Intel® Core™ M Processor Family

Specification Update

December 2014

Revision 003

Reference Number: 330836-003

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

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

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

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

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

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit: http://www.intel.com/go/virtualization.

Intel® Turbo Boost Technology requires a system with Intel® Turbo Boost Technology. Intel Turbo Boost Technology and Intel Turbo Boost Technology 2.0 are only available on select Intel® processors. Consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit: http://www.intel.com/go/turbo.

Intel® Hyper-Threading Technology requires an Intel® HT Technology enabled system, check with your PC manufacturer. Performance will vary depending on the specific hardware and software used. Not available on Intel® Core™ i5-750. For more information including details on which processors support HT Technology, visit http://www.intel.com/info/hyperthreading.

Intel® 64 architecture requires a system with a 64-bit enabled processor, chipset, BIOS and software. Performance will vary depending on the specific hardware and software you use. Consult your PC manufacturer for more information. For more information, visit: http://www.intel.com/info/em64t.

Contents

§ §

Revision History

Revision	Description	Date
001	- Initial Release.	September 2014
002	- Added F-0 Stepping - Errata — Added errata BDM58-66 - Component Marking Information — Updated Table 2 — Updated Table 3	November 2014
003	- Errata — Added errata BDM67-75	December 2014

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
Intel® Core™ M Processor Family Datasheet	330834

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/content/www/us/en/processors/architectures-software-developer-manuals.html
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
	E-0	F-0		
BDM1	X	X	No Fix	LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode
BDM2	X	X	No Fix	EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change
BDM3	X	X	No Fix	MCi_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error
BDM4	X	X	No Fix	LER MSRs May Be Unreliable
BDM5	X	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
BDM6	X	X	No Fix	An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang
BDM7	X	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code

Errata (Sheet 2 of 3)

Number	Steppings		Status	ERRATA
	E-0	F-0		
BDM8	X	X	No Fix	FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM
HSM9	X	X	No Fix	APIC Error “Received Illegal Vector” May be Lost
BDM10	X	X	No Fix	Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations
BDM11	X	X	No Fix	Performance Monitor Precise Instruction Retired Event May Present Wrong Indications
BDM12	X	X	No Fix	CR0.CD Is Ignored in VMX Operation
BDM13	X	X	No Fix	LER MSRs May Be Unreliable
BDM14	X	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
BDM15	X	X	No Fix	Processor May Fail to Acknowledge a TLP Request
BDM16	X	X	No Fix	Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered
BDM17	X	X	No Fix	PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect
BDM18	X	X	No Fix	PCIe* Controller May Incorrectly Log Errors on Transition to RxL0s
BDM19	X	X	No Fix	Unused PCIe* Lanes May Report Correctable Errors
BDM20	X	X	No Fix	PCIe Root Port May Not Initiate Link Speed Change
BDM21	X	X	No Fix	Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected
BDM22	X	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
BDM23	X	X	No Fix	VEX.L is Not Ignored with VCVT*2SI Instructions
BDM24	X	X	No Fix	PCIe* Atomic Transactions From Two or More PCIe Controllers May Cause Starvation
BDM25	X	X	No Fix	The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS is Not Updated After a UC Error is Logged
BDM26	X	X	No Fix	PCIe* Controller May Initiate Speed Change While in DL_Init State Causing Certain PCIe Devices to Fail to Train
BDM27	X	X	No Fix	Spurious VT-d Interrupts May Occur When the PFO Bit is Set
BDM28	X	X	No Fix	Processor May Livelock During On Demand Clock Modulation
BDM29	X	X	No Fix	Internal Parity Errors May Incorrectly Report Overflow in The IA32_MCi_STATUS MSR
BDM30	X	X	No Fix	Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count
BDM31	X	X	No Fix	Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count
BDM32	X	X	No Fix	Timed MWAIT May Use Deadline of a Previous Execution
BDM33	X	X	No Fix	IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding
BDM34	X	X	No Fix	Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed
BDM35	X	X	No Fix	Locked Load Performance Monitoring Events May Under Count
BDM36	X	X	No Fix	Transactional Abort May Produce an Incorrect Branch Record
BDM37	X	X	No Fix	SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior
BDM38	X	X	No Fix	PMI May be Signaled More Than Once For Performance Monitor Counter Overflow
BDM39	X	X	No Fix	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
BDM40	X	X	No Fix	Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on 5th Generation Intel® Core™ i3 U-series, and select Pentium® processors
BDM41	X	X	No Fix	The SAMPLE/PRELOAD JTAG Command Does Not Sample The Display Transmit Signals
BDM42	X	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
BDM43	X	X	No Fix	CHAP Counter Values May be Cleared After Package C7 or Deeper C-State
BDM44	X	X	No Fix	Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID

Errata (Sheet 3 of 3)

Number	Steppings		Status	ERRATA
	E-0	F-0		
BDM45	X	X	No Fix	Back to Back Updates of The VT-d Root Table Pointer May Lead to an Unexpected DMA Remapping Fault
BDM46	X	X	No Fix	A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation
BDM47	X	X	No Fix	Peer IO Device Writes to The GMADR May Lead to a System Hang
BDM48	X	X	No Fix	Spurious Corrected Errors May be Reported
BDM49	X	X	No Fix	Intel® PT Packet Generation May Stop Sooner Than Expected
BDM50	X	X	No Fix	PEBS Eventing IP Field May be Incorrect After Not-Taken Branch
BDM51	X	X	No Fix	Reading The Memory Destination of an Instruction That Begins an HLE Transaction May Return The Original Value
BDM52	X	X	No Fix	Package C7 Entry May Cause Display Artifact
BDM53 [1]	X		Fixed	Intel® TSX Instructions Not Available
BDM54	X	X	No Fix	Spurious Corrected Errors May be Reported
BDM55	X	X	No Fix	Performance Monitoring Event INSTR_RETIRED.ALL May Generate Redundant PEBS Records For an Overflow
BDM56	X	X	No Fix	Concurrent Core And Graphics Operation at Turbo Ratios May Lead to System Hang
BDM57	X	X	No Fix	The System May Hang on First Package C6 or deeper C-State
BDM58	X	X	No Fix	SVM Doorbells Are Not Correctly Preserved Across Package C-States
BDM59	X	X	No Fix	Using The FIVR Spread Spectrum Control Mailbox May Not Produce The Requested Range
BDM60	X	X	No Fix	Intel® Processor Trace (Intel® PT) MODE.Exec, PIP, and CBR Packets Are Not Generated as Expected
BDM61	X	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
BDM62	X	X	No Fix	General-Purpose Performance Counters May be Inaccurate with Any Thread
BDM63	X		Fixed	Glitches on Internal Voltage Planes During Package C9/C10 Exit May Cause a System Hang
BDM64 [1]	X		Fixed	An Invalid LBR May Be Recorded Following a Transactional Abort
BDM65	X	X	No Fix	Executing an RSM Instruction With Intel® Processor Trace Enabled Will Signal a #GP
BDM66	X		Fixed	Intel® Processor Trace PIP May be Unexpectedly Generated
BDM67	X		Fixed	A #VE May Not Invalidate Cached Translation Information
BDM68	X		Fixed	Frequent Entries Into Package C8, C9, or C10 May Cause a Hang
BDM69	X		Fixed	Some Performance Monitor Events May Overcount During TLB Misses
BDM70	X		Fixed	Intel® Processor Trace PSB+ Packets May Contain Unexpected Packets
BDM71	X		Fixed	Writing Non-Zero Value to IA32_RTIT_CR3_MATCH [63:48] Will Cause #GP
BDM72	X		Fixed	Core C6 May Cause Interrupts to be Serviced Out of Order
BDM73	X		Fixed	The Display May Not Resume Correctly After Package C8-C10 Exit
BDM74	X		Fixed	LPDDR3 Memory Training May Cause Platform Boot Failure
BDM75		X	No Fix	Aggressive Ramp Down of Voltage May Result in Unpredictable Behavior

Note:

1. Applies to Intel® Core™ M-5Y70 processor. Intel® TSX is supported on Intel® Core™ M-5Y70 processor with Intel® vPro Technology. Intel® TSX is not supported on other processor SKUs.

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
	None for this revision of this specification update.

Identification Information

Component Identification using Programming Interface

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

Table 1. 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	1101b	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.

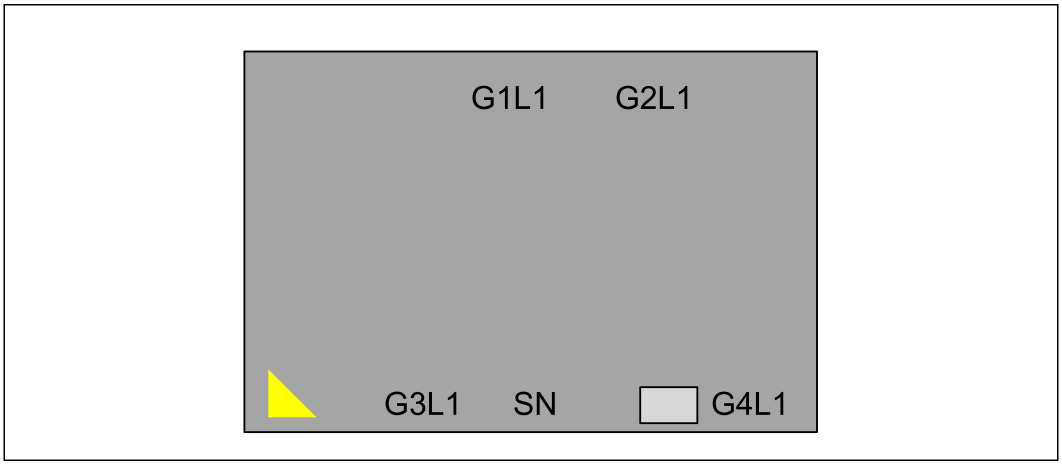
Table 2. Processor Identification by Register Contents

Processor Line	Stepping	Vendor ID	Host Device ID	Processor Graphics Device ID	Revision ID	Compatibility Revision ID
Intel® Core™ M Processor	E-0	8086h	1604h	GT2 = 161Eh	8	8
Intel® Core™ M Processor	F-0	8086h	1604h	GT2 = 161Eh	9	9

Component Marking Information

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

Figure 1. Intel® Core™ M Processor Family Multi-Chip Package BGA Top-Side Markings



Pin Count: 1234 Package Size: 30 mm x 16.5 mm

Production (SSPEC)		**Max Characters/ Line:**
G1L1:	Intel logo	15
G2L1:	{FPO}	15
G3L1:	SSPEC	15
G4L1:	{e1}	15

Table 3. Intel® Core™ M Processor Family Processor Identification

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Frequency Rate (GHz)	Memory (MHz)	Core Frequency (GHz)	Thermal Design Power (W)
R216	5Y70	E-0	4	2	2	2.6	1600	1.1	4.5
R217	5Y10	E-0	4	2	2	2.0	1600	0.8	4.5
R218	5Y10A	E-0	4	2	2	2.0	1600	0.8	4.5
R23Q	5Y71	F-0	4	2	2	2.9	1600	1.2	4.5
R23L	5Y51	F-0	4	2	2	2.6	1600	1.1	4.5
R23G	5Y31	F-0	4	2	2	2.4	1600	0.9	4.5
R23C	5Y10C	F-0	4	2	2	2.0	1600	0.8	4.5

Errata

BDM1. 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*.

BDM2. 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*.

BDM3. 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*.

BDM4. 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*.

BDM5. 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*.

BDM6. 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*.

BDM7. #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*.

BDM8. 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*.

BDM9. 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*.

BDM10. 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*.

BDM11. 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*.

BDM12. 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*.

BDM13. 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*.

BDM14. 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*.

BDM15. 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*.

BDM16. 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*.

BDM17. 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*.

BDM18. 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*.

BDM19. 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*.

BDM20. 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*.

BDM21. 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*.

BDM22. 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*.

BDM23. 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*.

BDM24. 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*.

BDM25. 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*.

BDM26. 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*.

BDM27. 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*.

BDM28. 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*.

BDM29. 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*.

BDM30. 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*.

BDM31. 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.

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

BDM32. Timed MWAIT May Use Deadline of a Previous Execution

Problem: A timed MWAIT instruction specifies a TSC deadline for execution resumption. If a wake event causes execution to resume before the deadline is reached, a subsequent timed MWAIT instruction may incorrectly use the deadline of the previous timed MWAIT when that previous deadline is earlier than the new one.

Implication: A timed MWAIT may end earlier than 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*.

BDM33. IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding

Problem: IA32_VMX_VMCS_ENUM MSR (48AH) bits 9:1 report the highest index value used for any VMCS encoding. Due to this erratum, the value 21 is returned in bits 9:1 although there is a VMCS field whose encoding uses the index value 23.

Implication: Software that uses the value reported in IA32_VMX_VMCS_ENUM[9:1] to read and write all VMCS fields may omit one field.

Workaround: None identified.

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

BDM34. Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed

Problem: During RTM (Restricted Transactional Memory) operation when branch tracing is enabled using BTM (Branch Trace Message) or BTS (Branch Trace Store), the incorrect EIP value (From_IP pointer) may be observed for an RTM abort.

Implication: Due to this erratum, the From_IP pointer may be the same as that of the immediately preceding taken branch.

Workaround: None identified.

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

BDM35. Locked Load Performance Monitoring Events May Under Count

Problem: The performance monitoring events MEM_TRANS_RETIRED.LOAD_LATENCY (Event CDH; Umask 01H), MEM_LOAD_RETIRED.L2_HIT (Event D1H; Umask 02H), and MEM_UOPS_RETIRED.LOCKED (Event DOH; Umask 20H) should count the number of locked loads. Due to this erratum, these events may under count for locked transactions that hit the L2 cache.

Implication: The above event count will under count on locked loads hitting the L2 cache.

Workaround: None identified.

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

BDM36. Transactional Abort May Produce an Incorrect Branch Record

Problem: If an Intel® TSX transactional abort event occurs during a string instruction, the From-IP in the LBR (Last Branch Record) is not correctly reported.

Implication: Due to this erratum, an incorrect From-IP on the LBR stack may be observed.

Workaround: None identified.

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

BDM37. SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior

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

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

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

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

BDM38. PMI May be Signaled More Than Once For Performance Monitor Counter Overflow

Problem: Due to this erratum, PMI (Performance Monitoring Interrupt) may be repeatedly issued until the counter overflow bit is cleared in the overflowing counter.

Implication: Multiple PMIs may be received when a performance monitor counter overflows.

Workaround: None identified. If the PMI is programmed to generate an NMI, software may delay the EOI (end-of- Interrupt) register write for the interrupt until after the overflow indications have been cleared.

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

BDM39. Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception

Problem: Attempt to use FXSAVE or FXRSTOR with a VEX prefix should produce a #UD (Invalid-Opcode) exception. If either the TS or EM flag bits in CR0 are set, a #NM (device-not-available) exception will be raised instead of #UD exception.

Implication: Due to this erratum a #NM exception may be signaled instead of a #UD exception on an FXSAVE or an FXRSTOR with a VEX prefix.

Workaround: Software should not use FXSAVE or FXRSTOR with the VEX prefix.

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

BDM40. Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on 5th Generation Intel® Core™ i3 U-series, and select Pentium® processors

Problem: The 5th Generation Intel Core™ i3 U-series, and select Mobile Intel Pentium processors may incorrectly report support for Intel Turbo Boost Technology via CPUID.06H.EAX bit 1.

Implication: The CPUID instruction may report Turbo Boost Technology as supported even though the processor does not permit operation above the Maximum Non-Turbo Frequency.

Workaround: None identified.

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

BDM41. The SAMPLE/PRELOAD JTAG Command Does Not Sample The Display Transmit Signals

Problem: The Display Transmit signals are not correctly sampled by the SAMPLE/PRELOAD JTAG Command, violating the Boundary Scan specification (IEEE 1149.1).

Implication: The SAMPLE/PRELOAD command cannot be used to sample Display Transmit signals.

Workaround: None identified.

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

BDM42. VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1

Problem: When “XD Bit Disable” in the IA32_MISC_ENABLE MSR (1A0H) bit 34 is set to 1, it should not be possible to enable the “execute disable” feature by setting IA32_EFER.NXE. Due to this erratum, a VM exit that occurs with the 1-setting of the “load IA32_EFER” VM-exit control may set IA32_EFER.NXE even if IA32_MISC_ENABLE bit 34 is set to 1. This erratum can occur only if IA32_MISC_ENABLE bit 34 was set by guest software in VMX non-root operation.

Implication: Software in VMX root operation may execute with the “execute disable” feature enabled despite the fact that the feature should be disabled by the IA32_MISC_ENABLE MSR. Intel has not observed this erratum with any commercially available software.

Workaround: A virtual-machine monitor should not allow guest software to write to the IA32_MISC_ENABLE MSR.

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

BDM43. CHAP Counter Values May be Cleared After Package C7 or Deeper C-State

Problem: The CHAP (Chipset Hardware Architecture Performance) counters which do not have a "Start" OpCode present in the CMD register will not be preserved across a Package C7 or deeper C-State.

Implication: CHAP Counter data is not saved/restored after Package C7 or deeper C-state causing counts to be lost; actions based on those counts may not occur as expected.

Workaround: None identified.

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

BDM44. Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID

Problem: If CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 1 then opcode bytes F3 0F BC should be interpreted as TZCNT otherwise they will be interpreted as REP BSF. Due to this erratum, opcode bytes F3 0F BC may execute as TZCNT even if CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 0.

Implication: Software that expects REP prefix before a BSF instruction to be ignored may not operate correctly since there are cases in which BSF and TZCNT differ with regard to the flags that are set and how the destination operand is established.

Workaround: Software should use the opcode bytes F3 0F BC only if CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 1 and only if the functionality of TZCNT (and not BSF) is desired.

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

BDM45. Back to Back Updates of The VT-d Root Table Pointer May Lead to an Unexpected DMA Remapping Fault

Problem: A VT-d (Intel® Virtualization Technology for Directed I/O) Root Table Pointer update that completes followed by a second Root Table Pointer update that also completes, without performing a global invalidation of either the context-cache or the IOTLB between the two updates, may lead to an unexpected DMA remapping fault.

Implication: Back to back Root Table Pointer updates may cause an unexpected DMA remapping fault. Intel has not observed this erratum with any commercially available software.

Workaround: Software must not perform a second Root Table Pointer update before doing a global invalidation of either the context-cache or the IOTLB.

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

BDM46. A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation

Problem: If EPT (extended page tables) is enabled, a MOV to CR3 or VMFUNC may be followed by an unexpected page fault or the use of an incorrect page translation.

Implication: Guest software may crash or experience unpredictable behavior as a result of 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*.

BDM47. Peer IO Device Writes to The GMADR May Lead to a System Hang

Problem: The system may hang when a peer IO device uses the peer aperture to directly write into the GMADR (Graphics Memory Address range).

Implication: Due to this erratum, the system 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*.

BDM48. Spurious Corrected Errors May be Reported

Problem: Due this erratum, spurious corrected errors may be logged in the IA32_MC0_STATUS register with the valid field (bit 63) set, the uncorrected error field (bit 61) not set, a Model Specific Error Code (bits [31:16]) of 0x000F, and an MCA Error Code (bits [15:0]) of 0x0005. If CMCI is enabled, these spurious corrected errors also signal interrupts.

Implication: When this erratum occurs, software may see corrected errors that are benign. These corrected errors may be safely ignored.

Workaround: None identified.

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

BDM49. Intel® PT Packet Generation May Stop Sooner Than Expected

Problem: Setting the STOP bit (bit 4) in a Table of Physical Addresses entry directs the processor to stop Intel PT (Processor Trace) packet generation when the associated output region is filled. The processor indicates this has occurred by setting the Stopped bit (bit 5) of IA32_RTIT_STATUS MSR (571H). Due to this erratum, packet generation may stop earlier than expected.

Implication: When this erratum occurs, the OutputOffset field (bits [62:32]) of the IA32_RTIT_OUTPUT_MASK_PTRS MSR (561H) holds a value that is less than the size of the output region which triggered the STOP condition; Intel PT analysis software should not attempt to decode packet data bytes beyond the OutputOffset.

Workaround: None identified.

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

BDM50. PEBS Eventing IP Field May be Incorrect After Not-Taken Branch

Problem: When a PEBS (Precise-Event-Based-Sampling) record is logged immediately after a not-taken conditional branch (Jcc instruction), the Eventing IP field should contain the address of the first byte of the Jcc instruction. Due to this erratum, it may instead contain the address of the instruction preceding the Jcc instruction.

Implication: Performance monitoring software using PEBS may incorrectly attribute PEBS events that occur on a Jcc to the preceding instruction.

Workaround: None identified.

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

BDM51. Reading The Memory Destination of an Instruction That Begins an HLE Transaction May Return The Original Value

Problem: An HLE (Hardware Lock Elision) transactional region begins with an instruction with the XACQUIRE prefix. Due to this erratum, reads from within the transactional region of the memory destination of that instruction may return the value that was in memory before the transactional region began.

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

BDM52. Package C7 Entry May Cause Display Artifact

Problem: Due to this erratum, Package C7 entry may exceed published latencies.

Implication: When this erratum occurs, it is possible that isochronous requirements may not be met. Intel has not observed this erratum to affect isochronous elements other than 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*.

BDM53. Intel® TSX Instructions Not Available

Problem: Intel TSX (Transactional Synchronization Extensions) instructions are not supported and not reported by CPUID.

Implication: The Intel TSX feature is not available.

Workaround: None identified.

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

BDM54. Spurious Corrected Errors May be Reported

Problem: Due this erratum, spurious corrected errors may be logged in the MC0_STATUS register with the valid (bit 63) set, the uncorrected error (bit 61) not set, a Model Specific Error Code (bits [31:16]) of 0x000F, and an MCA Error Code (bits [15:0]) of 0x0005. If CMCI is enabled, these spurious corrected errors also signal interrupts.

Implication: When this erratum occurs, software may see corrected errors that are benign. These corrected errors may be safely 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*.

BDM55. Performance Monitoring Event INSTR_RETIRED.ALL May Generate Redundant PEBS Records For an Overflow

Problem: Due to this erratum, the performance monitoring feature PDIR (Precise Distribution of Instructions Retired) for INSTR_RETIRED.ALL (Event C0H; Umask 01H) will generate redundant PEBS (Precise Event Based Sample) records for a counter overflow. This can occur if the lower 6 bits of the performance monitoring counter are not initialized or reset to 0, in the PEBS counter reset field of the DS Buffer Management Area.

Implication: The performance monitor feature PDIR, may generate redundant PEBS records for an overflow.

Workaround: Initialize or reset the counters such that lower 6 bits are 0.

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

BDM56. Concurrent Core And Graphics Operation at Turbo Ratios May Lead to System Hang

Problem: Workloads that attempt concurrent operation of cores and graphics in their respective turbo ranges, under certain conditions may result in a system hang.

Implication: Concurrent core and graphics operation may hang the system.

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*.

BDM57. The System May Hang on First Package C6 or deeper C-State

Problem: Under certain conditions following a cold boot, exiting the first package C6 or deeper C-state may hang the system.

Implication: Due to this erratum, the system may hang exiting a package C6 or deeper C-State.

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*.

BDM58. SVM Doorbells Are Not Correctly Preserved Across Package C-States

Problem: SVM (Shared Virtual Memory) doorbell registers are incorrectly preserved across package C-states (C7 and deeper).

Implication: Due to this erratum, software that uses SVM may experience unreliable behavior from the graphics device.

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*.

BDM59. Using The FIVR Spread Spectrum Control Mailbox May Not Produce The Requested Range

Problem: Values programmed into the FIVR SSC (Fully Integrated Voltage Regulator Spread Spectrum Control) Mailbox may not result in the expected spread spectrum range.

Implication: The actual FIVR spread spectrum range may not be the same as the programmed values affecting the usefulness of FIVR SSC Mailbox as a means to reduce EMI (Electromagnetic Interference).

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

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

BDM60. Intel® Processor Trace (Intel® PT) MODE.Exec, PIP, and CBR Packets Are Not Generated as Expected

Problem: The Intel® PT MODE.Exec (MODE packet – Execution mode leaf), PIP (Paging Information Packet), and CBR (Core:Bus Ratio) packets are generated at the following PSB+ (Packet Stream Boundary) event rather than at the time of the originating event as expected.

Implication: The decoder may not be able to properly disassemble portions of the binary or interpret portions of the trace because many packets may be generated between the MODE.Exec, PIP, and CBR events and the following PSB+ event.

Workaround: The processor inserts these packets as status packets in the PSB+ block. The decoder may have to skip forward to the next PSB+ block in the trace to obtain the proper updated information to continue decoding.

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

BDM61. Performance Monitor Instructions Retired Event May Not Count Consistently

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

Implication: A performance counter counting instructions retired may over count 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 Table of Changes*.

BDM62. General-Purpose Performance Counters May be Inaccurate with Any Thread

Problem: The IA32_PMCx MSR (C1H - C8H) general-purpose performance counters may report inaccurate counts when the associated event selection IA32_PERFEVTSELx MSR's (186H - 18DH) AnyThread field (bit 21) is set and either the OS field (bit 17) or USR field (bit 16) is set (but not both set).

Implication: Due to this erratum, IA32_PMCx counters may be inaccurate.

Workaround: None identified

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

BDM63. Glitches on Internal Voltage Planes During Package C9/C10 Exit May Cause a System Hang

Problem: Internally generated processor voltage planes may exhibit unexpected voltage glitches during a package C9/C10 exit.

Implication: When this erratum occurs, the system may hang. Intel has not observed this erratum with any commercially available system.

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

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

BDM64. An Invalid LBR May Be Recorded Following a Transactional Abort

Problem: Use of Intel® Transactional Synchronization Extensions (Intel® TSX) may result in a transactional abort. If an abort occurs immediately following a branch instruction, an invalid LBR (Last Branch Record) may be recorded before the LBR produced by the abort.

Implication: The invalid LBR may interfere with execution path reconstruction prior to the transactional abort.

Workaround: None identified.

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

BDM65. Executing an RSM Instruction With Intel® Processor Trace Enabled Will Signal a #GP

Problem: Upon delivery of a System Management Interrupt (SMI), the processor saves and then clears TraceEn in the IA32_RTIT_CTL MSR (570H), thus disabling Intel® Processor Trace (Intel® PT). If the SMI handler enables Intel PT and it remains enabled when an RSM instruction is executed, a shutdown event should occur. Due to this erratum, the processor does not shutdown but instead generates a #GP (general-protection exception).

Implication: When this erratum occurs, a #GP will be signaled.

Workaround: If software enables Intel® PT in system-management mode, it should disable Intel® PT before executing RSM.

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

BDM66. Intel® Processor Trace PIP May be Unexpectedly Generated

Problem: When Intel® Processor Trace (Intel® PT) is enabled, PSB+ (Packet Stream Boundary) packets may include a PIP (Paging Information Packet) even though the OS field (bit 2) of IA32_RTIT_CTL MSR (570H) is 0.

Implication: When this erratum occurs, user-mode tracing (indicated by IA32_RTIT_CTL.OS = 0) may include CR3 address information. This may be an undesirable leakage of kernel information.

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

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

BDM67. A #VE May Not Invalidate Cached Translation Information

Problem: An EPT (Extended Page Table) violation that causes a #VE (virtualization exception) may not invalidate the guest-physical mappings that were used to translate the guest-physical address that caused the EPT violation.

Implication: Due to this erratum, the system 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*.

BDM68. Frequent Entries Into Package C8, C9, or C10 May Cause a Hang

Problem: It is possible for the processor to signal a machine check exception when deep packages C-states, C8, C9, or C10, are entered too frequently, typically less than 200us apart. The processor will not be able to process the machine check and will hang.

Implication: Due to this erratum, the processor may signal a machine check exception (IA32_MCi_STATUS.MCCOD = 0x0400) and the processor will hang.

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

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

BDM69. Some Performance Monitor Events May Overcount During TLB Misses

Problem: The following Performance Monitor Events may significantly overcount when multiple TLB misses happen nearly concurrently:

1. EMON_EPT_INTERNAL (sub events 0 through 4)
2. EMON_ITLB_MISSES (sub events 0 through 4)
3. EMON_DTLB_LOAD_MISSES (sub events 0 through 4)
4. EMON_DTLB_PREFETCH_LOAD_MISSES (sub events 0 through 4)
5. EMON_DTLB_STORE_MISSES (sub events 0 through 4)
6. EMON_PDE_CACHE_MISS (sub events 0 through 3)
7. EMON_PAGE_WALKS (sub events 0 through 5)
8. EMON_PAGE_WALKER_LOADS (sub events 0 through 7)

Implication: When this erratum occurs, counts accumulated for the listed events may significantly exceed the correct counts.

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*.

BDM70. Intel® Processor Trace PSB+ Packets May Contain Unexpected Packets

Problem: Some Intel Processor Trace packets should be issued only between TIP.PGE (Target IP Packet.Packet Generation Enable) and TIP.PGD (Target IP Packet.Packet Generation Disable) packets. Due to this erratum, when a TIP.PGE packet is generated it may be preceded by a PSB+ (Packet Stream Boundary) that incorrectly includes FUP (Flow Update Packet) and MODE.Exec packets.

Implication: Due to this erratum, FUP and MODE.Exec may be generated unexpectedly.

Workaround: Decoders should ignore FUP and MODE.Exec packets that are not between TIP.PGE and TIP.PGD packets.

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

BDM71. Writing Non-Zero Value to IA32_RTIT_CR3_MATCH [63:48] Will Cause #GP

Problem: Bits [63:48] of the IA32_RTIT_CR3_MATCH MSR (0572H) are incorrectly treated as reserved and therefore writing non-zero values to them will cause a #GP

Implication: Due to this erratum, a #GP fault will occur if a non-zero value is written to IA32_RTIT_CR3_MATCH[63:48].

Workaround: Software should avoid writing non-zero values to bits [63:48] of the IA32_RTIT_CR3_MATCH MSR.

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

BDM72. Core C6 May Cause Interrupts to be Serviced Out of Order

Problem: If the APIC ISR (In-Service Register) indicates in-progress interrupt(s) at Core C6 entry, a lower priority interrupt pending in the IRR (Interrupt Request Register) may be executed after Core C6 exit, delaying completion of the higher priority interrupt's service routine.

Implication: An interrupt may be processed out of its intended priority order immediately after Core C6 exit.

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

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

BDM73. The Display May Not Resume Correctly After Package C8-C10 Exit

Problem: Display configuration is not properly restored after a package C8-C10 exit.

Implication: The display engine may not function correctly after package C8-C10 exit leading to an incorrect display.

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

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

BDM74. LPDDR3 Memory Training May Cause Platform Boot Failure

Problem: Due to this erratum, LPDDR3 memory sub-systems may not successfully complete training.

Implication: When this erratum occurs, the platform may fail to boot successfully

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

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

BDM75. Aggressive Ramp Down of Voltage May Result in Unpredictable Behavior

Problem: Aggressive ramp down of Vcc voltage may result in insufficient voltage to meet power demand.

Implication: Due to this erratum, unpredictable system behavior or hangs 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*.

§ §

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 access this file: http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html

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

§ §