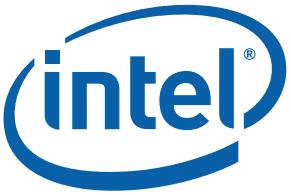


Mobile 4th Generation Intel® Core™ Processor Family

Specification Update

Supporting 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines

Supporting 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines

June 2013

Reference Number: 328903-001

Contents

§ §

Revision History

Revision	Description	Date
001	• Initial Release.	June 2013

Preface

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

Information types defined in Nomenclature are consolidated into the specification update and are no longer published in other documents.

This document may also contain information that was not previously published.

Affected Documents

Document Title	Document Number
Mobile 4th Generation Intel® Core™ Processor Family Datasheet – Volume 1 of 2 Subtitle: *Supporting 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines*	328901
Mobile 4th Generation Intel® Core™ Processor Family Datasheet – Volume 2 of 2 Subtitle: *Supporting 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines*	328902
Mobile 4th Generation Intel® Core™ Processor Family Datasheet – Volume 1 of 2 Subtitle: *Supporting 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines*	329001
Mobile 4th Generation Intel® Core™ Processor Family Datasheet – Volume 2 of 2 Subtitle: *Supporting 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines*	329002

Related Documents

Document Title	Document Number/ Location
AP-485, Intel® Processor Identification and the CPUID Instruction	http://www.intel.com/design/processor/applnots/241618.htm
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/design/processor/specupdt/252046.htm
ACPI Specifications	www.acpi.info

Nomenclature

Errata are design defects or errors. These may cause the processor 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 such as, core speed, L2 cache size, package type, etc. 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 on).

Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the processor. 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 uses the following notations.

Codes Used in Summary Tables

Stepping

X:	Errata exists in the stepping indicated. 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 listed stepping.

Page

(Page):	Page location of item in this document.

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.
No Fix:	There are no plans to fix this erratum.

Row

Change bar to left of a table row indicates this erratum is either new or modified from the previous version of the document.

Errata (Sheet 1 of 3)

Number	Steppings	Status	ERRATA
	C-0		
HSM1	X	No Fix	LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode
HSM2	X	No Fix	EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change
HSM3	X	No Fix	MCi_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error
HSM4	X	No Fix	LER MSRs May Be Unreliable
HSM5	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
HSM6	X	No Fix	An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang

Errata (Sheet 2 of 3)

Number	Steppings	Status	ERRATA
	C-0		
HSM7	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code
HSM8	X	No Fix	FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM
HSM9	X	No Fix	APIC Error “Received Illegal Vector” May be Lost
HSM10	X	No Fix	Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations
HSM11	X	No Fix	Performance Monitor Precise Instruction Retired Event May Present Wrong Indications
HSM12	X	No Fix	CR0.CD Is Ignored in VMX Operation
HSM13	X	No Fix	LER MSRs May Be Unreliable
HSM14	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
HSM15	X	No Fix	Processor May Fail to Acknowledge a TLP Request
HSM16	X	No Fix	Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered
HSM17	X	No Fix	PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect
HSM18	X	No Fix	PCIe* Controller May Incorrectly Log Errors on Transition to RxL0s
HSM19	X	No Fix	Unused PCIe* Lanes May Report Correctable Errors
HSM20	X	No Fix	Accessing Physical Memory Space 0-640K through the Graphics Aperture May Cause Unpredictable System Behavior
HSM21	X	No Fix	PCIe Root Port May Not Initiate Link Speed Change
HSM22	X	No Fix	Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected
HSM23	X	No Fix	DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction
HSM24	X	No Fix	VEX.L is Not Ignored with VCVT*2SI Instructions
HSM25 [1]	X	No Fix	Processor May Shut Down During Boundary Scan Testing
HSM26	X	No Fix	Certain Local Memory Read / Load Retired PerfMon Events May Undercount
HSM27	X	No Fix	Specific Graphics Blitter Instructions May Result in Unpredictable Graphics Controller Behavior
HSM28	X	No Fix	Processor May Enter Shutdown Unexpectedly on a Second Uncorrectable Error
HSM29	X	No Fix	Modified Compliance Patterns for 2.5 GT/s and 5 GT/s Transfer Rates Do Not Follow PCIe* Specification
HSM30	X	No Fix	Performance Monitor Counters May Produce Incorrect Results
HSM31	X	No Fix	Performance Monitor UOPS_EXECUTED Event May Undercount
HSM32	X	No Fix	MSR_PERF_STATUS May Report an Incorrect Core Voltage
HSM33	X	No Fix	PCIe* Atomic Transactions From Two or More PCIe Controllers May Cause Starvation
HSM34	X	No Fix	The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS is Not Updated After a UC Error is Logged
HSM35	X	No Fix	An AVX Gather Instruction That Causes an EPT Violation May Not Update Previous Elements
HSM36	X	No Fix	PLATFORM_POWER_LIMIT MSR Not Visible
HSM37	X	No Fix	LPDDR Memory May Report Incorrect Temperature

Errata (Sheet 3 of 3)

Number	Steppings	Status	ERRATA
	C-0		
HSM38	X	No Fix	PCIe* Host Bridge DID May Be Incorrect
HSM39	X	No Fix	TSC May be Incorrect After a Deep C-State Exit
HSM40	X	No Fix	PCIe* Controller May Initiate Speed Change While in DL_Init State Causing Certain PCIe Devices to Fail to Train
HSM41	X	No Fix	Spurious VT-d Interrupts May Occur When the PFO Bit is Set
HSM42	X	No Fix	Turbo Ratio Limits Cannot be Lowered
HSM43	X	No Fix	AVX Gather Instruction That Causes a Fault or VM Exit May Incorrectly Modify Its Destination Register
HSM44	X	No Fix	Inconsistent NaN Propagation May Occur When Executing (V)DPPS Instruction
HSM45	X	No Fix	Display May Flicker When Package C-States Are Enabled
HSM46	X	No Fix	Certain Combinations of AVX Instructions May Cause Unpredictable System Behavior
HSM47	X	No Fix	Processor May Incorrectly Estimate Peak Power Delivery Requirements
HSM48	X	No Fix	IA32_PERF_CTL MSR is Incorrectly Reset
HSM49	X	No Fix	Processor May Hang During a Function Level Reset of the Display
HSM50	X	No Fix	AVX Gather Instruction That Should Result in #DF May Cause Unexpected System Behavior
HSM51	X	No Fix	Throttling and Refresh Rate Maybe be Incorrect After Exiting Package C-State
HSM52	X	No Fix	Processor May Livelock During On Demand Clock Modulation
HSM53	X	No Fix	IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI
HSM54	X	No Fix	The From-IP for Branch Tracing May be Incorrect
HSM55	X	No Fix	TM1 Throttling May Continue indefinitely
HSM56	X	No Fix	Internal Parity Errors May Incorrectly Report Overflow in The IA32_MCi_STATUS MSR
HSM57	X	No Fix	Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count
HSM58	X	No Fix	Processor May Run at Incorrect P-State
HSM59	X	No Fix	Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count

Notes:
1. Applies to 4th Generation Intel® Core™ Processor based on Mobile U-Processor and V-Processor Lines

Specification Changes

Number	SPECIFICATION CHANGES
	None for this revision of this specification update.

Specification Clarifications

Number	SPECIFICATION CLARIFICATIONS
	None for this revision of this specification update.

Documentation Changes

Number	DOCUMENTATION CHANGES
HSM1	”On-Demand Clock Modulation Feature Clarification”

Identification Information

Component Identification using Programming Interface

The processor stepping can be identified by the following register contents.

Table 1. 4th Generation Intel® Core™ Processor based on Mobile M-Processor Line Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0011b		00b	0110b	1100b	xxxxb

Table 2. 4th Generation Intel® Core™ Processor based on Mobile H-Processor Line Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0100b		00b	0110b	0110b	xxxxb

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 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's family.
3. 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.
4. 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 accessible through Boundary Scan.
5. The Stepping ID in Bits [3:0] indicates the revision number of that model. See the processor Identification table for the processor stepping ID number in the CPUID information.

When EAX is initialized to a value of '1', the CPUID instruction returns the Extended Family, Extended Model, Processor Type, Family Code, Model Number and Stepping ID value in the EAX register. Note that the EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

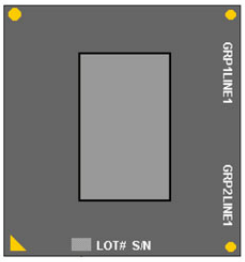
Cache and TLB descriptor parameters are provided in the EAX, EBX, ECX and EDX registers after the CPUID instruction is executed with a 2 in the EAX register.

The processor can be identified by the following register contents.

Component Marking Information

The processor stepping can be identified by the following component markings.

Figure 1. Mobile 4th Generation Intel® Core™ Processor Family BGA Top-Side Markings



Pkg Size = 37.5mm x 32mm
Pin Count = 1364

Sample (QDF)

GRP1LINE1: i{M}{C}YY {FPO}QDF ES	22 max char/line, 16 pt font
GRP2LINE1: {e1}	2 max char/line, 29 pt font

Production (SSPEC)

GRP1LINE1: i{M}{C}YY {FPO} SSPEC	22 max char/line, 16 pt font
GRP2LINE1: {e1}	2 max char/line, 29 pt font

FOL Mark:
2D Matrix and Human Readable Lot# (9 characters) and Serial# (5 characters)

Errata

HSM1. LBR, BTS, BTM May Report a Wrong Address when an Exception/ Interrupt Occurs in 64-bit Mode

Problem: An exception/interrupt event should be transparent to the LBR (Last Branch Record), BTS (Branch Trace Store) and BTM (Branch Trace Message) mechanisms. However, during a specific boundary condition where the exception/interrupt occurs right after the execution of an instruction at the lower canonical boundary (0x00007FFFFFFFFFFF) in 64-bit mode, the LBR return registers will save a wrong return address with bits 63 to 48 incorrectly sign extended to all 1's. Subsequent BTS and BTM operations which report the LBR will also be incorrect.

Implication: LBR, BTS and BTM may report incorrect information in the event of an exception/ interrupt.

Workaround: None identified.

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

HSM2. EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change

Problem: This erratum is regarding the case where paging structures are modified to change a linear address from writable to non-writable without software performing an appropriate TLB invalidation. When a subsequent access to that address by a specific instruction (ADD, AND, BTC, BTR, BTS, CMPXCHG, DEC, INC, NEG, NOT, OR, ROL/ROR, SAL/SAR/SHL/SHR, SHLD, SHRD, SUB, XOR, and XADD) causes a page fault or an EPT-induced VM exit, the value saved for EFLAGS may incorrectly contain the arithmetic flag values that the EFLAGS register would have held had the instruction completed without fault or VM exit. For page faults, this can occur even if the fault causes a VM exit or if its delivery causes a nested fault.

Implication: None identified. Although the EFLAGS value saved by an affected event (a page fault or an EPT-induced VM exit) may contain incorrect arithmetic flag values, Intel has not identified software that is affected by this erratum. This erratum will have no further effects once the original instruction is restarted because the instruction will produce the same results as if it had initially completed without fault or VM exit.

Workaround: If the handler of the affected events inspects the arithmetic portion of the saved EFLAGS value, then system software should perform a synchronized paging structure modification and TLB invalidation.

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

HSM3. MCi_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error

Problem: A single Data Translation Look Aside Buffer (DTLB) error can incorrectly set the Overflow (bit [62]) in the MCi_Status register. A DTLB error is indicated by MCA error code (bits [15:0]) appearing as binary value, 000x 0000 0001 0100, in the MCi_Status register.

Implication: Due to this erratum, the Overflow bit in the MCi_Status register may not be an accurate indication of multiple occurrences of DTLB errors. There is no other impact to normal processor functionality.

Workaround: None identified.

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

HSM4. LER MSRs May Be Unreliable

Problem: Due to certain internal processor events, updates to the LER (Last Exception Record) MSRs, MSR_LER_FROM_LIP (1DDH) and MSR_LER_TO_LIP (1DEH), may happen when no update was expected.

Implication: The values of the LER MSRs may be unreliable.

Workaround: None Identified.

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

HSM5. MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang

Problem: If the target linear address range for a MONITOR or CLFLUSH is mapped to the local xAPIC's address space, the processor will hang.

Implication: When this erratum occurs, the processor will hang. The local xAPIC's address space must be uncached. The MONITOR instruction only functions correctly if the specified linear address range is of the type write-back. CLFLUSH flushes data from the cache. Intel has not observed this erratum with any commercially available software.

Workaround: Do not execute MONITOR or CLFLUSH instructions on the local xAPIC address space.

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

HSM6. An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang

Problem: Uncorrectable errors logged in IA32_CR_MC2_STATUS MSR (409H) may also result in a system hang causing an Internal Timer Error (MCACOD = 0x0400h) to be logged in another machine check bank (IA32_MCi_STATUS).

Implication: Uncorrectable errors logged in IA32_CR_MC2_STATUS can further cause a system hang and an Internal Timer Error to be logged.

Workaround: None identified.

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

HSM7. #GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code

Problem: During a #GP (General Protection Exception), the processor pushes an error code on to the exception handler’s stack. If the segment selector descriptor straddles the canonical boundary, the error code pushed onto the stack may be incorrect.

Implication: An incorrect error code may be pushed onto the stack. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

HSM8. FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM

Problem: In general, a PEBS record should be generated on the first count of the event after the counter has overflowed. However, IA32_DEBUGCTL_MSR.FREEZE_WHILE_SMM (MSR 1D9H, bit [14]) prevents performance counters from counting during SMM (System Management Mode). Due to this erratum, if

1. A performance counter overflowed before an SMI
2. A PEBS record has not yet been generated because another count of the event has not occurred
3. The monitored event occurs during SMM

then a PEBS record will be saved after the next RSM instruction.

When FREEZE_WHILE_SMM is set, a PEBS should not be generated until the event occurs outside of SMM.

Implication: A PEBS record may be saved after an RSM instruction due to the associated performance counter detecting the monitored event during SMM; even when FREEZE_WHILE_SMM is set.

Workaround: None identified.

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

HSM9. APIC Error "Received Illegal Vector" May be Lost

Problem: APIC (Advanced Programmable Interrupt Controller) may not update the ESR (Error Status Register) flag Received Illegal Vector bit [6] properly when an illegal vector error is received on the same internal clock that the ESR is being written (as part of the write-read ESR access flow). The corresponding error interrupt will also not be generated for this case.

Implication: Due to this erratum, an incoming illegal vector error may not be logged into ESR properly and may not generate an error interrupt.

Workaround: None identified.

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

HSM10. Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations

Problem: Under complex microarchitectural conditions, if software changes the memory type for data being actively used and shared by multiple threads without the use of semaphores or barriers, software may see load operations execute out of order.

Implication: Memory ordering may be violated. Intel has not observed this erratum with any commercially available software.

Workaround: Software should ensure pages are not being actively used before requesting their memory type be changed.

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

HSM11. Performance Monitor Precise Instruction Retired Event May Present Wrong Indications

Problem: When the PDIR (Precise Distribution for Instructions Retired) mechanism is activated (INST_RETIRED.ALL (event C0H, umask value 00H) on Counter 1 programmed in PEBS mode), the processor may return wrong PEBS/PMI interrupts and/or incorrect counter values if the counter is reset with a SAV below 100 (Sample-After-Value is the counter reset value software programs in MSR IA32_PMC1[47:0] in order to control interrupt frequency).

Implication: Due to this erratum, when using low SAV values, the program may get incorrect PEBS or PMI interrupts and/or an invalid counter state.

Workaround: The sampling driver should avoid using SAV<100.

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

HSM12. CR0.CD Is Ignored in VMX Operation

Problem: If CR0.CD=1, the MTRRs and PAT should be ignored and the UC memory type should be used for all memory accesses. Due to this erratum, a logical processor in VMX operation will operate as if CR0.CD=0 even if that bit is set to 1.

Implication: Algorithms that rely on cache disabling may not function properly in VMX operation.

Workaround: Algorithms that rely on cache disabling should not be executed in VMX root operation.

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

HSM13. Instruction Fetch May Cause Machine Check if Page Size and Memory Type Was Changed Without Invalidation

Problem: This erratum may cause a machine-check error (IA32_MCi_STATUS.MCACOD=0150H) on the fetch of an instruction that crosses a 4-KByte address boundary. It applies only if (1) the 4-KByte linear region on which the instruction begins is originally translated using a 4-KByte page with the WB memory type; (2) the paging structures are later modified so that linear region is translated using a large page (2-MByte, 4-MByte, or 1-GByte) with the UC memory type; and (3) the instruction fetch occurs after the paging-structure modification but before software invalidates any TLB entries for the linear region.

Implication: Due to this erratum an unexpected machine check with error code 0150H may occur, possibly resulting in a shutdown. Intel has not observed this erratum with any commercially available software.

Workaround: Software should not write to a paging-structure entry in a way that would change, for any linear address, both the page size and the memory type. It can instead use the following algorithm: first clear the P flag in the relevant paging-structure entry (e.g., PDE); then invalidate any translations for the affected linear addresses; and then modify the relevant paging-structure entry to set the P flag and establish the new page size and memory type.

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

HSM14. Execution of VAESIMC or VAESKEYGENASSIST With An Illegal Value for VEX.vvvv May Produce a #NM Exception

Problem: The VAESIMC and VAESKEYGENASSIST instructions should produce a #UD (Invalid-Opcode) exception if the value of the vvvv field in the VEX prefix is not 1111b. Due to this erratum, if CR0.TS is "1", the processor may instead produce a #NM (Device-Not-Available) exception.

Implication: Due to this erratum, some undefined instruction encodings may produce a #NM instead of a #UD exception.

Workaround: Software should always set the vvvv field of the VEX prefix to 1111b for instances of the VAESIMC and VAESKEYGENASSIST instructions.

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

HSM15. Processor May Fail to Acknowledge a TLP Request

Problem: When a PCIe root port's receiver is in Receiver L0s power state and the port initiates a Recovery event, it will issue Training Sets to the link partner. The link partner will respond by initiating an L0s exit sequence. Prior to transmitting its own Training Sets, the link partner may transmit a TLP (Transaction Layer Packet) request. Due to this erratum, the root port may not acknowledge the TLP request.

Implication: After completing the Recovery event, the PCIe link partner will replay the TLP request. The link partner may set a Correctable Error status bit, which has no functional effect.

Workaround: None identified.

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

HSM16. Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered

Problem: If the local-APIC timer's CCR (current-count register) is 0, software should be able to determine whether a previously generated timer interrupt is being delivered by first reading the delivery-status bit in the LVT timer register and then reading the bit in the IRR (interrupt-request register) corresponding to the vector in the LVT timer register. If both values are read as 0, no timer interrupt should be in the process of being delivered. Due to this erratum, a timer interrupt may be delivered even if the CCR is 0 and the LVT and IRR bits are read as 0. This can occur only if the DCR (Divide Configuration Register) is greater than or equal to 4. The erratum does not occur if software writes zero to the Initial Count Register before reading the LVT and IRR bits.

Implication: Software that relies on reads of the LVT and IRR bits to determine whether a timer interrupt is being delivered may not operate properly.

Workaround: Software that uses the local-APIC timer must be prepared to handle the timer interrupts, even those that would not be expected based on reading CCR and the LVT and IRR bits; alternatively, software can avoid the problem by writing zero to the Initial Count Register before reading the LVT and IRR bits.

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

HSM17. PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect

Problem: If the processor is directed to enter PCIe Polling.Compliance at 5.0 GT/s or 8.0 GT/s transfer rates, it should use the Link Control 2 Compliance Preset/De-emphasis field (bits [15:12]) to determine the correct de-emphasis level. Due to this erratum, when the processor is directed to enter Polling.Compliance from 2.5 GT/s transfer rate, it retains 2.5 GT/s de-emphasis values.

Implication: The processor may operate in Polling.Compliance mode with an incorrect transmitter de-emphasis level.

Workaround: None identified.

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

HSM18. PCIe* Controller May Incorrectly Log Errors on Transition to RxL0s

Problem: Due to this erratum, if a link partner transitions to RxL0s state within 20 ns of entering L0 state, the PCIe controller may incorrectly log an error in "Correctable Error Status.Receiver Error Status" field (Bus 0, Device 2, Function 0, 1, 2 and Device 6, Function 0, offset 1D0H, bit 0).

Implication: Correctable receiver errors may be incorrectly logged. Intel has not observed any functional impact due to this erratum with any commercially available add-in cards.

Workaround: None identified.

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

HSM19. Unused PCIe* Lanes May Report Correctable Errors

Problem: Due to this erratum, during PCIe* link down configuration, unused lanes may report a Correctable Error Detected in Bus 0, Device 1, Function 0-2, and Device 6, Function 0, Offset 158H, Bit 0.

Implication: Correctable Errors may be reported by a PCIe controller for unused lanes.

Workaround: None identified.

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

HSM20. Accessing Physical Memory Space 0-640K through the Graphics Aperture May Cause Unpredictable System Behavior

Problem: The physical memory space 0-640K when accessed through the graphics aperture may result in a failure for writes to complete or reads to return incorrect results.

Implication: A hang or functional failure may occur during graphics operation such as OGL or OCL conformance tests, 2D/3D games and graphics intensive application.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM21. PCIe Root Port May Not Initiate Link Speed Change

Problem: The PCIe Base specification requires the upstream component to maintain the PCIe link at the target link speed or the highest speed supported by both components on the link, whichever is lower. PCIe root port will not initiate the link speed change without being triggered by the software when the root port maximum link speed is configured to be 5.0 GT/s. System BIOS will trigger the link speed change under normal boot scenarios. However, BIOS is not involved in some scenarios such as link disable/re-enable or secondary bus reset and therefore the speed change may not occur unless initiated by the downstream component. This erratum does not affect the ability of the downstream component to initiate a link speed change. All known 5.0Gb/s-capable PCIe downstream components have been observed to initiate the link speed change without relying on the root port to do so.

Implication: Due to this erratum, the PCIe root port may not initiate a link speed change during some hardware scenarios causing the PCIe link to operate at a lower than expected speed. Intel has not observed this erratum with any commercially available platform.

Workaround: None identified.

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

HSM22. Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected

Problem: x87 instructions that trigger #MF normally service interrupts before the #MF. Due to this erratum, if an instruction that triggers #MF is executed while Enhanced Intel SpeedStep® Technology transitions, Intel® Turbo Boost Technology transitions, or Thermal Monitor events occur, the pending #MF may be signaled before pending interrupts are serviced.

Implication: Software may observe #MF being-signaled before pending interrupts are serviced.

Workaround: None identified.

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

HSM23. DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction

Problem: Normally, data breakpoints matches that occur on a MOV SS, r/m or POP SS will not cause a debug exception immediately after MOV/POP SS but will be delayed until the instruction boundary following the next instruction is reached. After the debug exception occurs, DR6.B0-B3 bits will contain information about data breakpoints matched during the MOV/POP SS as well as breakpoints detected by the following instruction. Due to this erratum, DR6.B0-B3 bits may not contain information about data breakpoints matched during the MOV/POP SS when the following instruction is either an MMX instruction that uses a memory addressing mode with an index or a store instruction.

Implication: When this erratum occurs, DR6 may not contain information about all breakpoints matched. This erratum will not be observed under the recommended usage of the MOV SS,r/m or POP SS instructions (i.e., following them only with an instruction that writes (E/R)SP).

Workaround: None identified.

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

HSM24. VEX.L is Not Ignored with VCVT*2SI Instructions

Problem: The VEX.L bit should be ignored for the VCVTSS2SI, VCVTSD2SI, VCVTTSS2SI, and VCVTTSD2SI instructions, however due to this erratum the VEX.L bit is not ignored and will cause a #UD.

Implication: Unexpected #UDs will be seen when the VEX.L bit is set to 1 with VCVTSS2SI, VCVTSD2SI, VCVTTSS2SI, and VCVTTSD2SI instructions.

Workaround: Software should ensure that the VEX.L bit is set to 0 for all scalar instructions.

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

HSM25. Processor May Shut Down During Boundary Scan Testing

Problem: If the HIGHZ TAP command is run before initializing the Boundary Scan chain, the VR_EN pin may be tristated. The VR_EN pin may also be tristated by the EXTEST TAP command. The VR_EN signal controls the external voltage regulator; tristating VR_EN may disable the voltage regulator.

Implication: Due to this erratum, the processor may shut down.

Workaround: Initialize the Boundary Scan chain by running the PRELOAD TAP command before running HIGHZ TAP command or EXTEST TAP command.

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

HSM26. Certain Local Memory Read / Load Retired PerfMon Events May Undercount

Problem: Due to this erratum, the Local Memory Read / Load Retired PerfMon events listed below may undercount.

MEM_LOAD_RETIRED.L3_HIT
MEM_LOAD_RETIRED.L3_MISS
MEM_LOAD_L3_HIT_RETIRED.XSNP_MISS
MEM_LOAD_L3_HIT_RETIRED.XSNP_HIT
MEM_LOAD_L3_HIT_RETIRED.XSNP_HITM
MEM_LOAD_L3_HIT_RETIRED.XSNP_NONE
MEM_LOAD_L3_MISS_RETIRED.LOCAL_DRAM
MEM_LOAD_L4_RETIRED.LOCAL_HIT
MEM_TRANS_RETIRED.LOAD_LATENCY

Implication: The affected events may undercount, resulting in inaccurate memory profiles. Intel has observed undercounts as much as 40%..

Workaround: None identified.

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

HSM27. Specific Graphics Blitter Instructions May Result in Unpredictable Graphics Controller Behavior

Problem: Specific source-copy blitter instructions in Intel® HD Graphics 4600 Processor may result in unpredictable behavior when a blit source and destination overlap.

Implication: Due to this erratum, the processor may exhibit unpredictable graphics controller behavior. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

HSM28. Processor May Enter Shutdown Unexpectedly on a Second Uncorrectable Error

Problem: If an IA32_MCi_STATUS MSR contains an uncorrectable error with MCACOD=0x406 and a second uncorrectable error occurs after warm reset but before the first error is cleared by zeroing the IA32_MCi_STATUS MSR, a shutdown will occur.

Implication: When this erratum occurs, the processor will unexpectedly shut down instead of executing the machine check handler.

Workaround: None identified. Software should clear IA32_MCi_STATUS MSRs as early as possible to minimize the possibility of this erratum occurring.

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

HSM29. Modified Compliance Patterns for 2.5 GT/s and 5 GT/s Transfer Rates Do Not Follow PCIe* Specification

Problem: The PCIe controller does not produce the PCIe specification defined sequence for the Modified Compliance Pattern at 2.5 GT/s and 5 GT/s transfer rates. This erratum is not seen at 8 GT/s transfer rates.

Implication: Normal PCIe operation is unaffected by this erratum.

Workaround: None identified.

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

HSM30. Performance Monitor Counters May Produce Incorrect Results

Problem: When operating in hyper-threaded mode, a memory at-retirement performance monitoring event (from the list below) may be dropped or may increment an enabled counter on the physical core's other thread rather than the thread experiencing the event.

The list of affected memory at-retirement events is as follows:

MEM_UOP_RETIRED.LOADS
MEM_UOP_RETIRED.STORES
MEM_UOP_RETIRED.LOCK
MEM_UOP_RETIRED.SPLIT
MEM_UOP_RETIRED.STLB_MISS
MEM_LOAD_UOPS_RETIRED.HIT_LFB
MEM_LOAD_UOPS_RETIRED.L1_HIT
MEM_LOAD_UOPS_RETIRED.L2_HIT
MEM_LOAD_UOPS_RETIRED.LLC_HIT
MEM_LOAD_UOPS_MISC_RETIRED.LLC_MISS
MEM_LOAD_UOPS_LLC_HIT_RETIRED.XSNP_HIT
MEM_LOAD_UOPS_LLC_HIT_RETIRED.XSNP_HITM
MEM_LOAD_UOPS_LLC_HIT_RETIRED.XSNP_MISS
MEM_LOAD_UOPS_LLC_HIT_RETIRED.XSNP_NONE
MEM_LOAD_UOPS_RETIRED.LLC_MISS
MEM_LOAD_UOPS_LLC_MISS_RETIRED.LOCAL_DRAM
MEM_LOAD_UOPS_LLC_MISS_RETIRED.REMOTE_DRAM
MEM_LOAD_UOPS_RETIRED.L2_MISS

Implication: Due to this erratum, certain performance monitoring event will produce unreliable results during hyper-threaded operation.

Workaround: None identified.

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

HSM31. Performance Monitor UOPS_EXECUTED Event May Undercount

Problem: The performance monitor event UOPS_EXECUTED (Event B1H, any Unmask) should count the number of UOPs executed each cycle. However due to this erratum, when eight UOPs execute in one cycle, these UOPs will not be counted.

Implication: The performance monitor event UOPS_EXECUTED may reflect a count lower than the actual number of events.

Workaround: None identified.

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

HSM32. MSR_PERF_STATUS May Report an Incorrect Core Voltage

Problem: The core operating voltage can be determined by dividing MSR_PERF_STATUS MSR (198H) bits [47:32] by 2^13. However, due to this erratum, this calculation may report half the actual core voltage.

Implication: The core operating voltage may be reported incorrectly.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM33. PCIe* Atomic Transactions From Two or More PCIe Controllers May Cause Starvation

Problem: On a Processor PCIe controller configuration in which two or more controllers receive concurrent atomic transactions, a PCIe controller may experience starvation which eventually can lead to a completion timeout.

Implication: Atomic transactions from two or more PCIe controllers may lead to a completion timeout. Atomic transactions from only one controller will not be affected by this erratum. Intel has not observed this erratum with any commercially available device.

Workaround: None identified.

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

HSM34. The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS is Not Updated After a UC Error is Logged

Problem: When a UC (uncorrected) error is logged in the IA32_MC0_STATUS MSR (401H), corrected errors will continue to update the lower 14 bits (bits 51:38) of the Corrected Error Count. Due to this erratum, the sticky count overflow bit (bit 52) of the Corrected Error Count will not get updated after a UC error is logged.

Implication: The Corrected Error Count Overflow indication will be lost if the overflow occurs after an uncorrectable error has been logged.

Workaround: None identified.

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

HSM35. An AVX Gather Instruction That Causes an EPT Violation May Not Update Previous Elements

Problem: When execution of an AVX gather instruction causes an EPT (extended page table) violation due to a specific element, all previous elements should be complete. Due to this erratum, such an execution may fail to complete previous elements. In addition, the instruction's mask operand is not updated. This erratum applies only if the EPT violation occurs while updating an accessed or dirty flag in a paging-structure entry. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.

Implication: This erratum may prevent a gather instruction from making forward progress.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM36. PLATFORM_POWER_LIMIT MSR Not Visible

Problem: The PLATFORM_POWER_LIMIT MSR (615H) is used to control the PL3 (power limit 3) mechanism of the processor. Due to this erratum, this MSR is not visible to software.

Implication: Software is unable to read or write the PLATFORM_POWER_LIMIT MSR. If software attempts to access this MSR, a general protection fault will occur.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM37. LPDDR Memory May Report Incorrect Temperature

Problem: When any of the four possible LPDDR ranks are not populated, the unpopulated ranks will report a default temperature of 85C as a three bit value of 011b. If the system has unpopulated ranks the temperature of memory will be reported as 85C in PCU_CR_DDR_DIMM_HOTTEST_ABSOLUTE (MCHBAR Bus 0; Device 0; Function 0; offset 58B8H) in bits [5:7], until any of the populated ranks report a higher temperature than this.

Implication: When the memory temperature is less than or equal to 85C it may be reported as 85C. This erratum does not affect DDR3 and DDR3L memory types.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM38. PCIe* Host Bridge DID May Be Incorrect

Problem: The PCIe Host Bridge DID register (Bus 0; Device 0; Offset 2H) contents may be incorrect after a Package C7 exit.

Implication: Software that depends on the Host Bridge DID value may not behave as expected after a Package C7 exit.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM39. TSC May be Incorrect After a Deep C-State Exit

Problem: On exiting from Package C6 or deeper, the processor may incorrectly restore the TSC (Time Stamp Counter).

Implication: Software using the TSC may produce incorrect result and/or may not behave as expected.-

Workaround: It is possible for BIOS to contain a workaround for this erratum.

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

HSM40. PCIe* Controller May Initiate Speed Change While in DL_Init State Causing Certain PCIe Devices to Fail to Train

Problem: The PCIe controller supports hardware autonomous speed change capabilities. Due to this erratum, the PCIe controller may initiate speed change while in the DL_Init state which may prevent link training for certain PCIe devices.

Implication: Certain PCIe devices may fail to complete DL_Init causing the PCIe link to fail to train.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM41. Spurious VT-d Interrupts May Occur When the PFO Bit is Set

Problem: When the PFO (Primary Fault Overflow) field (bit [0] in the VT-d FSTS [Fault Status] register) is set to 1, further faults should not generate an interrupt. Due to this erratum, further interrupts may still occur.

Implication: Unexpected Invalidation Queue Error interrupts may occur. Intel has not observed this erratum with any commercially available software.

Workaround: Software should be written to handle spurious VT-d fault interrupts.

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

HSM42. Turbo Ratio Limits Cannot be Lowered

Problem: When ratio overclocking is enabled, customers can write to the MSR_TURBO_RATIO_LIMIT MSR (1ADH) to raise the core turbo ratio limits (per number of active cores) above the factory configured values. Due to this erratum, after raising turbo ratio limits, they cannot be lowered without a platform reset.

Implication: Any attempt to lower the turbo ratio limits will be ignored.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM43. AVX Gather Instruction That Causes a Fault or VM Exit May Incorrectly Modify Its Destination Register

Problem: An execution of a 128-bit AVX gather instruction zeroes the upper 128 bits of the instruction's destination register unless access to the first unmasked element causes a fault or VM exit. Due to this erratum, these bits may be cleared even when accessing the first unmasked element causes a fault or VM exit. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.

Implication: Software that depends on the destination register of a 128-bit AVX gather instruction to remain unchanged after access of the first unmasked element results in fault or VM exit may not behave as expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM44. Inconsistent NaN Propagation May Occur When Executing (V)DPPS Instruction

Problem: Upon completion of the (V)DPPS instruction with multiple different NaN encodings in the input elements, software may observe different NaN encodings in the destination elements.

Implication: Inconsistent NaN encodings in the destination elements for the (V) DPPS instruction may be observed.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM45. Display May Flicker When Package C-States Are Enabled

Problem: When package C-States are enabled, the display may not be refreshed at the correct rate.

Implication: When this erratum occurs, the user may observe flickering on the display.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM46. Certain Combinations of AVX Instructions May Cause Unpredictable System Behavior

Problem: Execution of certain combinations of AVX instructions may lead to unpredictable system behavior.

Implication: When this erratum occurs, unpredictable system behaviors, including system hang or incorrect results can occur.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM47. Processor May Incorrectly Estimate Peak Power Delivery Requirements

Problem: Under certain conditions, the processor may incorrectly calculate the frequency at which the cores and graphics engine can operate while still meeting voltage regulator and power supply peak power delivery capabilities. When this occurs, combined with high power workloads, system shutdown may be observed.

Implication: When this erratum occurs, system shutdown may be observed under high power workloads.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM48. IA32_PERF_CTL MSR is Incorrectly Reset

Problem: The IA32_PERF_CTL MSR (199H) is not initialized correctly after a processor reset.

Implication: If software reads the IA32_PERF_CTL MSR before writing it, software can observe an incorrect reset value. Although incorrect values are reported to software, the correct default values for this register are still used by the processor. No performance or power impact occurs due to this erratum.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM49. Processor May Hang During a Function Level Reset of the Display

Problem: When package C-States are enabled, it is possible that the processor may hang when software performs a Function Level Reset of the display via bit 1 of the Advanced Features Control Register (Bus 0; Device 2; Function 0; Offset 0A8H).

Implication: When this erratum occurs, the processor may hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM50. AVX Gather Instruction That Should Result in #DF May Cause Unexpected System Behavior

Problem: Due to this erratum, an execution of a 128-bit AVX gather instruction may fail to generate a #DF (double fault) when expected. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.

Implication: When this erratum occurs, an operation which should cause a #DF may result in unexpected system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM51. Throttling and Refresh Rate Maybe be Incorrect After Exiting Package C-State

Problem: When the OLTM (Open Loop Thermal Management) feature is enabled, the DIMM thermal status reported in DDR_THERM_PERDIMM_STATUS (MCHBAR Offset 588CH) may be incorrect following an exit from Package C3 or deeper.

Implication: The incorrect DIMM thermal status may result in degraded performance from unneeded memory throttling and excessive DIMM refresh rates.

Workaround: It is possible for BIOS to contain a workaround for this erratum.

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

HSM52. Processor May Livelock During On Demand Clock Modulation

Problem: The processor may livelock when (1) a processor thread has enabled on demand clock modulation via bit 4 of the IA32_CLOCK_MODULATION MSR (19AH) and the clock modulation duty cycle is set to 12.5 % (02H in bits 3:0 of the same MSR), and (2) the other processor thread does not have on demand clock modulation enabled and that thread is executing a stream of instructions with the lock prefix that either split a cacheline or access UC memory.

Implication: Program execution may stall on both threads of the core subject to this erratum.

Workaround: This erratum will not occur if clock modulation is enabled on all threads when using on demand clock modulation or if the duty cycle programmed in the IA32_CLOCK_MODULATION MSR is 18.75% or higher.

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

HSM53. IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI

Problem: FREEZE_PERFMON_ON_PMI (bit 12) in the IA32_DEBUGCTL MSR (1D9H) is erroneously cleared during delivery of an SMI (system-management interrupt).

Implication: As a result of this erratum, the performance monitoring counters will continue to count after a PMI occurs in SMM (system-management Mode).

Workaround: None identified.

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

HSM54. The From-IP for Branch Tracing May be Incorrect

Problem: BTM (Branch Trace Message) and BTS (Branch Trace Store) report the "From-IP" indicating the source address of the branch instruction. Due to this erratum, BTM and BTS may repeat the "From-IP" value previously reported. The "To-IP" value is not affected.

Implication: Using BTM or BTS reports to reconstruct program execution may be unreliable.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM55. TM1 Throttling May Continue indefinitely

Problem: TM1 (Thermal Monitor 1) throttling may continue when the processor's temperature decreases below the throttling point while the processor is in Package C3 or deeper.

Implication: The processor will continue thermal throttling but does not indicate it is hot.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM56. Internal Parity Errors May Incorrectly Report Overflow in The IA32_MCi_STATUS MSR

Problem: Due to this erratum, uncorrectable internal parity error reports with an IA32_MCi_STATUS.MCACOD (bits [15:0]) value of 0005H and an IA32_MCi_STATUS.MSCOD (bits [31:16]) value of 0004H may incorrectly set the IA32_MCi_STATUS.OVER flag (bit 62) indicating an overflow even when only a single error has been observed.

Implication: IA32_MCi_STATUS.OVER may not accurately indicate multiple occurrences of uncorrectable internal parity errors. There is no other impact to normal processor functionality.

Workaround: None identified.

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

HSM57. Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count

Problem: The Performance Monitor events OTHER_ASSISTS.AVX_TO_SSE (Event C1H; Umask 08H) and OTHER_ASSISTS.SSE_TO_AVX (Event C1H; Umask 10H) incorrectly increment and over count when an HLE (Hardware Lock Elision) abort occurs.

Implication: The Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX may over count.

Workaround: None identified.

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

HSM58. Processor May Run at Incorrect P-State

Problem: The processor package may use stale software P-State (performance state) requests when one or more logical processors are idle.

Implication: The processor package may run at a higher or lower than expected P-State. This issue may persist as long as any logical processor is idle.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

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

HSM59. Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count

Problem: The Performance Monitor Event DSB2MITE_SWITCHES.COUNT (Event ABH; Umask 01H) should count the number of DSB (Decode Stream Buffer) to MITE (Macro Instruction Translation Engine) switches. Due to this erratum, the DSB2MITE_SWITCHES.COUNT event will count speculative switches and cause the count to be higher than expected.

Implication: The Performance Monitor Event DSB2MITE_SWITCHES.COUNT may report count higher than expected.

Workaround: None identified.

§ §

Specification Changes

The Specification Changes listed in this section apply to the following documents:

- *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*

There are no new Specification Changes in this Specification Update revision.

§ §

Specification Clarifications

The Specification Clarifications listed in this section may apply to the following documents:

- *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*

There are no new Specification Changes in this Specification Update revision.

§ §

Documentation Changes

The Documentation Changes listed in this section apply to the following documents:

- *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*

All Documentation Changes will be incorporated into a future version of the appropriate Processor documentation.

Note: Documentation changes for Intel® 64 and IA-32 Architecture Software Developer's Manual volumes 1, 2A, 2B, 3A, and 3B will be posted in a separate document, Intel® 64 and IA-32 Architecture Software Developer's Manual Documentation Changes. Use the following link to become familiar with this file: http://developer.intel.com/products/processor/manuals/index.htm

There are no new Documentation Changes in this Specification Update revision.

HSM1. On-Demand Clock Modulation Feature Clarification

Software Controlled Clock Modulation section of the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide will be modified to differentiate On-demand clock modulation feature on different processors. The clarification will state:

For Hyper-Threading Technology enabled processors, the IA32_CLOCK_MODULATION register is duplicated for each logical processor. In order for the On-demand clock modulation feature to work properly, the feature must be enabled on all the logical processors within a physical processor. If the programmed duty cycle is not identical for all the logical processors, the processor clock will modulate to the highest duty cycle programmed for processors if the CPUID DisplayFamily_DisplayModel signatures is listed in Table 14-2. For all other processors, if the programmed duty cycle is not identical for all logical processors in the same core, the processor will modulate at the lowest programmed duty cycle.

For multiple processor cores in a physical package, each core can modulate to a programmed duty cycle independently.

For the P6 family processors, on-demand clock modulation was implemented through the chipset, which controlled clock modulation through the processor's STPCLK# pin.

Table 14-2. CPUID Signatures for Legacy Processors That Resolve to Higher Performance Setting of Conflicting Duty Cycle Requests

Display Family Display Model	Display Family Display Model	Display Family Display Model	Display Family Display Model
0F_xx	06_1C	06_1A	06_1E
06_1F	06_25	06_26	06_27
06_2C	06_2E	06_2F	06_35
06_36			

§ §