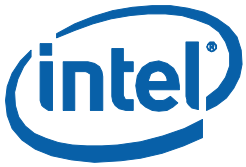


Intel® Celeron® and Pentium® Processor N- and J- Series

Specification Update

March 2014

Revision 006

Document Number: 329671

Contents

Figures

Tables

§

Revision History

Document Number	Revision Number	Description	Date
329671	001	• Initial Release	October 2013
329671	003	• Revision 002 skipped to align with current release • Added B3 to Table 1 stepping ID • Added 8 Refresh Sku detail to Table 2 • Removal of CSI Erratum (was VLP7) • Added Gen2 to VLP6 content • Newly added Errata VLP34 to VLP46 • Added Errata VLP48-VLP53 • Added Erratum VLP54	January 2014
329671	004	• Updated Errata status to 'Plan Fix'	February 2014
329671	004 v2	• Minor corrections to 004 release	February 2014
329671	005	• Added Errata VLP55 – VLP59 • Removed Q-Spec SKUs from Table 2	March 2014
329671	006	• Updated Table 2, "Identification Table for Intel® Celeron® and Pentium® Processor N- and J- Series" • Added C0 Stepping to the Errata Summary Table	March 2014

§

1 Preface

This document contains specification updates for Intel® Celeron® and Pentium® Processor N- and J- Series. It is intended for hardware system manufacturers and software developers. It contains:

- Device Errata
- Document Errata
- Specification clarifications
- Specification changes

Note: Information types defined in the Nomenclature section of this document are consolidated and are no longer published in other documents. Refer to the section Summary Table of Changes for more information.

1.1 Affected Documents

Document Title	Document Number
Intel® Pentium® Processor N3520, J2850 & Intel® Celeron® Processor N2920, N2820, N2815, N2806, J1850, J1750 Datasheet	329670

1.2 Related Documents

Document Title	Document Number/ Location
Intel® 64 and IA-32 Architectures Software Developer's Manuals: • Volume 1: Basic Architecture • Volume 2A: Instruction Set Reference, A-M • Volume 2B: Instruction Set Reference, N-Z • Volume 3A: System Programming Guide • Volume 3B: System Programming Guide	http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html
IA-32 Intel® Architectures Optimization Reference Manual	248966
Intel® Processor Identification and the CPUID Instruction Application Note (AP-485)	241618
Intel® 64 and IA-32 Architectures Application Note TLBs, Paging-Structure Caches, and Their Invalidation	317080

1.3 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, for example, 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.).

§

2 Identification Information

Intel® Celeron® and Pentium® Processor N- and J- Series on 22-nm process stepping can be identified by the following register contents:

Table 1. Component Identification using Programming Interface

Reserved	Extended Family[1]	Extended Model[2]	Reserved	Processor Type[3]	Family Code[4]	Model Number[5]	Stepping ID[6]
31:28	27:20	19:16	15:13	12	11:8	7:4	3:0
0000b	0000000b	0011b	000b	0b	0110b	0111b	B1: 0010b B2/B3: 0011b

NOTES:

1. The Extended Family, bits [27:20] are used in conjunction with the Family Code, specified in bits [11:8], to indicate whether the processor belongs to the Intel386®, Intel486®, Pentium®, Pentium Pro, Pentium 4, or Intel Core processor family.
2. The Extended Model, bits [19:16] in conjunction with the Model Number, specified in bits [7:4], are used to identify the model of the processor within the processor's family.
3. The Processor Type, specified in bits [13:12] indicates whether the processor is an original OEM processor, an OverDrive processor, or a dual processor (capable of being used in a dual processor system).
4. 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 1 in the EAX register, and the generation field of the Device ID register, accessible through Boundary Scan.
5. 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 1 in the EAX register, and the model field of the Device ID register, accessible through Boundary Scan.
6. The Stepping ID in bits [3:0] indicates the revision number of that model. See Table 2 for the processor stepping ID number in the CPUID information.

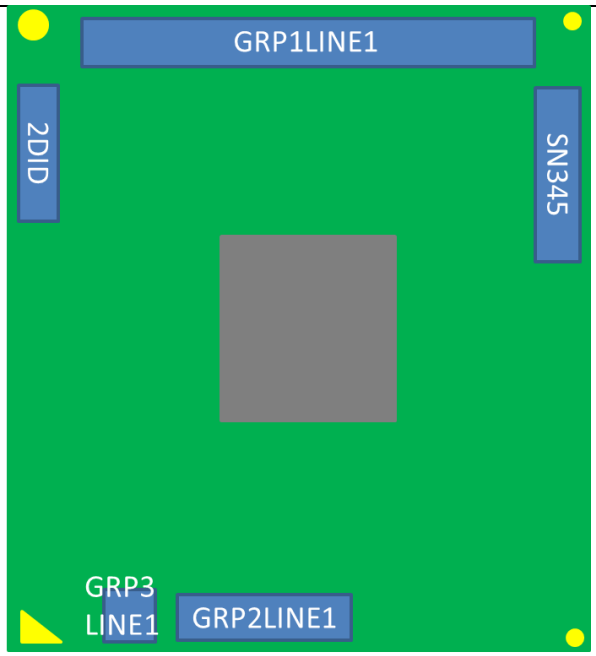
When EAX is initialized to a value of 1, the CPUID instruction returns the Extended Family, Extended Model, Type, Family, Model and Stepping value in the EAX register.

Note: The EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

2.1 Component Marking Information

Intel® Celeron® and Pentium® Processor N- and J- Series are identified by the following component markings.

Figure 1. Intel® Celeron® and Pentium® Processor N- and J- Series (Micro-FCBGA13) Markings



SAMPLE MARKING INFORMATION:
GRP1LINE1: i{M}{C}YY_FPO12345
GRP2LINE1: QDF / SSPEC
GRP3LINE1: {e1}

Table 2. Identification Table for Intel® Celeron® and Pentium® Processor N- and J-Series

S-Spec	MM#	Product Stepping	Processor Number	CPUID	Core Speed		Package	Cache Size (KB)
					Highest Freq. Mode (HFM)/ GHz	Lowest Freq. Mode (LFM)/ MHz		
SR1LM	931090	B2	J2850	00030673	2.41	1333	Micro-FCBGA13	2 x1024

S-Spec	MM#	Product Stepping	Processor Number	CPUID	Core Speed		Package	Cache Size (KB)
					Highest Freq. Mode (HFM)/ GHz	Lowest Freq. Mode (LFM)/ MHz		
SR1LN	931092	B2	J1850	00030673	2.0	500	Micro-FCBGA13	2 x1024
SR1LP	931094	B2	J1750	00030673	2.41	500	Micro-FCBGA13	1s x1024
SR1LV	931112	B2	N3510	00030673	2	500	Micro-FCBGA13	2 x1024
SR1LW	931114	B2	N2810	00030673	2	533	Micro-FCBGA13	1 x1024
SR1LX	931116	B2	N2805	00030673	1.46	533	Micro-FCBGA13	1 x1024
SR1LY	931118	B2	N2910	00030673	1.6	533	Micro-FCBGA13	2 x1024
SR1SE	932485	B3	N3520	00030673	2.17/2.42 (B)	500	Micro-FCBGA13	2 x1024
SR1SF	932490	B3	N2920	00030673	1.86/2.00 (B)	532	Micro-FCBGA13	2 x1024
SR1SG	932492	B3	N2820	00030673	2.13/2.39 (B)	532	Micro-FCBGA13	1 x1024
SR1SH	932494	B3	N2806	00030673	1.6/2.00 (B)	532	Micro-FCBGA13	1 x1024
SR1SJ	932579	B3	N2815	00030673	1.86/2.13 (B)	532	Micro-FCBGA13	1 x1024
SR1SB	932479	B3	J2900	00030673	2.41/2.67 (B)	1333	Micro-FCBGA13	2 x1024
SR1SC	932481	B3	J1900	00030673	2.0/2.42 (B)	1333	Micro-FCBGA13	2 x1024
SR1SD	932483	B3	J1800	00030673	2.41/2.58 (B)	1333	Micro-FCBGA13	1 x1024
SR1W2	934895	C0	N3530	30678	2.17/2.58 (B)	1333	Micro-FCBGA13	2 x1024
SR1W3	934896	C0	N2930	30678	1.83/2.17 (B)	1333	Micro-FCBGA13	2 x1024
SR1W4	934897	C0	N2830	30678	2.17/2.42 (B)	1333	Micro-FCBGA13	1 x1024
SR1W5	934898	C0	N2807	30678	1.58/2.17 (B)	1333	Micro-FCBGA13	1 x1024

Note: 'B' is the Burst Technology feature which included to the Refresh sku. §

§

3 Summary Table of Changes

The table included in this section indicates the sightings that apply to the Intel® Celeron® and Pentium® Processor N- and J- Series. If a sighting becomes an Erratum, 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. This table uses the following notations:

3.1 Codes Used in Summary Table

3.2 Stepping

X: This sighting applies to this stepping.

Blank (No mark): This sighting is fixed or does not exist in the listed stepping.

3.3 Status

Doc: Document change or update will be implemented.

Plan Fix: Root caused to a silicon issue and will be fixed in a future stepping.

Fixed: Root caused to a silicon issue and has been fixed in a subsequent stepping.

No Fix: Root caused to a silicon issue that will not be fixed.

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

Note: 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 for details.

Number	Status	Affected Stepping			Sighting Description
		B2	B3	C0	
VLP1	No Fix	X	X	X	GPIO Registers Do Not Support 8 or 16-Bit Transactions
VLP2	No Fix	X	X	X	Quad Word Transactions in Violation of Programming Model May Result in Hang
VLP3	No Fix	X	X	X	SoC PCIe LTSSM May Not Enter Detect Within 20 ms
VLP4	No Fix	X	X	X	LFPS Detect Threshold

Number	Status	Affected Stepping			Sighting Description
		B2	B3	C0	
VLP5	No Fix	X	X	X	Set Latency Tolerance Value Command Completion Event Issue
VLP6	No Fix	X	X	X	SATA Signal Voltage Level Violation
VLP8	Plan Fix	X	X	X	Anomalies in USB xHCI PME Enable and PME Status
VLP9	No Fix	X	X	X	xHCI Port Assigned Highest SlotID When Resuming From Sx Issue
VLP10	No Fix	X	X	X	xHCI Data Packet Header and Payload Mismatch Error Condition
VLP11	No Fix	X	X	X	USB xHCI SuperSpeed Packet with Invalid Type Field Issue
VLP12	No Fix	X	X	X	USB xHCI Behavior with Three Consecutive Failed U3 Entry Attempts
VLP13	No Fix	X	X	X	USB xHCI Max Packet Size and Transfer Descriptor Length Mismatch
VLP14	No Fix	X	X	X	PCIe Root Ports Unsupported Request Completion
VLP15	No Fix	X	X	X	USB EHCI RMH Port Disabled Due to Device Initiated Remote Wake
VLP16	No Fix	X	X	X	SMBus Hold Time
VLP17	No Fix	X	X	X	USB EHCI Isoch In Transfer Error Issue
VLP18	No Fix	X	X	X	USB EHCI Babble Detected with SW Overscheduling
VLP19	No Fix	X	X	X	USB EHCI Full-/low-speed EOP Issue
VLP20	No Fix	X	X	X	USB EHCI Asynchronous Retries Prioritized Over Periodic Transfers
VLP21	No Fix	X	X	X	USB EHCI FS/LS Incorrect Number of Retries
VLP22	No Fix	X	X	X	USB EHCI Full-/Low-speed Port Reset or Clear TT Buffer Request
VLP23	No Fix	X	X	X	USB EHCI RMH Think Time Issue
VLP24	No Fix	X	X	X	USB EHCI Full-/low-speed Device Removal Issue
VLP25	No Fix	X	X	X	Reported Memory Type May Not Be Used to Access the VMCS and Referenced Data Structures
VLP26	No Fix	X	X	X	A Page Fault May Not be Generated When the PS Bit is set to "1" in a PML4E or PDPTE
VLP27	No Fix	X	X	X	CS Limit Violations May Not be Detected After VM Entry
VLP28	No Fix	X	X	X	IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI
VLP29	No Fix	X	X	X	PEBS Record EventingIP Field May be Incorrect After CS.Base Change
VLP30	No Fix	X	X	X	Some Performance Counter Overflows May Not be Logged in IA32_PERF_GLOBAL_STATUS When FREEZE_PERFMON_ON_PMI is Enabled
VLP31	No Fix	X	X	X	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions

Number	Status	Affected Stepping			Sighting Description
		B2	B3	C0	
VLP32	No Fix	X	X	X	Performance Monitor Instructions Retired Event May Not Count Consistently
VLP33	No Fix	X	X	X	Unsynchronized Cross-Modifying Code Operations Can Cause Unexpected Instruction Execution Results
VLP34	No Fix	X	X	X	USB HSIC Ports Incorrectly Reported as Removable
VLP35	No Fix	X	X	X	Paging Structure Entry May be Used Before Accessed And Dirty Flags Are Updated
VLP36	No Fix	X	X	X	VGA Max Luminance Voltage May Exceed VESA Limits
VLP37	No Fix	X	X	X	Certain eMMC Host Controller Registers Are Not Cleared by Software Reset
VLP38	No Fix	X	X	X	SD Host Controller Incorrectly Reports Supporting of Suspend/ Resume Feature
VLP39	No Fix	X	X	X	SD Host Controller Error Status Registers May be Incorrectly Set
VLP40	No Fix	X	X	X	SD Host Controller Registers Are Not Cleared by Software Reset
VLP41	No Fix	X	X	X	eMMC Asynchronous Abort May Cause a Hang
VLP42	No Fix	X	X	X	Timing Specification Violation on SD Card Interface
VLP43	No Fix	X	X	X	SD Card Controller Does Not Disable Clock During Card Power Down
VLP44	No Fix	X	X	X	Reset Sequence May Take longer Than Expected When ACG is Enabled in SD And SDIO Controllers
VLP45	No Fix	X	X	X	SDIO Host Controller Does Not Control the SDIO Bus Power
VLP46	No Fix	X	X	X	Premature Asynchronous Interrupt Enabling May Lead to Loss of SDIO WiFi Functionality
VLP47	No Fix	X	X	X	MTF VM Exit May be Delayed Following a VM Entry That Injects a Software Interrupt
VLP48	No Fix	X	X	X	LBR Stack And Performance Counter Freeze on PMI May Not Function Correctly
VLP49	No Fix	X	X	X	USB Legacy Support SMI Not Available from xHCI Controller
VLP50	No Fix	X	X	X	SD Card UHS-I Mode is Not Fully Supported
VLP51	No Fix	X	X	X	HD Audio Recording And Playback May Glitch or Stop
VLP52	No Fix	X	X	X	EOI Transactions May Not be Sent if Software Enters Core C6 During an Interrupt Service Routine
VLP53	No Fix	X	X	X	USB xHCI May Execute a Stale Transfer Request Block (TRB)
VLP54	No Fix	X	X	X	Frequency Reported by CPUID Instruction May Not Match Published Frequency
VLP55	No Fix	X	X	X	Reset Sequence May Not Complete Under Certain Conditions
VLP56	No Fix	X	X	X	Multiple Drivers That Access the GPIO Registers Concurrently May Result in Unpredictable System Behavior

Number	Status	Affected Stepping			Sighting Description
		B2	B3	C0	
VLP57	No Fix	X	X	X	Boot May Not Complete When SMI Occurs during Boot
VLP58	No Fix	X	X	X	Interrupts That Target an APIC That is Being Disabled May Result in a System Hang
VLP59	No Fix	X	X	X	Corrected or Uncorrected L2 Cache Machine Check Errors May Log Incorrect Address in IA32_MCi_ADDR

Number	Specification Clarifications
	There are no Specification Clarifications in this revision of the specification Update

Number	Documentation Changes
	There are no Document Changes in this revision of the specification Update

§

4 Errata

VLP1 GPIO Registers Do Not Support 8 or 16 Bit Transactions

Problem: Due to this erratum, only aligned DWord accesses to GPIO registers function correctly. This erratum applies to GPIO registers whether in MMIO space or IO space.

Implication: GPIO register transactions using byte or word accesses or unaligned DWord accesses will not work correctly.

Workaround: Always use aligned 32 Bit transactions when accessing GPIO registers.

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

VLP2 Quad Word Transactions in Violation of Programming Model May Result in System Hang

Problem: Quad word (64 Bit data) transactions to access two adjacent 32 Bit registers of SoC internal devices that do not support such transactions may cause system hang.

Implication: Due to this erratum, violations of a device programming model may result in a hang instead of a fatal Target Abort / Completer Abort error. Software written in compliance to correct programming model will not be affected.

Workaround: Software must be written and compiled in compliance to correct programming model.

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

VLP3 SoC PCIe LTSSM May Not Enter Detect Within 20 ms

Problem: The PCIe specification requires the LTSSM (Link Training and Status State Machine) to enter Detect within 20 ms of the end of Fundamental Reset. Due to this erratum, the SoC may violate this specification.

Implication: Intel has not observed this erratum to impact operation of any commercially available add-in card.

Workaround: None identified.

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

VLP4 LFPS Detect Threshold

Problem: The USB 3.0 host and device controllers' LFPS (Low Frequency Periodic Signal) detect threshold is higher than the USB 3.0 specification maximum of 300 mV.

Implication: The USB 3.0 host and device controllers may not recognize LFPS from SuperSpeed devices transmitting at the minimum low power peak-to-peak differential voltage (400 mV) as defined by USB 3.0 specification for the optional capability for Low-Power swing mode. Intel has not observed this erratum to impact the operation of any commercially available system.

Workaround: None identified.

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

VLP5 Set Latency Tolerance Value Command Completion Event Issue

Problem: The xHCI controller does not return a value of '0' for slot ID in the command completion event TRB (Transfer Request Block) for a set latency tolerance value command.

Note: This violates the command completion event TRB description in section 6.4.2.2 of the extensible Host Controller Interface for Universal Serial Bus (xHCI) specification, revision 1.0.

Implication: There are no known functional failures due to this issue.

Note: Set latency tolerance value command is specific to the controller and not the slot. Software knows which command was issued and which fields are valid to check for the event.

Note: xHCI CV compliance test suite: Test TD4.10: Set Latency Tolerance Value Command Test may issue a warning.

Workaround: None identified.

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

VLP6 SATA Signal Voltage Level Violation

Problem: SATA transmit buffers have been designed to maximize performance and robustness over a variety of routing scenarios. As a result, the SATA transmit signaling voltage levels may exceed the maximum motherboard TX connector and device RX connector voltage specifications as defined in section 7.2.2.3 of the Serial ATA specification, rev 3.1. This issue applies to Gen 1 (1.5 Gb/s) and Gen 2 (3Gb/s).

Implication: None known.

Workaround: None identified.

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

VLP8 Anomalies in USB xHCI PME Enable and PME Status

Problem: The PME_En (Bit 8) and PME_Status (Bit 15) in xHCI's PCI PMCSR (Bus 0, Device 20, Function 0, Offset 0x74) do not comply with the PCI specification.

Implication: If a standard bus driver model for this register is applied, wake issues and system slowness may happen.

Workaround: None identified

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

VLP9 xHCI Port Assigned Highest SlotID When Resuming from Sx Issue

Problem: If a device is attached while the platform is in S3 or S4 and the device is assigned the highest assignable Slot ID upon resume, the xHCI may attempt to access an unassigned main memory address.

Implication: Accessing unassigned main memory address may cause a system software timeout leading to possible system hang.

Workaround: System SW can detect the timeout and perform a host controller reset prior to avoid a system hang.

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

VLP10 xHCI Data Packet Header and Payload Mismatch Error Condition

Problem: If a SuperSpeed device sends a DPH (Data Packet Header) to the xHCI with a data length field that specifies less data than is actually sent in the RSM (Data Packet Payload), the xHCI will accept the packet instead of discarding the packet as invalid.

Note: The USB 3.0 specification requires a device to send a DPP matching the amount of data specified by the DPH.

Implication: The amount of data specified in the DPH will be accepted by the xHCI and the remaining data will be discarded and may result in anomalous system behavior.

Note: This issue has only been observed in a synthetic test environment with a synthetic device.

Workaround: None identified

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

VLP11 USB xHCI SuperSpeed Packet with Invalid Type Field Issue

Problem: If the encoding for the "type" field for a SuperSpeed packet is set to a reserved value and the encoding for the "subtype" field is set to "ACK", the xHCI may accept the packet as a valid acknowledgement transaction packet instead of ignoring the packet.

Note: The USB 3.0 specification requires that a device never set any defined fields to reserved values.

Implication: System implication is dependent on the misbehaving device and may result in anomalous system behavior.

Note: This issue has only been observed in a synthetic test environment with a synthetic device.

Workaround: None identified

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

VLP12 USB xHCI Behavior with Three Consecutive Failed U3 Entry Attempts

Problem: The xHCI does not transition to the SS.Inactive USB 3.0 LTSSM (Link Training and Status State Machine) state after a SuperSpeed device fails to enter U3 upon three consecutive attempts.

Note: The USB 3.0 specification requires a SuperSpeed device to enter U3 when directed.

Implication: The xHCI will continue to try to initiate U3. The implication is driver and operating system dependent.

Workaround: None identified.

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

VLP13 USB xHCI Max Packet Size and Transfer Descriptor Length Mismatch

Problem: The xHCI may incorrectly handle a request from a low-speed or full-speed device when all the following conditions are true:

- The sum of the packet fragments equals the length specified by the TD (Transfer Descriptor)
- The TD length is less than the MPS (Max Packet Size) for the device
- The last packet received in the transfer is "0" or babble bytes

Implication: The xHCI will halt the endpoint if all the above conditions are met. All functions associated with the endpoint will stop functioning until the device is unplugged and reinserted.

Workaround: None identified

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

VLP14 PCIe Root Ports Unsupported Request Completion

Problem: The PCIe root ports may return an Unsupported Request (UR) completion with an incorrect lower address field in response to a memory read if any of the following occur:

- Bus Master Enable is disabled in the PCIe Root Port's Command register (PCICMD Bit 2 =0)
- Address Type (AT) field of the Transaction Layer Packet (TLP) header is non-zero
- The requested upstream address falls within the memory range claimed by the secondary side of the bridge
- Requester ID with Bus Number of 0

Implication: The UR Completion with an incorrect lower address field may be handled as a Malformed TLP causing the Requestor to send an ERR_NONFATAL or ERR_FATAL message.

Workaround: None identified.

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

VLP15 USB EHCI RMH Port Disabled Due to Device Initiated Remote Wake

Problem: During resume from Global Suspend, the RMH controller may not send SOF soon enough to prevent a device from entering suspend again. A collision on the port may occur if a device initiated remote wake occurs before the RMH controller sends SOF.

Note: Intel has only observed this issue when two USB devices on the same RMH controller send remote wake within 30 ms window while RMH controller is resuming from Global Suspend

Implication: The RMH host controller may detect the collision as babble and disable the port.

Workaround: Intel recommends system software to check Bit 3 (Port Enable/Disable Change) together with Bit 7 (Suspend) of Port N Status and Control PORTC registers when determining which port(s) have initiated remote wake. Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP16 SMBus Hold Time

Problem: The SMBus data hold time may be less than the 300 ns minimum defined by the Bay Trail-D/M SoC (System On Chip) External Design Specification (EDS).

Implication: There are no known functional failures due to this issue.

Workaround: None identified

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

VLP17 USB EHCI Isoch in Transfer Error Issue

Problem: If a USB full-speed inbound isochronous transaction with a packet length 190 bytes or greater is started near the end of a microframe the SoC may see more than 189 bytes in the next microframe.

Implication: If the SoC sees more than 189 bytes for a microframe an error will be sent to software and the isochronous transfer will be lost. If a single data packet is lost no perceptible impact for the end user is expected.

NOTES: Intel has only observed the issue in a synthetic test environment where precise control of packet scheduling is available, and has not observed this failure in its compatibility validation testing.

- Isochronous traffic is periodic and cannot be retried thus it is considered good practice for software to schedule isochronous transactions to start at the beginning of a microframe. Known software solutions follow this practice.
- To sensitize the system to the issue additional traffic such as other isochronous transactions or retries of asynchronous transactions would be required to push the inbound isochronous transaction to the end of the microframe.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP18 USB EHCI Babble Detected with SW Overscheduling

Problem: If software violates USB periodic scheduling rules for full-speed isochronous traffic by overscheduling, the RMH may not handle the error condition properly and return a completion split with more data than the length expected.

Implication: If the RMH returns more data than expected, the endpoint will detect packet babble for that transaction and the packet will be dropped. Since overscheduling occurred to create the error condition, the packet would be dropped regardless of RMH behavior. If a single isochronous data packet is lost, no perceptible impact to the end user is expected.

Note: USB software overscheduling occurs when the amount of data scheduled for a microframe exceeds the maximum budget. This is an error condition that violates the USB periodic scheduling rule.

Note: This failure has only been recreated synthetically with USB software intentionally overscheduling traffic to hit the error condition.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP19 USB EHCI Full-/Low-Speed EOP Issue

Problem: If the EOP of the last packet in a USB Isochronous split transaction (Transaction >189 bytes) is dropped or delayed 3 ms or longer the following may occur:

- If there are no other pending low-speed or full-speed transactions the RMH will not send SOF, or Keep-Alive. Devices connected to the RMH will interpret this condition as idle and will enter suspend.
- If there is other pending low-speed or full-speed transactions, the RMH will drop the isochronous transaction and resume normal operation.

Implication: If there are no other transactions pending, the RMH is unaware a device has entered suspend and may start sending a transaction without waking the device. The implication is device dependent, but a device may stall and require a reset to resume functionality. If there are other transactions present, only the initial isochronous transaction may be lost. The loss of a single isochronous transaction may not result in end user perceptible impact.

Note: Intel has only observed this failure when using software that does not comply with the USB specification and violates the hardware isochronous scheduling threshold by terminating transactions that are already in progress

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP20 USB EHCI Asynchronous Retries Prioritized Over Periodic Transfers

Problem: The integrated USB RMH incorrectly prioritizes full-speed and low-speed asynchronous retries over dispatchable periodic transfers.

Implication: Periodic transfers may be delayed or aborted. If the asynchronous retry latency causes the periodic transfer to be aborted, the impact varies depending on the nature of periodic transfer:

- If a periodic interrupt transfer is aborted, the data may be recovered by the next instance of the interrupt or the data could be dropped.
- If a periodic isochronous transfer is aborted, the data will be dropped. A single dropped periodic transaction should not be noticeable by end user.

Note: This issue has only been seen in a synthetic environment. The USB spec does not consider the occasional loss of periodic traffic a violation

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP21 USB EHCI FS/LS Incorrect Number of Retries

Problem: A USB low-speed transaction may be retried more than three times, and a USB full-speed transaction may be retried less than three times if all of the following conditions are met:

- A USB low-speed transaction with errors or the first retry of the transaction occurs near the end of a microframe, and there is not enough time to complete another retry of the low-speed transaction in the same microframe.
- There is pending USB full-speed traffic and there is enough time left in the microframe to complete one or more attempts of the full-speed transaction.
- Both the low-speed and full-speed transactions must be asynchronous (Bulk/Control) and must have the same direction either in or out.

Note: Per the USB EHCI Specification a transaction with errors should be attempted a maximum of 3 times if it continues to fail.

Implication: For low-speed transactions the extra retry(s) allow a transaction additional chance(s) to recover regardless of if the full-speed transaction has errors or not. If the full-speed transactions also have errors, the SoC may retry the transaction fewer times than required, stalling the device prematurely. Once stalled, the implication is software dependent, but the device may be reset by software.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP22 USB EHCI Full-/Low-speed Port Reset or Clear TT Buffer Request

Problem: One or more full-/low-speed USB devices on the same RMH controller may be affected if the devices are not suspended and either (a) software issues a Port Reset OR (b) software issues a Clear TT Buffer request to a port executing a split full-/low-speed Asynchronous Out command. The small window of exposure for full-speed device is around 1.5 microseconds and around 12 microseconds for a low-speed device.

Implication: The affected port may stall or receive stale data for a newly arrived split transfer occurring at the time of the Port Reset or Clear TT Buffer request.

Note: This issue has only been observed in a synthetic test environment.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP23 USB EHCI RMH Think Time Issue

Problem: The USB RMH Think Time may exceed its declared value in the RMH hub descriptor register of 8 full-speed Bit times.

Implication: If the USB driver fully subscribes a USB microframe, LS/FS transactions may exceed the microframe boundary.

Note: No functional failures have been observed.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP24 USB EHCI Full-/low-speed Device Removal Issue

Problem: If two or more USB full-/low-speed devices are connected to the EHCI USB controller, the devices are not suspended, and one device is removed, one or more of the devices remaining in the system may be affected by the disconnect.

Implication: The implication is device dependent. A device may experience a delayed transaction, stall and be recovered via software, or stall and require a reset such as a hot plug to resume normal functionality.

Workaround: Intel recommends the use of the USB xHCI controller which is not affected by this erratum.

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

VLP25 Reported Memory Type may not be used to Access the VMCS and Referenced Data Structures

Problem: Bits 53:50 of the IA32_VMX_BASIC MSR report the memory type that the processor uses to access the VMCS and data structures referenced by pointers in the VMCS. Due to this erratum, a VMX access to the VMCS or referenced data structures will instead use the memory type that the MTRRs (memory-type range registers) specify for the physical address of the access.

Implication: Bits 53:50 of the IA32_VMX_BASIC MSR report that the WB (write-back) memory type will be used but the processor may use a different memory type.

Workaround: Software should ensure that the VMCS and referenced data structures are located at physical addresses that are mapped to WB memory type by the MTRRs.

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

VLP26 A Page Fault may not be generated when the PS Bit is set to "1" in PML4E or PDPTE

Problem: On processors supporting Intel® 64 architecture the PS Bit (Page Size Bit 7) is reserved in PML4Es and PDPTEs. If the translation of the linear address of a memory access encounters a PML4E or a PDPTE with PS set to 1 a page fault should occur. Due to this erratum, PS of such an entry is ignored and no page fault will occur due to its being set.

Implication: Software may not operate properly if it relies on the processor to deliver page faults when reserved bits are set in paging-structure entries.

Workaround: Software should not set Bit 7 in any PML4E or PDPTE that has Present Bit (Bit 0) set to "1".

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

VLP27 CS Limit Violations may not be Detected after VM Entry

Problem: The processor may fail to detect a CS limit violation on fetching the first instruction after VM entry if the first byte of that instruction is outside the CS limit but the last byte of the instruction is inside the limit.

Implication: The processor may erroneously execute an instruction that should have caused a general protection exception.

Workaround: When a VMM emulates a branch instruction it should inject a general protection exception if the instruction's target EIP is beyond the CS limit.

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

VLP28 IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI

Problem: FREEZE_PERFMON_ON_PMI (Bit 12) in the IA32_DEBUGCTL MSR (1D9H) is erroneously cleared during delivery of an SMI (system-management interrupt).

Implication: As a result of this erratum the performance monitoring counters will continue to count after a PMI occurs in SMM (system-management Mode).

Workaround: None identified.

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

VLP29 PEBS Record EventingIP Field May be Incorrect after CS.Base Change

Problem: Due to this erratum a PEBS (Precise Event Base Sampling) record generated after an operation which changes CS.Base may contain an incorrect address in the EventingIP field.

Implication: Software attempting to identify the instruction which caused the PEBS event may identify the incorrect instruction when non-zero CS.Base is supported and CS.Base is changed. Intel has not observed this erratum to impact the operation of any commercially available system.

Workaround: None identified.

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

VLP30 Some Performance Counter Overflows may not be Logged in IA32_PERF_GLOBAL_STATUS When FREEZE_PERFMON_ON_PMI is Enabled

Problem: When enabled, FREEZE_PERFMON_ON_PMI Bit 12 in IA32_DEBUGCTL MSR (1D9H) freezes PMCs (performance monitoring counters) on a PMI (Performance Monitoring Interrupt) request by clearing the IA32_PERF_GLOBAL_CTRL MSR (38FH). Due to this erratum, when FREEZE_PERFMON_ON_PMI is enabled and two or more PMCs overflow within a small window of time and PMI is requested, then subsequent PMC overflows may not be logged in IA32_PERF_GLOBAL_STATUS MSR (38EH).

Implication: On a PMI, subsequent PMC overflows may not be logged in IA32_PERF_GLOBAL_STATUS MSR.

Workaround: Re-enabling the PMCs in IA32_PERF_GLOBAL_CTRL will log the overflows that were not previously logged in IA32_PERF_GLOBAL_STATUS.

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

VLP31 MOVNTDQA from WC Memory May Pass Earlier Locked Instructions

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

Implication: Software that expects a lock to fence subsequent MOVNTDQA instructions may not operate properly. If the software does not rely on locked instructions to fence the subsequent execution of MOVNTDQA then this erratum does not apply.

Workaround: Software that requires a locked instruction to fence subsequent executions of MOVNTDQA should insert an LFENCE instruction before the first execution of MOVNTDQA following the locked instruction. If there is already fencing or serializing instruction between the locked instruction and the MOVNTDQA, then an additional LFENCE is not necessary.

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

VLP32 Performance Monitor Instructions Retired Event May Not Count Consistently

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

Implication: A performance counter counting instructions retired may over or under count. The count may not be consistent between multiple executions of the same code.

Workaround: None identified.

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

VLP33 Unsynchronized Cross-Modifying Code Operations Can Cause Unexpected Instruction Execution Results

Problem: The act of one processor or system bus master writing data into a currently executing code segment of a second processor with the intent of having the second processor execute that data as code is called cross-modifying code (XMC). XMC that does not force the second processor to execute a synchronizing instruction prior to execution of the new code is called unsynchronized XMC. Software using unsynchronized XMC to modify the instruction byte stream of a processor can see unexpected or unpredictable execution behavior from the processor that is executing the modified code.

Implication: In this case the phrase "unexpected or unpredictable execution behavior" encompasses the generation of most of the exceptions listed in the Intel Architecture Software Developer's Manual Volume 3: System Programming Guide including a General Protection Fault (GPF) or other unexpected behaviors. In the event that unpredictable execution causes a GPF the application executing the unsynchronized XMC operation would be terminated by the operating system.

Workaround: In order to avoid this erratum programmers should use the XMC synchronization algorithm as detailed in the Intel Architecture Software Developer's Manual Volume 3: System Programming Guide Section: Handling Self- and Cross-Modifying Code.

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

VLP34 USB HSIC Ports Incorrectly Reported as Removable

Problem: The DR (Device Removable) bit in the PORTSC registers of the two USB HSIC ports incorrectly indicates that devices on these ports may be removed.

Implication: Software that relies solely on the state of DR bits will consider fixed devices to be removable. This may lead the software to improper actions (e.g. requesting the user remove a fixed device).

Workaround: In conjunction with the DR bits, software should use BIOS-configured ACPI tables and factor in the CONNECTABLE field of the USB Port Capabilities object when determining whether a port is removable.

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

VLP35 Paging Structure Entry May be Used before Accessed and Dirty Flags Are Updated

Problem: If software modifies a paging structure entry while the processor is using the entry for linear address translation, the processor may erroneously use the old value of the entry to form a translation in a Translation Lookaside Buffer (TLB) (or an entry in a paging structure cache) and then update the entry's new value to set the accessed flag or dirty flag. This will occur only if both the old and new values of the entry result in valid translations.

Implication: Incorrect behavior may occur with algorithms that atomically check that the accessed flag or the dirty flag of a paging structure entry is clear and modify other parts of that paging structure entry in a manner that results in a different valid translation.

Workaround: Affected algorithms must ensure that appropriate TLB invalidation is done before assuming that future accesses do not use translations based on the old value of the paging structure entry.

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

VLP36 VGA Max Luminance Voltage May Exceed VESA Limits

Problem: The max luminance voltage on the VGA video outputs may range from 640 mV to 810mV (the VESA specification range is 665 mV to 770mV) with linearity (INL/DNL) of up to ±3 LSB (the VESA linearity specification is ±1 LSB).

Implication: Intel has not observed any functional issues due to this erratum.

Workaround: None identified.

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

VLP37 Certain eMMC Host Controller Registers Are Not Cleared by Software Reset

Problem: Due to this erratum, when an eMMC Host Controller software reset is requested by setting bit 0 of the Software Reset Register (Offset 2FH), the Command Response Register (Offset 10H) and ADMA Error Status Register (Offset 54H) are not cleared. This does not comply with the SD Host Controller Specification 3.0.

Implication: Intel has not observed this erratum to impact any commercially available software.

Workaround: Software should not read these registers until a response is received from the eMMC device.

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

VLP38 SD Host Controller Incorrectly Reports Supporting of Suspend/ Resume Feature

Problem: SDIO, SD Card, and eMMC Controllers should not indicate the support of optional Suspend/Resume feature documented in the SD Host Controller Standard Specification Version 3.0. Due to this erratum, the default value in the Capabilities Register (offset 040H) incorrectly indicates to the software that this feature is supported.

Implication: If software utilizes the Suspend/Resume feature, data may not be correctly transferred between memory and SD Device.

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

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

VLP39 SD Host Controller Error Status Registers May be Incorrectly Set

Problem: This erratum impacts SDIO, SD Card, and eMMC SD Host Controllers. Auto CMD Error Status Register (offset 03CH, bits [7:1]) may be incorrectly set for software-issued commands (for example: CMD13) that generate errors when issued close to the transmission of an Auto CMD12 command. In addition, the Error Interrupt Status Register bits (offset 032H) are similarly affected.

Implication: Software may not be able to interpret SD Host controller error status.

Workaround: Software should follow the same error recovery flow whenever an error status bit is set. Alternatively, don’t use software-issued commands which have Auto CMD12 enabled.

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

VLP 40 SD Host Controller Registers Are Not Cleared by Software Reset

Problem: This erratum impacts SDIO, SD Card, and eMMC SD Host Controllers. When Software Reset is asserted, registers such as SDMA System Address / Argument 2 (offset 00H) in SD Host Controller are not cleared, failing to comply with the SD Host Controller Specification 3.0.

Implication: Intel has not observed this erratum to impact any commercially available software.

Workaround: Driver is expected to reprogram these registers before issuing a new command.

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

VLP41 eMMC Asynchronous Abort May Cause a Hang

Problem: Use of an Asynchronous Abort command to recover from an eMMC transfer error or use of a high priority interrupt STOP_TRANSMISSION command may result in a hang.

Implication: Using Asynchronous Abort command may cause a hang. Intel has not observed this erratum to impact the operation of any commercially available system.

Workaround: The eMMC driver should use High Priority Interrupt SEND_STATUS mode per JEDEC STANDARD eMMC, version 4.5. A minimum wait time of 128us between getting an error interrupt and issuing a software reset will avoid this erratum.

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

VLP42 Timing Specification Violation on SD Card Interface

Problem: SD Card interface IO circuitry is not optimized for platform conditions during operation at 3.3V.

Implication: Due to this erratum, there is an increased risk of a transfer error.

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

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

VLP43 SD Card Controller Does Not Disable Clock During Card Power Down

Problem: The clock and power control of the SD card controller are not linked. Therefore, the SD card controller does not automatically disable the SD card clock when the SD card power is disabled.

Implication: When an SD card is inserted into the system and powered off, the clock to the SD card will continue to be driven. Although this behavior is common, it is a violation of the SD Card Spec 3.0.

Workaround: To address this problem, the SD card clock should be enabled/disabled in conjunction with SD card power.

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

VLP44 Reset Sequence May Take longer Than Expected When ACG is Enabled in SD And SDIO Controllers

Problem: When ACG (Auto Clock Gating) is enabled in SD and SDIO controllers, the reset sequence may take longer than expected, possibly resulting in a software timeout.

Implication: Due to this erratum, a longer response time may be observed after software initiates reset.

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

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

VLP45 SDIO Host Controller Does Not Control the SDIO Bus Power

Problem: The SD Bus Power bit in Power Control Register (Bus 0; Device 17; Function 0; Offset 029H) is not connected to any SOC IO pin that can reset the SDIO bus power. Due to this erratum, SDIO device Power-On-Reset cannot be controlled by Power Control Register. SDIO Controller may fail to comply with SD Host Controller Specification Version 3.00.

Implication: SDIO devices may not be powered up and initialized correctly.

Workaround: A GPIO pin must be implemented on the platform to control the SDIO bus power. GPIO pin can be asserted/de-asserted from ASL methods in firmware.

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

VLP46 Premature Asynchronous Interrupt Enabling May Lead to Loss of SDIO WiFi Functionality

Problem: Setting the SDIO controller's Host Control 2 Register Asynchronous Interrupt Enable (Bus 0; Device 17; Function 0; Offset 03EH, bit 14) to '1' before the signal voltage switch sequence completion may result in SDIO card initialization failure.

Implication: SDIO card initialization failure may lead to software time out and loss of WiFi device functionality. Currently released common operating system drivers do not use Asynchronous Interrupt mode.

Workaround: The SDIO driver should either use SDIO Synchronous Interrupt Mode or enable SDIO Asynchronous Interrupt Mode after the SDIO card signal voltage switch sequence completes.

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

VLP47 MTF VM Exit May be Delayed Following a VM Entry That Injects a Software Interrupt

Problem: If the "monitor trap flag" VM-execution control is 1 and VM entry is performing event injection, an MTF VM exit should be delivered immediately after the VM entry. Due to this erratum, delivery of the MTF VM exit may be delayed by one instruction if the event being injected is a software interrupt and if the guest state being loaded has RFLAGS.VM = CR4.VME = 1. In this case, the MTF VM exit is delivered following the first instruction of the software interrupt handler.

Implication: Software using the monitor trap flag to trace guest execution may fail to get a notifying VM exit after injecting a software interrupt. Intel has not observed this erratum with any commercially available system.

Workaround: None identified. An affected virtual-machine monitor could emulate delivery of the software interrupt before VM entry.

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

VLP48 LBR Stack and Performance Counter Freeze on PMI May Not Function Correctly

Problem: When FREEZE_LBRS_ON_PMI flag (bit 11) in IA32_DEBUGCTL MSR (1D9H) is set, the LBR (Last Branch Record) stack is frozen on a hardware PMI (Performance Monitoring Interrupt) request. When FREEZE_PERFMON_ON_PMI flag (bit 12) in IA32_DEBUGCTL MSR is set, a PMI request clears each of the ENABLE fields of the IA32_PERF_GLOBAL_CTRL MSR (38FH) to disable counters. Due to this erratum, when FREEZE_LBRS_ON_PMI and/or FREEZE_PERFMON_ON_PMI is set in IA32_DEBUGCTL MSR and the local APIC is disabled or the PMI LVT is masked, the LBR Stack and/or Performance Counters Freeze on PMI may not function correctly.

Implication: Performance monitoring software may not function properly if the LBR Stack and Performance Counters Freeze on PMI do not operate as expected. Intel has not observed this erratum to impact any commercially available system.

Workaround: None identified.

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

VLP49 USB Legacy Support SMI Not Available from xHCI Controller

Problem: SMIs are routed using the PMC (Power Management Controller) SMI_STS and SMI_EN registers. However, the USB SMI Enable (USB_SMI_EN) and USB Status (USB_STS) fields only reflect SMIs for the EHCI USB controller. SMIs triggered by the xHCI controller's USBLEGCTLSTS mechanism are not available.

Implication: BIOS is unable to receive SMI interrupts from the xHCI controller. BIOS mechanisms such as legacy keyboard emulation for pre-OS environments will be impacted.

Workaround: Use the EHCI controller for legacy keyboard emulation that require legacy USB SMI support by BIOS.

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

VLP50 SD Card UHS-I Mode is Not Fully Supported

Problem: The SD Card Specification rev 3.01 Addendum 1 specifies a relaxed NCRC (Number of clocks to Cyclic Redundancy Check) timing specification for UHS-I (DDR50) mode. Due to this erratum, the SD Host Controller is not fully compatible with this relaxed timing specification.

Implication: Using UHS-I mode with SD devices that rely upon relaxed NCRC may cause SD host commands to fail to complete, resulting in device access failures.

Workaround: BIOS and driver code changes have been identified and may be implemented as a workaround for this erratum.

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

VLP51 HD Audio Recording and Playback May Glitch or Stop

Problem: Under certain conditions generally involving extended simultaneous video and HD audio playback and/or recording, glitches, distortion, or persistent muting of the audio stream may occur due to improper processing of input stream data or response packets.

Implication: Due to this erratum, media device operation may not be reliable.

Workaround: A BIOS code change has been identified and may be implemented to minimize the effect of this erratum. The 3rd party codec driver should minimize HD audio device command traffic.

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

VLP52 EOI Transactions May Not be Sent if Software Enters Core C6 During an Interrupt Service Routine

Problem: If core C6 is entered after the start of an interrupt service routine but before a write to the APIC EOI (End of Interrupt) register, and the core is woken up by an event other than a fixed interrupt source the core may drop the EOI transaction the next time APIC EOI register is written and further interrupts from the same or lower priority level will be blocked.

Implication: EOI transactions may be lost and interrupts may be blocked when core C6 is used during interrupt service routines.

Workaround: It is possible for the firmware to contain a workaround for this erratum. Please refer to the Bay Trail-M Platform, CPU Signature 30673 Microcode+Punit+PMC Patch – Utility Software – Rev. M0230673318 or later.

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

VLP53 USB xHCI May Execute a Stale Transfer Request Block (TRB)

Problem: When a USB 3.0 or USB 2.0 hub with numerous active Full-Speed (FS) or Low-Speed (LS) periodic endpoints attached is removed and then reconnected to an USB xHCI port, the xHCI controller may fail to fully refresh its cache of TRB records. The controller may read and execute a stale TRB and place a pointer to it in a Transfer Event TRB.

Implication: In some cases, the xHCI controller may read de-allocated memory pointed to by a TRB of a disabled slot. The xHCI controller may also place a pointer to that memory in the event ring, causing the xHCI driver to access that memory and process its contents, resulting in system hang, failure to enumerate devices, or other anomalous system behavior.

Note: This issue has only been observed in a stress test environment.

Workaround: None Identified

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

VLP54 Frequency Reported by CPUID Instruction May Not Match Published Frequency

Problem: When the CPUID instruction is executed with EAX = 80000002H, 80000003H, and 80000004H, the frequency reported in the brand string may be truncated while the published frequency is rounded. For example a processor with a frequency of 2.166667GHz may be reported as 2.16GHz in the brand string instead of the published frequency of 2.17GHz

Implication: Intel® Pentium® Processor N3000 and J2000 series, and Intel® Celeron® N2000, J1700, J1800, and J1900 series processors may report in the brand string a frequency lower than the published frequency.

Workaround: None identified

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

VLP55 Reset Sequence May Not Complete Under Certain Conditions

Problem: Under certain conditions, the SoC may not complete initialization either during a reset issued while the system is running or from the G3 (mechanically off) global system state.

Implication: When this erratum occurs, the SoC will detect an initialization problem and halt the initialization sequence prior to normal operation, leading to a system hang. The system will subsequently require a power cycle via the system power button.

Workaround: For the erratum occurring during reset while the system is running, a firmware code change has been identified which significantly reduces the likelihood of this erratum after the initial reset at power on. Refer to the Bay Trail-M/-D Platform, Microcode+Punit+PMC Patch – Utility Software – M0C3067331A or later and release notes.

In the rare situation of this sighting occurring, the end user is expected to execute a global reset by performing a Power Button Override by pressing the power button for approx. 4 seconds.

Contact your Intel representative on the guidance to implement these workarounds.

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

VLP56 Multiple Drivers That Access the GPIO Registers Concurrently May Result in Unpredictable System Behavior

Problem: The PCU (Platform Control Unit) in SoC may not be able to process concurrent accesses to the GPIO registers. Due to this erratum, read instructions may return 0xFFFFFFFF and write instructions may be dropped.

Implication: Multiple drivers concurrently accessing GPIO registers may result in unpredictable system behavior.

Workaround: GPIO drivers should not access GPIO registers concurrently. Each driver should acquire a global lock before accessing the GPIO register, and then release the lock after the access is completed. The Intel-provided drivers implement this workaround.

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

VLP57 Boot May Not Complete When SMI Occurs during Boot

Problem: During boot, the system should be able to handle SMIs (System Management Interrupt). Due to this erratum, boot may not complete when SMI occurs during boot.

Implication: If the system receives an SMI during boot, the boot may not complete.

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

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

VLP58 Interrupts That Target an APIC That is Being Disabled May Result in a System Hang

Problem: Interrupts that target a Logical Processor whose Local APIC is either in the process of being hardware disabled by clearing bit 11 in the IA32_APIC_BASE_MSR or software disabled by clearing bit 8 in the Spurious-Interrupt Vector Register at offset 0F0H from the APIC base are neither delivered nor discarded.

Implication: When this erratum occurs, the processor may hang.

Workaround: None identified. Software must follow the recommendation that all interrupt sources that target an APIC must be masked or changed to no longer target the APIC, and that any interrupts targeting the APIC be quashed, before the APIC is disabled.

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

VLP59 Corrected or Uncorrected L2 Cache Machine Check Errors May Log Incorrect Address in IA32_MCi_ADDR

Problem: For L2 Cache errors with IA32_MCi_STATUS.MCACOD (bits [15:0]) value 0000_0001_0000_1010b, the address reported in IA32_MCi_ADDR MSR may not be the address that caused the machine check.

Implication: Due to this erratum, the address reported in IA32_MCi_ADDR may be incorrect.

Workaround: None identified.

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

§

5 Specification Changes

There are no specification changes in this revision of the specification update.

§

6 Specification Clarifications

There are no specification clarifications in this revision of the specification update.

§

7 Documentation Changes

There are no documentation changes in this revision of the specification update.

§