB 3.1 Gen 1 host controller when resuming from S3, S4, S5, or G3, the port may enter into Compliance Mode or an inactive state if Compliance Mode is disabled. 3. The port is connected to a USB 3.1 Gen 2 host controller when resuming from S3, S4, S5, or G3, the port may enter an inactive state.
Implication:	PCH USB Type-C* port configured in Device Mode (or in DbC mode) may fail to enumerate or become unavailable.
Workaround:	Non-available.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL13 Intel® Trace Hub Pipe Line Empty

Problem:	The Intel® Trace Hub Pipe Line Empty bit (CSR_MTB_BAR, Offset 0xD4) for a given output port may be set while the Input Buffer Empty for the associated output port is not set. This will only happen when the captureDone signal is de-asserted by clearing the ForceCaptureDone bit (CSR_MTB_BAR, Offset 0xD8) is cleared or the StoreQual[0] signal is de-asserted by the Trigger Unit before the pipe line is empty, and the destination is either system memory or USB (DCI).
Implication:	There may be valid trace data in the trace source input buffer that did not get sent to the destination (output port).
Workaround:	None identified. CaptureDone should be cleared or de-asserted after the pipe line is empty.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL14 eSPI SBLCL Register Bit Not Cleared by PMC_PLTRST_N

Problem:	The IOSF-SB eSPI Link Configuration Lock (SBLCL) bit (offset 4000h, bit 27 in eSPI PCR space) is reset by PMC_RSMRST_N assertion instead of PMC_PLTRST_N assertion.
Implication:	If the SBLCL bit is set to 1, software will not be able to access the eSPI device Capabilities and Configuration register in the reserved address range (0h - 7FFh) until PMC_RSMRST_N asserts.
Workaround:	Non-available. If software needs to access the eSPI device reserved range 0h - 7FFh, SBLCL while SBLCL bit is set to 1, a PMC_RSMRST_N assertion should be performed.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL15 xHCI USB 2.0 ISOCH Device Missed Service Interval

Problem:	When the xHCI controller is stressed with concurrent traffic across multiple USB ports, the xHCI controller may fail to service USB 2.0 Isochronous IN endpoints within the required service interval.
Implication:	USB 2.0 isochronous devices connected to the xHCI controller may experience dropped packets. ***Note:*** This issue has only been observed in a synthetic environment.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL16 xHCI Protocol Speed ID Count Field

Problem:	The xHCI Host Controller reports an incorrect Protocol Speed ID Count value for the USB 3.1 Supported Protocol Capability register - xHCI MMIO offset 8028 bits [31:28].
Implication:	No functional impact is expected.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL17 xHCI Short Packet Event Using Non-Event Data TRB

Problem:	The xHCI may generate an unexpected short packet event for the last transfer's Transfer Request Block (TRB) when using Non-Event Data TRB with multiples TRBs.
Implication:	Transfer may fail due to the packet size error. ***Note:*** This issue has only been observed in a synthetic environment. No known implication has been identified with commercial software.
Workaround:	None identified. Intel recommends software to use Data Event TRBs for short packet completion.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL18 S0ix Entry When Connecting a USB-C* Power Adapter

Problem:	Connecting a USB-C* power adapter to a PCH USB port may cause a race condition that can prevent the system from entering S0ix. This issue occurs only on designs where the USB-C* Power Delivery (PD) implements Out-Of-Band (OOB) messaging to communicate with the PCH for port mapping.
Implication:	The system may fail to enter S0ix.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL19 PCIe Clock Maximum Rising/Falling Edge Rate and V_{CROSS}

Problem:	The PCIe Clock Output signals (CLKOUT_PCIE_P/N) may not meet the maximum Rising/Falling Edge Rate and V_{CROSS} specifications as defined in the PCI Express Card Electromechanical Specification Revision 3.0, section 2.1.3, REFCLK AC Specifications.
Implication:	There are no known functional failures due to this erratum.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL20 USB VTIO Device Capabilities Field Length

Problem:	The xHCI spec version 1.2 defines the PCI Express Capability structure offset 04h Device Capabilities (DVSEC) field to be 8 bytes. The USB Virtualization Based Trusted IO (VTIO) Management controller implements the DVSEC field as 12 bytes.
Implication:	A USB controller driver may not be able to enable the USB VTIO controller.
Workaround:	None identified. To mitigate this erratum, an Independent Software Vendor could account for the field length in the USB controller driver.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL21 PCH Thermal Subsystem Not Updated After S0ix Exit

Problem:	The PMC firmware may not correctly reenable the PCH thermal subsystem after S0ix exit.
Implication:	The temperature used by the PCH thermal subsystem may not be updated. This may result in incorrect temperature reporting or thermal throttling. Catastrophic temperature event handling is not impacted by this erratum.
Workaround:	A BIOS code change has been identified and may be implemented as a workaround for this erratum.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL22 Intel® PSE GbE Controllers Incorrectly Advertised RX & TX FIFO Size

Problem:	The Intel® Programmable Services Engine (Intel® PSE) GbE Controllers MTL Receive FIFO Size (RXFIFOSIZE) bits [4:0] and MTL Transmit FIFO Size (TXFIFOSIZE) bits [10:6] in register MAC_HW_FEATURE1 (MMIO offset 120h) each advertise 64 KB as the allowable RX & TX FIFO size, while the implemented size is 32 KB each.
Implication:	The maximum aggregate size for MTL RX & TX queues is 32 KB each. If software allocation of TX & RX queues exceeds this amount, then data attempted to be queued greater than 32 KB will be lost.
Workaround:	None identified. Software should not allocate an aggregate size of more than 32 KB each for MTL RX & TX queues. A mitigation for this erratum is available in the Yocto Project*-based BSP PV release or later. A BIOS code change has been identified for the Intel® PSE's embedded processor and may be implemented as a mitigation for this erratum. ***Note:*** Intel provided drivers do not require this mitigation.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL23 Processor Unable to Enter DnX Mode

Problem:	When the Intel® CSE (Intel® Converged Security Engine) detects that BIOS IBB (Initial Boot Block) or OBB (OEM Boot Block) is corrupted and triggers a Global Reset, DnX mode may not be entered. ***Note:*** This issue does not occur in processor SKUs that implement the Intel® SI (Intel® Safety Island).
Implication:	When this erratum occurs, the system may not boot.
Workaround:	A BIOS code change has been identified and may be implemented as a workaround for this erratum.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL24 No S0i3.0 State when Device is Connected to DDI2 Interface

Problem:	When a device that uses physical DDC (Display Data Channel) signals is connected to the DDI2 display interface, the PCH may be unable to complete the internal clock gating required for transition to a S0i3.0-ready state.
Implication:	The processor may be unable to enter a S0i3.0 state.
Workaround:	A display driver should set and clear register field GTTMMADR (PCI[B:0,D:2,F:0,Off.10h]) + 0xC2000, Bit 7 as the last step in programming south display registers in preparation for entering a S0ix state. Alternatively, the display driver should set register field GTTMMADR + 0xC2000, Bit 7 on S0ix entry and clear it on S0ix exit. A workaround for this erratum is available in the Yocto Project*-based BSP PV release or later and Intel® Graphics Driver Production Version 100.9079 for Elkhart Lake Platforms or later.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL25 xHCI Force Header Command Incorrect Return Code

Problem:	The xHCI controller does not return the correct completion code for the Force Header Command as defined in the Section 4.6.16 of the eXtensible Host Controller Interface for Universal Serial Bus (xHCI) Requirements Specification Rev 1.2.
Implication:	xHCI CV TD4.12 - Force Header Command Test may report an error. The Force Header Command is only used by the USB-IF Command Verifier (xHCI CV) tool for device testing. There are no known functional failures due to this erratum.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL26 Leakage Current from VCC_1P8A Power Rail

Problem:	When the VCC_1P8A is off and the VCC_3P3A is powered on during G3 to S5, there may be a leakage current from the VCC_3P3A power rail to VCC_1P8A power rail.
Implication:	The leakage voltage may be observed on VCC_1P8A power rail. There is no known functional or reliability impact.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL27 USB 2.0 Device Interrupt IN Endpoint Split Transaction Error

Problem:	When a USB Full-speed or Low-speed (with an Interrupt IN Endpoint) device is connected behind a USB hub and a USB bulk device is also connected to any port on the xHCI controller, a split transaction error may occur on the USB Full-speed or Low-speed device.
Implication:	The USB Controller driver may reset the USB Full-speed or Low-speed Interrupt IN Endpoint. The observed behavior is USB device specific. For example, a delay in response may be observed from a Low-speed USB mouse or keyboard device.
Workaround:	A BIOS code change has been identified and may be implemented as a workaround for this erratum. For a more power optimized solution, a xHCI controller driver may dynamically clear the xHCI MMIO offset 0x8144 bit 8 when a USB Full-speed or Low-speed device is not connected behind a USB Hub and ensure the bit is set as configured by the BIOS.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL28 Processor May Not Wake From TPAUSE/UMWAIT in Limited Situations

Problem:	External interrupts should cause the processor to exit the implementation-dependent optimized state reached by the TPAUSE and UMWAIT instructions regardless of the value of RFLAGS.IF. Due to this erratum, an interrupt may not wake the processor from such a state when RFLAGS.IF is 0. Additionally, the processor may not exit from UMWAIT/TPAUSE sleep state if the virtualization execution control of Interrupt-Window Exiting is active (bit[2] of Primary Processor Based VM Execution Control is set to 1), or if Virtual-interrupt Delivery is active (bit[9] of Secondary Processor Based VM Execution Control is 1 and bit[31] of Primary Processor Based VM Execution Control is 1). Note that the only method to reach UMWAIT/TPAUSE sleep state with interrupt-window exiting pending is if the previous instruction is a STI, MOV SS, POP SS, or VM-entry, which sets MOV/POP SS blocking or STI blocking.
Implication:	If interrupts are masked because RFLAGS.IF = 0, arrival of an interrupt (or virtual interrupt) will not wake the processor from TPAUSE/UWMAIT. For operating systems that ensure that RFLAGS.IF = 1 whenever CPL > 0, this erratum applies only if TPAUSE or UMWAIT is used with interrupts disabled by RFLAGS.IF while CPL = 0. Intel is not aware of production software affected by this erratum.

Workaround:	It may be possible for the BIOS to contain a workaround for this erratum.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL29 Processor C-States with USB Full-speed or Low-speed Device Hotplug

Problem:	When doing a hotplug on a USB hub with two or more USB Full-speed or Low-speed devices each with a 1 ms service interval interrupt endpoint, a race condition may occur between the PMC and the xHCI controller.
Implication:	The processor may fail to enter C3 or deeper package C-States. ***Note:*** This erratum has only been observed in a synthetic environment.
Workaround:	None identified. This condition is recovered after the xHCI controller has successfully entered D3.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL30 USB 3.2 Gen 1x1 Port Does Not Send 16 Polling LFPS Burst

Problem:	On USB 3.2 Gen 1x1 only capable ports, including ports configured as USB 3.2 Gen 1x1 by soft strap, the xHCI controller may send only 15 LFPS signals instead of a burst of 16 LFPS signals as specified by the USB 3.2 specification.
Implication:	There are no known functional implications due to this erratum. LFPS handshake requires the receiver link partner to only detect 2 LFPS signals. This issue may impact the SuperSpeed compliance test case which checks for the 16 LFPS burst requirements: TD6.4, TD6.5, and TD7.31.
Workaround:	None identified.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL31 PMC_TGPIO Event May Have a Mismatched Time Stamp

Problem:	When a Time-Aware GPIO (PMC_TGPIO) event is counted in the Event Counter Capture (TGPIOECCV) register (PWRMBASE (PCI[B:0,D:31,F:2,Off.:10h) + 1238h), the Time Capture (TGPIOTCV) register (PWRMBASE (PCI[B:0,D:31,F:2,Off.:10h) + 1230h) value is not immediately updated after that event is counted.
Implication:	When the erratum occurs, a PMC_TGPIO event may have a mismatched time stamp.
Workaround:	None identified. A PMC_TGPIO driver can partially mitigate for this erratum by detecting that a TGPIOECCV register change has occurred without a TGPIOTCV register change and then repeatedly re-read the TGPIOTCV register until a change does occur.
Status:	For the steppings affected, refer Summary Table of Changes.

EHL32 EPT-based Address Translation May Not Operate Correctly After Posted-interrupt Processing

Problem:	If the “enable EPT” VM-execution control is 1, the processor uses extended page tables (EPT) to translate guest-physical addresses to physical addresses. If the “process posted interrupts” VM-execution control is 1, the processor may interpret some interrupts as notifications and respond to them by processing posted virtual interrupts on the virtual-APIC page. Under complex microarchitectural conditions, guest-physical addresses may be translated incorrectly after posted-interrupt processing.
Implication:	Incorrect data may be fetched for guest instructions, leading to unexpected operation of guest software or unexpected exceptions being delivered to the guest operating system. This erratum only affects software operating in a virtual machine.
Workaround:	It may be possible for BIOS to contain a workaround for this erratum.
Status:	For the steppings affected, refer Summary Tables of Changes.

§

Specification Changes

There are no specification changes in this revision of the Specification Update.

§

Specification Clarifications

There are no specification clarifications in this revision of the Specification Update.

§

Documentation Changes

1. Datasheet Updates

The SIO I2C ic_clk internal clock frequency (called f_input in Volume 1) is incorrectly documented in Sections 14.2.31 and 14.2.36 of Datasheet Volume 2, Book 2. These sections will be updated to match the ic_clk value stated in Volume 1: 133MHz

§