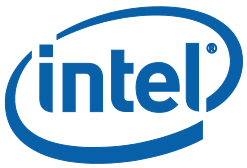


6th Generation Intel® Processor Family

Specification Update

Supporting the Intel® Pentium® Processor Family based on the U-Processor

Supporting the 6th Generation Intel® Core™ Processor Family based on the Y-Processor

September 2015

Version 1.0

Order Number: 332994-001EN

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

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

The products described 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.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

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

Intel® Hyper-Threading Technology (Intel® HT Technology) is available on select Intel® Core™ processors. It requires an Intel® HT Technology enabled system. Consult 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 Intel® 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/content/www/us/en/architecture-and-technology/microarchitecture/intel-64-architecture-general.html.

Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, and 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.

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

For Enhanced Intel SpeedStep® Technology, see the Processor Spec Finder at http://ark.intel.com/ or contact your Intel representative for more information.

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security.

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 https://www-ssl.intel.com/content/www/us/en/architecture-and-technology/turbo-boost/turbo-boost-technology.html.

Intel® Advanced Vector Extensions (Intel® AVX) are designed to achieve higher throughput to certain integer and floating point operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you should consult your system manufacturer for more information. Intel® Advanced Vector Extensions refers to Intel® AVX, Intel® AVX2 or Intel® AVX-512. For more information on Intel® Turbo Boost Technology 2.0, visit https://www-ssl.intel.com/content/www/us/en/architecture-and-technology/turbo-boost/turbo-boost-technology.html

Intel, 6th Generation Intel® Core™ processor, Intel® Xeon® processor, Intel® Pentium® processor, Intel® Celeron® processor, Intel386™, Intel486™, Intel® Processor Trace (Intel® PT), Intel® Virtualization Technology (Intel® VT), Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel Architecture (Intel® VT-x), Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d), Intel® Trusted Execution Technology (Intel® TXT), Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), Intel® Secure Key, Boot Guard, Intel® Memory Protection Extensions (Intel® MPX), Intel® Software Guard Extensions (Intel® SGX), Intel® Hyper-Threading Technology (Intel® HT Technology), Intel® Turbo Boost Technology, Intel® Advanced Vector Extensions 2 (Intel® AVX2), and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2015, Intel Corporation. All rights reserved

Contents

Revision History

Revision	Version	Description	Date
001	1.0	Initial release	September 2015

§

Preface

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

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

Affected Documents

Document Title	Document Number/Location
6th Generation Intel® Processor Datasheet for U/Y Platforms, Volume 1 of 2	332990-001EN
6th Generation Intel® Processor Datasheet for U/Y Platforms, Volume 2 of 2	332991-001EN

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/architec-tures-software-developer-manuals.html
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	D51397-001

Document Title	Document Number/Location
ACPI Specifications	www.acpi.info

Nomenclature

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

QDF Number – A several digit code used to distinguish between engineering samples. These processors are used for qualification and early design validation. The functionality of these parts can range from mechanical only to fully functional. The NDA specification update has a processor identification information table that lists these QDF numbers and the corresponding product sample details.

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

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 the next release of the specifications.

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

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, etc.).

§

Summary Tables of Changes

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

Codes Used in Summary Table

Stepping

X:	Erratum, Specification Change or Clarification that applies to this stepping.
(No mark) or (Blank Box):	This erratum is fixed in listed stepping or specification change does not apply to listed stepping.

Status

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

Row

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

Table 1. Errata Summary Table

Number		Status	Title
SKD001		No Fix	Reported Memory Type May Not Be Used to Access the VMCS and Referenced Data Structures
SKD002		No Fix	Instruction Fetch May Cause Machine Check if Page Size and Memory Type Was Changed Without Invalidation
SKD003		No Fix	Execution of VAESIMC or VAESKEYGENASSIST With An Illegal Value for VEX.vvvv May Produce a #NM Exception
SKD004		No Fix	The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS is Not Updated When The UC Bit is Set
SKD005		No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
SKD006		No Fix	SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior
SKD007		No Fix	x87 FPU Exception (#MF) May be Signaled Earlier Than Expected
SKD008		No Fix	Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed
SKD009		No Fix	DR6 Register May Contain an Incorrect Value When a MOV to SS or POP SS Instruction is Followed by an XBEGIN Instruction
SKD010		No Fix	Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID
SKD011		No Fix	PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect
SKD012		No Fix	SMSW Instruction Does Not #UD When Executed Within an Enclave
SKD013		No Fix	PEBS Record After a WRMSR to IA32_BIOS_UPDT_TRIG May be Incorrect
SKD014		No Fix	Intel® PT TIP.PGD May Not Have Target IP Payload
SKD015		No Fix	Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause a #UD
SKD016		No Fix	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
SKD017		No Fix	WRMSR May Not Clear The Sticky Count Overflow Bit in The IA32_MCi_STATUS MSRs' Corrected Error Count Field
SKD018		No Fix	PEBS Eventing IP Field May be Incorrect After Not-Taken Branch
SKD019		No Fix	Debug Exceptions May Be Lost or Misreported Following WRMSR to IA32_BIOS_UPDT_TRIG
SKD020		No Fix	Attempts to Retrain a PCIe* Link May be Ignored
SKD021		No Fix	Intel® Processor Trace PSB+ Packets May Contain Unexpected Packets
SKD022		No Fix	An APIC Timer Interrupt During Core C6 Entry May be Lost

SKD023		No Fix	Placing an Intel® PT ToPA in Non-WB Memory or Writing It Within a Transactional Region May Lead to System Instability
SKD024		No Fix	VM Entry That Clears TraceEn May Generate a FUP
SKD025		No Fix	EDRAM Corrected Error Events May Not be Properly Logged After a Warm Reset
SKD026		No Fix	Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May be Incorrect
SKD027		No Fix	Machine Check or Shutdown May Occur When Using The PECI RdIAMSR Command
SKD028		No Fix	ENCLU[EGETKEY] Ignores KEYREQUEST.MISCMASK
SKD029		No Fix	POPCNT Instruction May Take Longer to Execute Than Expected
SKD030		No Fix	ENCLU[EREPORT] May Cause a #GP When TARGETINFO.MISCSELECT is Non-Zero
SKD031		No Fix	A VMX Transition Attempting to Load a Non-Existent MSR May Result in a Shutdown
SKD032		No Fix	Transitions Out of 64-bit Mode May Lead to an Incorrect FDP And FIP
SKD033		No Fix	Intel® PT FUP May be Dropped After OVF
SKD034		No Fix	ENCLS[ECREATE] Causes #GP if Enclave Base Address is Not Canonical
SKD035		No Fix	Title: Data Breakpoint May Not be Detected on a REP MOVS
SKD036		No Fix	A Spurious APIC Timer Interrupt May Occur After Timed MWAIT
SKD037		No Fix	PCIe* and DMI Links With Lane Polarity Inversion May Result in Link Failure
SKD038		No Fix	PCIe* Expansion ROM Base Address Register May be Incorrect
SKD039		No Fix	PCIe* Perform Equalization May Lead to Link Failure
SKD040		No Fix	Two DIMMs Per Channel 2133 MHz DDR4 SODIMM Daisy-Chain Systems With Different Vendors May Hang
SKD041		No Fix	ENCLS[EINIT] Instruction May Unexpectedly #GP
SKD042		No Fix	Intel® PT OVF Packet May be Lost if Immediately Preceding a TraceStop
SKD043		No Fix	Detecting an Intel® PT Stopped or Error Condition Within an Intel® TSX Region May Result in a System Hang
SKD044		No Fix	WRMSR to IA32_BIOS_UPDT_TRIG May be Counted as Multiple Instructions
SKD045		No Fix	The x87 FIP May be Incorrect
SKD046		No Fix	Branch Instructions May Initialize MPX Bound Registers Incorrectly
SKD047		No Fix	Writing a Non-Canonical Value to an LBR MSR Does Not Signal a #GP When Intel® PT is Enabled
SKD048		No Fix	Processor May Run Intel® AVX Code Much Slower Than Expected
SKD049		No Fix	Intel® PT Buffer Overflow May Result in Incorrect Packets
SKD050		No Fix	Intel® PT PSB+ Packets May be Omitted on a C6 Transition

SKD051		No Fix	IA32_PERF_GLOBAL_STATUS.TRACE_TOPA_PMI Bit Cannot be Set by Software
SKD052 [1]		No Fix	CPUID Incorrectly Reports Bit Manipulation Instructions Support
SKD053 [2]		No Fix	Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on Intel® Core™ i3 U/H/S, Select Intel® Mobile Pentium®, Intel® Mobile Celeron®, Select Intel® Pentium® G4xxx and Intel® Celeron® G3xxx Processors

Note:

1. Affects 6th Generation Intel® Pentium® processor family and Intel® Celeron® processor family.
2. Affects 6th Generation Intel® Core™ i3 U/H/S, Intel® Pentium®, Intel® Celeron®, Intel® Pentium® G4xxx and Intel® Celeron® G3xxx Processors.

§

Identification Information

Component Identification via Programming Interface

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

Table 2. 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
	0000000b	0100b		00b	0110b	1110b	xxxxb

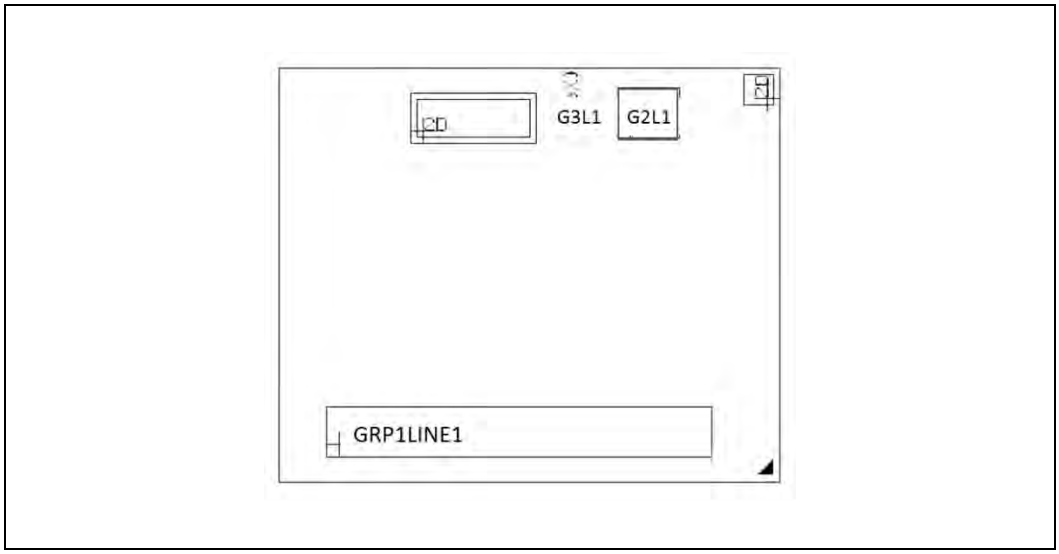
Notes:

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 Table 1 for the processor stepping ID number in the CPUID information.
6. 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.

Component Marking Information

Figure 1. Y-Processor Line BGA Top-Side Markings



Pin Count: 1515 Package Size: 20 mm x 16.5 mm

Sample (QDF):

GRP1LINE1: FPOxxxxxQxxx
GRP2LINE1 (G2L1): Intel logo
GRP3LINE1 (G3L1): {eX}

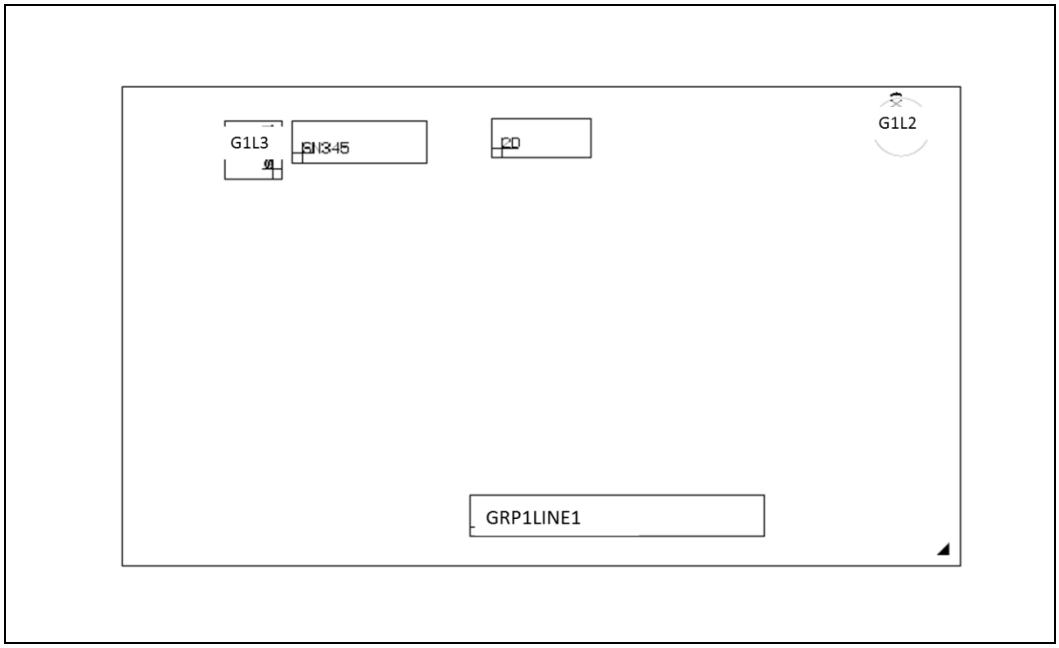
Production (SSPEC):

GRP1LINE1: FPOxxxxxSSPEC
GRP2LINE1 (G2L1): Intel logo
GRP3LINE1 (G3L1): {eX}

Table 3. Y-Processor Line

S-Spec #	Processor Number	Step-ping	Cache Size (MB)	Func-tional Core	Processor Graphics Cores	Processor Graphics Freq. (MHz)	Processor Graphics Turbo Freq. (GHz)	DDR3L Mem. (MHz)	LPDDR3 Mem. (MHz)	Core Freq. (GHz)	Turbo 1 Core Freq. Rate (GHz)	Thermal Design Power (W)	Slot / Socket Type
SR2ER	Pentium 4405Y	D-1	2	2	2	300	800	1600	1866	1500	1500	6	BGA1515
SR2EN	m3-6Y30	D-1	4	2	2	300	850	1600	1866	900	2200	4.5	BGA1515
SR2EM	m5-6Y54	D-1	4	2	2	300	900	1600	1866	1100	2700	4.5	BGA1515
SR2EH	m7-6Y75	D-1	4	2	2	300	1000	1600	1866	1200	3100	4.5	BGA1515
SR2EG	m5-6Y57	D-1	4	2	2	300	900	1600	1866	1100	2800	4.5	BGA1515

Figure 2. U-Processor Line BGA Top-Side Markings



Pin Count: 1356 Package Size: 42 mm x 24 mm

Sample (SSPEC):

GRP1LINE1: FPOxxxxxQxxx
GRP2LINE1 (G2L1): {eX}
GRP3LINE1 (G3L1): Intel logo

Table 4. U-Processor Line

S-Spec #	Processor Number	Step-ping	Cache Size (MB)	Func-tional Core	Processor Graphics Cores	Processor Graphics Freq. (MHz)	Processor Graphics Turbo Freq. (GHz)	DDR3L Mem. (MHz)	DDR4 Mem. (MHz)	LPDDR3 Mem. (MHz)	Core Freq. (GHz)	Turbo 1 Core Freq. Rate (GHz)	Thermal Design Power (W)	Slot / Socket Type
SR2F0	i5-6300U	D-1	3	2	2	300	1000	1600	2133	1866	2400	3000	15	BGA1356
SR2F1	i7-6600U	D-1	4	2	2	300	1050	1600	2133	1866	2600	3400	15	BGA1356
SR2EY	i5-6200U	D-1	3	2	2	300	1000	1600	2133	1866	2300	2800	15	BGA1356
SR2EZ	i7-6500U	D-1	4	2	2	300	1050	1600	2133	1866	2500	3100	15	BGA1356
SR2EX	Pentium 4405U	D-1	2	2	1	300	950	1600	2133	1866	2100	2100	15	BGA1356
SR2EV	Celeron 3855U	D-1	2	2	1	300	900	1600	2133	1866	1600	1600	15	BGA1356
SR2EW	Celeron 3955U	D-1	2	2	1	300	900	1600	2133	1866	2000	2000	15	BGA1356
SR2EU	i3-6100U	D-1	3	2	2	300	1000	1600	2133	1866	2300	2300	15	BGA1356

§

Errata

SKD001	**Reported Memory Type May Not Be Used to Access the VMCS and Referenced Data Structures**
Problem	Bits 53:50 of the IA32_VMX_BASIC MSR report the memory type that the processor uses to access the VMCS and data structures referenced by pointers in the VMCS. Due to this erratum, a VMX access to the VMCS or referenced data structures will instead use the memory type that the MTRRs (memory-type range registers) specify for the physical address of the access.
Implication	Bits 53:50 of the IA32_VMX_BASIC MSR report that the WB (write-back) memory type will be used but the processor may use a different memory type.
Workaround	Software should ensure that the VMCS and referenced data structures are located at physical addresses that are mapped to WB memory type by the MTRRs.
Status	For the steppings affected, see the Summary Table of Changes.

SKD002	**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.

SKD003	**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.

SKD004	**The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS is Not Updated When The UC Bit is Set**
Problem	After a UC (uncorrected) error is logged in the IA32_MC0_STATUS MSR (401H), corrected errors will continue to be counted in 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 when the UC bit (bit 61) is set to 1.
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.

SKD005	**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.

SKD006	**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.

SKD007	x87 FPU Exception (#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 executing when an Enhanced Intel SpeedStep® Technology transitions, an Intel® Turbo Boost Technology transitions, or a Thermal Monitor events occurs, the #MF may be taken 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.

SKD008	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.

SKD009	DR6 Register May Contain an Incorrect Value When a MOV to SS or POP SS Instruction is Followed by an XBEGIN Instruction
Problem	If XBEGIN is executed immediately after an execution of MOV to SS or POP SS, a transactional abort occurs and the logical processor restarts execution from the fallback instruction address. If execution of the instruction at that address causes a debug exception, bits [3:0] of the DR6 register may contain an incorrect value.
Implication	When the instruction at the fallback instruction address causes a debug exception, DR6 may report a breakpoint that was not triggered by that instruction, or it may fail to report a breakpoint that was triggered by the instruction.
Workaround	Avoid following a MOV SS or POP SS instruction immediately with an XBEGIN instruction.
Status	For the steppings affected, see the Summary Table of Changes.

SKD010	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.

SKD011	**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.

SKD012	**SMSW Instruction Does Not #UD When Executed Within an Enclave**
Problem	Attempting to execute the SMSW instruction within an SGX (Software Guard Extensions) enclave does not, as expected, result in a #UD exception.
Implication	The SMSW instruction may be executed within an enclave.
Workaround	None identified. Software should not execute SMSW within an enclave
Status	For the steppings affected, see the Summary Table of Changes.

SKD013	**PEBS Record After a WRMSR to IA32_BIOS_UPDT_TRIG May be Incorrect**
Problem	A PEBS record generated by a WRMSR to IA32_BIOS_UPDT_TRIG MSR (79H) may have an incorrect value in the Eventing EIP field if an instruction prefix was used on the WRMSR.
Implication	The Eventing EIP field of the generated PEBS record may be incorrect. Intel has not observed this erratum with any commercially available software.
Workaround	Instruction prefixes have no architecturally-defined function for the WRMSR instruction; instruction prefixes should not be used with the WRMSR instruction.
Status	For the steppings affected, see the Summary Table of Changes.

SKD014	**Intel® PT TIP.PGD May Not Have Target IP Payload**
Problem	When Intel PT (Intel Processor Trace) is enabled and a direct unconditional branch clears IA32_RTIT_STATUS.FilterEn (MSR 571H, bit 0), due to this erratum, the resulting TIP.PGD (Target IP Packet, Packet Generation Disable) may not have an IP payload with the target IP.
Implication	It may not be possible to tell which instruction in the flow caused the TIP.PGD using only the information in trace packets when this erratum occurs.
Workaround	The Intel PT trace decoder can compare direct unconditional branch targets in the source with the FilterEn address range(s) to determine which branch cleared FilterEn.
Status	For the steppings affected, see the Summary Table of Changes.

SKD015	Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause a #UD
Problem	Execution of a 64 bit operand MOVBE instruction with an operand-size override instruction prefix (66H) may incorrectly cause an invalid-opcode exception (#UD).
Implication	A MOVBE instruction with both REX.W=1 and a 66H prefix will unexpectedly cause an #UD (invalid-opcode exception). Intel has not observed this erratum with any commercially available software.
Workaround	Do not use a 66H instruction prefix with a 64-bit operand MOVBE instruction.
Status	For the steppings affected, see the Summary Table of Changes.

SKD016	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.

SKD017	WRMSR May Not Clear The Sticky Count Overflow Bit in The IA32_MCi_STATUS MSRs' Corrected Error Count Field
Problem	The sticky count overflow bit is the most significant bit (bit 52) of the Corrected Error Count Field (bits[52:38]) in IA32_MCi_STATUS MSRs. Once set, the sticky count overflow bit may not be cleared by a WRMSR instruction. When this occurs, that bit can only be cleared by power-on reset.
Implication	Software that uses the Corrected Error Count field and expects to be able to clear the sticky count overflow bit may misinterpret the number of corrected errors when the sticky count overflow bit is set. This erratum does not affect threshold-based CMCI (Corrected Machine Check Error Interrupt) signaling.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

SKD018	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.

SKD019	Debug Exceptions May Be Lost or Misreported Following WRMSR to IA32_BIOS_UPDT_TRIG
Problem	If the WRMSR instruction writes to the IA32_BIOS_UPDT_TRIG MSR (79H) immediately after an execution of MOV SS or POP SS that generated a debug exception, the processor may fail to deliver the debug exception or, if it does, the DR6 register contents may not correctly reflect the causes of the debug exception.
Implication	Debugging software may fail to operate properly if a debug exception is lost or does not report complete information.
Workaround	Software should avoid using WRMSR instruction immediately after executing MOV SS or POP SS
Status	For the steppings affected, see the Summary Table of Changes.

SKD020	Attempts to Retrain a PCIe* Link May be Ignored
Problem	A PCIe link should retrain when Retrain Link (bit 5) in the Link Control register (Bus 0; Device 1; Functions 0,1,2; Offset 0xB0) is set. Due to this erratum, if the link is in the L1 state, it may ignore the retrain request.
Implication	The PCIe link 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.

SKD021	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.

SKD022	An APIC Timer Interrupt During Core C6 Entry May be Lost
Problem	Due to this erratum, an APIC timer interrupt coincident with the core entering C6 state may be lost rather than held for servicing later.
Implication	A lost APIC timer interrupt may lead to missed deadlines or a system 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.

SKD023	Placing an Intel® PT ToPA in Non-WB Memory or Writing It Within a Transactional Region May Lead to System Instability
Problem	If an Intel PT (Intel® Processor Trace) ToPA (Table of Physical Addresses) is not placed in WB (writeback) memory or is written by software executing within an Intel® TSX (Intel® Transactional Synchronization Extension) transactional region, the system may become unstable.
Implication	Unusual treatment of the ToPA may lead to system instability.
Workaround	None identified. Intel PT ToPA should reside in WB memory and should not be written within a Transactional Region.
Status	For the steppings affected, see the Summary Table of Changes.

SKD024	VM Entry That Clears TraceEn May Generate a FUP
Problem	If VM entry clears Intel® PT (Intel Processor Trace) IA32_RTIT_CTL.TraceEn (MSR 570H, bit 0) while PacketEn is 1 then a FUP (Flow Update Packet) will precede the TIP.PGD (Target IP Packet, Packet Generation Disable). VM entry can clear TraceEn if the VM-entry MSR-load area includes an entry for the IA32_RTIT_CTL MSR.
Implication	When this erratum occurs, an unexpected FUP may be generated that creates the appearance of an asynchronous event taking place immediately before or during the VM entry.
Workaround	The Intel PT trace decoder may opt to ignore any FUP whose IP matches that of a VM entry instruction.
Status	For the steppings affected, see the Summary Table of Changes.

SKD025	EDRAM Corrected Error Events May Not be Properly Logged After a Warm Reset
Problem	After a warm reset, an EDRAM corrected error may not be logged correctly until the associated machine check register is initialized. This erratum may affect IA32_MC8_STATUS or IA32_MC10_STATUS.
Implication	The EDRAM corrected error information may be lost when this erratum occurs.
Workaround	Data from the affected machine check registers should be read and the registers initialized as soon as practical after a warm reset.
Status	For the steppings affected, see the Summary Table of Changes.

SKD026	Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May be Incorrect
Problem	The performance monitor event OFFCORE_REQUESTS_OUTSTANDING (Event 60H, any Umask Value) should count the number of offcore outstanding transactions each cycle. Due to this erratum, the counts may be higher or lower than expected.
Implication	The performance monitor event OFFCORE_REQUESTS_OUTSTANDING may reflect an incorrect count.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

SKD027	Machine Check or Shutdown May Occur When Using The PECI RdIAMSR Command
Problem	Under certain circumstances, reading a core Machine Check register using the PECI (Platform Environmental Control Interface) RdIAMSR command may result in a Machine Check or Shutdown.
Implication	Machine Check or Shutdown 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.

SKD028	ENCLU[EGETKEY] Ignores KEYREQUEST.MISCMASK
Problem	The Intel® SGX (Software Guard Extensions) ENCLU[EGETKEY] instruction ignores the MISCMASK field in KEYREQUEST structure when computing a provisioning key, a provisioning seal key, or a seal key.
Implication	ENCLU[EGETKEY] will return the same key in response to two requests that differ only in the value of KEYREQUEST.MISCMASK. Intel has not observed this erratum with any commercially available software.
Workaround	When executing the ENCLU[EGETKEY] instruction, software should ensure the bits set in KEYREQUEST.MISCMASK are a subset of the bits set in the current SECS's MISCSELECT field.
Status	For the steppings affected, see the Summary Table of Changes.

SKD029	POPCNT Instruction May Take Longer to Execute Than Expected
Problem	POPCNT instruction execution with a 32 or 64 bit operand may be delayed until previous non-dependent instructions have executed.
Implication	Software using the POPCNT instruction may experience lower performance than expected.
Workaround	None identified
Status	For the steppings affected, see the Summary Table of Changes.

SKD030	ENCLU[EREPORT] May Cause a #GP When TARGETINFO.MISCSELECT is Non-Zero
Problem	The Intel® SGX (Software Guard extensions) ENCLU[EREPORT] instruction may cause a #GP (general protection fault) if any bit is set in TARGETINFO structure's MISCSELECT field.
Implication	This erratum may cause unexpected general-protection exceptions inside enclaves.
Workaround	When executing the ENCLU[EREPORT] instruction, software should ensure the bits set in TARGETINFO.MISCSELECT are a subset of the bits set in the current SECS's MISCSELECT field.
Status	For the steppings affected, see the Summary Table of Changes.

SKD031	A VMX Transition Attempting to Load a Non-Existent MSR May Result in a Shutdown
Problem	A VMX transition may result in a shutdown (without generating a machine-check event) if a non-existent MSR is included in the associated MSR-load area. When such a shutdown occurs, a machine check error will be logged with IA32_MCi_STATUS.MCACOD (bits [15:0]) of 406H, but the processor does not issue the special shutdown cycle. A hardware reset must be used to restart the processor.
Implication	Due to this erratum, the hypervisor may experience an unexpected shutdown.
Workaround	Software should not configure VMX transitions to load non-existent MSRs.
Status	For the steppings affected, see the Summary Table of Changes.

SKD032	Transitions Out of 64-bit Mode May Lead to an Incorrect FDP And FIP
Problem	A transition from 64-bit mode to compatibility or legacy modes may result in cause a subsequent x87 FPU state save to zeroing bits [63:32] of the FDP (x87 FPU Data Pointer Offset) and the FIP (x87 FPU Instruction Pointer Offset).
Implication	Leaving 64-bit mode may result in incorrect FDP and FIP values when x87 FPU state is saved.
Workaround	None identified. 64-bit software should save x87 FPU state before leaving 64-bit mode if it needs to access the FDP and/or FIP values.
Status	For the steppings affected, see the Summary Table of Changes.

SKD033	Intel® PT FUP May be Dropped After OVF
Problem	Some Intel PT (Intel Processor Trace) OVF (Overflow) packets may not be followed by a FUP (Flow Update Packet) or TIP.PGE (Target IP Packet, Packet Generation Enable).
Implication	When this erratum occurs, an unexpected packet sequence is generated.
Workaround	When it encounters an OVF without a following FUP or TIP.PGE, the Intel PT trace decoder should scan for the next TIP, TIP.PGE, or PSB+ to resume operation.
Status	For the steppings affected, see the Summary Table of Changes.

SKD034	ENCLS[ECREATE] Causes #GP if Enclave Base Address is Not Canonical
Problem	The ENCLS[ECREATE] instruction uses an SECS (SGX enclave control structure) referenced by the SRCPAGE pointer in the PAGEINFO structure, which is referenced by the RBX register. Due to this erratum, the instruction causes a #GP (general-protection fault) if the SECS attributes indicate that the enclave should operate in 64-bit mode and the enclave base linear address in the SECS is not canonical.
Implication	System software will incur a general-protection fault if it mistakenly programs the SECS with a non-canonical address. Intel has not observed this erratum with any commercially available software.
Workaround	System software should always specify a canonical address as the base address of the 64-bit mode enclave.
Status	For the steppings affected, see the Summary Table of Changes.

SKD035	Title: Data Breakpoint May Not be Detected on a REP MOVS
Problem	A REP MOVS instruction that causes an exception or a VM exit may not detect a data breakpoint that occurred on an earlier memory access of that REP MOVS instruction.
Implication	A debugger may miss a data read/write access if it is done by a REP MOVS instruction.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.Problem: If a data breakpoint is set and supposed to be triggered by a REP MOVS instruction then, due to this erratum, the breakpoint match may be ignored if it happens in the vicinity of another fault that the REP MOVS instruction produces, such as #PF or #GP.Implication: Missing data breakpoints.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.

SKD036	Processor Graphics IOMMU Unit May Report Spurious Faults
Problem	The IOMMU unit for Processor Graphics pre-fetches context (or extended-context) entries to improve performance. Due to the erratum, the IOMMU unit may report spurious DMA remapping faults if prefetching encounters a context (or extended-context) entry which is not marked present.
Implication	Software may observe spurious DMA remapping faults when the present bit for the context (or extended-context) entry corresponding to the Processor Graphics device (Bus: 0; Device: 2; Function: 0) is cleared. These faults may be reported when the Processor Graphics device is quiescent.
Workaround	None identified. Instead of marking a context not present, software should mark the context (or extended-context) entry present while using the page table to indicate all the memory pages referenced by the context entry is not present.
Status	For the steppings affected, see the Summary Table of Changes.

SKD037	PCIe* and DMI Links With Lane Polarity Inversion May Result in Link Failure
Problem	The processor's PCIe and DMI links may fail after exiting Package C7 or deeper if the platform requires the link to utilize lane polarity inversion.
Implication	Due to this erratum, the processor cannot support lane polarity inversion on the PCIe or DMI links when Package C7 or deeper is enabled.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

SKD038	PCIe* Expansion ROM Base Address Register May be Incorrect
Problem	After PCIe 8.0 GT/s Link Equalization on a root port (Bus 0; Device 1; Function 0, 1, 2) has completed, the Expansion ROM Base Address Register (Offset 38H) may be incorrect.
Implication	Software that uses this BAR may behave unexpectedly. Intel has not observed this erratum with any commercially available software.
Workaround	It is possible for the BIOS to contain a partial workaround for this erratum. Software should wait at least 5ms following link equalization before accessing these Expansion ROM Base Address Register.

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

SKD039	**PCIe* Perform Equalization May Lead to Link Failure**
Problem	Due to this erratum, when a processor PCIe port operating at 8.0 GT/s is directed to redo equalization, either via software or from the link partner, incorrect coefficients may be conveyed during Equalization Phase 3.
Implication	If the link partner accepts the incorrect coefficients, the link may become unstable. Note this affects 8.0 GT/s only.
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.

SKD040	**Two DIMMs Per Channel 2133 MHz DDR4 SODIMM Daisy-Chain Systems With Different Vendors May Hang**
Problem	When, on a single memory channel with 2133 MHz DDR4 SODIMMs, mixing different vendors or mixing single rank and dual rank DIMMs, may lead to a higher rate of correctable errors or system hangs.
Implication	Due to this erratum, reported correctable error counts may increase or system may hang. 1
Workaround	Use a single vendor for and do not mix single rank and dual rank 2133 MHz DDR4 SODIMM.
Status	For the steppings affected, see the Summary Table of Changes.

SKD041	**ENCLS[EINIT] Instruction May Unexpectedly #GP**
Problem	When using Intel® SGX (Software Guard Extensions), the ENCLS[EINIT] instruction will incorrectly cause a #GP (general protection fault) if the MISCSELECT field of the SIGSTRUCT structure is not zero.
Implication	This erratum may cause an unexpected #GP, but only if software has set bits in the MISCSELECT field in SIGSTRUCT structure that do not correspond to extended features that can be written to the MISC region of the SSA (State Save Area). Intel has not observed this erratum with any commercially available software.
Workaround	When executing the ENCLS[EINIT] instruction, software should only set bits in the MISCSELECT field in the SIGSTRUCT structure that are enumerated as 1 by CPUID.(EAX=12H,ECX=0):EBX (the bit vector of extended features that can be written to the MISC region of the SSA).
Status	For the steppings affected, see the Summary Table of Changes.

SKD042	**Intel® PT OVF Packet May be Lost if Immediately Preceding a TraceStop**
Problem	If an Intel PT (Intel® Processor Trace) internal buffer overflow occurs immediately before software executes a taken branch or event that enters an Intel PT TraceStop region, the OVF (Overflow) packet may be lost.
Implication	The trace decoder will not see the OVF packet, nor any subsequent packets (e.g., TraceStop) that were lost due to overflow.
Workaround	None identified.

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

SKD043	**Detecting an Intel® PT Stopped or Error Condition Within an Intel® TSX Region May Result in a System Hang**
Problem	While executing within an Intel TSX (Intel® Transactional Synchronization Extensions) transactional region with Intel PT (Intel® Processor Trace) enabled and an event occurs that causes either the Error bit (bit 4) or Stopped bit (bit 5) in the IA32_RTIT_STATUS MSR (0571H) to be set then, due to this erratum, the system may hang.
Implication	A system hang may occur when Intel PT and Intel TSX are used together.
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.

SKD044	**WRMSR to IA32_BIOS_UPDT_TRIG May be Counted as Multiple Instructions**
Problem	When software loads a microcode update by writing to MSR IA32_BIOS_UPDT_TRIG (79H) on multiple logical processors in parallel, a logical processor may, due to this erratum, count the WRMSR instruction as multiple instruction-retired events.
Implication	Performance monitoring with the instruction-retired event may over count by up to four extra events per instance of WRMSR which targets the IA32_BIOS_UPDT_TRIG register.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

SKD045	**The x87 FIP May be Incorrect**
Problem	The x87 FPU should update the x87 FIP (FPU instruction pointer) for every non-control x87 instruction executed. Due to this erratum, the FIP is valid only if the last non-control FP instruction had an unmasked exception.
Implication	When this erratum occurs, an instruction that saves FIP (e.g., FSTENV) may save an incorrect value. Software that depends on the FIP value for x87 non-control instructions without unmasked exceptions may not operate 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.

SKD046	**Branch Instructions May Initialize MPX Bound Registers Incorrectly**
Problem	Depending on the current Intel® MPX (Memory Protection Extensions) configuration, execution of certain branch instructions (near CALL, near RET, near JMP, and Jcc instructions) without a BND prefix (F2H) initialize the MPX bound registers. Due to this erratum, such a branch instruction that is executed both with CPL = 3 and with CPL < 3 may not use the correct MPX configuration register (BNDCFGU or BNDCFGS, respectively) for determining whether to initialize the bound registers; it may thus initialize the bound registers when it should not, or fail to initialize them when it should.

Implication	A branch instruction that has executed both in user mode and in supervisor mode (from the same linear address) may cause a #BR (bound range fault) when it should not have or may not cause a #BR when it should have.
Workaround	An operating system can avoid this erratum by setting CR4.SMEP[bit 20] to enable supervisor-mode execution prevention (SMEP). When SMEP is enabled, no code can be executed both with CPL = 3 and with CPL < 3.
Status	For the steppings affected, see the Summary Table of Changes.

SKD047	**Writing a Non-Canonical Value to an LBR MSR Does Not Signal a #GP When Intel® PT is Enabled**
Problem	If Intel PT (Intel Processor Trace) is enabled, WRMSR will not cause a general-protection exception (#GP) on an attempt to write a non-canonical value to any of the following MSRs: • MSR_LASTBRANCH_{0 - 31}_FROM_IP (680H – 69FH) • MSR_LASTBRANCH__{0 - 31}_TO_IP (6C0H – 6DFH) • MSR_LASTBRANCH_FROM_IP (1DBH) • MSR_LASTBRANCH_TO_IP (1DCH) • MSR_LASTINT_FROM_IP (1DDH) • MSR_LASTINT_TO_IP (1DEH)Instead the same behavior will occur as if a canonical value had been written. Specifically, the WRMSR will be dropped and the MSR value will not be changed.
Implication	Due to this erratum, an expected #GP may not be signaled.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

SKD048	**Processor May Run Intel® AVX Code Much Slower Than Expected**
Problem	After a C6 state exit, the execution rate of AVX instructions may be reduced.
Implication	Applications using AVX instructions may run slower than expected.
Workaround	It is possible for the BIOS to contain a workaround
Status	For the steppings affected, see the Summary Table of Changes.

SKD049	**Intel® PT Buffer Overflow May Result in Incorrect Packets**
Problem	Under complex micro-architectural conditions, an Intel PT (Processor Trace) OVF (Overflow) packet may be issued after the first byte of a multi-byte CYC (Cycle Count) packet, instead of any remaining bytes of the CYC.
Implication	When this erratum occurs, the splicing of the CYC and OVF packets may prevent the Intel PT decoder from recognizing the overflow. The Intel PT decoder may then encounter subsequent packets that are not consistent with expected behavior.
Workaround	None Identified. The decoder may be able to recognize that this erratum has occurred when a two-byte CYC packet is followed by a single byte CYC, where the latter 2 bytes are 0xf302, and where the CYC packets are followed by a FUP (Flow Update Packet) and a PSB+ (Packet Stream Boundary+). It should then treat the two CYC packets as indicating an overflow.
Status	For the steppings affected, see the Summary Table of Changes.

SKD050	Intel® PT PSB+ Packets May be Omitted on a C6 Transition
Problem	An Intel PT (Processor Trace) PSB+ (Packet Stream Boundary+) set of packets may not be generated as expected when IA32_RTIT_STATUS.PacketByteCnt[48:32] (MSR 0x571) reaches the PSB threshold and a logical processor C6 entry occurs within the following one KByte of trace output.
Implication	After a logical processor enters C6, Intel PT output may be missing PSB+ sets of packets.
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.

SKD051	IA32_PERF_GLOBAL_STATUS.TRACE_TOPA_PMI Bit Cannot be Set by Software
Problem	A WRMSR that attempts to set Trace_ToPA_PMI (bit 55) in the IA32_PERF_GLOBAL_STATUS MSR (38EH) by writing a '1' to bit 55 in the IA32_PERF_GLOBAL_STATUS_SET (MSR (391H) will cause a #GP fault.
Implication	Software cannot set the Trace_ToPA_PMI bit.
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.

SKD052	CPUID Incorrectly Reports Bit Manipulation Instructions Support
Problem	Executing CPUID with EAX = 7 and ECX = 0 may return EBX with bits [3] and [8] set, incorrectly indicating the presence of BMI1 and BMI2 instruction set extensions.
Implication	Attempting to use instructions from the BMI1 or BMI2 instruction set extensions will result in a #UD exception.
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.

SKD053	Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on Intel® Core™ i3 U/H/S, Select Intel® Mobile Pentium®, Intel® Mobile Celeron®, Select Intel® Pentium® G4xxx and Intel® Celeron® G3xxx Processors
Problem	These 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 Base Frequency.
Workaround	None identified.
Status	For the steppings affected, see the Summary Table of Changes.

§

Specification Changes

There are no Specification Changes in this Specification Update revision.

§

Specification Clarifications

There are no specification clarifications in this Specification Update revision.

§

Documentation Changes

There are no documentation changes in this Specification Update revision.

§