Intel® Xeon® Processor E7-8800/4800 v3 Product Family

Specification Update

September 2015
## Contents

Revision History ........................................................................................................... 4

Preface .......................................................................................................................... 5
  Affected Documents................................................................................................. 5
  Nomenclature ........................................................................................................... 5

Identification Information ............................................................................................ 6
  Component Identification via Programming Interface .............................................. 6
  Component Marking Information ............................................................................. 6

Summary Tables of Changes ......................................................................................... 8
  Codes Used in Summary Tables............................................................................... 8

Errata ............................................................................................................................ 12

Specification Changes ................................................................................................. 24

Specification Clarifications ......................................................................................... 25

Documentation Changes ............................................................................................. 26

BIOS Sightings Issues and Workarounds Revision History ........................................ 27

BIOS Sightings Issues, Workarounds and Documentation Changes ............................ 28
  Codes Used in Summary Tables............................................................................... 28

BIOS Sightings, Issues and Workarounds ................................................................... 30

Specification Clarifications ......................................................................................... 35

Documentation Changes ............................................................................................. 36
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2015</td>
<td>003</td>
<td>• Added erratum HSX54</td>
</tr>
<tr>
<td>August 2015</td>
<td>002</td>
<td>• Added errata HSX48 - HSX53.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated Table 1.</td>
</tr>
<tr>
<td>May 2015</td>
<td>001</td>
<td>• Initial Release</td>
</tr>
</tbody>
</table>
Preface

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

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

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

Affected Documents

<table>
<thead>
<tr>
<th>Document title</th>
<th>Document number/location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel® Xeon® Processor E7-4800/8800 v3 Product Families Datasheet - Volume 1:</td>
<td>332314</td>
</tr>
<tr>
<td>Electrical, Mechanical and Thermal</td>
<td></td>
</tr>
<tr>
<td>Intel® Xeon® Processor E7-8800/4800 v3 Product Families Datasheet Volume 2:</td>
<td>332315</td>
</tr>
<tr>
<td>Registers</td>
<td></td>
</tr>
</tbody>
</table>

Nomenclature

**Errata** are design defects or errors. These may cause the Intel® Xeon® Processor E7 v3 Product Family’ 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.

**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.

**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, and so forth, as described in the processor identification information table. Read all notes associated with each S-Spec number.

**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).
Identification Information

Component Identification via Programming Interface

The Intel® Xeon® Processor E7 v3 Product Family stepping can be identified by the following register contents:

<table>
<thead>
<tr>
<th>Reserved</th>
<th>Extended Family</th>
<th>Extended Model</th>
<th>Reserved</th>
<th>Processor Type</th>
<th>Family Code</th>
<th>Model Number</th>
<th>Stepping ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00000000b</td>
<td>0011b</td>
<td>00b</td>
<td>0110b</td>
<td>1111b</td>
<td>0100b</td>
<td></td>
</tr>
</tbody>
</table>

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® 386, Intel® 486, 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.
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.

Refer to the Intel® 64 and IA-32 Architectures Software Developer’s Manual documentation for additional information.

Component Marking Information

Table 1. Intel Xeon Processor E7 v3 Product Family Identification

<table>
<thead>
<tr>
<th>S-Spec No</th>
<th>Stepping</th>
<th>Model Number</th>
<th>CPUID</th>
<th>Core frequency (GHz)/Intel QPI (GT/s)/Intel SM12 (GT/s)/DDR4 1:1 Speed (MHz)</th>
<th>TDP (W)</th>
<th># Cores</th>
<th>LLC Cache Size (MB)</th>
<th>Number of Supported Sockets</th>
</tr>
</thead>
<tbody>
<tr>
<td>R21V</td>
<td>E0</td>
<td>E7-8890V3</td>
<td>0x306F4</td>
<td>2.5/9.6/2.6/1866</td>
<td>165</td>
<td>18</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R21X</td>
<td>E0</td>
<td>E7-8880V3</td>
<td>0x306F4</td>
<td>2.3/9.6/2.6/1866</td>
<td>150</td>
<td>18</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R21Y</td>
<td>E0</td>
<td>E7-8870V3</td>
<td>0x306F4</td>
<td>2.1/9.6/2.6/1866</td>
<td>140</td>
<td>18</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R21Z</td>
<td>E0</td>
<td>E7-8860V3</td>
<td>0x306F4</td>
<td>2.2/9.6/2.6/1866</td>
<td>140</td>
<td>16</td>
<td>40</td>
<td>8</td>
</tr>
<tr>
<td>R221</td>
<td>E0</td>
<td>E7-4850V3</td>
<td>0x306F4</td>
<td>2.2/8/2.6/1866</td>
<td>115</td>
<td>14</td>
<td>35</td>
<td>4</td>
</tr>
<tr>
<td>R222</td>
<td>E0</td>
<td>E7-4830V3</td>
<td>0x306F4</td>
<td>2.1/8/2.6/1866</td>
<td>115</td>
<td>12</td>
<td>30</td>
<td>4</td>
</tr>
<tr>
<td>R223</td>
<td>E0</td>
<td>E7-4809V3(^5)</td>
<td>0x306F4</td>
<td>2/6.4/2.6/1866</td>
<td>115</td>
<td>8</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>R224</td>
<td>E0</td>
<td>E7-4820V3(^4,5)</td>
<td>0x306F4</td>
<td>1.9/6.4/2.6/1866</td>
<td>115</td>
<td>10</td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>R225</td>
<td>E0</td>
<td>E7-8891V3</td>
<td>0x306F4</td>
<td>2.8/9.6/2.6/1866</td>
<td>165</td>
<td>10</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R226</td>
<td>E0</td>
<td>E7-8893V3</td>
<td>0x306F4</td>
<td>3.2/9.6/2.6/1866</td>
<td>140</td>
<td>4</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R227</td>
<td>E0</td>
<td>E7-8880LV3</td>
<td>0x306F4</td>
<td>2/9.6/2.6/1866</td>
<td>115</td>
<td>18</td>
<td>45</td>
<td>8</td>
</tr>
<tr>
<td>R228</td>
<td>E0</td>
<td>E7-8867V3</td>
<td>0x306F4</td>
<td>2.5/9.6/2.6/1866</td>
<td>165</td>
<td>16</td>
<td>45</td>
<td>8</td>
</tr>
</tbody>
</table>

Notes:
1. Intel® Xeon® Processor E7-4800/8800 v3 Product Families VID codes will change due to temperature and/or current load changes in order to minimize power of the part. For specific voltages, refer to the latest Intel® Xeon® Processor E7-4800/8800 v3 Product Families Datasheet - Volume 1, #332314.

2. Refer to the latest revision of the following documents for information on processor specifications and features: Intel® Xeon® Processor E7-4800/8800 v3 Product Families Datasheet - Volume 1, #332314; Intel® Xeon® Processor E7-8800/4800 v3 Product Families Datasheet Volume 2: Registers, #332315.

3. Refer to the latest Intel® Xeon® Processor E7 v3 Product Family Thermal/ Mechanical Specifications and Design Guide, #332318 for information on processor operating temperature and thermal specifications.

4. This SKU does not support Intel® Hyper-Threading Technology.

5. This SKU does not support Intel® Turbo Boost Technology.

6. This SKU is intended for workstations only and uses workstation specific use conditions for reliability assumptions.

7. Intel® Turbo Boost Technology performance varies depending on hardware, software and overall system configuration.
Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the Intel® Xeon® Processor E7 v3 Product Family. 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>
<thead>
<tr>
<th>Number</th>
<th>Stepping</th>
<th>Status</th>
<th>Errata</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSX1</td>
<td>E0</td>
<td>No Fix</td>
<td>Intel® QuickPath Interconnect (Intel® QPI) Layer May Report Spurious Correctable Errors</td>
</tr>
<tr>
<td>HSX2</td>
<td>E0</td>
<td>No Fix</td>
<td>PECI DDR DIMM Digital Thermal Reading Returns Incorrect Value</td>
</tr>
<tr>
<td>HSX3</td>
<td>E0</td>
<td>No Fix</td>
<td>IIO CSR Lnkcon2 Field Selectable_De_Empahsis Cannot Be Set For DMI2 Mode</td>
</tr>
<tr>
<td>HSX4</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe* Receiver May Not Meet the Specification for AC Common Mode Voltage And Jitter</td>
</tr>
<tr>
<td>HSX5</td>
<td>E0</td>
<td>No Fix</td>
<td>Receiver Termination Impedance On PCIe 3.0 Does Not Comply With The Specification</td>
</tr>
<tr>
<td>HSX6</td>
<td>E0</td>
<td>No Fix</td>
<td>A Memory Channel With More Than 4 Ranks May Lead to a System Hang</td>
</tr>
<tr>
<td>HSX7</td>
<td>E0</td>
<td>No Fix</td>
<td>Writing R3QPI Performance Monitor Registers May Fail</td>
</tr>
<tr>
<td>HSX8</td>
<td>E0</td>
<td>No Fix</td>
<td>Intel® QPI Link Re-training After a Warm Reset or L1 Exit May be Unsuccessful</td>
</tr>
<tr>
<td>HSX9</td>
<td>E0</td>
<td>No Fix</td>
<td>VCIN VR Phase Shedding is Disabled</td>
</tr>
<tr>
<td>HSX10</td>
<td>E0</td>
<td>No Fix</td>
<td>PECI Commands During Reset May Result in Persistent Timeout Response</td>
</tr>
<tr>
<td>HSX11</td>
<td>E0</td>
<td>No Fix</td>
<td>System May Hang When Using the TPH Prefetch Hint</td>
</tr>
<tr>
<td>HSX12</td>
<td>E0</td>
<td>No Fix</td>
<td>TSIs Do Not Convey The Correct Transmitter Equalization Values During Recovery.RcvtLock</td>
</tr>
<tr>
<td>HSX13</td>
<td>E0</td>
<td>No Fix</td>
<td>MSR_TEMPERATURE_TARGET MSR May Read as '0'</td>
</tr>
<tr>
<td>HSX14</td>
<td>E0</td>
<td>No Fix</td>
<td>PECI RdIAMSR() Command May Fail After Core C6 State is Entered</td>
</tr>
<tr>
<td>HSX15</td>
<td>E0</td>
<td>No Fix</td>
<td>CLTT May Cause BIOS To Hang On a Subsequent Warm Reset</td>
</tr>
<tr>
<td>HSX16</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe* Extended Tag Field May be Improperly Set</td>
</tr>
<tr>
<td>HSX17</td>
<td>E0</td>
<td>No Fix</td>
<td>A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation</td>
</tr>
<tr>
<td>HSX18</td>
<td>E0</td>
<td>No Fix</td>
<td>Memory Controller tsod_present Settings Being Improperly Cleared</td>
</tr>
<tr>
<td>HSX19</td>
<td>E0</td>
<td>No Fix</td>
<td>DDR4 Power Down Timing Violation</td>
</tr>
<tr>
<td>HSX20</td>
<td>E0</td>
<td>No Fix</td>
<td>Correctable Memory ECC Errors May Occur at Boot</td>
</tr>
<tr>
<td>HSX21</td>
<td>E0</td>
<td>No Fix</td>
<td>BT Timeouts May Cause Spurious Machine Checks</td>
</tr>
<tr>
<td>HSX22</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe Type 1 VDMs May be Silently Dropped</td>
</tr>
<tr>
<td>HSX23</td>
<td>E0</td>
<td>No Fix</td>
<td>CONFIG_TDP_NOMINAL CSR Implemented at Incorrect Offset</td>
</tr>
<tr>
<td>HSX24</td>
<td>E0</td>
<td>No Fix</td>
<td>A Machine-Check Exception Due To Instruction Fetch May Be Delivered Before an Instruction Breakpoint</td>
</tr>
<tr>
<td>HSX25</td>
<td>E0</td>
<td>No Fix</td>
<td>Power Consumed During Package C6 May Exceed Specification</td>
</tr>
<tr>
<td>HSX26</td>
<td>E0</td>
<td>No Fix</td>
<td>Platform Performance Degradation When C1E is Enabled</td>
</tr>
<tr>
<td>HSX27</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe Correctable Error Status Register May Not Log Receiver Error at 8.0 GT/s</td>
</tr>
<tr>
<td>HSX28</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe Hot-Plug Slot Status Register May not Indicate Command Completed</td>
</tr>
<tr>
<td>HSX29</td>
<td>E0</td>
<td>No Fix</td>
<td>Local PCIe P2P Traffic on x4 Ports May Cause a System Hang</td>
</tr>
<tr>
<td>HSX30</td>
<td>E0</td>
<td>No Fix</td>
<td>ILLC Error Conditions May Be Dropped or Incorrectly Signaled</td>
</tr>
<tr>
<td>HSX31</td>
<td>E0</td>
<td>No Fix</td>
<td>A DDR4 C/A Parity Error in Lockstep Mode May Result in a Spurious Uncorrectable Error</td>
</tr>
<tr>
<td>HSX32</td>
<td>E0</td>
<td>No Fix</td>
<td>Some IMC and Intel QPI Functions Have Incorrect PCI CAPPTR Values</td>
</tr>
<tr>
<td>HSX33</td>
<td>E0</td>
<td>No Fix</td>
<td>PCIe TLP Translation Request Errors Are Not Properly Logged For Invalid Memory Writes</td>
</tr>
<tr>
<td>HSX34</td>
<td>E0</td>
<td>No Fix</td>
<td>Consecutive PECI RdIAMSR Commands When Core C6 is Enabled May Cause a System Hang</td>
</tr>
<tr>
<td>HSX35</td>
<td>E0</td>
<td>No Fix</td>
<td>Enabling TRR With DDR4 LRDIMMs May Lead to Unpredictable System Behavior</td>
</tr>
<tr>
<td>HSX36</td>
<td>E0</td>
<td>No Fix</td>
<td>C/A Parity Error Injection May Cause the System to Hang</td>
</tr>
<tr>
<td>HSX37</td>
<td>E0</td>
<td>No Fix</td>
<td>The System May Shut Down Unexpectedly During a Warm Reset.</td>
</tr>
</tbody>
</table>
Table 2. Errata (Sheet 2 of 2)

<table>
<thead>
<tr>
<th>Number</th>
<th>Stepping</th>
<th>Status</th>
<th>Errata</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSX38</td>
<td>X</td>
<td>No Fix</td>
<td>Patrol Scrubbing of Mirrored Memory May Log Spurious Memory Errors</td>
</tr>
<tr>
<td>HSX39</td>
<td>X</td>
<td>No Fix</td>
<td>MSR_TURBO_ACTIVATION_RATIO MSR Cannot be Locked</td>
</tr>
<tr>
<td>HSX40</td>
<td>X</td>
<td>No Fix</td>
<td>The System May Shut Down Unexpectedly During a Warm Reset</td>
</tr>
<tr>
<td>HSX41</td>
<td>X</td>
<td>No Fix</td>
<td>Invalid Intel® QuickData Technology XOR Descriptor Source Addressing May Lead to Unpredictable System Behavior</td>
</tr>
<tr>
<td>HSX42</td>
<td>X</td>
<td>No Fix</td>
<td>Warm Reset May Cause PCIe Hot-Plug Sequencing Failure</td>
</tr>
<tr>
<td>HSX43</td>
<td>X</td>
<td>No Fix</td>
<td>PCIe* UR And CA Responses May be Sent Before Link Enters LER State</td>
</tr>
<tr>
<td>HSX44</td>
<td>X</td>
<td>No Fix</td>
<td>Surprise Down Error Status is Not Set Correctly on DMI Port</td>
</tr>
<tr>
<td>HSX45</td>
<td>X</td>
<td>No Fix</td>
<td>Intel SMi2 in Half Width Mode With DDDC Enabled Will Not Report RdECC Errors</td>
</tr>
<tr>
<td>HSX46</td>
<td>X</td>
<td>No Fix</td>
<td>PCIe* SLTCON CSRs electromechanical_interlock_control Field Read as 1</td>
</tr>
<tr>
<td>HSX47</td>
<td>X</td>
<td>No Fix</td>
<td>Intel DDR3 SMi2 CAP Errors Are Ignored Leading to Unpredictable System Behavior</td>
</tr>
<tr>
<td>HSX48</td>
<td>X</td>
<td>No Fix</td>
<td>PECI RdPkgConfig Command DRAM Services May Behave Incorrectly</td>
</tr>
<tr>
<td>HSX49</td>
<td>X</td>
<td>No Fix</td>
<td>Some OFFCORE_RESPONSE Performance Monitoring Events May Undercount</td>
</tr>
<tr>
<td>HSX50</td>
<td>X</td>
<td>No Fix</td>
<td>Performance Monitoring OFFCORE_RESPONSE_(1,2) Events May Miscount</td>
</tr>
<tr>
<td>HSX51</td>
<td>X</td>
<td>No Fix</td>
<td>Certain Local Memory Read / Load Retired PerfMon Events May Undercount</td>
</tr>
<tr>
<td>HSX52</td>
<td>X</td>
<td>No Fix</td>
<td>Certain Settings of VM-Execution Controls May Result in Incorrect Linear-Address Translations</td>
</tr>
<tr>
<td>HSX53</td>
<td>X</td>
<td>No Fix</td>
<td>An IRET Instruction That Results in a Task Switch Does Not Serialize The Processor</td>
</tr>
<tr>
<td>HSX54</td>
<td>X</td>
<td>No Fix</td>
<td>A P-State or C-State Transition May Lead to a System Hang</td>
</tr>
</tbody>
</table>
Table 3. Specification Clarifications

<table>
<thead>
<tr>
<th>No.</th>
<th>Specification clarifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 4. Specification Changes

<table>
<thead>
<tr>
<th>No.</th>
<th>Specification changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 5. Documentation Changes

<table>
<thead>
<tr>
<th>No.</th>
<th>Documentation changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>
## Errata

### HSX1  Intel® QuickPath Interconnect (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.

### HSX2  PECI DDR DIMM Digital Thermal Reading Returns Incorrect Value

**Problem:** When using the PECI 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.

### HSX3  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 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. This erratum does not occur when link is operating as a PCIe* port.

**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.

### HSX4  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.

### HSX5  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.

**HSX6 A Memory Channel With More Than 4 Ranks May Lead to a System Hang**

Problem: A memory controller channel with more than 4 ranks and with TRR (Targeted Row Refresh) enabled may fail leading to a system hang. This erratum only impacts memory channels with three dual-rank DDR4 RDIMMs.

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.

**HSX7 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.

**HSX8 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.

**HSX9 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.

**HSX10 PECI Commands During Reset May Result in Persistent Timeout Response**

Problem: Due to this erratum, a PECI (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 PECI 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.

**HSX11 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.

**HSX12 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.

**HSX13 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.

**HSX14 PECI RdIAMSR() Command May Fail After Core C6 State is Entered**

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

Implication: Invalid data may be returned when using PECI 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.

**HSX15 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 subsequence warm reset attempts. The failing condition is cleared by a cold reset.

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.
HSX16  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.

HSX17  A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation
Problem: If EPT (extended page tables) is enabled, a MOV to CR3 or VMFUNC may be followed by an unexpected page fault or the use of an incorrect page translation.
Implication: Guest software may crash or experience unpredictable behavior as a result of this erratum.
Workaround: It is possible for the BIOS to contain a workaround for this erratum.
Status: For the affected steppings, see the Summary Tables of Changes.

HSX18  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.

HSX19  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: Violation of timing specifications can lead to unpredictable system behavior; however, Intel has not observed this erratum to impact the operation of any commercially available system using validated DIMMs by Intel Platform Memory Operations.
Workaround: None identified.
Status: For the affected steppings, see the Summary Tables of Changes.

HSX20  Correctable Memory ECC Errors May Occur at Boot
Problem: With memory lockstep enabled, the system may experience correctable memory errors during boot with IA32_MCI_STATUS.MCACOD= 0x009x (where x is 0,1,2, or 3 and indicates the channel number reporting the error)
Implication: The system may experience correctable memory errors.
Workaround: None identified.
Status: For the affected steppings, see the Summary Tables of Changes.

HSX21  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.

**HSX22 PCIe Type 1 VDMs May Be Silently Dropped**
Problem: Due to this erratum, a PCIe Type 1 VDMs (Vendor Defined Message) is silently dropped unless the vendor ID is the MCTP (Management Component Transport Protocol) value of 0x1AB4.
Implication: PCIe Type 1 VDMs may be unexpectedly dropped. 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.

**HSX23 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.

**HSX24 A Machine-Check Exception Due to Instruction Fetch May Be Delivered Before an Instruction Breakpoint**
Problem: Debug exceptions due to instruction breakpoints take priority over exceptions resulting 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.

**HSX25 Power Consumed During Package C6 May Exceed Specification**
Problem: Due to this erratum, the processor power usage may be higher than specified for the VCCIN and/or IIO domains while in Package C6 state.
Implication: Systems may experience increased power consumption while the processor is in Package C6.
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.

**HSX26 Platform Performance Degradation When C1E is Enabled**
Problem: Due to this erratum, when C1E is enabled and after the processor has entered Package C1E state, core clock frequency becomes limited to its minimum value (sometimes referred to as Pn) until the system exits Package C3 state (or deeper) or the system is reset.
Implication: When this erratum occurs, operating frequency will be lower than expected.
Note: After a Package C3 exit, re-entering Package C1E state re-imposes this erratum's frequency limit.

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.

HSX27 PCIe Correctable Error Status Register May Not Log Receiver Error at 8.0 GT/s

Problem: Due to this erratum, correctable PCIe receiver errors may not be logged in the DPE field (bit 15) of the PCISTR CSR (Bus: 0; Device 1,2,3; Function 0-1, 0-3, 0-3; Offset 6H) when operating at 8.0 GT/s.

Implication: Correctable receiver errors during 8.0 GT/s operation may not be visible to the OS or driver software.

Workaround: None identified.

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

HSX28 PCIe Hot-Plug Slot Status Register May Not Indicate Command Completed

Problem: The PCIe Base Specification requires a write to the Slot Control register (Offset A8H) to generate a hot plug command when the downstream port is hot plug capable. Due to this erratum, a hot plug command is generated only when one or more of the Slot Control register bits [11:6] are changed.

Implication: Writes to the Slot Control register that leave bits [11:6] unchanged will not generate a hot plug command and will therefore not generate a command completed event. Software that expects a command completed event may not behave as expected.

Workaround: It is possible for software to implement a one-second timeout in lieu of receiving a command completed event.

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

HSX29 Local PCIe P2P Traffic on x4 Ports May Cause a System Hang

Problem: Under certain conditions, P2P (Peer-to-Peer) traffic with x4 PCIe ports on the same processor (i.e., local) may cause a system hang.

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

Workaround: None identified. Local P2P traffic should not be used to or from x4 PCIe ports.

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

HSX30 ILLC Error Conditions May be Dropped or Incorrectly Signaled

Problem: When two LLC (last level cache) errors happen in close proximity, a UCNA (uncorrectable no action required) machine check may be dropped or a spurious machine check or CMCI (Corrected Machine Check Interrupt) may be issued. Further, when this erratum occurs, the merged CBo LLC machine check bank IA32_MC[17-19]_STATUS MSRs may be incorrect.

Implication: IA32_MC[17-19]_STATUS MSR may not reflect most current error.

Workaround: It is possible for the BIOS to contain a partial workaround for this erratum. The workaround does not address the potential dropped UCNA machine check.

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

HSX31 A DDR4 C/A Parity Error in Lockstep Mode May Result in a Spurious Uncorrectable Error

Problem: If a memory C/A (Command/Address) parity error occurs while the memory subsystem is configured in lockstep mode then the channel that observed the error will properly
log the error but the associated channel in lockstep will incorrectly log an uncorrectable error in its IA32_MCi_STATUS MSR.

**Implication:** Due to this erratum, incorrect logging of an uncorrectable memory error in IA32_MCi_STATUS may occur.

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

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

---

**HSX32** Some IMC and Intel QPI Functions Have Incorrect PCI CAPPTR Values

**Problem:** The PCI CAPPTR (Capability Pointer Register) is defined to contain the offset to the capabilities list structure when the PCI PCISTS (PCI Status Register) bit 4 (Capabilities_List) is set to 1. Due to this erratum, CAPPTR (offset 0x34) should hold a value of 0x40 but is instead zero for these IMC (Integrated Memory Controller) and Intel® QPI (QuickPath Interconnect) device:

- Device 8, functions 3,5,6
- Device 9, functions 3,5,6
- Device 10, functions 3,5,6
- Device 19, functions 0-5
- Device 20, functions 0-3
- Device 21, functions 0-3
- Device 22, functions 0-3
- Device 23, functions 0-3

**Implication:** Software that depends on CAPPTR to access additional capabilities may not behave as expected.

**Workaround:** Software that needs to access these capabilities must take this erratum into account.

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

---

**HSX33** PCIe TLP Translation Request Errors Are Not Properly Logged For Invalid Memory Writes

**Problem:** A PCIe Memory Write TLP (Transaction Layer Packet) with an AT field value of 01b (address translation request) does not set the UR (Unsupported Request) bit (UNCERRSTS CSR, Bus 0; Device 0; Function 0; Offset 0x14C; Bit 20) as required by the PCIe Base Specification.

**Implication:** System or software monitoring error status bits may not be notified of an unsupported request. When this erratum occurs, the processor sets the 'advisory_non_fatal_error_status' bit (CORERRSTS CSR, Bus 0; Device 0; Function 0; Offset 0x158; Bit 13) and drops the failing transaction.

**Workaround:** None identified.

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

---

**HSX34** Consecutive PECI RdIAMSR Commands When Core C6 is Enabled May Cause a System Hang

**Problem:** Consecutive PECI (Platform Environment Control Interface) RdIAMSR commands to access core Machine Check MSRs can result in a system hang when core C6 state is enabled.

**Implication:** When this erratum occurs, PECI commands can lead to 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.

**HSX35 Enabling TRR With DDR4 LRDIMMs May Lead to Unpredictable System Behavior**

Problem: Due to this erratum, TRR (Targeted Row Refresh) is not compatible with DDR4 LRDIMMs.
Implication: Unpredictable system behavior may occur.
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.

**HSX36 C/A Parity Error Injection May Cause the System to Hang**

Problem: When C/A (Command Address) parity error injections are occurring too frequently, the home agent may be prevented from completing memory transactions. This may result in an internal timer error indicated by IA32_MCI_STATUS. MSCOD=0x0080 and IA32_MCI_STATUS. MCACOD=0x0400.
Implication: Due to this erratum, the system may hang.
Workaround: Ensure there is at least 30 µs of delay between injections.
Status: For the affected steppings, see the Summary Tables of Changes.

**HSX37 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.

**HSX38 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 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.

**HSX39 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.

**HSX40 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.

**HSX41  Invalid Intel® QuickData Technology XOR Descriptor Source Addressing May Lead to Unpredictable System Behavior**

Problem: Intel® QuickData Technology (i.e. Crystal Beach DMA v3.2) does not correctly halt and report aborts on illegal source addresses placed in a CBDMA descriptor regardless of type (Legacy or PQ). This abort condition may cause unpredictable system behavior.

Implication: This erratum may lead to unpredictable system behavior.
Workaround: Ensure XOR DMA descriptor source addresses targets valid DRAM memory locations.
Status: For the affected steppings, see the Summary Tables of Changes.

**HSX42  Warm Reset May Cause PCIe Hot-Plug Sequencing Failure**

Problem: The Integrated I/O unit uses the VPP (Virtual Pin Port) to communicate with power controllers, switches, and LEDs associated with PCIe Hot-Plug sequencing. Due to this erratum, a warm reset occurring when a VPP transaction is in progress may result in an extended VPP stall, termination of the in-flight VPP transaction, or a transient power down of slots subject to VPP power control.

Implication: During or shortly after a warm reset, when this erratum occurs, PCIe Hot-Plug sequencing may experience transient or persistent failures or slots may experience unexpected transient power down events. In certain instances, a cold reset may be needed to fully restore operation.
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.

**HSX43  PCIe* UR And CA Responses May be Sent Before Link Enters LER State**

Problem: Completions with UR (Uncorrectable Response) and CA (Completer Abort) status should trigger LER (Live Error Recovery). Further, these packets should be dropped upon entering LER. Due to this erratum, these completions may not be dropped when LER is triggered.

Implication: Since these packets contain no data, there is no loss of error containment. These packets will trigger LER mode; the link will be disabled.
Workaround: None identified.
Status: None identified.

**HSX44  Surprise Down Error Status is Not Set Correctly on DMI Port**

Problem: Due to this erratum, the Surprise_down_error_status (UNCERRSTS Device0; Function); Offset 0x14C; bit5) is not set to 1 when DMI port detects a surprise down error.

Implication: Surprise down errors will not be logged for the DMI port. This violates the PCIe* Base Specification. Software that relies on this status bit may not behave as expected.
Workaround: None identified.
Status: For the affected steppings, see the Summary Tables of Changes.

**HSX45  Intel SMI2 in Half Width Mode With DDDC Enabled Will Not Report RdECC Errors**

Problem: When a RdECC error occurs on an Intel SMI2 channel operating at a 1:1 ratio half-width mode and DDDC (Dual Device Data Correction) enabled, the error logging in the Intel® C102/104/112/114 Scalable Memory Buffer and the processor is not properly coordinated.
Implication: Although the error flow is correct, error isolation may be affected because the processor may log a RdECC error while the Intel C102/104/112/114 Scalable Memory Buffer does not log an error.

Workaround: None identified.

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

**HSX46 PCIe* SLTCON CSRs electromechanical_interlock_control Field Read as 1**

**Problem:**
The PCI Express Base Specification rev 3.1 requires that the SLTCON (Bus 0;Device 3-0;Function 3-0;Offset 0xA8) CSRs' electromechanical_interlock_control (bit 11) "always returns aa 0 when read". Due to this erratum, a read of this bit returns the last value written.

**Implication:** Software expecting a value of 0 may not function as expected. Intel has not observed this erratum to impact the operation of any commercially available software.

**Workaround:** Software should ignore read values returned from this register field.

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

**HSX47 Intel DDR3 SMI2 CAP Errors Are Ignored Leading to Unpredictable System Behavior**

**Problem:**
An Intel SMI2 DDR3 CAP (Command Address Parity) error, rather than initiating a mirroring event as expected, is ignored leading to unpredictable system behavior.

**Implication:** When this erratum occurs, it may lead to unpredictable system behavior. Note that this behavior does not affect DDR4 memory subsystems.

**Workaround:** It is possible for BIOS to contain processor configuration data and code changes as a workaround for this erratum.

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

**HSX48 PECI RdPkgConfig Command DRAM Services May Behave Incorrectly**

**Problem:**
The PECI (Platform Environment Control Interface) RdPkgConfig command may return incorrect results when accessing the DRAM Thermal Interface (indices 14 and 22).

**Implication:** Thermal monitoring and control using PECI may not behave as expected.

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

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

**HSX49 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 STREAMINGSTORES (bit 15) 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 stepings, see the Summary Tables of Changes.

**HSX50 Performance Monitoring OFFCORE_RESPONSE_{1,2} Events May Miscount L3_MISS_REMOTE_HOP**

**Problem:**
When a Performance Monitoring counter is configured to count OFF_CORE_RESPONSE_{1,2} (Events B7H and B8H), data obtained for remote DRAM
may be attributed to L3_MISS_REMOTE_HOP0 (as programmed by MSR_OFFCORE_RSP_{1,2} (MSRs 1A6H, 1A7H) bit 27) instead of L3_MISS_REMOTE_HOP1 (bit 28) or L3_MISS_REMOTE_HOP2P (bit 29). Data provided from remote caching agent associated with remote DRAM is unaffected.

Implication: L3_MISS_REMOTE_HOP0 may over count, while L3_MISS_REMOTE_HOP1 and L3_MISS_REMOTE_HOP2P may undercount.

Workaround: None identified. Set all three configuration bits (L3_MISS_REMOTE_HOP0, L3_MISS_REMOTE_HOP1, L3_MISS_REMOTE_HOP2P) to obtain the total count of data supplied by remote agents.

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

HSX51 Certain Local Memory Read / Load Retired PerfMon Events May Undercount

Problem: Due to this erratum, the Local Memory Read / Load Retired PerfMon events listed below may undercount.
MEM_LOAD_UOPS_RETIRED.L3_HIT (Event D1H Umask 04H)
MEM_LOAD_UOPS_RETIRED.L3_MISS (Event D1H Umask 20H)
MEM_LOAD_UOPS_L3_HIT_RETIRED.XSNP_MISS (Event D2H Umask 01H)
MEM_LOAD_UOPS_L3_HIT_RETIRED.XSNP_HIT (Event D2H Umask 02H)
MEM_LOAD_UOPS_L3_HIT_RETIRED.XSNP_HITM (Event D2H Umask 04H)
MEM_LOAD_UOPS_L3_HIT_RETIRED.XSNP_NONE (Event D2H Umask 08H)
MEM_LOAD_UOPS_L3_MISS_RETIRED.LOCAL_DRAM (Event D3H Umask 01H)
MEM_TRANS_RETIRED.LOAD_LATENCY (Event CDH Umask 01H)
PAGE_WALKER_LOADS.DTLB_L3 (Event BCH Umask 14H)
PAGE_WALKER_LOADS.ITLB_L3 (Event BCH Umask 24H)
PAGE_WALKER_LOADS.DTLB_Memory (Event BCH Umask 18H)
PAGE_WALKER_LOADS.ITLB_Memory (Event BCH Umask 28H)

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

Workaround: None identified.

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

HSX52 Certain Settings of VM-Execution Controls May Result in Incorrect Linear-Address Translations

Problem: If VM exit occurs from a guest with primary processor-based VM-execution control “activate secondary controls” set to 0 and the secondary processor-based VM-execution control “enable VPID” set to 1, then after a later VM entry with VPID fully enabled (“activate secondary controls” and “enable VPID” set to 1), the processor may use stale linear address translations.

Implication: The processor may incorrectly translate linear addresses. Intel has not observed this erratum with any commercially available software.

Workaround: Software should not enter a guest with “enable VPID” set to 1 when “activate secondary controls” is set to 0.

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

HSX53 An IRET Instruction That Results in a Task Switch Does Not Serialize The Processor

Problem: An IRET instruction that results in a task switch by returning from a nested task does not serialize the processor (contrary to the Software Developer’s Manual Vol. 3 section titled “Serializing Instructions”).
Implication: Software which depends on the serialization property of IRET during task switching may not behave as expected. Intel has not observed this erratum to impact the operation of any commercially available software.

Workaround: None identified. Software can execute an MFENCE instruction immediately prior to the IRET instruction if serialization is needed.

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

**HSX54 A P-State or C-State Transition May Lead to a System Hang**

Problem: For a small subset of parts under elevated die temperature conditions, a P-state or C-state transition may result in a system timeout or system shutdown.

Implication: When this erratum occurs, the system may shutdown or report a timeout error; Intel has observed transaction completion timeouts and other internal timeouts.

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.
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.

§