Intel® Pentium® Silver and Intel® Celeron® Processors

Specification Update

October 2020

Revision 007

Document Number: 336562-007

Contents

Figures

Tables

Revision History

Revision Date	Revision Number	Description
October 2020	007	Updated errata 006
March 2020	006	Added Errata 038
January 2020	005	Updated Section 7
November 2019	004	• Added Errata 037 • Updated Table 3-3
October 2019	003	Added Errata 026 to 036
July 2018	002	Added Errata 023 to 025
February 2018	001	Initial Release

§ §

1 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® Silver and Intel® Celeron® Processor is referred as Processor or SoC.

Throughout this document Intel® Pentium® Silver and Intel® Celeron® Processors families refer to:

- Intel® Pentium® Silver N5000
- Intel® Pentium® Silver J5005
- Intel® Celeron® N4000 and N4100
- Intel® Celeron® J4105 and J4005

1.1 Affected Documents

Document Title	Document Number
Intel® Pentium® Silver and Intel® Celeron® Processors Datasheet Volume 1 of 2	336560-003
Intel® Pentium® Silver and Intel® Celeron® Processors Datasheet Volume 2 of 2	336561-001

1.2 Related Documents

Document Title	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	Vol:1 Vol.2A Vol.2B Vol.3A Vol.3B
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	Click here

1.3 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).

§ §

2 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:

2.1 Codes Used in Summary Table

2.2 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.

2.3 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.

2.4 Row

Number	Stepping		Status	Errata Title
	B-0	R-0		
001	X	X	No Fix	Certain MCA Events May Incorrectly Set Overflow Bit
002	X	X	No Fix	SATA Interface May Not Loopback Patterns in BIST-L Mode
003	X	X	No Fix	SATA Host Controller Does Not Pass Certain Compliance Tests
004	X	X	No Fix	HD Audio Recording May Experience a Glitch While Opening or Closing Audio Streams

Number	Stepping		Status	Errata Title
	B-0	R-0		
005	X	X	No Fix	USB 2.0 Timing Responsiveness Degradation. Status rejected
006	X	X	No Fix	Trace Data to Multiple Destinations is Not Supported
007	X	X	No Fix	Storage Controllers May Not Be Power Gated
008	X	X	No Fix	Certain VT-d SVM Registers Are Writeable
009	X	X	No Fix	Changing VT-d Event Interrupt Configuration Control Registers May Not Behave as Expected
010	X	X	No Fix	SoC May Not Meet The VOL(MAX) Specification for THERMTRIP_N.
011	X	X	No Fix	Intermittent CATERR may occur when back to back Host controller reset is performed
012	X	X	No Fix	USB xHCI Controller May Not Re-enter a D3 State After a USB Wake Event
013	X	X	No Fix	USB Device Controller Incorrectly Interprets U3 Wakeup For Warm Reset
014	X	X	No Fix	Start/Stop Bits in MOT packets are not set on an IMR Violation
015	X	X	No Fix	URES contents may be lost after entering S0ix
016	X	X	No Fix	Performance Monitoring Event TLB_FLUSHES.STLB_ANY Double Counts
017	X	X	No Fix	Non Canonical Instruction Fetch May Not Signal #GP Fault
018	X	X	No Fix	Intel PT CR3 Filtering Compares Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH outside of PAE Paging Mode
019	X	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
020	X	X	No Fix	RF May be Incorrectly Set In The EFLAGS That is Saved to The Stack or to The Enclave SSA

Number	Stepping		Status	Errata Title
	B-0	R-0		
021	X	X	No Fix	IA32_PERF_GLOBAL_INUSE[62] May be Non-Zero
022	X	X	No Fix	Intel PT OVF Packet May Be Followed By TIP.PGD
023	X	X	No Fix	Intel® PT OVF Packet May Not Be Followed By A FUP Or TIP.PGE Packet
024	X	X	No Fix	PWRBTN_STS And PWRBTNOR_STS Status Bits Not Set Following A Power Button Override Event
025	X	X	No Fix	PM1_STS_EN.WAK_STS is Not Set Waking From A Valid Sleep Type
026	X	X	No Fix	Intel® Processor Trace Output May Over-write ToPA Output Region
027	X	X	No Fix	IA32_PERF_GLOBAL_INUSE[PMI_InUse] Reports an Incorrect Value.
028	X	X	No Fix	A single VM Entry or VM Exit That Both Disables And Re-enables Intel® PT May Cause Unpredictable System Behavior
029	X	X	No Fix	I2C TX_HOLD Hold Time Specification May be Violated
030	X	X	No Fix	System May Experience Inability to Boot or May Cease Operation or Nonfunctioning of LPC, I2C and GPIO Circuitry
031	X	X	No Fix	eMMC controller may fail to detect a CRC error in HS400 mode
032	X	X	No Fix	Certain MIPI Display Panels May Remain Blank
033	X	X	No Fix	An Indirect JMP or Indirect CALL Whose Last Instruction Byte is on The Last Byte of a 4GB Region of Memory May Lead to Unpredictable System Behavior
034	X	X	No Fix	Processor Energy Usage Calculation May Be Incorrect
035	X	X	No Fix	Unexpected #PF, #GP, #UD, or Other Unpredictable System Behavior May Occur

Number	Stepping		Status	Errata Title
	B-0	R-0		
036	X	X	No Fix	PEBS DLA May Report Incorrect Value
037	X	X	No Fix	System May Hang Under Complex Conditions
038	X	X	No Fix	Intel® PT TMA Packets Have Incorrect Payload

Table 2-1: Specification Changes

Number	Specification Changes
	None

Table 2-2: Specification Clarifications

Number	Specification Clarifications
	None

Table 2-3: Documentation Changes

Number	Documentation Changes
	None

§ §

3 Identification Information

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

Table 3-1: 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	0x7	0	0	0x6	0xA	1

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 3-2: 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	B0	8086	31F0	3184	0x3

NOTE:

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 3-3: Identification Table for Processor Series

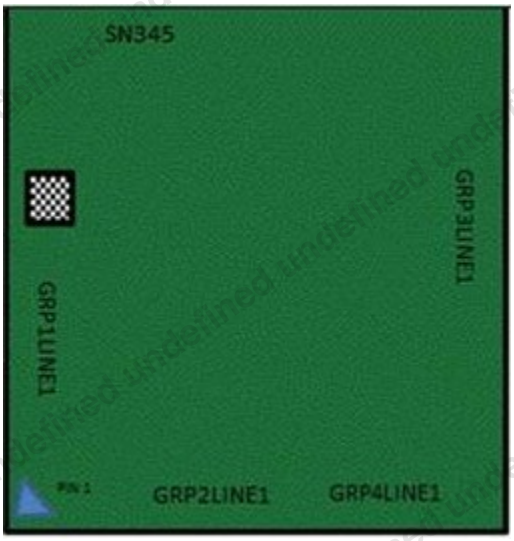
S-Spec	MM#	Stepping	Functional Core	Core Speed		Integrated Graphics Core Speed		TDP (W)
				Burst Frequency Mode (BFM) 1C	High Frequency Mode (HFM)	Burst Frequency	LFM Frequency	
R3RZ	961638	B-0	4	2.7GHz	1.1GHz	750 MHz	100MHz	6
R3S0	961639	B-0	4	2.4GHz	1.1GHz	700 MHz	100MHz	6
R3S1	961640	B-0	2	2.6GHz	1.1GHz	650 MHz	100MHz	6
R3S3	961642	B-0	4	2.8GHz	1.5GHz	800 MHz	100MHz	10
R3S4	961643	B-0	4	2.5GHz	1.5GHz	750 MHz	100MHz	10
R3S5	961644	B-0	2	2.7GHz	2.0GHz	700 MHz	100MHz	10
RFDC	999DAV	R-0	4	3.1GHz	1.1GHz	750 MHz	100MHz	6
RESZ	984729	R-0	4	2.6GHz	1.1GHz	700 MHz	100MHz	6
RET0	984730	R-0	2	2.8GHz	1.1GHz	650 MHz	100MHz	6
RFDB	999DAL	R-0	4	3.2GHz	2.0GHz	800 MHz	100MHz	10
RGZS	999PVK	R-0	4	2.7GHz	2.0GHz	750 MHz	100MHz	10
RET3	984796	R-0	2	2.9GHz	2.0GHz	700 MHz	100MHz	10

§ §

4 Component Marking Information

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

Figure 4-1: SoC Markings



SAMPLE MARKING INFORMATION:

Legend	Mark Text	Orientation
GRP1LINE1		North
GRP2LINE1	SR3S1	North
GRP3LINE1	J746B854	North
GRP4LINE1	{ e1}	North

§ §

5 Errata

001 : 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.

002 : 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.

003 : 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.

004 : 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.

005 : 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.

006 : Trace Data to Multiple Destinations Is Not Supported	
Problem	Trace data from one trace source (i.e. ODLA, STH, SoCHAP, DTF) containing several STP Masters and sent in one Grant Duration will all be sent to a single destination, even if the SWDEST [0-31] registers (CSR_MTB_BAR Offsets 4h-8Bh) are configured to send data from those Masters to different destinations.
Implication	Trace data from a given Master can be sent to the wrong destination.
Workaround	For Intel® Trace Hub to support multiple destinations, Grant Duration should be set to 11111111h in PGD0 (CSR_MTB_BAR Offset AC). This may impact aggregate trace throughput.
Status	For the steppings affected, see the Summary Tables of Changes.

007 : 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.

008 : 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.

009 : 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.

010 : SoC May Not Meet The VOL(MAX) Specification for THERMTRIP_N	
Problem	Under certain platform configurations and conditions, when the SoC asserts THERMTRIP_N, it may not meet the VOL(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	Platforms designs should not have a pull-up resistor on the THERMTRIP_N signal and per Intel simulation analysis, platform design can limit exposure to this issue by ensuring IOL(MAX) does not exceed 4uA.
Status	For the steppings affected, see the Summary Tables of Changes.

011 : 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.

012 : 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.

013 : 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 xHCIinitiated U3 wakeup request.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

014 : Start/Stop Bits In Mot Packets Are Not Set On An IMR Violation	
Problem	Memory Order Tracing (MOT) does not set the start/stop bits in the header packet if the traced packet is aborted due to an IMR (Isolated Memory Regions) violation.
Implication	The MOT trace may be missing start/stop indications. Intel has not observed this erratum to impact the operation of any commercially available software.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

015 : URES Contents May Be Lost After Entering S0ix	
Problem	The contents of URES (Unsupported Request Error Status) CSR (Bus:0, Device:13, Function:0, Offset: F0H) should be preserved across a S0ix transition. However, due to this erratum, the register gets cleared upon entry to S0ix and its error logging information is lost.
Implication	Software on a system that enters S0ix after an error is logged in URES will no longer be able to see the error details in URES.
Workaround	The system can be configured to generate an NMI on an error logged in URES, enabling software to manage the error prior to S0ix entry.
Status	For the steppings affected, see the Summary Tables of Changes.

016 : Performance Monitoring Event TLB_FLUSHES.STLB_ANY Double Counts	
Problem	A performance monitoring counter programmed to count the event TLB_FLUSHES.STLB_ANY (EventID 0BDH, Mask 20H) will increment twice for each STLB flush operation instead of incrementing once.
Implication	Performance analysis software will read double the number of STLB flushes that have actually occurred.
Workaround	Software should treat every two counts of TLB_FLUSHES.STLB_ANY as an indication of a single STLB flush.
Status	For the steppings affected, see the Summary Tables of Changes.

017 : Non Canonical Instruction Fetch May Not Signal #GP Fault	
Problem	An instruction fetch that includes linear address 8000_0000_0000H should signal a #GP fault due to a non-canonical violation. Due to this erratum, the instruction may be decoded using bytes starting from address ffff_8000_0000_0000H instead.
Implication	Software that relies on the signaling of a #GP fault to indicate the boundary between canonical and non-canonical spaces may not work as intended. Intel has not observed this erratum to affect any commercially available software.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

018 : Intel PT CR3 Filtering Compares Bits [11:5] Of CR3 And IA32_RTIT_CR3_MATCH Outside Of PAE Paging Mode	
Problem	R3[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.

019 : 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.

020 : RF May Be Incorrectly Set In The EFLAGS That Is Saved To The Stack Or To The Enclave SSA	
Problem	After a page fault due to failed DS (debug store) save area address translation, the RF (resume flag) may be incorrectly set in the EFLAGS image that is saved to the stack or to the enclave SSA (State Save Area) in case of AEX (Asynchronous Enclave Exit)
Implication	When this erratum occurs, a code breakpoint on the RIP of the instruction following a BTS (Branch Trace Store) trap will not be detected. In the case of AEX, it applies to the following enclave instruction.
Workaround	None identified. The VMM and the OS should pin DS save area pages to avoid DS page faults
Status	For the steppings affected, see the Summary Tables of Changes.

021 : IA32_PERF_GLOBAL_INUSE[62] May Be Non-Zero	
Problem	IA32_PERF_GLOBAL_INUSE[62] MSR (392H), which is a reserved bit, may contain a non-zero value when PEBS is enabled.
Implication	Software reading IA32_PERF_GLOBAL_INUSE MSR and expects reserved bits to be zero, may see a non-zero value in bit 62.
Workaround	Software must not rely on the value of reserved bits to always be zero.
Status	For the steppings affected, see the Summary Tables of Changes.

022 : Intel PT OVF Packet May Be Followed By TIP.PGD	
Problem	Intel® Processor Trace internal buffer overflow that resolves during a far transfer that changes bit 1 (ContextEn) in IA32_RTIT_STATUS (MSR 571H) from 1 to 0 may cause a TIP.PGD (Target IP Packet - Packet Generation Disabled) packet to be generated immediately following the OVF (Overflow) packet.
Implication	The trace decoder may signal an error due to the OVF packet being followed by an unexpected TIP.PGD.
Workaround	None identified.

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

023 : Intel® PT OVF Packet May Not Be Followed By A FUP Or TIP.PGE Packet	
Problem	If Intel® PT (Processor Trace) encounters an internal buffer overflow and generates an OVF (Overflow) packet, in some rare cases that packet may not be immediately followed by the expected FUP (Flow Update Packet) or TIP.PGE (Target IP - Packet Generation Enabled) packet.
Implication	An Intel® PT decoder may encounter a TNT (Taken Not Taken), TIP (Target IP), or other control flow packet immediately following an OVF packet.
Workaround	An Intel® PT decoder should scan ahead to the next FUP, TIP, or TIP.PGE packet following the OVF to determine the current IP.
Status	For the steppings affected, see the Summary Tables of Changes.

024 : PWRBTN_STS And PWRBTNOR_STS Status Bits Not Set Following A Power Button Override Event	
Problem	The PWRBTN_STS (bit 8) and PWRBTNOR _STS (bit 11) fields of PM1_STS_EN register (ABASE + 0x00) are incorrectly cleared on system wake following a Power Button Override Event.
Implication	System software is unable to detect the Power Button Override Event and may take the wrong boot path when Fastboot feature is enabled.
Workaround	A BIOS workaround has been identified.
Status	For the steppings affected, see the Summary Tables of Changes.

025 : PM1_STS_EN.WAK_STS Is Not Set Waking From A Valid Sleep Type	
Problem	PM1_STS_EN.WAK_STS (Bus 0; Device 0; Function 2; Offset 0h, Bit 15) is supposed to be set to '1' only upon exit from a valid sleep type (SLP_TYP). Due to this erratum, this bit is not set upon exit from a valid SLP_TYP.
Implication	SCI (System Control Interrupt) flows that read PM1_STS_EN.WAK_STS may not operate as expected.
Workaround	The platform may use an alternate GPE (General Purpose Event) to signal Wake event from a given valid SLP_TYP. Software should clear WAK_STS prior to enabling a valid SLP_TYP.
Status	For the steppings affected, see the Summary Tables of Changes.

026: Intel® Processor Trace Output May Over-write ToPA Output Region	
Problem	Due to a very rare microarchitectural condition, Intel® PT (Processor Trace) may over-write the most recently filled ToPA (Table of Physical Addresses) output region, rather than writing to the next ToPA output region.
Implication	The trace will be corrupted and an Intel® PT decoder error is likely to result. Intel has only observed this erratum in a synthetic test environment.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

027: IA32_PERF_GLOBAL_INUSE[PMI_InUse] Reports An Incorrect Value	
Problem	IA32_PERF_GLOBAL_INUSE[PMI_InUse] (MSR 392H, bit 63) should be set when any performance monitoring counter is configured to cause a PMI (Performance Monitoring Interrupt) when it overflows or is configured to generate PEBS records. Due to this erratum, this bit may not be set if no counter is configured to generate a PMI on overflow and only fixed-function performance counters are configured to cause PEBS records to be generated.
Implication	Software relying on PMI_InUse may not operate correctly. Intel has not observed this erratum to affect any production software.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

028: A Single VM Entry Or VM Exit That Both Disables And Re-enables Intel® PT May Cause Unpredictable System Behavior	
Problem	If TraceEn[bit 0] and ToPA[bit 8] in IA32_RTIT_CTL (MSR 0570H) are set and if a single VM entry or VM exit uses the MSR load list to both clear TraceEn and then restore it, or if a VM exit caused by a VM entry failure clears TraceEn in the VM entry MSR load list and then restores it in the VM exit MSR load list, the Intel PT (Processor Trace) output may be written to an unexpected location within the ToPA (Table of Physical Addresses) tables or output regions or to an unpredictable memory location.
Implication	Disabling and re-enabling Intel® PT during a single VM-exit, VM-entry, or failed VM-entry VM-exit, while using ToPA output can result in incorrect trace output or unpredictable system behavior.
Workaround	None identified. A hypervisor should take care to ensure that Intel® PT cannot be both disabled and re-enabled during VMX transitions when using ToPA output mode.

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

029 : I2C TX_HOLD Hold Time Specification May be Violated	
Problem	The processor may not meet the I2C specification minimum hold time for TX_HOLD on the PMIC I2C interface (PMIC I2C TX_HOLD parameter)..
Implication	The I2C TX_HOLD time specification may not be met for the PMIC I2C interface. Intel has not observed this erratum to affect any commercially available system.
Workaround	None identified.
Status	For the steppings affected, see the Summary Tables of Changes.

030 : System May Experience Inability To Boot Or May Cease Operation Or Nonfunctioning Of LPC, I2C and GPIO Circuitry	
Problem	Under certain conditions LPC, I2C and GPIO circuitry may stop functioning in the outer years of use.
Implication	LPC circuitry that stops functioning may cause operation to cease or inability to boot. I2C circuitry that stops functioning may cause operation to cease. Intel has only observed this behavior in simulation. Designs that implement the LPC interface at 1.8V signal voltage are not affected by the LPC portion of this sighting. Clockrun Protocol is not mandatory for GLK designs with LPC circuitry operating at 1.8V. When the platform drives the GPIO pin low, GPIO's programmed with weak pull-up circuitry may fail to maintain a value above VIH when not actively driven.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, see the Summary Tables of Changes.

031 : eMMC Controller May Fail To Detect A CRC Error In HS400 Mode	
Problem	The eMMC controller may fail to detect a CRC error if a bit error occurs on the DATA3 signal during read operations when in eMMC HS400 mode. CRC detection on other DATA signals is not impacted.
Implication	The controller will not flag the CRC error to the driver or application, which could result in data integrity issues. Bit errors on eMMC DATA signals are not expected on platforms that follow Intel recommended design guidelines and tuning processes.
Workaround	None identified. To mitigate the issue, eMMC HS200 mode can be used instead of HS400.
Status	For the steppings affected, see the Summary Tables of Changes.

032 : Certain MIPI Display Panels May Remain Blank	
Problem	Certain sizes of the "Type 39 Long Write DCS" MIPI command, typically used to configure the MIPI panel during POST, do not work as intended.
Implication	Due to this erratum, the MIPI display will remain blank due to the MIPI enable sequence timing out when the LP FIFO empty status register (LP_DATA_FIFO, BDF XYZ, offset 74h, bit 10) fails to indicate it is not empty. It can also be observed, that the type 39 packets are not transmitted properly on the link.
Workaround	None Identified
Status	For the steppings affected, see the Summary Tables of Changes.

033 : An Indirect JMP Or Indirect CALL Whose Last Instruction Byte Is On The Last Byte Of A 4GB Region Of Memory May Lead To Unpredictable System Behavior	
Problem	Under complex microarchitectural conditions when a near indirect JMP or near indirect Call whose last instruction byte is on the last byte of a 4GB region of memory and whose target is in the same 4GB space, incorrect instructions may execute leading to unpredictable system behavior.
Implication	When this erratum occurs, unpredictable system behavior may occur.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, see the Summary Tables of Changes.

034 : Processor Energy Usage Calculation May Be Incorrect	
Problem	After an S3 exit with initial high core activity, the processor may not calculate energy usage correctly until c-states are entered.
Implication	Due to this erratum, energy reported (Imon) may be lower than what was actually used.
Workaround	It is possible for BIOS to contain a workaround for this erratum
Status	For the steppings affected, see the Summary Tables of Changes.

035 : Unexpected #PF, #GP, #UD, Or Other Unpredictable System Behavior May Occur	
Problem	Under complex microarchitectural conditions, incorrect instruction bytes may be used for code with linear addresses bits 5:4 = 10b.
Implication	When this erratum occurs, unpredictable system behavior may occur. This unpredictable behavior often results in an unexpected #PF, #GP or #UD exception which causes an application to unexpectedly close.
Workaround	It is possible for BIOS to contain a workaround for this erratum
Status	For the steppings affected, see the Summary Tables of Changes.

036 : 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, see the Summary Tables of Changes.

037 : System May Hang Under Complex Conditions	
Problem	Under complex conditions, insufficient access control in graphics subsystem may lead to a system hang or crash upon a register read.
Implication	When this erratum occurs a system hang or crash may occur.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, see the Summary Tables of Changes.

038 : Intel® PT TMA Packets Have Incorrect Payloads	
Problem	Intel® PT (Processor Trace) TMA (TSC/MTC Alignment) packets hae incorrect values in both the CTC (Core Timer Copy) and FC (Fast Counter) fields. The FC value is always zero.
Implication	In Intel® PT decoder will be confused when using the TMA packet to align cycle time with wall-clock time.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, see the Summary Tables of Changes.

§§

6 Specification Changes

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

§§

7 Specification Clarifications

001: Power Leakage during system boot	
Implication	Intel® Pentium™ and Intel® Celeron™ J and N Series processors may exhibit power leakage on P1V8A platform rail within few milliseconds before platform power completion.
Workaround	None identified.
Status	Expected Behavior

§§

8 Documentation Changes

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

§§