

# **Intel<sup>®</sup> Core<sup>™</sup> i7 Processor Family for LGA2011-v3 Socket**

## **Specification Update**

---

***Supporting Desktop Intel<sup>®</sup> Core<sup>™</sup> i7-5960X Extreme Edition Processor Series for the LGA2011-v3 Socket***

***Supporting Desktop Intel<sup>®</sup> Core<sup>™</sup> i7-59xx and i7-58xx Processor Series for the LGA2011-v3 Socket***

***September 2020***



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

The code names presented in this document are only for use by Intel to identify products, technologies, or services in development, that have not been made commercially available to the public, i.e., announced, launched or shipped. They are not "commercial" names for products or services and are not intended to function as trademarks.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See [http://www.intel.com/products/processor\\_number](http://www.intel.com/products/processor_number) for details.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

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

I<sup>2</sup>C is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I<sup>2</sup>C bus/protocol and was developed by Intel. Implementations of the I<sup>2</sup>C bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Alert on LAN is a result of the Intel-IBM Advanced Manageability Alliance and is a trademark of IBM.

Intel, Intel Core, Intel386, Intel486, Pentium, Intel Enhanced SpeedStep Technology, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

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

Copyright © 2014-2020 Intel Corporation. All rights reserved.



# Contents

---

<b>Revision History</b> .....	4
<b>Preface</b> .....	5
<b>Identification Information</b> .....	7
<b>Summary Tables of Changes</b> .....	8
<b>Errata</b> .....	11
<b>Specification Changes</b> .....	20
<b>Specification Clarifications</b> .....	21
<b>Documentation Changes</b> .....	22



# Revision History

---

Version	Description	Date
001	Initial release.	August 2014
002	Added Errata HSH35~HSH39	May 2019
003	Added Errata HSH40	July 2020
004	Added Errata HSH35~HSH38 and updated the existing Errata numbers	September 2020

§ §



# Preface

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

Information types defined in [Nomenclature](#) are consolidated into the specification update and are no longer published in other documents.

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

**Note:** Throughout this document, the Intel® Core™ i7 processor family may be referred to as “processor”.

## Affected Documents

Document Title	Document Number
Intel® Core™ i7 Processor Family for LGA2011-v3 Socket Datasheet – Volume 1 of 2	330839
Intel® Core™ i7 Processor Family for LGA2011-v3 Socket Datasheet – Volume 2 of 2	330840

## Related Documents

Document Title	Document Number / Location
<i>AP-485, Intel® Processor Identification and the CPUID Instruction</i>	241618
<ul style="list-style-type: none"><li>• Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 1: Basic Architecture</li><li>• Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A: Instruction Set Reference Manual A-M</li><li>• Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2B: Instruction Set Reference Manual N-Z</li><li>• Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A: System Programming Guide</li><li>• Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B: System Programming Guide</li><li>• Intel® 64 and IA-32 Intel Architecture Optimization Reference Manual</li></ul>	<a href="http://www.intel.com/products/processor/manuals/index.htm">http://www.intel.com/products/processor/manuals/index.htm</a>



## Nomenclature

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

**S-Spec Number** is a five-digit code used to identify products. Products are differentiated by their unique characteristics such as, core speed, L2 cache size, package type, etc. as described in the processor identification information table. Read all notes associated with each S-Spec number.

**Specification changes** are modifications to the current published specifications. These changes will be incorporated in any new release of the specification.

**Specification clarifications** describe a specification in greater detail or further highlight a specification's impact to a complex design situation. These clarifications will be incorporated in any new release of the specification.

**Documentation changes** include typos, errors, or omissions from the current published specifications. These will be incorporated in any new release of the specification.

*Note:* Errata remain in the specification update throughout the product's lifecycle, or until a particular stepping is no longer commercially available. Under these circumstances, errata removed from the specification update are archived and available upon request. Specification changes, specification clarifications and documentation changes are removed from the specification update when the appropriate changes are made to the appropriate product specification or user documentation (datasheets, manuals, etc.).

# Identification Information

## Component Identification using Programming Interface

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

**Table 1. Processor Signature / Version**

Reserved	Extended family <sup>1</sup>	Extended model <sup>2</sup>	Reserved	Processor type	Family code <sup>3</sup>	Model number <sup>4</sup>	Stepping ID <sup>5</sup>
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0011b		00b	0110b	1111b	0010

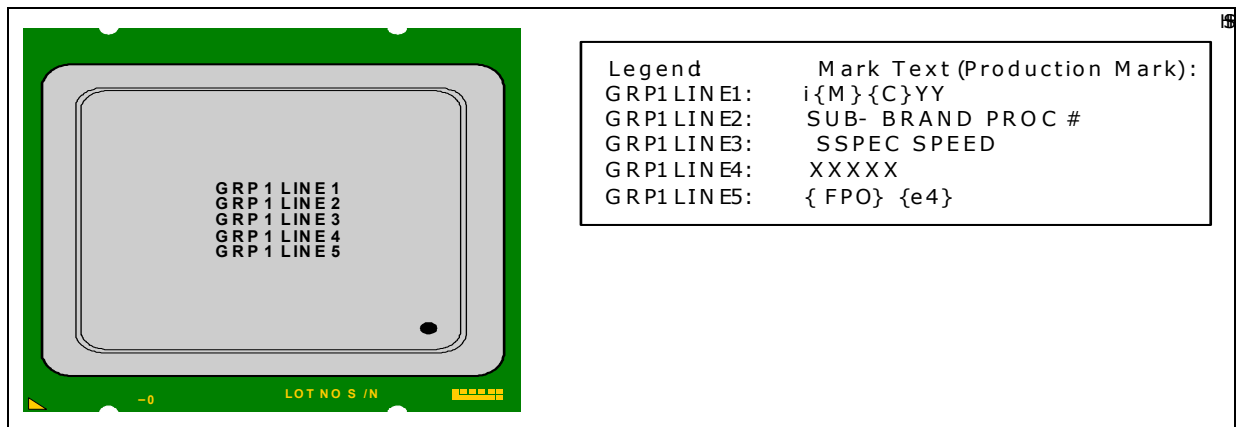
**Notes:**

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 Intel<sup>®</sup>386™, Intel<sup>®</sup>486™, Pentium<sup>®</sup>, Pentium 4, or Intel<sup>®</sup> 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.

## Component Marking

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

**Figure 1. Processor Top-side Markings (example)**



**Table 2. Processor Family identification**

S-spec number	Processor Number	Stepping	CPUID	Max Turbo Frequency (GHz)	Memory Frequency (MHz)	TDP (W)	# Cores	Cache size (MB)
R20Q	i7-5960X	R-2	000306F2h	3.5	2133	140	8	20
R20R	i7-5930K	R-2	000306F2h	3.7	2133	140	6	15
R20S	i7-5820K	R-2	000306F2h	3.6	2133	140	6	15



# Summary Tables of Changes

---

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes that apply to the processor product. Intel may fix some of the errata in a future stepping of the component, and account for the other outstanding issues through documentation or specification changes as noted. These tables use the following notations:

## Codes used in summary tables

### Stepping

- X: Errata exists in the stepping indicated. Specification Change or Clarification that applies to this stepping.
- (No mark)  
or (Blank box): This erratum is fixed in listed stepping or specification change does not apply to listed stepping.

### Page

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

### Status

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

### Row



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





**Table 3. Errata (Sheet 1 of 2)**

Number	Stepping	Status	ERRATA
	R-2		
HSH1	X	No Fix	Intel® QPI Layer May Report Spurious Correctable Errors
HSH2	X	No Fix	NTB May Incorrectly Set MSI or MSI-X Interrupt Pending Bits
HSH3	X	No Fix	Memory Controller May Incorrectly Issue a Refresh Command Immediately After a Precharge Command
HSH4	X	No Fix	Processor May Issue Unexpected NAK DLLP Upon PCIe* L1 Exit
HSH5	X	No Fix	PECI DDR DIMM Digital Thermal Reading Returns Incorrect Value
HSH6	X	No Fix	IIO CSR Lnkcon2 Field Selectable_De_Emphasis Cannot Be Set For DMI2 Mode
HSH7	X	No Fix	PCIe* Receiver May Not Meet the Specification for AC Common Mode Voltage And Jitter
HSH8	X	No Fix	Receiver Termination Impedance On PCIe* 3.0 Does Not Comply With The Specification
HSH9	X	No Fix	USB3 xHCI Not compatible with MSIs
HSH10	X	No Fix	Writing R3QPI Performance Monitor Registers May Fail
HSH11	X	No Fix	CPUID Extended Topology Enumeration Leaf May Indicate an Incorrect Number of Logical Processors
HSH12	X	No Fix	Intel QPI Link Re-training After a Warm Reset or L1 Exit May be Unsuccessful
HSH13	X	No Fix	VCCIN VR Phase Shedding is Disabled
HSH14	X	No Fix	Possible Non-Optimal Electrical Margins on The DDR Command Bus
HSH15	X	No Fix	PECI Commands During Reset May Result in Persistent Timeout Response
HSH16	X	No Fix	System May Hang When Using the TPH Prefetch Hint
HSH17	X	No Fix	TS1s Do Not Convey The Correct Transmitter Equalization Values During Recovery.RcvrLock
HSH18	X	No Fix	MSR_TEMPERATURE_TARGET MSR May Read as '0'
HSH19	X	No Fix	PECI RdIAMS() Command May Fail After Core C6 State is Entered
HSH20	X	No Fix	CLTT May Cause BIOS To Hang On a Subsequent Warm Reset
HSH21	X	No Fix	DDR4 Power Down Timing Violation
HSH22	X	No Fix	PCIe* Extended Tag Field May be Improperly Set
HSH23	X	No Fix	A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation
HSH24	X	No Fix	The System May Hang When a C/A Parity Error is Detected
HSH25	X	No Fix	A C/A Parity Error When DDR4 is Operating at 2133 MHz May Result in Unpredictable System Behavior
HSH26	X	No Fix	Enabling Isochronous Transfers May Result in Unpredictable System Behavior
HSH27	X	No Fix	Enabling Secondary To Primary Snoop Overrides On NTB May Cause a Hang
HSH28	X	No Fix	Memory Controller tsod_present Settings Being Improperly Cleared
HSH29	X	No Fix	Reserving Resources For Isochronous Transfers With Non-Posted Prefetching Enabled May Cause a Hang
HSH30	X	No Fix	BT Timeouts May Cause Spurious Machine Checks
HSH31	X	No Fix	Full Duplex NTB Traffic Can Cause a System Hang
HSH32	X	No Fix	CONFIG_TDP_NOMINAL CSR Implemented at Incorrect Offset
HSH33	X	No Fix	Software Using Intel® Transactional Synchronization Extensions (Intel® TSX) May Result in Unpredictable System Behavior
HSH34	X	No Fix	A Machine-Check Exception Due to Instruction Fetch May Be Delivered Before an Instruction Breakpoint
HSH35	X	No Fix	Patrol Scrubbing of Mirrored Memory May Log Spurious Memory Errors
HSH36	X	No Fix	MSR_TURBO_ACTIVATION_RATIO MSR Cannot be Locked



**Table 3. Errata (Sheet 2 of 2)**

Number	Stepping	Status	ERRATA
	R-2		
HSH37	X	No Fix	The System May Shut Down Unexpectedly During a Warm Reset
HSH38	X	No Fix	An APIC Timer Interrupt During Core C6 Entry May Be Lost
HSH39	X	No Fix	Some OFFCORE_RESPONSE Performance Monitoring Events May Undercount
HSH40	X	No Fix	PEBS Record May Be Generated After Being Disabled
HSH41	X	No Fix	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions
HSH42	X	No Fix	Data Breakpoint Coincident With a Machine Check Exception May be Lost
HSH43	X	No Fix	APIC Timer Interrupt May Not be Generated at The Correct Time In TSC-Deadline Mode
HSH44	X	No Fix	Performance Monitoring General Counter 2 May Have Invalid Value Written When TSX Is Enabled

**Table 4. Specification Clarifications**

No.	Specification clarifications
	None

**Table 5. Specification Changes**

No.	Specification changes
	None

**Table 6. Documentation Changes**

No.	Documentation changes
	None



# Errata

---

## **HS1** Intel® QPI Layer May Report Spurious Correctable Errors

**Problem:** Intel QPI may report an inband reset with no width change (error 0x22) correctable error upon exit from the L1 power state as logged in its IA32\_MC{5, 20, 21}\_STATUS MSRs (415H,451H,455H).

**Implication:** An unexpected inband reset with no width change error may be logged.

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

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

## **HS2** NTB May Incorrectly Set MSI or MSI-X Interrupt Pending Bits

**Problem:** The NTB (Non-transparent Bridge) may incorrectly set MSI (Message Signaled Interrupt) pending bits in MSIPENDING (BAR PB01BASE,SB01BASE; Offset 74H) while operating in MSI-X mode or set MSI-X pending bits in PMSIXPBA (BAR PB01BASE, SB01BASE; Offset 03000H) while operating in MSI mode.

**Implication:** Due to this erratum, NTB incorrectly sets MSI or MSI-X pending bits. The correct pending bits are also set and it is safe to ignore the incorrectly set bits.

**Workaround:** None identified.

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

## **HS3** Memory Controller May Incorrectly Issue a Refresh Command Immediately After a Precharge Command

**Problem:** In PPD (Precharge Power Down) mode, the memory controller may incorrectly issue a REF (refresh) command one cycle after a PREA (precharge) command, violating JEDEC specifications.

**Implication:** Memory contents may be affected in precharge Power Down mode leading to unpredictable system behavior.

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

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

## **HS4** Processor May Issue Unexpected NAK DLLP Upon PCIe\* L1 Exit

**Problem:** Upon exiting the L1 link power state, the processor's PCIe port may unexpectedly issue a NAK DLLP (Data Link Layer Packet).

**Implication:** PCIe endpoints may unexpectedly receive and log a NAK DLLP.

**Workaround:** None identified.

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

## **HS5** PECCI DDR DIMM Digital Thermal Reading Returns Incorrect Value

**Problem:** When using the PECCI RdPkgConfig() command to read PCS (Package Config Space) Service 14 "DDR DIMM Digital Thermal Reading", the value returned is incorrect.

**Implication:** Platform thermal management may not behave as expected.

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

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



## **HSH6 IIO CSR Lnkcon2 Field Selectable\_De\_Emphasis Cannot Be Set For DMI2 Mode**

**Problem:** The CSR Lnkcon2 (Bus 0; Device 0; Function 0, Offset 0x1C0) field selectable\_de\_emphasis (bit 6) cannot be set for a link in DMI2 Mode when the DMI port is operating at 5 GT/s. The documentation has the attribute of RW-O (read, write once), but the processor incorrectly operates as read-only.

**Implication:** When the link is in DMI2 mode, the de-emphasis cannot be changed for an upstream component.

**Workaround:** None identified.

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

## **HSH7 PCIe\* Receiver May Not Meet the Specification for AC Common Mode Voltage And Jitter**

**Problem:** Due to this erratum, PCIe receivers may not meet the specification for AC common mode voltage (300 mV) and jitter (78.1 ps) at high temperatures when operating at 5 GT/s.

**Implication:** Specifications for PCIe receiver AC common mode voltage and jitter may not be met. Intel has not observed this erratum on any commercially available system with any commercially available PCIe devices.

**Workaround:** None identified.

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

## **HSH8 Receiver Termination Impedance On PCIe\* 3.0 Does Not Comply With The Specification**

**Problem:** The PCIe\* Base Specification revision 3.0 defines ZRX-HIGH-IMP-DC-NEG and ZRX-HIGH-IMP-DC-POS for termination impedance of the receiver. The specified impedance for a negative voltage (-150 mV to 0V) is expected to be greater than 1 Kohm. Sampled measurements of this impedance as low as 400 ohms have been seen. The specified impedance for a positive voltage (> 200 mV) is greater than 20 Kohms. Sampled measurements of this impedance as low as 14.6 Kohms have been seen.

**Implication:** Intel has not observed functional failures from this erratum on any commercially available platforms using any commercially available PCIe device.

**Workaround:** None identified.

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

## **HSH9 USB3 xHCI Not compatible with MSIs**

**Problem:** When the PCH xHCI (Extensible Host Controller Interface) is configured to use MSI interrupts, a PCIe device number conflict between the processor and xHCI controller may cause the interrupts be routed incorrectly.

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

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

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

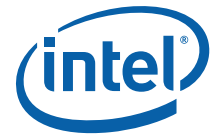
## **HSH10 Writing R3QPI Performance Monitor Registers May Fail**

**Problem:** Due to this erratum, attempting to write R3QPI performance monitor registers (Bus 0; Device 11; Functions 1,2,5,6; Offset 0xA0-0xF7) may be unsuccessful.

**Implication:** A failed write to one or more R3QPI performance monitor registers is likely to yield incorrect performance events counts.

**Workaround:** Consecutively write the identified registers twice with the same value before performance monitoring is globally enabled.

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



### **HS11 CPUID Extended Topology Enumeration Leaf May Indicate an Incorrect Number of Logical Processors**

**Problem:** The Extended Topology Enumeration Leaf of CPUID (EAX = 0xB) may return an incorrect value in EBX[15:0] for the core level type (ECX[15:8] = 2). In this instance, the number of logical processors at the core level reported in EBX[15:0] should reflect the configuration as shipped by Intel.

**Implication:** Software that uses the referenced CPUID function may not properly initialize all logical processors in the system or correctly report the actual number of factory-configured logical processors.

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

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

### **HS12 Intel QPI Link Re-training After a Warm Reset or L1 Exit May be Unsuccessful**

**Problem:** After a warm reset or an L1 exit, the Intel® QPI (Intel QuickPath Interconnect) links may not train successfully.

**Implication:** A failed Intel QPI link can lead to reduced system performance or an inoperable system.

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

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

### **HS13 VCCIN VR Phase Shedding is Disabled**

**Problem:** Due to this erratum, the processor does not direct the VCCIN VR (voltage regulator) to shed phases during low power states.

**Implication:** Platform power consumption may exceed expected levels during deep package C-states.

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

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

### **HS14 Possible Non-Optimal Electrical Margins on The DDR Command Bus**

**Problem:** The processor periodically adjusts drive strength for DDR signals to optimize electrical margins. Due to this erratum, the drive strength on the DDR command bus may be incorrectly adjusted.

**Implication:** Reduced electrical margins on the command bus can lead to higher error rates possibly affecting system stability.

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

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

### **HS15 PECE Commands During Reset May Result in Persistent Timeout Response**

**Problem:** Due to this erratum, a PECE (Platform Environment Control Interface) command other than GetDIB(), Ping(), or GetTemp() received before RESET\_N is de-asserted may result in a timeout (0x81 completion code) for all subsequent such commands.

**Implication:** Future PECE commands other than GetDIB(), Ping(), and GetTemp() will not be serviced after this erratum occurs.

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

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



### **HS16 System May Hang When Using the TPH Prefetch Hint**

**Problem:** When all enabled cores on a socket are simultaneously in core C3, core C6, or package C6 state and a PCIe\* TPH (Transaction layer packet Processing Hint) with the prefetch hint set is received, the system may hang.

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

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

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

### **HS17 TS1s Do Not Convey The Correct Transmitter Equalization Values During Recovery.RcvrLock**

**Problem:** The PCIe\* 3.1 Base Specification requires that TS1s sent during Recovery.RcvrLock following 8.0 GT/s EQ (adaptive equalization) contain the final transmitter preset number and coefficient values that were requested by an endpoint during phase 2 of EQ. Due to this erratum, TS1s with incorrect transmitter preset number values may be sent during Recovery.RcvrLock following 8.0 GT/s adaptive equalization.

**Implication:** Endpoints that check these values may, when unexpected values are found, request equalization restart in subsequent TSs it sends. If EQ requests from the endpoint are supported in the BIOS or OS, EQ will be restarted and the link may continue this EQ loop indefinitely.

**Workaround:** None identified.

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

### **HS18 MSR\_TEMPERATURE\_TARGET MSR May Read as '0'**

**Problem:** Due to this erratum, reading the MSR\_TEMPERATURE\_TARGET MSR (1A2H) may incorrectly return '0'.

**Implication:** Software that depends on the contents of the MSR\_TEMPERATURE\_TARGET MSR may not behave as expected.

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

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

### **HS19 PECCI RdIAMSRR() Command May Fail After Core C6 State is Entered**

**Problem:** Reading core Machine Check Bank registers using the PECCI (Platform Environment Control Interface) RdIAMSRR() command may fail after core C6 state has been entered.

**Implication:** Invalid data may be returned when using PECCI to read core Machine Check Bank registers.

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

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

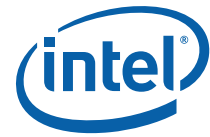
### **HS20 CLTT May Cause BIOS To Hang On a Subsequent Warm Reset**

**Problem:** If CLTT (Closed Loop Thermal Throttling) is enabled when a warm reset is requested, due to this erratum, the processor will resume DIMM temperature polling before the memory sub-system has been re-initialized.

**Implication:** This erratum may lead to a BIOS hang. The warm reset request will fail, along with subsequent warm reset attempts. The failing condition is cleared by a cold reset.

**Workaround:** A BIOS workaround has been identified. Please refer to the latest version of the Platform Reference Code (RC).

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



### **HS21 DDR4 Power Down Timing Violation**

**Problem:** When DDR4 is operating at 2133 MHz, the processor's memory control may violate the JEDEC tPRPDEN timing specification.

**Implication:** Intel has not observed this erratum to impact the operation of any commercially available system

**Workaround:** None identified.

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

### **HS22 PCIe\* Extended Tag Field May be Improperly Set**

**Problem:** The Extended Tag field in the TLP Header will not be zero for TLPs issued by PCIe ports 1a, 1b, 2c, 2d, 3c, and 3d even when the Extended Tag Field Enable bit in the Device Control Register (Offset 08H, bit 8) is 0.

**Implication:** This does not affect ports 0, 2a, 2b, 3a and 3b. This will not result in any functional issues when using device that properly track and return the full 8 bit Extended Tag value with the affected ports. However, if the Extended Tag field is not returned by a device connected to an affected port then this may result in unexpected completions and completion timeouts.

**Workaround:** None identified.

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

### **HS23 A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation**

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

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

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

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

### **HS24 The System May Hang When a C/A Parity Error is Detected**

**Problem:** Due to this erratum, detection of a C/A (Command/Address) parity error by the memory controller can lead to a system hang.

**Implication:** System may experience a hang condition in the presence of C/A parity errors.

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

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

### **HS25 A C/A Parity Error When DDR4 is Operating at 2133 MHz May Result in Unpredictable System Behavior**

**Problem:** Due to this erratum, when DDR4 is operating at 2133MHz and a C/A (Command/Address) parity error occurs while exiting a package C-state then unpredictable system behavior may occur.

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

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

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



## **HSH26 Enabling Isochronous Transfers May Result in Unpredictable System Behavior**

- Problem:** Enabling isochronous transfers may lead to spurious correctable memory errors, uncorrectable memory errors, patrol scrub errors and unpredictable system behavior.
- Implication:** The system may hang, or report spurious memory errors, or behave unpredictably.
- Workaround:** A BIOS code change has been identified and may be implemented as a workaround for this erratum.
- Status:** For the affected steppings, see the Summary Tables of Changes.

## **HSH27 Enabling Secondary To Primary Snoop Overrides On NTB May Cause a Hang**

- Problem:** Due to this erratum, NTB (Non-Transparent Bridge) completions may be dropped when Secondary to Primary Snoop Overrides are enabled.
- Implication:** The system may hang or experience timeout machine checks when the secondary to primary snoop override is enabled. This erratum does not affect primary to secondary snoop override.
- Workaround:** None identified. To avoid this erratum, set the bar45\_s2p\_snpov field (bits[7:6]) and the bar23\_s2p\_snpov field (bits[3:2]) of the ntbcntl CSR (Bus: 0; Device: 3; Function: 0; Offset: 0x58) to 0.
- Status:** For the affected steppings, see the Summary Tables of Changes.

## **HSH28 Memory Controller tsod\_present Settings Being Improperly Cleared**

- Problem:** On single Home Agent configurations, due to this erratum, the processor interferes with TSOD (thermal sensor on DIMM) usage by incorrectly clearing the tsod\_present field (bits[7:0]) of the smbcntl\_1 CSR (Bus 0; Device 19; Function 0; Offset 0x198) after BIOS writes that field.
- Implication:** Closed Loop Thermal Throttle will not work as expected.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the affected steppings, see the Summary Tables of Changes.

## **HSH29 Reserving Resources For Isochronous Transfers With Non-Posted Prefetching Enabled May Cause a Hang**

- Problem:** Resources in the IIO (Integrated I/O) unit are reserved for isochronous transfers to ensure performance guarantees are met. Due to this erratum, enabling non-posted prefetching in the IIO when resources are reserved for isochronous traffic may result in a hang.
- Implication:** Due to this erratum, configuring the IIO unit to prefetch may result in a system hang.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the affected steppings, see the Summary Tables of Changes.

## **HSH30 BT Timeouts May Cause Spurious Machine Checks**

- Problem:** The BT (Backup Tracker) timeout logic in the Home Agent can trigger spuriously, causing false machine checks indicated by IA32\_MCi\_STATUS.MSCOD=0x0200.
- Implication:** Due to this erratum, timeout machine check may occur.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the affected steppings, see the Summary Tables of Changes.

## **HSH31 Full Duplex NTB Traffic Can Cause a System Hang**

- Problem:** If two PCIe\* endpoints target traffic to PB23BASE (Bus 0; Device 3; Function 0; Offset 0x18, 0x1c) and PB45BASE (Bus 0; Device 3; Function 0; Offset 0x20, 0x24) registers at the same time, a deadlock can result.
- Implication:** Due to this erratum, the system may hang.





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

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

### **HS32 CONFIG\_TDP\_NOMINAL CSR Implemented at Incorrect Offset**

**Problem:** The PCIe\* Base Specification indicates that Configuration Space Headers have a base address register at offset 0x10. Due to this erratum, the Power Control Unit's CONFIG\_TDP\_NOMINAL CSR (Bus 1; Device 30; Function 3; Offset 0x10) is located where a base address register is expected.

**Implication:** Software may treat the CONFIG\_TDP\_NOMINAL CSR as a base address register leading to a failure to boot.

**Workaround:** None identified.

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

### **HS33 Software Using Intel® Transactional Synchronization Extensions (Intel® TSX) May Result in Unpredictable System Behavior**

**Problem:** Under a complex set of internal timing conditions and system events, software using the Intel TSX instructions may result in unpredictable system behavior.

**Implication:** This erratum may result in unpredictable system behavior.

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

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

### **HS34 A Machine-Check Exception Due to Instruction Fetch May Be Delivered Before an Instruction Breakpoint**

**Problem:** from fetching an instruction. Due to this erratum, a machine-check exception resulting from the fetch of an instruction may take priority over an instruction breakpoint if the instruction crosses a 32-byte boundary and the second part of the instruction is in a 32-byte poisoned instruction fetch block.

**Implication:** Instruction breakpoints may not operate as expected in the presence of a poisoned instruction fetch block.

**Workaround:** None identified.

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

### **HS35 Patrol Scrubbing of Mirrored Memory May Log Spurious Memory Errors**

**Problem:** The Patrol scrubber, when mirroring is enabled, may incorrectly identify certain data patterns as poison data or as memory errors.

**Implication:** Spurious memory errors and poisoned data may be logged when mirroring is enabled.

**Workaround:** A BIOS workaround has been identified. Please refer to the Grantley-EP Platform Reference Code (RC) version 1.01 or later.

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

### **HS36 MSR\_TURBO\_ACTIVATION\_RATIO MSR Cannot be Locked**

**Problem:** Setting the TURBO\_ACTIVATION\_RATIO\_LOCK field (bit 31) of the MSR\_TURBO\_ACTIVATION\_RATIO MSR (64CH) has no effect; it does not block future writes to the MSR\_TURBO\_ACTIVATION\_RATIO MSR.

**Implication:** Software cannot rely on locking MSR\_TURBO\_ACTIVATION\_RATIO MSR.

**Workaround:** None identified.

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



### **HSH37 The System May Shut Down Unexpectedly During a Warm Reset**

**Problem:** Certain complex internal timing conditions present when a warm reset is requested can prevent the orderly completion of in-flight transactions. It is possible under these conditions that the warm reset will fail and trigger a full system shutdown.

**Implication:** When this erratum occurs, the system will shut down and all machine check error logs will be lost.

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

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

### **HSH38 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 affected steppings, see the Summary Tables of Changes.

### **HSH39 Some OFFCORE\_RESPONSE Performance Monitoring Events May Undercount**

**Problem:** The performance monitoring events OFFCORE\_RESPONSE (Events B7H and BBH) should count uncore responses matching the request-response configuration specified in MSR\_OFFCORE\_RSPs (1A6H and 1A7H, respectively) for core-originated requests. However, due to this erratum, COREWB (bit 3), PF\_L3\_DATA\_RD (bit 7), PF\_L3\_RFO (bit 8), PR\_L3\_CODE\_RD (bit 9), SPLIT\_LOCK\_UC\_LOCK (bit 10), and STREAMING\_STORES (bit 11) request types may undercount.

**Implication:** These performance monitoring events may not produce reliable results for the listed request types.

**Workaround:** None identified.

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

### **HSH40 PEBS Record May Be Generated After Being Disabled**

**Problem:** A performance monitoring counter may generate a PEBS (Precise Event Based Sampling) record after disabling PEBS or the performance monitoring counter by clearing the corresponding enable bit in IA32\_PEBS\_ENABLE MSR (3F1H) or IA32\_PERF\_GLOBAL\_CTRL MSR (38FH).

**Implication:** A PEBS record generated after a VMX transition will store into memory according to the post-transition DS (Debug Store) configuration. These stores may be unexpected if PEBS is not enabled following the transition.

**Workaround:** It is possible for the BIOS to contain a workaround for this erratum. A software workaround is possible through disallowing PEBS during VMX non-root operation and disabling PEBS prior to VM entry.

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

### **HSH41 MOVNTDQA From WC Memory May Pass Earlier Locked Instructions**

**Problem:** An execution of (V)MOVNTDQA (streaming load instruction) that loads from WC (write combining) memory may appear to pass an earlier locked instruction that accesses a different cache line.

**Implication:** Software that expects a lock to fence subsequent (V)MOVNTDQA instructions may not operate properly.

**Workaround:** None identified. Software that relies on a locked instruction to fence subsequent executions of (V)MOVNTDQA should insert an MFENCE instruction between the locked instruction and subsequent (V)MOVNTDQA instruction.

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



#### **HS42 Data Breakpoint Coincident With a Machine Check Exception May be Lost**

**Problem:** If a data breakpoint occurs coincident with a machine check exception, then the data breakpoint may be lost.

**Implication:** Due to this erratum, a valid data breakpoint may be lost.

**Workaround:** None identified.

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

#### **HS43 APIC Timer Interrupt May Not be Generated at The Correct Time In TSC-Deadline Mode**

**Problem:** After writing to the IA32\_TSC\_ADJUST MSR (3BH), any subsequent write to the IA32\_TSC\_DEADLINE MSR (6E0H) may incorrectly process the desired deadline. When this erratum occurs, the resulting timer interrupt may be generated at the incorrect time.

**Implication:** When the local APIC (Advanced Programmable Interrupt Controller) timer is configured for TSC-Deadline mode, a timer interrupt may be generated much earlier than expected or much later than expected. Intel has not observed this erratum with most commercially available software.

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

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

#### **HS44 Performance Monitoring General Counter 2 May Have Invalid Value Written When TSX Is Enabled**

**Problem:** When Intel® Transactional Synchronization Extensions (TSX) is enabled, and there are aborts (HLE or RTM) overlapping with access or manipulation of the IA32\_PMC2 general-purpose performance counter (Offset: C3h) it may return invalid value.

**Implication:** Software may read invalid value from IA32\_PMC2.

**Workaround:** None identified

**Status:** For the affected steppings, see the Summary Tables 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

---

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

- Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture
- Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M
- Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z
- Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide
- Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide

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

**Note:**

Documentation changes for Intel® 64 and IA-32 Architecture Software Developer's Manual volumes 1, 2A, 2B, 3A, and 3B will be posted in a separate document, Intel® 64 and IA-32 Architecture Software Developer's Manual Documentation Changes. Follow the link below to become familiar with this file.

<http://developer.intel.com/products/processor/manuals/index.htm>

There are no documentation changes in this specification update revision.

