Intel® Pentium® and Celeron® Processor N- and J- Series

Specification Update

July 2017

Revision 006

Document Number: 334820-006

Contents

Preface 5
Summary Tables of Changes 7
Identification Information 11
Component Marking Information 14
Errata 15
Specification Changes 28
Specification Clarifications 29
Documentation Changes 30

§

Revision History

Revision Number	Description	Revision Date
001	Initial release	August 2016
002	• Errata — Added APL25-APL29	October 2016
003	• Errata — Added APL30-APL37	December 2016
004	• Errata — Added APL38-APL42 — Modified APL27	January 2017
005	• Errata — Added APL43-APL45 — Modified APL40	February 2017
006	• Errata — Added APL46	July 2017

§

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, and 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.

Note: Throughout this document Intel® Pentium® and Celeron® N- and J- Series Processor is referred as Processor or SoC.

Affected Documents

Document Title	Document Number
Intel® Pentium® and Celeron® Processor N- and J- Series Datasheet Volume 1 of 3	334817-001
Intel® Pentium® and Celeron® Processor N- and J- Series Datasheet Volume 2 of 3	334818-001
Intel® Pentium® and Celeron® Processor N- and J- Series Datasheet Volume 3 of 3	334819-001

Related Documents

Document Title	Document Number/Location
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide Intel® 64 and IA-32 Intel Architecture Optimization Reference Manual	http://www.intel.com/products/processor/manuals/index.htm
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	http://www.intel.com/content/www/us/en/architecture-and-technology/64-ia-32-architectures-software-developers-manual.html

Nomenclature

Errata are design defects or errors in engineering samples. Errata may cause the processor behavior to deviate from published specifications. Hardware and software designed to be used with any given stepping assumes 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, and so forth).

§

Summary Tables of Changes

The following table indicates the Specification Changes, Errata, Specification Clarifications, or Documentation Changes, which apply to the listed steppings. Intel intends to fix some of the errata in a future stepping of the component, and to account for the other outstanding issues through documentation or Specification Changes as noted. This table uses the following notations:

Codes Used in Summary Table

Stepping

X: Erratum, Specification Change or Clarification that applies to this stepping.

(No mark) or (Blank Box): This erratum is fixed in listed stepping or specification change does not apply to list stepping.

Status

Doc: Document change or update that will be implemented.

Plan Fix: This erratum may be fixed in a future stepping of the product.

Fixed: This erratum has been previously fixed.

No Fix: There is no plan to fix this erratum.

Row

Number	Stepping		Status	Errata Title
	B-0	B-1		
APL1	X	X	No Fix	Split Access to APIC-access Page May Access Virtual-APIC Page
APL2	X	X	No Fix	PEBS Record EventingIP Field May be Incorrect After CS.Base Change
APL3	X	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently

Number	Stepping		Status	Errata Title
	B-0	B-1		
APL4	X	X	No Fix	SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behaviour
APL5	X	X	No Fix	POPCNT Instruction May Take Longer to Execute Than Expected
APL6	X	X	No Fix	APIC-access VM Exit May Occur instead of SMAP #PF
APL7	X	X	No Fix	Some Performance Counter Overflows May Not Be Logged in IA32_PERF_GLOBAL_STATUS When FREEZE_PERFMON_ON_PMI is Enabled
APL8	X	X	No Fix	Performance Monitoring OFFCORE_RESPONSE1 Event May Improperly Count L2 Evictions
APL9	X	X	No Fix	Debug Exception May Not be Generated on Memory Read Spanning a Cacheline Boundary
APL10	X	X	No Fix	Intel® PT CR3 Filtering Compares Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH Outside of PAE Paging Mode
APL11	X	X	No Fix	Intel® PT OVF Packet May Be Followed by TIP.PGD Packet
APL12	X	X	No Fix	Intel® PT OVF May Be Followed By an Unexpected FUP Packet
APL13	X	X	No Fix	Performance Monitoring COREWB Offcore Response Event May Overcount
APL14	X	X	No Fix	FBSTP May Update FOP/FIP/FDP/FSW Before Exception or VM Exit
APL15	X	X	No Fix	PEBS Record May be Generated When Counters Frozen
APL16	X	X	No Fix	IA32_PERF_GLOBAL_INUSE[62] May be Set
APL17	X	X	No Fix	SATA Interface May Not Loopback Patterns in BIST-L Mode
APL18	X	X	No Fix	Using 32-bit Addressing Mode With SD/eMMC Controller May Lead to Unpredictable System Behavior

Number	Stepping		Status	Errata Title
	B-0	B-1		
APL19	X	X	No Fix	VDD2 Cannot Operate at 1.35V
APL20	X	X	No Fix	SATA Host Controller Does Not Pass Certain Compliance Tests
APL21	X	X	No Fix	Certain MCA Events May Incorrectly Set Overflow Bit
APL22	X	X	No Fix	The Shadow Register For DDR3L MR2 is 10 Bits Wide Instead of 11 Bits
APL23	X	X	No Fix	HD Audio Recording May Experience a Glitch While Opening or Closing Audio Streams
APL24	X	X	No Fix	xHCI Host Initiated LPM L1 May Cause a Hang
APL25	X	X	No Fix	USB Device Controller Incorrectly Interprets U3 Wakeup For Warm Reset
APL26	X	X	No Fix	SPI Flash Transaction Failure With Software Sequencing
APL27	X	-	Fixed	USB 2.0 Timing Responsiveness Degradation
APL28	X	X	No Fix	D3 Entry or D3 Exit May Fail For Certain Integrated PCIe Functions
APL29	X	X	No Fix	PM1_STS_EN.WAK_STS Gets Set During S0
APL30	X	X	No Fix	A Store Instruction May Not Wake up MWAIT
APL31	X	X	No Fix	De-asserting BME Bit May Cause System Hang
APL32	X	X	No Fix	Storage Controllers May Not Be Power Gated
APL33	X	X	No Fix	Reading an Intel® Trace Hub Register After a Write to an Undefined Register May Fail
APL34	X	X	No Fix	Deasserting PCICMD_PCISTS.BME Before Stopping ISP Camera Driver May Lead to a System Hang
APL35	X	X	No Fix	Certain Invalidation Wait Descriptors May Cause VT-d to Hang
APL36	X	X	No Fix	Certain VT-d SVM Registers Are Writeable

Number	Stepping		Status	Errata Title
	B-0	B-1		
APL37	X	X	No Fix	Changing VT-d Event Interrupt Configuration Control Registers May Not Behave as Expected
APL38	X	X	No Fix	SoC May Not Meet The $V_{OL(MAX)}$ Specification for THERMTRIP_N
APL39	X	X	No Fix	Intermittent CATERR may occur when back to back Host controller reset is performed
APL40	X	X	No Fix	Discrete TPM May Not be Accessible Through Fast SPI Bus
APL41	X	X	No Fix	USB xHCI Controller May Not Re-enter a D3 State After a USB Wake Event
APL42	X	X	No Fix	Updating or Disabling xHCI Controller Driver May Prevent Entering S0ix
APL43	X	X	No Fix	Intel® Trace Hub PTI Pattern Generator May Stop Working When Width is Changed While Enabled
APL44	X	X	No Fix	STHCAP1.RTITCNT Field Value Does Not Correctly Indicate The Number of Channels Supported
APL45	X	X	No Fix	Camera Device Does Not Issue an MSI When INTx is Enabled
APL46	X	X	No Fix	System May Experience Inability to Boot or May Cease Operation

Number	Specification Changes
	None

Number	Specification Clarifications
	None

Number	Documentation Changes
	None

§

Identification Information

The processor stepping can be identified by the following registers contents:

Table 1. Processor Signature by Using 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	15:13	12	11:8	7:4	3:0
0x0	0x00	0x5	0	0	0x6	0xC	0x9

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 Intel386™, Intel486™, Pentium®, Pentium® Pro, Pentium® 4, Intel® Core™2, or Intel® Atom™ processor series.
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's 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 is 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 a 1 in the EAX register, and the model field of the Device ID register is accessible through Boundary Scan.
6. The Stepping ID in Bits [3:0] indicates the revision number of that model.

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: The EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

Table 2. Processor Identification by Register Contents

Processor Line	Stepping	Vendor ID[1]	Host Device ID[2]	Processor Graphics Device ID[3]	Revision ID[4]
Intel® Pentium® Processor Series and Intel® Celeron® Processor Series	B-0	8086	5AF0	Pentium®: 0x5A84 Celeron®: 0x5A85	0x0A
Intel® Pentium® Processor Series and Intel® Celeron® Processor Series	B-1	8086	5AF0	Pentium®: 0x5A84 Celeron®: 0x5A85	0x0B

NOTES:

1. The Vendor ID corresponds to bits 15:0 of the Vendor ID Register located at offset 00h–01h in the PCI function 0 configuration space.
2. The Host Device ID corresponds to bits 15:0 of the Device ID Register located at Device 0 offset 02h– 03h in the PCI function 0 configuration space.
3. The Processor Graphics Device ID (DID2) corresponds to bits 15:0 of the Device ID Register located at Device 2 offset 02h–03h in the PCI function 0 configuration space.
4. The Revision Number corresponds to bits 7:0 of the Revision ID Register located at offset 08h in the PCI function 0 configuration space.

Table 3. Identification Table for Processor Series

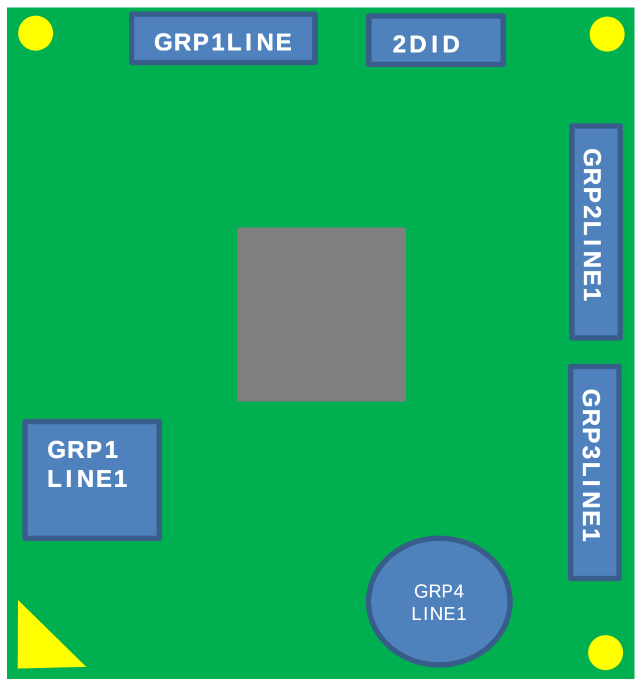
S-Spec	MM#	Stepping	Processor Number	Functional Core	Core Speed		Integrated Graphics Core Speed		TDP (W)
					Burst Frequency Mode (BFM) 2C/1C	High Frequency Mode (HFM)	Burst Frequency	Base Frequency	
R2Y9	951483	B-0	Pentium® N4200	4	2.4 GHz/2.5 GHz	1.1 GHz	750 MHz	200 MHz	6
R2YA	951484	B-0	Celeron® N3450	4	2.1 GHz/2.2 GHz	1.1 GHz	700 MHz	200 MHz	6
R2YB	951485	B-0	Celeron® N3350	2	2.3 GHz/2.4 GHz	1.1 GHz	650 MHz	200 MHz	6
R2ZA	951843	B-1	Pentium® J4205	4	2.5 GHz/2.6 GHz	1.5 GHz	800 MHz	250 MHz	10
R2Z9	951842	B-1	Celeron® J3455	4	2.2 GHz/2.3 GHz	1.5 GHz	750 MHz	250 MHz	10
R2Z8	951841	B-1	Celeron® J3355	2	2.4 GHz/2.5 GHz	2.0 GHz	700 MHz	250 MHz	10
R2Z5	951830	B-1	Pentium® N4200	4	2.4 GHz/2.5 GHz	1.1 GHz	750 MHz	200 MHz	6
R2Z6	951833	B-1	Celeron® N3450	4	2.1 GHz/2.2 GHz	1.1 GHz	700 MHz	200 MHz	6
R2Z7	951834	B-1	Celeron® N3350	2	2.3 GHz/2.4 GHz	1.1 GHz	650 MHz	200 MHz	6

§

Component Marking Information

Processor shipments can be identified by the following component markings and example pictures.

Figure 1. Processor Family Top-Side Markings



SAMPLE MARKING INFORMATION:
GRP1LINE: SN345
GRP1LINE1: swirl
GRP2LINE1: FPO45678
GRP3LINE1: SSPEC
GRP4LINE1: {eX}

§

Errata

APL1 Split Access to APIC-access Page May Access Virtual-APIC Page

Problem: A read from the APIC-access page that splits a cacheline boundary should cause an APIC-access VM exit. Due to this erratum, the processor may redirect such accesses to the virtual-APIC page without causing an APIC-access VM exit.

Implication: Guest software that attempts to access its APIC with a cacheline split may not be properly virtualized.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL2 PEBS Record EventingIP Field May be Incorrect After CS.Base Change

Problem: Due to this erratum, a PEBS (Precise Event Base Sampling) record generated after an operation that changes the CS.Base may contain an incorrect address in the EventingIP field.

Implication: Software attempting to identify the instruction that caused the PEBS event may report an incorrect instruction when non-zero CS.Base is supported and CS.Base is changed. Intel has not observed this erratum to impact the operation of any commercially available system.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL3 Performance Monitor Instructions Retired Event May Not Count Consistently

Problem: Performance Monitor Instructions Retired (Event C0H; Umask 00H) and the instruction retired fixed counter (IA32_FIXED_CTR0 MSR (309H)) are used to track the number of instructions retired. Due to this erratum, certain situations may cause the counter(s) to increment when no instruction has retired or to not increment when specific instructions have retired.

Implication: A performance counter counting instructions retired may over or under count. The count may not be consistent between multiple executions of the same code.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL4 SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior

Problem: If BIOS uses the RSM instruction to load the SMBASE register with a value that would cause any part of the SMRAM state-save area to have an address above 4-GBytes, subsequent transitions into and out of SMM (system-management mode) might save and restore processor state from incorrect addresses.

Implication: This erratum may cause unpredictable system behavior. Intel has not observed this erratum with any commercially available system.

Workaround: Ensure that the SMRAM state-save area is located entirely below the 4GB address boundary.

Status: For the steppings affected, see the Summary Tables of Changes.

APL5 POPCNT Instruction May Take Longer to Execute Than Expected

Problem: POPCNT instruction execution with a 32 or 64 bit operand may be delayed until previous non-dependent instructions have executed.

Implication: Software using the POPCNT instruction may experience lower performance than expected.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL6 APIC-access VM Exit May Occur Instead of SMAP #PF

Problem: A supervisor-mode data access through a user-mode page should cause a #PF if CR4.SMAP (Supervisor-Mode Access Prevention) is 1 and EFLAGS.AC is 0. Due to this erratum, a guest supervisor mode access to the APIC-access page may cause an APIC-access VM exit instead of a #PF due to SMAP.

Implication: A guest may miss an SMAP violation if it maps its APIC through a user-mode page. Intel has not observed this erratum with any commercially available software.

Workaround: Guest software should not map their APIC to a user mode page and attempt to access it from supervisor mode.

Status: For the steppings affected, see the Summary Tables of Changes.

APL7 Some Performance Counter Overflows May Not Be Logged in IA32_PERF_GLOBAL_STATUS When FREEZE_PERFMON_ON_PMI is Enabled

Problem: When enabled, FREEZE_PERFMON_ON_PMI bit 12 in IA32_DEBUGCTL MSR (1D9H) freezes PMCs (performance monitoring counters) on a PMI (Performance Monitoring Interrupt) request by setting CTR_Frz bit 49 in IA32_PERF_GLOBAL_STATUS MSR (38EH). Due to this erratum, if FREEZE_PERFMON_ON_PMI is enabled, PMC overflows that occur within a few cycles of a PMI being pended may not be logged in IA32_PERF_GLOBAL_STATUS MSR.

Implication: A performance counter may overflow but not set the overflow bit in IA32_PERF_GLOBAL_STATUS MSR.

Workaround: Re-enabling the PMCs in IA32_PERF_GLOBAL_CTRL will log the overflows that were not previously logged in IA32_PERF_GLOBAL_STATUS

Status: For the steppings affected, see the Summary Tables of Changes

APL8 Performance Monitoring OFFCORE_RESPONSE1 Event May Improperly Count L2 Evictions

Problem: Due to this erratum, a performance monitoring counter configured to count OFFCORE_RESPONSE1 (Event B7H, Umask 02H) uses MSR_OFFCORE_RSP0.COREWB (MSR 1A6H, bit 3) instead of the expected MSR_OFFCORE_RSP1.COREWB (MSR 1A7H, bit 3).

Implication: A performance monitoring counter using the OFFCORE_RESPONSE1 event will not count L2 evictions as expected when the COREWB value is not the same in MSR_OFFCORE_RSP1 and in MSR_OFFCORE_RSP0.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL9 Debug Exception May Not be Generated on Memory Read Spanning a Cacheline Boundary

Problem: A debug exception should be generated on a read which accesses an address specified by a breakpoint address register (DR0-DR3) and its LENn field (in DR7) configured to monitor data reads. Due to this erratum, under complex micro architectural conditions the processor may not trigger a debug exception on a memory read that spans a cacheline boundary.

Implication: When this erratum occurs, a debugger is not notified of a read that matches a data breakpoint.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL10 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 (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, see the Summary Tables of Changes.

APL11 Intel® PT OVF Packet May Be Followed by TIP.PGD Packet

Problem: If Intel PT (Processor Trace) encounters an internal buffer overflow and generates an OVF (Overflow) packet just as IA32_RTIT_CTL (MSR 570H) bit 0 (TraceEn) is cleared, or during a far transfer that causes IA32_RTIT_STATUS.ContextEn[1] (MSR 571H) to be cleared, the OVF may be followed by a TIP.PGD (Target Instruction Pointer - Packet Generation Disable) packet.

Implication: The Intel PT decoder may not expect a TIP.PGD to follow an OVF which could cause a decoder error.

Workaround: The Intel PT decoder should ignore a TIP.PGD that immediately follows OVF.

Status: For the steppings affected, see the Summary Tables of Changes.

APL12 Intel® PT OVF May Be Followed By an Unexpected FUP Packet

Problem: Certain Intel PT (Processor Trace) packets, including FUPs (Flow Update Packets), should be issued only between TIP.PGE (Target IP Packet - Packet Generation Enable) and TIP.PGD (Target IP Packet - Packet Generation Disable) packets. When outside a TIP.PGE/TIP.PGD pair, as a result of IA32_RTIT_STATUS.FilterEn[0] (MSR 571H) being cleared, an OVF (Overflow) packet may be unexpectedly followed by a FUP.

Implication: The Intel PT decoder may incorrectly assume that tracing is enabled and resume decoding from the FUP IP.

Workaround: The Intel PT decoder may opt to scan ahead for other packets to confirm whether PacketEn is set.

Status: For the steppings affected, see the Summary Tables of Changes.

APL13 Performance Monitoring COREWB Offcore Response Event May Overcount

Problem: An L2 eviction may affect the OFFCORE_RSP1 and OFFCORE_RSP2 events configured to count COREWB when the eviction is caused by an access made by a different core sharing the L2 cache.

Implication: The offcore response events may overcount when configured to count COREWB occurrence.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL14 FBSTP May Update FOP/FIP/FDP/FSW Before Exception or VM Exit

Problem: Due to this erratum, a FBSTP whose memory access causes an exception (e.g. #PF or #GP) or VM exit (e.g. EPT violation), may unexpectedly update FOP, FIP, FDP, FSW.IE or FSW.PE. FSW.ES is not affected by this erratum.

Implication: An x87 exception handler that executes an FBSTP but relies on the FP exception state being unchanged after taking a memory exception may not behave as expected. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL15 PEBS Record May be Generated When Counters Frozen

Problem: When Performance Monitoring counters are frozen due to IA32_PERF_GLOBAL_STATUS.CTR_Frz MSR (38EH, bit 59) being set, a PEBS (Processor Event Based Sampling) record may still be generated for counter 0 when the event specified by IA32_PERFEVTSEL0 MSR (186H) occurs.

Implication: An unexpected PEBS record may cause performance analysis software to behave unexpectedly.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes

APL16 IA32_PERF_GLOBAL_INUSE [62] May be Set

Problem: IA32_PERF_GLOBAL_INUSE MSR (392H) bit 62 is reserved. However, due to this erratum, it may sometimes be read as 1.

Implication: A read of IA32_PERF_GLOBAL_INUSE MSR may see bit 62 set in the result.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL17 SATA Interface May Not Loopback Patterns in BIST-L Mode

Problem: In certain BIST-L TX compliance test setups on SATA interface, the first 10b in the MFTP (Mid Frequency Test Pattern), i.e. 333h, inserted by J-BERT has disparity mismatch with the previous 10b, i.e. 363h, of previous HFTP (High Frequency Test Pattern) block. 333h has negative beginning disparity while 363h has positive ending disparity. When SoC detects disparity mismatch, it does not re-compute the running disparity based on the received 333h.

Implication: Due to this erratum, SATA interface may not correctly loopback patterns in BIST-L mode. This erratum does not impact BIST-T compliance mode.

Workaround: While using BIST-L loopback mode for SATA TX compliance testing, if a disparity error is encountered in subsequent MFTP block after receiving BIST-L FIS and HFTP block, insert a non-ALIGN primitive to correct back the disparity error at the beginning of MFTP pattern.

Status: For the steppings affected, see the Summary Tables of Changes.

APL18 Using 32-bit Addressing Mode With SD/eMMC Controller May Lead to Unpredictable System Behavior

Problem: SD/eMMC DMA transfers using 32-bit addressing mode may lead to unpredictable system behavior.

Implication: Due to this erratum, unpredictable system behavior may occur.

Workaround: SD/eMMC software should use the 64-bit addressing mode with the 96-bit descriptor format.

Status: For the steppings affected, see the Summary Tables of Changes.

APL19 VDD2 Cannot Operate at 1.35V

Problem: VDD2 power rail cannot operate at 1.35V.

Implication: Due to this erratum, merging VDD2 and VDDQ platform rails at 1.35V is not supported. This erratum does not impact the ability to merge VDD2 and VDDQ rails at 1.24V.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL20 SATA Host Controller Does Not Pass Certain Compliance Tests

Problem: The SoC SATA host controller OOB (Out of Band) Host Responses, OOB Transmit Gap, and OOB Transmit Burst Length do not pass Serial ATA Interoperability Program Revision 1.4.3, Unified Test Document Version 1.01 tests OOB-03[a/b], OOB-05, and OOB-06[a/b].

Implication: Intel has not observed any functional failures due to this erratum.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL21 Certain MCA Events May Incorrectly Set Overflow Bit

Problem: A single machine check event may incorrectly set OVER (bit 62) of IA32_MC4_STATUS (MSR 411H). The affected MCA events are Unsupported IDI opcode (MCACOD 0x0408, MSCOD 0x0000), WBMTo* access to MMIO (MCACOD 0x0408, MCACOD 0x0003) and CLFLUSH to MMIO (MCACOD 0x0408, MCACOD 0x0004).

Implication: Software analyzing system machine check error logs may incorrectly think that multiple errors have occurred. Intel has not observed this erratum impacting commercially available systems.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL22 The Shadow Register For DDR3L MR2 is 10 Bits Wide Instead of 11 Bits

Problem: The shadow register for DDR3L MR2 (D_CR_TQOFFSET.MR_VALUE) is only 10 bits whereas the MR2 register in DRAM devices is 11 bits.

Implication: At self-refresh entry, the memory controller writes the shadow MR2 register to the DRAM appending 0 for the 11^{th} bit.

Workaround: If a design needs to set MR2's 11^{th} bit, BIOS should set D_CR_TQCTL.SRTEN = 0 at MCHBAR offset 0x1A50 (multicast address) and write 1 to bit 7 of MR2 inside the DRAM to enable self-refresh Extended Temperature Mode all the time.

Status: For the steppings affected, see the Summary Tables of Changes.

APL23 HD Audio Recording May Experience a Glitch While Opening or Closing Audio Streams

Problem: Setting CRSTB (bit 0 at Intel HD Audio Base Address + 8) to zero when opening and closing audio streams may result in audio glitches.

Implication: Due to this erratum, audio glitches may occur while opening or closing audio streams.

Workaround: Avoid setting CRSTB (bit 0 at Intel HD Audio Base Address + 8) to zero unless entering D3 for system suspend or unless asserting platform reset for reboot.

Status: For the steppings affected, see the Summary Tables of Changes.

APL24 xHCI Host Initiated LPM L1 May Cause a Hang

Problem: If USB 2.0 device supports hardware LPM (Low Power Mode) and causes the host to initiate L1, then the host may inadvertently generate a transaction error during the Hardware LPM entry process.

Implication: The host will automatically re-enumerate the device repeatedly, resulting in a soft hang.

Workaround: A BIOS code change has been identified and may be implemented as a workaround for this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

APL25 USB Device Controller Incorrectly Interprets U3 Wakeup For Warm Reset

Problem: xHCI violates USB 3 specification for tU3WakeupRetryDelay, which dictates time to initiate the U3 wakeup LFPS Handshake signaling after an unsuccessful LFPS handshake. XHCI employs 12us for tU3WakeupRetryDelay instead of 100ms [as defined per spec].

Implication: Device may incorrectly interpret the LFPS asserted [due to the short tU3WakeupRetryDelay time] for duration greater than tResetDelay. If resume fails on the host side, this will be detected as a warm reset from xHCI and transition into Rx.Detect LTSSM state. Due to this erratum, the device may fail to respond to xHCI-initiated U3 wakeup request.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL26 SPI Flash Transaction Failure With Software Sequencing

Problem: Invalid instruction fields on Flash Invalid Instructions Registers (FLILL - FCBAh + 004h; FLILL1 - FCBAh + 008h) in flash descriptor contains opcodes that flash controller should protect against. SPI flash transactions will fail unless non-zero op-code is written to the invalid instruction fields.

Implication: Due to this erratum, SPI flash will not function with software sequencing if zero op-code is written to invalid instruction fields in flash descriptor data structure of the image.

Workaround: Program invalid instruction fields in flash descriptor with non-zero op-code. Hence, all illegal instructions and pre-opcode locations will have to be programmed with op-codes in the flash descriptor.

Status: For the steppings affected, see the Summary Tables of Changes.

APL27 USB 2.0 Timing Responsiveness Degradation

Problem: USB specification requires 1ms resume reflection time from platform to the device indicating USB resume/wake. Due to this erratum, SoC implementation violates the USB2 timing specification.

Implication: When this erratum occurs, USB devices that are sensitive to this timing specification may cease to function or re-enumerate upon waking from suspend.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL28 D3 Entry or D3 Exit May Fail For Certain Integrated PCIe Functions

Problem: Due to this erratum, the SoC may fail to correctly execute the D3 entry flow or the D3 exit flow for certain integrated PCIe functions.

Implication: If the affected PCI device fails to correctly enter D3, the SoC may not enter S0ix low power states. If the affected PCI device fails to correctly exit D3, the device will not function.

Workaround: To work around the D3 entry issue, software can implement an ACPI _PS3 method to verify PMCSR (bits 1:0) indicates the device has entered D3. If the device has not entered D3, the D3 entry steps should be repeated. To work around the D3 exit issue, software can issue a read to any device register prior to programming any DMA transfers.

Status: For the steppings affected, see the Summary Tables of Changes.

APL29 PM1_STS_EN.WAK_STS Gets Set During S0

Problem: PM1_STS_EN.WAK_STS (Offset 0h, Bit 15) is supposed to be set to '1' only upon exit from a valid sleep state. Due to this erratum, this bit gets set to '1' by a valid and enabled wake source during S0 and S0ix.

Implication: SCI (System Control Interrupt) OS flows from PM1_STS_EN or GPE0*_STS (B: 0, D: 13, F: 1, Offset 20h/24h/28h/2Ch) that also read PM1_STS_EN.WAK_STS may not operate as expected.

Workaround: The platform should either use an alternate GPE (General Purpose Event) to route the SCI or the OS should ignore WAK_STS in S0.

Status: For the steppings affected, see the Summary Tables of Changes.

APL30 A Store Instruction May Not Wake up MWAIT

Problem: One use of the MONITOR/MWAIT instruction pair is to allow a logical processor to wait in a sleep state until a store to the armed address range occurs. Due to this erratum, stores to the armed address range may not trigger MWAIT to resume execution.

Implication: The logical processor that executed the MWAIT instruction may not resume execution until it receives an interrupt. Software that does not rely on stores to the armed address range to wake a logical processor from an MWAIT sleep state is not affected by this erratum.

Workaround: Software needs to use interrupts to wake processors from MWAIT-induced sleep states.

Status: For the steppings affected, see the Summary Tables of Changes.

APL31 De-asserting BME Bit May Cause System Hang

Problem: If the BME (Bus Master Enable) bit in the ISP (Image Signal Processor) Device 3 PCI Configuration Space is de-asserted while the camera device is processing an image, the system may hang.

Implication: When this erratum occurs, the system may become non-responsive. Intel has not observed this erratum to impact commercially available software.

Workaround: Do not de-assert BME while the camera is active.

Status: For the steppings affected, see the Summary Tables of Changes.

APL32 Storage Controllers May Not Be Power Gated

Problem: When disabled or placed in D3 state by BIOS, the SD Card and SDIO storage controllers may not be power gated unless this is done prior to the eMMC controller being disabled or placed in D3 state.

Implication: Due to this erratum, storage controllers may not be power gated. This erratum does not apply to SKUs without eMMC controllers.

Workaround: BIOS should ensure the SD Card and SDIO controllers are disabled before disabling the eMMC controller or putting it into D3.

Status: For the steppings affected, see the Summary Tables of Changes.

APL33 Reading an Intel® Trace Hub Register After a Write to an Undefined Register May Fail

Problem: Reading an Intel TH (Trace Hub) register (Bus 0; Device 0; Function 2; Offset is register specific) may fail after attempting to write an undefined Intel TH register location (undefined locations are those not documented in the Intel Trace Hub Developer's Manual).

Implication: When this erratum occurs, reading a defined Intel TH register returns all zeroes regardless of its actual values.

Workaround: Software should not attempt to write to undefined Intel TH register locations.

Status: For the steppings affected, see the Summary Tables of Changes.

APL34 Deasserting PCICMD_PCISTS.BME Before Stopping ISP Camera Driver May Lead to a System Hang

Problem: If PCICMD_PCISTS.BME (Bus configured by BIOS: Device: 3; Function: 0; Offset: 4h; Bit 2) is de-asserted without first stopping the ISP camera driver, the system may hang.

Implication: If the PCICMD_PCISTS.BME register bit in the ISP is de-asserted, while the ISP (Image Signal Processor) is processing a data stream, the system may hang.

Workaround: Software should not de-assert BME without first stopping the ISP camera driver.

Status: For the steppings affected, see the Summary Tables of Changes.

APL35 Certain Invalidation Wait Descriptors May Cause VT-d to Hang

Problem: An inv_wait_dsc (Invalidation Wait Descriptor) with IF=0 (do not generate an interrupt on completion) and SW=0 (do not write status-word on completion) will prevent VT-d from processing subsequent commands.

Implication: When this erratum occurs, subsequent commands submitted to the Invalidation Queue will not be processed.

Workaround: Ensure all inv_wait_dsc have the IF bit and/or the SW bit set to '1'.

Status: For the steppings affected, see the Summary Tables of Changes.

APL36 Certain VT-d SVM Registers Are Writeable

Problem: VT-d engines that do not advertise SVM (Shared Virtual Memory) capability should treat the 32-bit registers at VTDBAR offsets 0xDC, 0xE0, 0xE4, 0xE8 and 0xEC as reserved and read-only. Due to this erratum, these registers are writeable.

Implication: Writing the listed registers does not affect the operation of the SoC.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL37 Changing VT-d Event Interrupt Configuration Control Registers May Not Behave as Expected

Problem: Due to this erratum, the sequence used to change VT-d event interrupt service routine configuration for Fault Events and for Invalidation Events may not work as expected. Specifically, reading one of the associated configuration registers does not serialize VT-d event interrupts. As a result, VT-d event interrupts that were issued using the previous interrupt service configuration may be delivered after software has observed the interrupt service configuration to be updated.

Implication: VT-d event interrupts using stale configuration information may be lost or cause unexpected behavior. Intel has not observed this erratum to impact commercially available software.

Workaround: Reading a VT-d event control register twice achieves the intended interrupt serialization.

Status: For the steppings affected, see the Summary Tables of Changes.

APL38 SoC May Not Meet The $V_{OL(MAX)}$ Specification for THERMTRIP_N

Problem: Under certain platform configurations and conditions, when the SoC asserts THERMTRIP_N, it may not meet the $V_{OL(MAX)}$ specification.

Implication: When this erratum occurs, the platform may not detect the assertion of THERMTRIP_N. This may, in turn, prevent the power-button override capability from resetting the platform-placing the platform in a non-responsive state requiring the platform to go to G3 (completely drained battery needed) in order to reboot.

Workaround: A platform design change has been identified as a workaround for this erratum.

Status: For the steppings affected, see the Summary Tables of Changes.

APL39 Intermittent CATERR may occur when back to back Host controller reset is performed

Problem: The xHCI host controller may fail to respond, due to an internal race condition, if consecutive xHCI Host Controller resets are performed.

Implication: A processor CATERR may occurs during long duration reboot testing or S4/S5 cycling tests.

Workaround: Software should add a 120ms delay in between consecutive xHCI host controller resets.

Status: For the steppings affected, see the Summary Tables of Changes.

APL40 Discrete TPM May Not be Accessible Through Fast SPI Bus

Problem: Accesses to a TPM device attached on Fast SPI bus will not succeed unless a flash device is also attached on Fast SPI bus.

Implication: Due to this erratum, the system is not able to communicate with a TPM device attached to the Fast SPI bus by itself. The integrated TPM (Intel Platform Trust Technology) is not affected by this erratum. Any TPM attached to the LPC bus is not affected by this erratum.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL41 USB xHCI Controller May Not Re-enter a D3 State After a USB Wake Event

Problem: After processing a USB 3.0 wake event, the USB xHCI controller may not re-enter D3 state.

Implication: When the failure occurs, the system will not enter an Sx state.

Workaround: Software should clear bit 8 PME Enable (PME_EN) of PM_CS--Power management Control/Status Register (USB xHCI-D21:F0: Offset 74h) after the controller enters D0 state following an exit from D3.

Status: For the steppings affected, see the Summary Tables of Changes.

APL42 Updating or Disabling xHCI Controller Driver May Prevent Entering S0ix

Problem: Updating or disabling xHCI controller driver will disable xHCI RTD3 Power Gating preventing the SoC from entering S0ix sleep states.

Implication: Due to this erratum, the SoC does not enter S0ix until the driver is updated/re-enabled following a system reboot.

Workaround: None identified.

Status: For the steppings affected, see the Summary Tables of Changes.

APL43 Intel® Trace Hub PTI Pattern Generator May Stop Working When Width is Changed While Enabled

Problem: Intel TH (Trace Hub) PTI (Parallel Trace Interface) pattern generator feature is used to test the connectivity between PTI port and trace capture hardware. Due to this erratum, once enabled the pattern generator may hang if the width is decreased.

Implication: Intel TH's pattern generator feature stops working when users decrease the width.

Workaround: Intel TH's PTI pattern generator width should be reconfigured only after an Intel® Trace Hub soft reset. Intel® Trace Hub Soft reset can be done by setting NPKDSC.FLR bit to '1'.

Status: For the steppings affected, see the Summary Tables of Changes.

APL44 STHCAP1.RTITCNT Field Value Does Not Correctly Indicate The Number of Channels Supported

Problem: The RTITCNT field (bits[19:16]) of the STHCAP1 CSR (offset 04004H from MTB_BAR) does not indicate the correct number of channels supported by Intel® Trace Hub for Intel® Processor Trace.

Implication: The RTITCNT field value cannot be used.

Workaround: The correct number of channels can be obtained from SoC datasheet.

Status: For the steppings affected, see the Summary Tables of Changes.

APL45 Camera Device Does Not Issue an MSI When INTx is Enabled

Problem: When both MSI (Message Signaled Interrupts) and legacy INTx are enabled by the camera device, INTx is asserted rather than issuing the MSI, in violation of the PCI Local Bus Specification.

Implication: Due to this erratum, camera device interrupts can be lost leading to device failure.

Workaround: The camera device must disable legacy INTx by setting bit 10 of PCICMD (Bus 0; Device 3; Function 0; Offset 04H) before MSI is enabled.

Status: For the steppings affected, see the Summary Tables of Changes.

APL46 System May Experience Inability to Boot or May Cease Operation

Problem: Under certain conditions where activity is high for several years the LPC, RTC, SD Card and GPIO Termination Circuitry may stop functioning in the outer years of use.

Implication: LPC and RTC circuitry that stops functioning may cause operation to cease or inability to boot. SD Card that stops functioning may cause SD Cards to be unrecognized. Intel has only observed this behavior in simulation. Designs that implement the LPC interface at the 1.8V signal voltage are not affected by the LPC part of this erratum. GPIO circuitry implications are platform implementation specific and may result in unexpected behavior.

Workaround: Firmware updates for LPC, RTC circuitry and GPIO Termination have been identified. Mitigations for SD Card circuitry and GPIO Termination have been identified and may be implemented for this erratum.

Status: For the stepping affected, see the 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

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

§