Intel® Xeon® E-2300 Processor Family

Specification Update

Revision 004US

May 2023

Reference Number: 709192

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

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.

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.

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.

Intel® Turbo Boost Technology requires a PC with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your PC manufacturer on whether your system delivers Intel Turbo Boost Technology. For more information, see http://www.intel.com/technology/turboboost

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

Intel, Pentium, Celeron, Intel Core, Intel Xeon, Intel Processor Trace, Intel Advanced Vector Extensions, Intel Trace Hub, Intel Transactional Synchronization Extensions, Intel Memory Protection Extensions, Intel Virtualization Technology for Directed I/O, Intel Software Guard Extensions, Intel Smart Sound Technology, Intel Graphics Driver, Intel Hyper-Threading Technology, Intel SpeedStep, and the Intel logo are trademarks of Intel Corporation or its subsidiaries.

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

Content

1 Revision History

Date	Revision	Description
May 2023	004US	Added erratum RKL33.
September 2022	003US	Added erratum RKL32
May 2022	002US	Added errata RKL26, RKL27, RKL28, RKL29, RKL30, RKL31
January 2022	001US	Initial release

§

2 Preface

This document is an update to the specifications contained in the documents listed in the Affected Documents and Related Documents tables below. 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 systems, and tools.

Information types defined in the Nomenclature section below 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.

2.1 Affected Documents

Document Title	Document Number/Location
Intel Xeon E-2300 Processor Product Family Datasheet, Volume 1 of 2	662318
Intel Xeon E-2300 Processor Product Family Datasheet, Volume 2 of 2	662319

2.2 Related Documents

Document Title	Document Number/Location
Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2A: Instruction Set Reference, A-L -- Refer to section "AP-485, Intel® Processor Identification and the CPUID Instruction"	www.intel.com/sdm
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, A-L* *Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2B: Instruction Set Reference, M-U* *Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2C: Instruction Set Reference, V-Z* *Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 3A: System Programming Guide, Part 1* *Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 3B: System Programming Guide, Part 2* *Intel® 64 and IA-32 Architectures Optimization Reference Manual*	https://software.intel.com/en-us/articles/intel-sdm
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	https://software.intel.com/en-us/download/intel-64-and-ia-32-architectures-software-developers-manual-documentation-changes
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	https://soco.intel.com/docs/DOC-19456542015-05-11
Advanced Configuration Power Interface (ACPI) Specifications	www.acpi.info

2.3 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.

Qualification Detail Form (QDF) Number is a multiple digits 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 Nondisclosure Agreement (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, and so forth).

§

3 Identification Information

3.1 Component Identification via Programming Interface

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

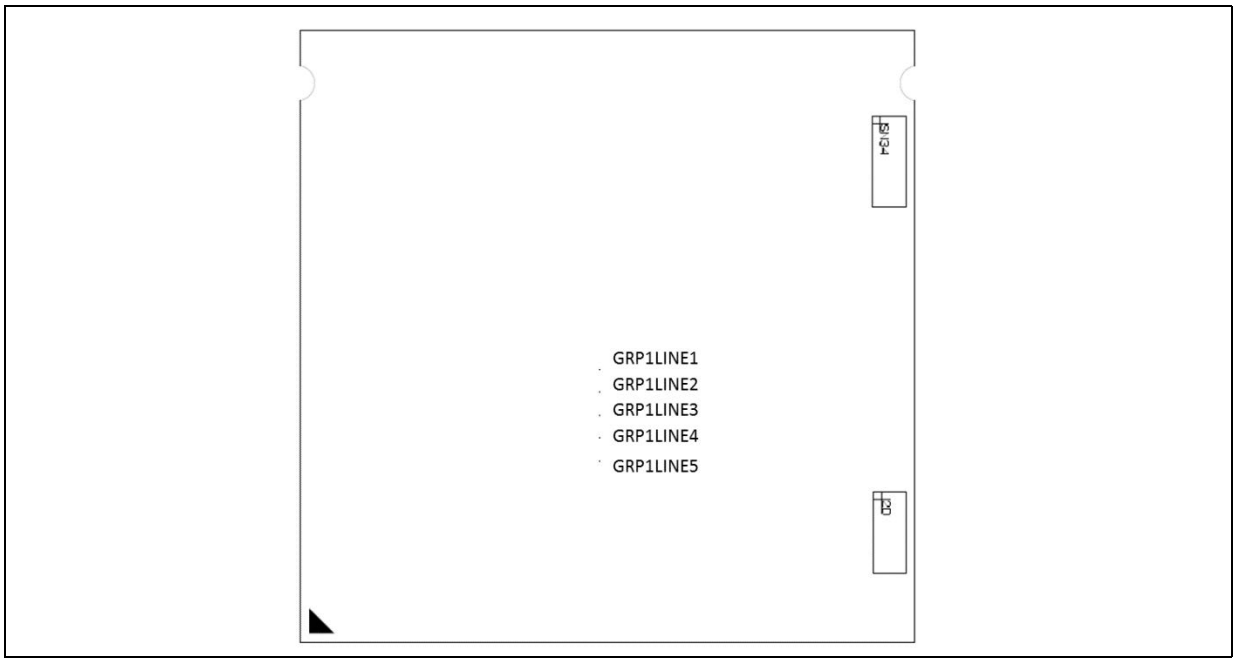
Samples	CPUID	Reserved [31:28]	Extended Family [27:20]	Extended Model [19:16]	Reserved [15:14]	Processor Type [13:12]	Family Code [11:8]	Model Number [7:4]	Stepping ID [3:0]
RKL-S	A0671h	Reserved	0000b	1010b	Reserved	00b	0110b	0111b	0001b

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 Celeron®, Pentium®, 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 Extended Data Register (EDX) register after RESET; bits [11:8] of the Extended Accumulator Register (EAX) register after the CPUID instruction are executed with a 1 in the EAX register and with the generation field of the Device ID register accessible through the 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 are executed with a 1 in the EAX register and with 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.
6. Refer to the *Skylake, Kaby Lake and Coffee Lake, Whiskey Lake and Comet Lake Processor Family Core and Uncore BIOS Specification Rev 3.2.0*, document number 550049, for additional information. When the 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.

The cache and the Translation Lookaside Buffer (TLB) descriptor parameters are provided in the EAX, in the Extended Base Register (EBX), in the Extended Count Register (ECX), and in the EDX registers after the CPUID instruction is executed with a 2 in the EAX register.

3.2 Component Marking Information

Figure 3-1. Land Grid Array (LGA) Top-Side Markings



Pin Count: 1200Package Size: 37.5 mm x 37.5 mm

Production (SSPEC):

GRP1LINE1:Intel logo
GRP1LINE2:BRAND
GRP1LINE3:PROC#
GRP1LINE4:SSPEC SPEED
GRP1LINE5:{FPO} {eX}

Note:

For Intel® Xeon® E-2300 Processor Family Stock Keeping Units (SKUs), see:
https://ark.intel.com/content/www/us/en/ark/products/series/134861/intel-xeon-e-processor.html

4 Summary Tables of Changes

The following table indicates the specification changes, errata, specification clarifications, or documentation changes, which apply to the listed processor stepping. 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:

4.1 Codes Used in Summary Tables

4.1.1 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.

4.1.2 Page

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

4.1.3 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.

4.1.4 Row

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

4.2 Errata Summary Table

Table 4-1. S-Processor Line Errata Summary Table (Sheet 1 of 2)

Erratum ID	Stepping	Status	Title
	B-0		
RKL1.	X	No Fix	"Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses."
RKL2.	X	No Fix	"Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation."
RKL3.	X	No Fix	"Usage Of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt."
RKL4.	X	No Fix	"Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set."
RKL5.	X	No Fix	"Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception."
RKL6.	X	No Fix	"VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values."
RKL7.	X	No Fix	"Processor May Hang if Warm Reset Triggers During BIOS Initialization."
RKL8.	X	No Fix	"IA32_RTIT_STATUS.FilterEn Bit Might Reflect A Previous Value."
RKL9.	X	No Fix	"Time Stamp Counters May Contain A Shifted Time Value."
RKL10.	X	No Fix	"Incorrect ECC Reporting Following Entry to PKG-C7."
RKL11.	X	No Fix	"PMU MSR_UNC_PERF_FIXED_CTR is Cleared After Pkg C7 or Deeper."
RKL12.	X	No Fix	"Unable to Transmit Modified Compliance Test Pattern at 2.5 GT/S or 5.0 GT/s Link Speeds."
RKL13.	X	No Fix	"PCIe Root Ports May Fail Tx Differential Return Loss Compliance Test."t
RKL14.	X	No Fix	"PEG10 PCIe Root Port May Report Incorrect Maximum Link Width."
RKL15.	X	No Fix	"DMI Link Failure During L1 Exit."
RKL16.	X	No Fix	"Processor Peg Ports 10,11, or 12 PCIe Link May Hang During S0ix/S3/S4/S5 Cycles."
RKL17.	X	No Fix	"PCIe Root Ports May Fail Tx Differential Return Loss."
RKL18.	X	No Fix	"System May Hang if Booted with Intel® Trusted Execution Technology (Intel® TXT) Disabled."
RKL19.	X	Fixed	"Single Core Configurations May Hang on S3/S4 Resume."
RKL20.	X	No Fix	"DMI Link May Hang During Package C-state Exits."
RKL21.	X	No Fix	"System May Hang When Booting in Single Core Configuration."
RKL22.	X	No Fix	"Processor May Generate Malformed TLP."
RKL23.	X	No Fix	"Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT Does Not Prevent The Three-strike Counter From Incrementing."
RKL24.	X	No Fix	"PCIe Link May Fail to Train Upon Exit From L1.2."
RKL25.	X	No Fix	"Processor May Exceed Thermal Limits."
RKL26.	X	No Fix	"Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May Cause a #GP."
RKL27.	X	No Fix	"PT TIP.PGD May Not Have Target IP Payload."
RKL28.	X	No Fix	"PT Trace May Drop Second Byte of CYC Packet."

Table 4-1. S-Processor Line Errata Summary Table (Sheet 2 of 2)

Erratum ID	Stepping	Status	Title
	B-0		
RKL29.	X	No Fix	"VM Entry That Clears TraceEn May Generate a FUP."
RKL30.	X	No Fix	"Platform May Not Resume From G3/S3/S4/S5."
RKL31.	X	No Fix	"WRMSR to a Few Core MSRs Might be Overwritten."
RKL32.	X	No Fix	"Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address."
RKL33.	X	No Fix	Branch Predictor May Produce Incorrect Instruction Pointer

5 Errata

RKL1. Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses

Problem: Guest-physical access using a guest-physical address that translates to an address on the APIC-access page (as identified by the APIC-access address field in the VMCS) should cause an APIC-access VM exit. This includes page table information accesses done as part of page translation (page walks). Due to this erratum placing page table information in the APIC-access page may result in a page fault instead of VM exit when the page translation is done as part of an enclave access.

Implication: Software that places page table information in the APIC access page may get page faults on executing enclave accesses, instead of exiting to the VMM (Virtual-Machine Monitor). Intel® has not observed this erratum with any commercially available software.

Workaround: Software should not place page table information in the APIC access page.

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

RKL2. Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation

Problem: Under complex micro-architectural conditions, using a REP MOVSB instruction in which at least one of the operands (destination or source) of the instruction is in a non-flat segment mode, might cause unpredictable system behavior.

Implication: When this erratum occurs, a spurious timer interrupt may occur causing unpredictable system behavior. Intel has not observed this erratum with any commercially available software.

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

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

RKL3. Usage Of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt

Problem: When using the APIC timer in Time Stamp Counter Deadline (TSC-deadline) mode, if the most significant set bit in the written value to the TSC-Deadline MSR is bit 55, the processor may generate a spurious timer interrupt.

Implication: When this erratum occurs, a spurious timer interrupt may occur causing unpredictable system behavior. Intel has not observed this erratum with any commercially available software.

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

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

RKL4. Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set

Problem: Under complex micro-architectural conditions, a single internal parity error seen in IA32_MC0_STATUS MSR (401h) with MCACOD (bits 15:0) value of 5h and MSCOD (bits 31:16) value of 7h, may set the overflow flag (bit 62) in the same MSR.

Implication: Due to this erratum,the IA32_MC0_STATUS overflow flag may be set after a single parity error. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

RKL5. Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception

Problem: When Intel® SGX extends an Enclave Page Cache (EPC) via the page permissions instruction (ENCLU[EMODPE]) and generates a Page Fault (#PF), even though the page permissions instruction access is a read access to the target page, the Page Fault Error Code (#PF's PFEC) will indicate that the fault occurred on a write (PFEC.W bit will be set) instead.

Implication: This erratum may impact debugging Intel® SGX enclaves software. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

RKL6. VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values

Problem: Under complex micro-architectural conditions, a VERR instruction that follows a VM-entry with a guest-state area indicating MOV SS blocking (bit 1 in the Interruptibility state) and at least one of B3-B0 bits set (bits 3:0 in the pending debug exception) may lead to incorrect values in DR6.

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

Workaround: Due to this erratum, DR6 may contain incorrect values. Intel has not observed this erratum with any commercially available software.

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

RKL7. Processor May Hang if Warm Reset Triggers During BIOS Initialization

Problem: Under complex micro-architectural conditions, when the processor receives a warm reset during BIOS initialization, the processor may hang with a machine check error reported in IA32_MCi_STATUS, with MCACOD (bits [15:0]) value of 0400H, and MSCOD (bits [31:16]) value of 0080H.

Implication: Due to this erratum, the processor may hang. Intel has only observed this erratum in a synthetic test environment.

Workaround: None identified.

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

RKL8. IA32_RTIT_STATUS.FilterEn Bit Might Reflect A Previous Value

Problem: Under complex micro-architectural conditions, reading the IA32_RTIT_STATUS. FilterEn bit (bit 0 in MSR 571h) after entering or exiting an RTIT region might reflect a previous value instead of the current one.

Implication: Due to this erratum, IA32_RTIT_STATUS.FilterEn bit might reflect a previous value. This erratum has not been seen in any commercially available software.

Workaround: Software should perform an LFENCE instruction prior to reading the IA32_RTIT_STATUS MSR to avoid this issue.

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

RKL9. Time Stamp Counters May Contain A Shifted Time Value

Problem: Under complex micro-architectural conditions, the processor's RDTSC and RDTSCP instructions may report a shifted value. In these cases, the shift value will be larger than a minute.

Implication: Software may experience a non-monotonic time stamp counte, misalignment across threads, or a spurious timer interrupt.

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

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

RKL10. Incorrect ECC Reporting Following Entry to PKG-C7

Problem: The Correctable and Uncorrectable ECC error address reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may be overwritten after a PKG-C7 event.

Implication: DDR Correctable and Uncorrectable ECC errors reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may report an incorrect error address after resuming from PKG-C.

Workaround: None Identified.

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

RKL11. PMU MSR_UNC_PERF_FIXED_CTR is Cleared After Pkg C7 or Deeper

Problem: The Performance Monitoring Unit Uncore Performance Fixed Counter (MSR_UNC_PERF_FIXED_CTR (MSR 395h)) is cleared after pkg C7 or deeper.

Implication: Due to this erratum, once the system enters pkg C7 or deeper the uncore fixed counter does not reflect the actual count.

Workaround: None identified.

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

RKL12. Unable to Transmit Modified Compliance Test Pattern at 2.5 GT/S or 5.0 GT/s Link Speeds

Problem: The processor's PCIe port (Bus 0, Device 1, Function 0/1/2 or Bus 0, Device 6, Function 0) does not transmit the Modified Compliance Test Pattern when in either 2.5 GT/S or 5.0 GT/s link speeds.

Implication: Due to this erratum, PCIe compliance testing may fail at 2.5 GT/S or 5.0 GT/s link speeds when enabling the Modified Compliance Test Pattern.

Workaround: None identified.

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

RKL13. PCIe Root Ports May Fail Tx Differential Return Loss Compliance Test

Problem: The processor's PCIe root ports may fail to meet the Tx Differential Return Loss Compliance Test's requirements as defined in PCIe Base Specification, version 4.0, section 9.3.6.

Implication: The processor may fail the Differential Return Loss compliance test. Intel has not observed this erratum to cause any functional failures.

Workaround: None identified.

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

RKL14. PEG10 PCIe Root Port May Report Incorrect Maximum Link Width

Problem: When the PEG10 root port (Bus 0, Device 1, Function 0) is bifurcated, the port will incorrectly report Maximum Link Width (MLW) in the Link Capabilities register (Bus 0, Device 1, Function 0, Offset 0Ch). The processor will always indicate the MLW of x16, rather than x8.

Implication: Due to this erratum, software may expect the link to support x16 link widths, which the port cannot do while bifurcated.

Workaround: Due to this erratum, software may expect the link to support x16 link widths, which the port cannot do while bifurcated. .

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

RKL15. DMI Link Failure During L1 Exit

Problem: During S3/S4/S5 and/or S0ix cycles, DMI may fail to exit L1 in the time required.

Implication: The system may hang with a machine check exception (MCACOD=2AH).

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

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

RKL16. Processor Peg Ports 10,11, or 12 PCIe Link May Hang During S0ix/S3/S4/S5 Cycles

Problem: During S0ix and/or S3/S4/S5 when processor exits a Package C-state, the PCIe link may hang for Peg ports 10, 11, or 12.

Implication: Due to this erratum, the PCIe link may hang with a machine check error (MCACOD=34H).

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

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

RKL17. PCIe Root Ports May Fail Tx Differential Return Loss

Problem: The processor's PCIe root ports may not meet the Tx Differential Return Loss specification as defined in PCIe Base Specification, version 4.0, section 8.3.7 Tx and Rx Return Loss.

Implication: The processor may fail the Tx Differential Return Loss specification. Intel has not observed any functional failures due to this erratum.

Workaround: None identified.

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

RKL18. System May Hang if Booted with Intel® Trusted Execution Technology (Intel® TXT) Disabled

Problem: A system with TXT disabled may experience a hang during the boot process.

Implication: Due to this erratum, the system may hang during boot.

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

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

RKL19. Single Core Configurations May Hang on S3/S4 Resume

Problem: When booting in a single core configuration, the system may hang when resuming from a S3/S4 or a warm reset.

Implication: Due to this erratum, the system may hang.

Workaround: None identified.

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

RKL20. DMI Link May Hang During Package C-state Exits

Problem: When the processor exits Package C-states, the DMI link may fail, showing RecoverySpeedReady (0x6C) in the DMI link status register (Base address 0xFEDA0000 Offset: 0x2328, bits [31:24] will be 0x6C), leading to an Internal Timer Error Machine Check (IA32_MCi_STATUS.MCACOD=400H; bits 15:0).

Implication: Due to this erratum, the DMI link may hang with a machine check error (MCACOD=400H).

Workaround: It may be possible for a BIOS code change to contain a workaround for this erratum.

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

RKL21. System May Hang When Booting in Single Core Configuration

Problem: When configured in single-core mode, the processor may issue non-posted transactions during BIOS boot that may not complete.

Implication: Due to this erratum, in single-core mode, the processor may hang during boot.

Workaround: None identified. Platforms can use multi-core configurations to work around this erratum.

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

RKL22. Processor May Generate Malformed TLP

Problem: If the processor root port receives an FetchAdd, Swap, or CAS TLP (an atomic operation) that is erroneous, it should generate a UR completion to the downstream requestor. If the TLP has an operand size greater than 4 bytes, the generated UR completion will report an operand size of 4 bytes, which will be interpreted as a malformed transaction.

Implication: When this erratum occurs, the processor may respond with a malformed transaction.

Workaround: None identified.

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

RKL23. Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT Does Not Prevent The Three-strike Counter From Incrementing

Problem: Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT (bit 11 in MSR 1A4h) does not prevent the three-strike counter from incrementing as documented; instead, it only prevents the signaling of the three-strike event once the counter has expired

Implication: Due to this erratum, software may be able to see the three-strike logged in the MC3_STATUS (MSR 40Dh, MCACOD = 400h [bits 15:0]) even when MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT is set.

Workaround: None identified

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

RKL24. PCIe Link May Fail to Train Upon Exit From L1.2

Problem: When the PCIe Link exits the L1.2 low-power link state, the link may fail to correctly train to L0

Implication: Due to this erratum, a PCIe link may incur unexpected link recovery events or it may enter a Link_Down state.

Workaround: It may be possible for a BIOS code change to workaround this erratum.

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

RKL25. Processor May Exceed Thermal Limits

Problem: Under heavy workloads, the processor may not thermally throttle correctly due to temperature gradients between the thermal sensor and other circuits.

Implication: Due to this erratum, the system may hang or unpredictable system behavior may occur

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

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

RKL26. Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May Cause a #GP

Problem: IA32_THERM_STATUS MSR (19CH) includes read-only (RO) fields as well as writable fields. Writing a non-zero value to any of the read-only fields may cause a #GP.

Implication: Due to this erratum, software that reads the IA32_THERM_STATUS MSR, modifies some of the writable fields, and attempts to write the MSR back may cause a #GP.

Workaround: Software should clear all read-only fields before writing to this MSR.

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

RKL27. PT TIP.PGD May Not Have Target IP Payload

Problem: When PT (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 Tables of Changes."

RKL28. PT Trace May Drop Second Byte of CYC Packet

Problem: Due to a rare microarchitectural condition, the second byte of a 2-byte CYC (Cycle Count) packet may be dropped without an OVF (Overflow) packet.

Implication: A trace decoder may signal a decode error due to the lost trace byte.

Workaround: None identified. A mitigation is available for this erratum. If a decoder encounters a multi-byte CYC packet where the second byte has bit 0 (Ext) set to 1, it should assume that 4095 cycles have passed since the prior CYC packet, and it should ignore the first byte of the CYC and treat the second byte as the start of a new packet.

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

RKL29. VM Entry That Clears TraceEn May Generate a FUP

Problem: If VM entry clears PT (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 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 Tables of Changes."

RKL30. Platform May Not Resume From G3/S3/S4/S5

Problem: Transient noise on the CPU crystal clock differential signals (CPU_NSSC_DP and CPU_NSSC_ DN) when resuming from G3/S3/S4/S5 may prevent the platform from booting.

Implication: Due to this erratum, the platform may fail boot when resuming from G3/S3/S4/S5.

Workaround: A fix is available for this erratum in PMC Firmware. Please see PMC FW revision 160.02.00.1036 or later.

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

RKL31. WRMSR to a Few Core MSRs Might be Overwritten

Problem: If any thread is in thread C6 while another thread is updating one of the following MSRs, a subsequent transition from single thread operation to multi-thread operation or vice versa might cause that MSR to revert to its previous value. The affected MSRs are: MEMORY_CONTROL (MSR 33h bit 28), QUIESCE_CTL1 (MSR 50h) and QUIESCE_CTL2 (MSR 51h).

Implication: Due to this erratum, the values of the above MSRs may be incorrect. Intel has not observed any functional impact due to this erratum.

Workaround: None identified. Software must ensure that the other thread is not in TC6 when writing this MSR.

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

RKL32. Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address

Problem: In 32-bit mode, a call instruction wrapping around the 32-bit address should save a return address near the bottom of the address space (low address) around address zero. Under complex micro-architectural conditions, a return instruction following such a call may return to the next sequential address instead (high address).

Implication: Due to this erratum, in 32-bit mode a return following a call instruction that wraps around the 32-bit address boundary may return to the next sequential IP without wrapping around the address, possibly resulting in a #PF. Intel has not observed this behavior on any commercially available software.

Workaround: Software should not place call instructions in addresses that wrap around the 32-bit address space in a 32-bit mode.

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

RKL33. Branch Predictor May Produce Incorrect Instruction Pointer

Problem: Under complex micro-architectural conditions, the branch predictor may produce an incorrect instruction pointer leading to unpredictable system behavior.

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

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

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

6 Specification Changes

There are no specification changes in this Specification Update revision.

§

7 Documentation Changes

There are no documentation changes in this Specification Update revision.

§