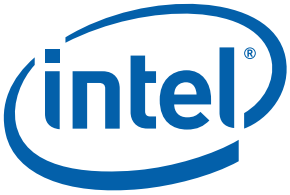


Intel Atom® Processor C2000 Product Family

Specification Update

May 2018

Order Number: 329460-019US

Contents

Revision History

Date	Revision	Description
May 2018	019US	Updated Erratum: • USB 2.0 Device May Not be Detected at System Power-On
April 2017	018US	Added C0 Stepping to Table 1, "Errata Summary Table." Updated Identification Information and Table 8, "SoC Stepping Information." Updated Table 9, "Component Identification." Updated Specification Change: • LPC Interface Signals
February 2017	017US	Added Specification Clarification: • ILB_SERIRQ Signal Pin
January 2017	016US	Added Erratum: • System May Experience Inability to Boot or May Cease Operation
April 2016	015US	Updated: • Table 5 in Component Identification using Programming Interface • Table 10 in Specification Changes
February 2016	014US	Added Erratum: • Malformed IPv6 Extension Headers May Result in LAN Device Hang Added Specification Change: • LPC Interface Signals Added Documentation Change: • PCIe Peer-to-peer transactions are not supported in the C2000 Product Family.
December 2015	013US	Added Errata: • PMI May be Pended When PMI LVT Mask Bit Set • Performance Monitoring Counter Overflows May Not be Reflected in IA32_PERF_GLOBAL_STATUS
November 2015	012US	Added Erratum: • LPC Clock Control Using the LPC_CLKRUN# May Not Behave As Expected Added Specification Clarification: • The GbE NCSI_CLK_OUT (P50) is not functional • Power Down Sequence Guidance
June 2015	011US	Added Erratum: • USB 2.0 Device May Not be Detected at System Power-On
March 2015	010US	Updated: • Top Markings Added Erratum: • Clearing IA32_MC0_CTL[5] May Prevent Machine Check Notification
January 2015	009US	Updated: • Table 9 in Component Marking Information with CPUID. Added: • Component Identification using Programming Interface to Identification Information section. Added Erratum: • VM Exits During Execution of INTn in Virtual-8086 Mode with Virtual-Mode Extensions May Save RFLAGS Incorrectly

Date	Revision	Description
November 2014	008US	Added Errata: • TLB Entries May Not Be Invalidated Properly When Bit 8 Is Set in EPT Paging-Structure Entries • Boundary Scan Chain is Not Functional in Two SKUs • RDTSC Values May Not be Unique • CPUID Instruction Leaf 0AH May Return an Unexpected Value • Uncorrectable Memory ECC Errors May be Improperly Logged • Soft Strap Disabling of SATA 2 or SATA 3 Breaks The Boundary Scan Chain
September 2014	007US	Updated: • Affected Documents/Related Documents • Component Identification Added Errata: • Attempts to Clear Performance Counter Overflow Bits May Not Succeed • SMI in 64 Bit Mode May Store an Incorrect RIP to SMRAM When CS has a Non-Zero Base • Machine Check Status Overflow Bit May Not be Set • VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1 • Top Swap Mechanism May Become Incorrectly configured Added Specification Clarification: • Top Swap Feature
May 2014	006US	Added Erratum: • Gigabit Ethernet Controller May Not be Functional After Booting the System From Mechanical Off
April 2014	005US	Added Erratum: • Processor May Fail to Discard PCIe* Flow Control Initialization Packets While in DL_Active State
March 2014	004US	Added Errata: • DTS Reading is Incorrect Below -27°C • Multiple Drivers That Access the GPIO Registers Concurrently May Result in Unpredictable System Behavior
November 2013	003US	Added Errata: • SMBus Controller May Detect Spurious Parity Errors • Interrupts That Target an APIC That is Being Disabled May Result in a System Hang
September 2013	002US	Added Erratum: • Disabling Gigabit Ethernet Controller Function 0 May Lead to Unexpected System Behavior Updated Erratum: • Internal Errors May Not be Escalated to The RCEC
September 2013	001US	Initial Public Release

§ §

Preface

This document is an update to the specifications contained in the Affected Documents/ Related 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/Related Documents

Document Title	Document Number/ Location
Intel Atom® Processor C2000 Product Family for Microserver Datasheet	330061
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide* *Intel® 64 and IA-32 Intel Architecture Optimization Reference Manual*	http://www.intel.com/products/processor/manuals/index.htm
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	D51397-001

Note: Documentation changes for *Intel® 64 and IA-32 Architecture Software Developer's Manual Volumes 1, 2A, 2B, 3A, and 3B* will be posted in a separate document, *Intel® 64 and IA-32 Architecture Software Developer's Manual Documentation Changes*. Use the following link to become familiar with this file: http://developer.intel.com/products/processor/manuals/index.htm.

Nomenclature

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

QDF Number is a four digit code used to distinguish between engineering samples. These samples are used for qualification and early design validation. The functionality of these parts can range from mechanical only to fully functional. This document has a processor identification information table that lists these QDF numbers and the corresponding product details.

Errata are design defects or errors. Errata may cause the behavior of the Intel Atom® Processor C2000 Product Family 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 in 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.

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

§ §

Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the Intel Atom® Processor C2000 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 uses 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 1. Errata Summary Table (Sheet 1 of 2)

Erratum Number	Stepping		Status	ERRATA
	B0	C0		
AVR1.	X	X	No Fix	Gigabit Ethernet Controller AUX1 Pin Cannot be Used for IEEE-1588* v2 Clock Synchronization
AVR2.	X	X	No Fix	SATA Transmit Signal Voltage Levels May Exceed Specification Value
AVR3.	X	X	No Fix	Disabling One UART Disables Both UARTs
AVR4.	X	X	No Fix	USB Full-Speed Traffic May be Lost
AVR5.	X	X	No Fix	Virtual Wire Mode B Will Result in a System Hang
AVR6.	X	X	No Fix	PCIe* May Experience Link Width Degradation During Power Up
AVR7.	X	X	No Fix	PCIe Root Ports May Incorrectly Indicate CRS Software Visibility Support
AVR8.	X	X	No Fix	PCIe Ports May Log a Receiver Overflow Error on an Unexpected Completion
AVR9.	X	X	No Fix	The Platform SMBus Device Incorrectly Advertises a 32-byte BAR Size
AVR10.	X	X	No Fix	Processor May Hang if Gigabit Ethernet Controller's EEPROM is Not Properly Configured or Absent
AVR11.	X	X	No Fix	Reported Memory Type May Not be Used to Access the VMCS and Referenced Data Structures
AVR12.	X	X	No Fix	A Page Fault May Not be Generated When the PS Bit is Set to 1 in a PML4E or PDPTE
AVR13.	X	X	No Fix	CS Limit Violations May Not be Detected After VM Entry
AVR14.	X	X	No Fix	IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is incorrectly Cleared by SMI
AVR15.	X	X	No Fix	PEBS Record EventingIP Field May be Incorrect After CS.Base Change
AVR16.	X	X	No Fix	Some Performance Counter Overflows May Not be Logged in IA32_PERF_GLOBAL_STATUS when FREEZE_PERFMON_ON_PMI is Enabled
AVR17.	X	X	No Fix	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions
AVR18.	X	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
AVR19.	X	X	No Fix	Unsynchronized Cross-modifying Code Operations Can Cause Unexpected Instruction Execution Results
AVR20.	X	X	No Fix	Redirection of RSM to Probe Mode May Not Generate an LBR Record
AVR21.	X	X	No Fix	USB EHCI RMH Port Disabled Due to Device Initiated Remote Wake
AVR22.	X	X	No Fix	AG3E Pin Strap Value May Not Affect Power Sequencing
AVR23.	X	X	No Fix	PCIe* Ports May Not Detect a 100MHz Toggle for Compliance Mode Switching
AVR24.	X	X	No Fix	PCIe* Elasticity Buffer Errors May be Detected When Not in Config/L0 LTSSM States
AVR25.	X	X	No Fix	A Spurious PCIe* Data Parity Error is Logged
AVR26.	X	X	No Fix	Interrupt May be Lost if I/O APIC is Programmed in Edge Mode
AVR27.	X	X	No Fix	PCIe* Link L1 Exit May Result in a System Hang
AVR28.	X	X	No Fix	Internal Errors May Not be Escalated to The RCEC
AVR29.	X	X	No Fix	Disabling Gigabit Ethernet Controller Function 0 May Lead to Unexpected System Behavior
AVR30.	X	X	No Fix	SMBus Controller May Detect Spurious Parity Errors
AVR31.	X	X	No Fix	Interrupts That Target an APIC That is Being Disabled May Result in a System Hang
AVR32.	X	X	No Fix	DTS Reading is Incorrect Below -27°C
AVR33.	X	X	No Fix	Multiple Drivers That Access the GPIO Registers Concurrently May Result in Unpredictable System Behavior

Table 1. Errata Summary Table (Sheet 2 of 2)

Erratum Number	Stepping		Status	ERRATA
	B0	C0		
AVR34.	X	X	No Fix	Processor May Fail to Discard PCIe* Flow Control Initialization Packets While in DL_Active State
AVR35.	X	X	No Fix	Gigabit Ethernet Controller May Not be Functional After Booting the System From Mechanical Off
AVR36.	X	X	No Fix	Attempts to Clear Performance Counter Overflow Bits May Not Succeed
AVR37.	X	X	No Fix	SMI in 64 Bit Mode May Store an Incorrect RIP to SMRAM When CS has a Non-Zero Base
AVR38.	X	X	No Fix	Machine Check Status Overflow Bit May Not be Set
AVR39.	X	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
AVR40.	X	X	No Fix	Top Swap Mechanism May Become Incorrectly configured
AVR41.	X	X	No Fix	TLB Entries May Not Be Invalidated Properly When Bit 8 Is Set in EPT Paging-Structure Entries
AVR42.	X	X	No Fix	Boundary Scan Chain is Not Functional in Two SKUs
AVR43.	X	X	No Fix	RDTSC Values May Not be Unique
AVR44.	X	X	No Fix	CPUID Instruction Leaf 0AH May Return an Unexpected Value
AVR45.	X	X	No Fix	Uncorrectable Memory ECC Errors May be Improperly Logged
AVR46.	X	X	No Fix	Soft Strap Disabling of SATA 2 or SATA 3 Breaks The Boundary Scan Chain
AVR47.	X	X	No Fix	VM Exits During Execution of INTn in Virtual-8086 Mode with Virtual-Mode Extensions May Save RFLAGS Incorrectly
AVR48.	X	X	No Fix	Clearing IA32_MC0_CTL[5] May Prevent Machine Check Notification
AVR49.	X	X	No Fix	USB 2.0 Device May Not be Detected at System Power-On
AVR50.	X	X	No Fix	LPC Clock Control Using the LPC_CLKRUN# May Not Behave As Expected
AVR51.	X	X	No Fix	PMI May be Pended When PMI LVT Mask Bit Set
AVR52.	X	X	No Fix	Performance Monitoring Counter Overflows May Not be Reflected in IA32_PERF_GLOBAL_STATUS
AVR53.	X	X	No Fix	Malformed IPv6 Extension Headers May Result in LAN Device Hang
AVR54.	X		Fixed	System May Experience Inability to Boot or May Cease Operation

Table 2. Specification Changes

Number	Specification Change
1.	LPC Interface Signals

Table 3. Specification Clarifications

Number	Specification Clarification
1.	Top Swap Feature
2.	The GbE NCSI_CLK_OUT (P50) is not functional
3.	Power Down Sequence Guidance
4.	ILB_SERIRQ Signal Pin

Table 4. Documentation Changes

Number	Documentation Change
1.	PCIe Peer-to-peer transactions are not supported in the C2000 Product Family.

§ §

Identification Information

Component Identification using Programming Interface

The CPUID Instruction returns the processor identification and feature information in the EAX, EBX, ECX, and EDX registers.

Leaf 1 (EAX =1) of the CPUID returns the processor model, family, and stepping IDs as well as the processor features supported. Table 5, Table 6, and Table 7 show these fields for the SoC B0 and earlier steppings.

Table 5. CPUID Leaf 1 Instruction - EAX and EBX Registers

Bit Field	Value	Description	Notes
EAX[31:0:] - Identity			
31:28	0h	Reserved	Family 6, Model 4Dh Intel® Atom™ processor family using the 22nm process
27:20	0h	Extended Family ID	
19:16	4h	Extended Model ID	
15:14	0h	Reserved	
13:12	0h	Processor Type ID	
11:8	6h	Family ID	
7:4	Dh	Model ID	
3:0	0h - A0/A1 8h - B0	Stepping ID	
EBX[31:0:] - Identity and Features			
31:24	Assigned	Local APIC ID	ID assigned to the Local APIC for each processor thread during powerup.
23:16	10h	Maximum number logical processor IDs in SoC	The maximum range of APIC IDs that can be assigned. All SKUs have the same value.
15:8	08h	CLFLUSH instruction cache line size	In 8-byte increments: 8 x 8 = 64 bytes
7:0	0	Brand ID feature supported	Not supported

Table 6. CPUID Leaf 1 Instruction - ECX Register

Bit Field	Value	Feature Description
31	0	Zero (0)
30	1	RDRAND - On-chip Random Number Generator
29	0	F16C Support
28	0	AVX - Advanced Vector Extensions
27	0	OSXSAVE
26	0	XSAVE
25	1	AES Instruction Set
24	1	TSC - Deadline
23	1	POPCNT Instruction
22	1	MOVBE Instruction
21	0	x2APIC Support
20	1	SSE4_2 - SSE4.2 Instructions
19	1	SSE4_1 - SSE4.1 Instructions
18	0	DCA - Direct Cache Access
17	0	PCID - Process-Context Identifiers
16	0	Reserved
15	1	PDCM - Perfmon and Debug Capability MSR
14	1	xTPR Update Control
13	1	CMPXCHG16B Instruction
12	0	FMA - Fused Multiply-Add
11	0	Reserved
10	0	CNXT-ID - L1 Context ID
9	1	SSSE3 - Supplemental SSE3 Extensions
8	1	TM2 - Thermal Monitor 2
7	1	EST - Enhanced Intel SpeedStep® Technology
6	0	SMX - Safer Mode Extensions
5	1	VMX - Virtual Machine eXtensions
4	1	DS-CPL - CPL Qualified Debug Store
3	1	MONITOR - MONITOR/MWAIT Instructions
2	1	DTES64 - 64-Bit DS Area
1	1	PCLMULQDQ - Carry-Less Multiplication
0	1	SSE3 - SSE3 Extensions

Table 7. CPUID Leaf 1 Instruction - EDX Register

Bit Field	Value	Feature Description
31	1	PBE - Pending Break Enable Wake-up Support
30	0	Reserved
29	1	TM - Thermal Monitor
28	1	HTT - Multi-threading. If 1, the SoC can support more than one logical processor per package.
27	1	SS - Self Snoop Support
26	1	SSE2 - SSE2 Instruction Extensions
25	1	SSE - SSE Instruction Extensions
24	1	FXSR - FXSAVE, FXRSTOR Instructions
23	1	MMX - MMX Technology
22	1	ACPI - Thermal Monitor and Clock Control
21	1	DS - Debug Store
20	0	Reserved
19	1	CLFSH - CFLUSH Instruction
18	0	PSN - Processor Serial Number
17	1	PSE-36 - 36-Bit Page-Size Extension
16	1	PAT - Page Attribute Table
15	1	CMOV - Conditional Move/Compare Instruction
14	1	MCA - Machine Check Architecture
13	1	PGE - PTE Global Bit
12	1	MTRR - Memory Type Range Registers
11	1	SEP - SYSENTER and SYSEXIT Instructions
10	0	Reserved
9	1	APIC - APIC on Chip
8	1	CX8 - CMPXCHG8B Instruction
7	1	MCE - Machine Check Exception
6	1	PAE - Physical Address Extensions
5	1	MSR - RDMSR and WRMSR Support
4	1	TSC - Time Stamp Counter
3	1	PSE - Page Size Extensions
2	1	DE - Debugging Extensions
1	1	VME - Virtual-8086 Mode Enhancement
0	1	FPU - x87 FPU on Chip

The BIOS is able to determine the silicon stepping of the entire SoC. This is accomplished by reading the 32-bit CUNIT_CFG_REG_CLASSCODE register in the configuration space, bus 0, device 0, function 0, offset 8h. The SoC stepping is shown in bits 7:0. Note that Ethernet Rev ID will not change from B0 to C0 stepping.

Table 8 shows the information received when this register is read.

Table 8. SoC Stepping Information

Parameter	A0 SoC	A1 SoC	B0 SoC	C0 SoC
Process	0.1	0.1	0.1	0.1
PCI Rev ID	0	1	2	3

In addition to verifying the processor signature, the BIOS needs the platform ID to properly target the microcode update. The platform ID is determined by reading bits [52:50] of the IA32_PLATFORM_ID register, (MSR 17h). This is a 64-bit register and is read using the RDMSR instruction. The three platform ID bits, when read as a Binary Coded Decimal (BCD) number, indicate the bit position in the microcode update header processor flags field that is associated with the installed processor.

Component Marking Information

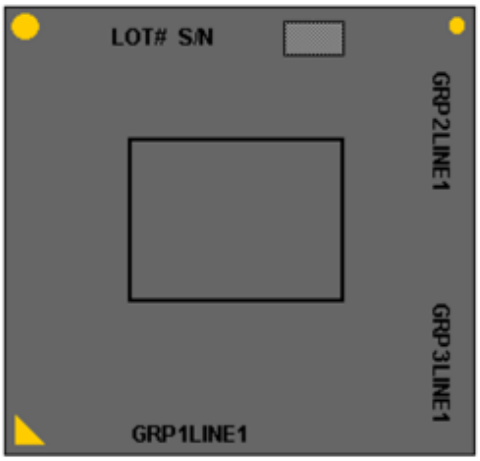
The Intel Atom® Processor C2000 Product Family is identified in the component markings in Table 9.

Table 9. Component Identification

Stepping	SKU Name	S-Spec	MM	CPUID
B0	C2308	R1UN	933655	406D8
B0	C2338	R1S8	930465	406D8
B0	C2350	R1CV	930447	406D8
B0	C2358	R1D2	930457	406D8
B0	C2508	R1VV	934745	406D8
B0	C2518	R1D1	930456	406D8
B0	C2530	R1CU	930446	406D8
B0	C2538	R1S9	930466	406D8
B0	C2550	R1CT	930445	406D8
B0	C2558	R1CZ	930454	406D8
B0	C2718	R1CY	930453	406D8
B0	C2730	R1CR	930443	406D8
B0	C2738	R1SA	930467	406D8
B0	C2750	R1CS	930444	406D8
B0	C2758	R1CW	930451	406D8
C0	C2730	R3GQ	957483	406D8
C0	C2750	R3GR	957484	406D8
C0	C2550	R3GS	957485	406D8
C0	C2530	R3GT	957486	406D8
C0	C2350	R3GU	957487	406D8
C0	C2758	R3GV	957488	406D8
C0	C2738	R3GW	957489	406D8
C0	C2558	R3GX	957490	406D8
C0	C2718	R3GY	957491	406D8
C0	C2538	R3GZ	957492	406D8
C0	C2518	R3H0	957493	406D8
C0	C2358	R3H1	957494	406D8
C0	C2338	R3H2	957495	406D8
C0	C2308	R3H3	957496	406D8
C0	C2508	R3H4	957497	406D8
C0	C2316	R3JU	958319	406D8
C0	C2516	R3JV	958320	406D8

Figure 1. Top Markings

Side	Group	Line	Sqnce	Text
TOP	1	1	1	S-Spec number i.e. "SRxxx" where xxx is SKU specific
TOP	2	1	1	i{M}{C}12{SYWWxnnn} S = Finish Code Y = Last digit of year WW = Work Week x = Site Code nnn = Finish Sequential Number
TOP	3	1	1	{e1}



§ §

Errata

AVR1. Gigabit Ethernet Controller AUX1 Pin Cannot be Used for IEEE-1588* v2 Clock Synchronization

Problem: The Gigabit Ethernet (Gigabit Ethernet) controller's Software Defined Pin AUX1, when used as the IEEE-1588 v2 auxiliary device connection for external clock synchronization, may miss incoming pulses.

Implication: Use of the Gigabit Ethernet AUX1 pin may cause incorrect external clock synchronization.

Workaround: Use the Gigabit Ethernet Controller's Software Defined Pin AUX0 as the IEEE-1588 v2 auxiliary device connection for external clock synchronization.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR2. SATA Transmit Signal Voltage Levels May Exceed Specification Value

Problem: The SATA transmit buffers have been designed to maximize performance including a variety of routing scenarios. As a result, the SATA transmit levels may exceed the maximum motherboard transmit (TX) connector and the device receive (RX) connector voltage specifications as defined in Section 7.2.1 of the Serial ATA Specification for both SATA Gen1 (1.5 Gb/s) and Gen2 (3 Gb/s) speeds.

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

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR3. Disabling One UART Disables Both UARTs

Problem: Disabling one UART (Universal Asynchronous Receiver Transmitter) by setting bit 0 or bit 1 in the UART_CONT register (Bus 0; Device 31; Function 0; offset 80H) will incorrectly disable both UARTs.

Implication: If either UART is disabled during active UART operations, a loss of serial communication results.

Workaround: Do not disable the unused UART.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR4. USB Full-Speed Traffic May be Lost

Problem: If a USB full-speed transaction is started near the end of a micro-frame, the SoC may receive more than 189 bytes for the next micro-frame.

Implication: If the SoC receives more than 189 bytes for a micro-frame, an NYET (No Response Yet) handshake packet error will be sent to the software and the transfer will be lost.

Workaround: None identified. USB driver recovery protocol may be applied to cause the transfer to be retried.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR5. Virtual Wire Mode B Will Result in a System Hang

Problem: When the local APIC is configured for Virtual Wire Mode B, the system may hang. The local APIC supports 8259 Virtual Wire A and Symmetric Interrupt modes.

Implication: The 8259 Virtual Wire B Mode external interrupts will be ignored leading the system to hang.

Workaround: Do not use the 8259 Virtual Mode B Mode when using the 8259 to deliver interrupts.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR6. PCIe* May Experience Link Width Degradation During Power Up

Problem: The PCIe receiver circuits may violate ZRX-HIGH-IMP-DCPOS as defined in section 4.3.4.5 of the *PCI Express Base Specification*, Revision 3.0. This applies to the 2.5 Gb/s and the 5 Gb/s transfer rates.

Implication: The attached PCIe device may falsely detect a receiver during power up resulting in link width degradation.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR7. PCIe Root Ports May Incorrectly Indicate CRS Software Visibility Support

Problem: The PCIe Root Port ROOTCAP.CRSSV (Bus 0; Device 1-4; Function 0; offset 5EH; bit 0) field indicates that the root port is capable of returning CRS (Configuration Request Retry Status) completion status to software. Due to this erratum, the default value of this bit is set to 1, incorrectly indicating that CRS is supported.

Implication: Due to this erratum, the software that expects the CRS completion status may not function as expected.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR8. PCIe Ports May Log a Receiver Overflow Error on an Unexpected Completion

Problem: Upon receipt of an unexpected completion, the PCIe Root Port (Bus 0; Device 1-4; Function 0) may log a receiver overflow error in addition to an unexpected completion error.

Implication: Due to this erratum, a receiver overflow error may be logged incorrectly. If receiver overflow errors are configured to be fatal errors, this may result in a system hang.

Workaround: To avoid a hang, it is possible to configure receiver overflow errors to be non-fatal errors.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR9. The Platform SMBus Device Incorrectly Advertises a 32-byte BAR Size

Problem: During BIOS enumeration, the legacy SMBus Controller indicates a 32 bytes BAR size while the design allocation size is 2KB.

Implication: When this erratum occurs, accessing the SMBus Controller BAR region may result in a device conflict.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR10. Processor May Hang if Gigabit Ethernet Controller's EEPROM is Not Properly Configured or Absent

Problem: Systems may fail to boot if the processor's Gigabit Ethernet controller's associated configuration EEPROM is not properly configured or has not been installed on the platform.

Implication: Systems that do not properly place and configure the Gigabit Ethernet controller's EEPROM may hang.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR11. 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 Table 1, "Errata Summary Table" on page 9.

AVR12. A Page Fault May Not be Generated When the PS Bit is Set to 1 in a PML4E or PDPTE

Problem: The processors supporting the 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 Table 1, "Errata Summary Table" on page 9.

AVR13. 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 target EIP is beyond the CS limit.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR14. 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 Table 1, “Errata Summary Table” on page 9.

AVR15. 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 Table 1, “Errata Summary Table” on page 9.

AVR16. 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 Table 1, “Errata Summary Table” on page 9.

AVR17. 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 a fencing or serializing instruction between the locked instruction and the MOVNTDQA, then an additional LFENCE is not necessary.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR18. 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 Table 1, “Errata Summary Table” on page 9.

AVR19. 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 Table 1, "Errata Summary Table" on page 9.

AVR20. Redirection of RSM to Probe Mode May Not Generate an LBR Record

Problem: A redirection of the RSM instruction to probe mode may not generate the LBR (Last Branch Record) record that would have been generated by a non-redirected RSM instruction.

Implication: The LBR stack may be missing a record when redirection of RSM to probe mode is used. The LBR stack will still properly describe the code flow of non-SMM code.

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR21. 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 Table 1, "Errata Summary Table" on page 9.

AVR22. AG3E Pin Strap Value May Not Affect Power Sequencing

Problem: AG3E (After G3 Enable) pin strap is correctly written to the GEN_PMCON1.AG3E register bit (Bus 0; Device 31; Function 0; Offset 44H; bit 0) after a power-on but may not be correctly utilized during power-on sequencing.

Implication: Due to this erratum, the SoC may proceed to S0 without waiting for a wake event when AG3E is asserted.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR23. PCIe* Ports May Not Detect a 100MHz Toggle for Compliance Mode Switching

Problem: The default behavior of the SoC PCIe electrical idle detection circuit does not guarantee detection of 100MHz toggling signal as recommended by the implementation note in *PCIe 3.0 Base Specification* Section 4.2.6.2.2.

Implication: The SoC may not cycle through all of the transmitter defined settings while under PCIe compliance load board test.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR24. PCIe* Elasticity Buffer Errors May be Detected When Not in Config/L0 LTSSM States

Problem: PCIe elasticity buffer errors may be observed by the LTSSM (Link Training Status State Machine) outside of the CONFIG/L0 states.

Implication: Due to this erratum, receiver errors may be logged in the PCIe ERRCORSTS.RE (Bus 0; Device 1-4; Function 0; Offset 110H; bit 0) and, as a consequence, possibly signaled to the OS.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR25. A Spurious PCIe* Data Parity Error is Logged

Problem: A PCIe root port may incorrectly determine a TLP (Transaction Layer Packet) is poisoned and logs an error in the PCISTS.DPE field (Bus 0; Devices 1-4; Function 0; Offset 06H, bit 15) and, if the associated PCICMD.PER field (Bus 0; Devices 1-4; Function 0; Offset 04H, bit 6) is set, the PCISTS.MDPE (Bus 0; Devices: 1-4; Function: 0; Offset 06H, bit 8) field.

Implication: Spurious errors may be logged in the PCI Status register but no poison TLP is received or sent. Intel has not observed this erratum to impact the operation of any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR26. Interrupt May be Lost if I/O APIC is Programmed in Edge Mode

Problem: An interrupt programmed in the I/O APIC to be triggered by a rising edge may be lost if the IRQ line is deasserted prior to the interrupt delivery to the core.

Implication: The interrupt will not be serviced. Intel has not observed this erratum to impact the operation of any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR27. PCIe* Link L1 Exit May Result in a System Hang

Problem: A processor PCIe link may hang while exiting the L1 link power state.

Implication: Due to this erratum, the system may hang during a PCIe L1 power state transition.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR28. Internal Errors May Not be Escalated to The RCEC

Problem: A masked unsupported request error occurring simultaneously with a detected internal parity or unexpected completion error within the PCIe* root complex may prevent the escalation of internally detected errors to the RCEC (Root Complex Event Collector) for interrupt generation.

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

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR29. Disabling Gigabit Ethernet Controller Function 0 May Lead to Unexpected System Behavior

Problem: When the Gigabit Ethernet Controller function 0 is disabled, that function should be replaced by a dummy function. Due to this erratum, the dummy function's address space is not compatible with the processor system fabric.

Implication: If the Gigabit Ethernet Controller's dummy function is enabled, the dummy function may be the target of requests intended for different devices, leading to unexpected system behavior.

Workaround: None identified. The Gigabit Ethernet Controller function 0 must remain enabled when the controller is enabled.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR30. SMBus Controller May Detect Spurious Parity Errors

Problem: If the address of the last data byte transferred (i.e., buffer base address + length - 1) in an SMBus master transaction modulo 16 is inclusively between 0 and 7, the SMBus controller may spuriously detect a parity error.

Implication: If the SMBus controller detects a data parity error then the transaction is discarded, the controller stops processing master transactions, MCTRL.SS (SMBus 2.0 Master Control Register; Base: SMTBAR; Offset: 108H; Bit: 0) is cleared, error status field ERRSTS.IRDPE (SMBus 2.0 Error Status register; Base: SMTBAR; Offset: 018H; Bit: 9) is set, and error status field ERRUNCSTS.PTLPE (SMBus 2.0 Uncorrectable Error Status Register; Bus: 0; Device: 13H; Function: 0; Offset: 104H; Bit: 12) is set. In some configurations, other error registers may be set and the TLP may be logged. This error does not cause a hang in the SMBus controller.

Workaround: For master transactions subject to this erratum, the device driver should ensure the data buffer is zero-filled to the next 16 byte boundary before initiating the transaction.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR31. 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 by 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 before the APIC is disabled.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR32. DTS Reading is Incorrect Below -27°C

Problem: The DTS (Digital Thermal Sensor) cannot report a value below -27°C for SKUs C2308 and C2508.

Implication: Core DTS readings will report a value of 0xFF (-27°C) for temperatures of -27°C and lower. For uncore DTS, instead of being limited to -27°C, the DTS’s TTR register (sideband port 0x4, offset 0xB1) will report an overflow and the DTS temperature will wrap around to a positive temperature. Thermal policies for high temperature events are not affected.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR33. 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.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR34. Processor May Fail to Discard PCIe* Flow Control Initialization Packets While in DL_Active State

Problem: After PCIe Flow Control initialization completes successfully, the link enters the DL_Active state and additional flow control initialization packets should not be received. Due to this erratum, the processor may fail to discard flow control initialization packets inadvertently received while in DL_Active state.

Implication: Receipt of InitFC2 DLLPs after link partner enters DL_Active state may lead to unpredictable system behavior. Intel has not observed this erratum with any commercially available system.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR35. Gigabit Ethernet Controller May Not be Functional After Booting the System From Mechanical Off

Problem: During boot, the Gigabit Ethernet controller loads a configuration image. Due to this erratum, when booting from ACPI state G3 (mechanical off) with WAKE-ON-LAN support disabled, the configuration image may not load correctly leading to non-functional Gigabit Ethernet interfaces.

Implication: The Gigabit Ethernet subsystem may not be functional when booting from mechanical off. A subsequent cold reset from soft off (ACPI state G2/S5) will not exhibit this erratum.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR36. Attempts to Clear Performance Counter Overflow Bits May Not Succeed

Problem: An MSR write which sets IA32_PERF_GLOBAL_OVF_CTRL MSR (390H) bits 1 and/or 0 may not clear the corresponding bit(s) of IA32_PERF_GLOBAL_STATUS MSR (38EH) if neither IA32_PMC0 nor IA32_PMC1 are enabled at the time of the MSR write and at least one of the fixed-function performance counters is enabled.

Implication: Software will not be able to rely on writes to this MSR to clear the overflow indication of the general-purpose performance counters.

Workaround: Software can avoid this erratum by disabling all fixed-function performance counters before writing to IA32_PERF_GLOBAL_OVF_CTRL MSR.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR37. SMI in 64 Bit Mode May Store an Incorrect RIP to SMRAM When CS has a Non-Zero Base

Problem: On an SMI (system-management interrupt), the processor stores the RIP of the next instruction in SMRAM (system-management RAM). Due to this erratum, an SMI that occurs while the processor is in 64-bit mode with a non-zero value in the CS segment base may result in an incorrect RIP being stored in SMRAM.

Implication: When this erratum occurs, the RIP stored in SMRAM will be incorrect and the RSM instruction will resume from that incorrect RIP, resulting in unpredictable system behavior. Intel has not observed this erratum with any commercially available system.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR38. Machine Check Status Overflow Bit May Not be Set

Problem: The OVER (error overflow) indication in bit [62] of the IA32_MC0_STATUS MSR (401H) may not be set if IA32_MC0_STATUS.MCACOD (bits [15:0]) held a value of 0x3 (External Error) when a second machine check occurred in the MC0 bank. Additionally, the OVER indication may not be set if the second machine check has an MCACOD value of 0x810, 0x820 or 0x410, regardless of the first error.

Implication: Software may not be notified that an overflow of MC0 bank occurred.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR39. VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1

Problem: When “XD Bit Disable” in the IA32_MISC_ENABLE MSR (1A0H) bit 34 is set to 1, it should not be possible to enable the “execute disable” feature by setting IA32_EFER.NXE. Due to this erratum, a VM exit that occurs with the 1-setting of the “load IA32_EFER” VM-exit control may set IA32_EFER.NXE even if IA32_MISC_ENABLE bit 34 is set to 1. This erratum can occur only if IA32_MISC_ENABLE bit 34 was set by guest software in VMX non-root operation.

Implication: Software in VMX root operation may execute with the “execute disable” feature enabled despite the fact that the feature should be disabled by the IA32_MISC_ENABLE MSR. Intel has not observed this erratum with any commercially available software.

Workaround: A virtual-machine monitor should not allow guest software to write to the IA32_MISC_ENABLE MSR.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR40. Top Swap Mechanism May Become Incorrectly configured

Problem: Writing the General Control Register may cause the top swap mechanism to become incorrectly configured, resulting in unreliable boot behavior.

Implication: Due to this erratum, boot behavior may become unreliable which may impact system availability.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR41. TLB Entries May Not Be Invalidated Properly When Bit 8 Is Set in EPT Paging-Structure Entries

Problem: The INVVPID and MOV to CR3 instructions may fail to invalidate TLB entries that were created using EPT paging-structure entries in which bit 8 was set.

Implication: The affected TLB entries may be incorrectly shared across linear-address spaces, possibly leading to unpredictable guest behavior.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR42. Boundary Scan Chain is Not Functional in Two SKUs

Problem: The boundary scan chain is not functional in C2308 and C2508 series processors.

Implication: Due to this erratum, boundary scan testing will give erroneous results.

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR43. RDTSC Values May Not be Unique

Problem: RDTSC instructions executed in close proximity may return the same value at high CPU frequencies.

Implication: Software that relies upon RDTSC values being strictly increasing may not operate properly.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR44. CPUID Instruction Leaf 0AH May Return an Unexpected Value

Problem: When a CPUID instruction is executed with EAX = 0AH (Architectural Performance Monitoring Leaf), the value returned in EDX may incorrectly set bit 14. CPUID leaf 0AH EDX bit 14 is reserved and should be zero.

Implication: When this erratum occurs, the processor will report an incorrect value in EDX.

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR45. Uncorrectable Memory ECC Errors May be Improperly Logged

Problem: In some cases, an uncorrectable memory ECC error is not logged in IA32_MC5_STATUS, but instead is logged in IA32_MC0_STATUS MSR (401H).

Implication: In some cases it may not be possible to identify uncorrectable memory ECC errors.

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR46. Soft Strap Disabling of SATA 2 or SATA 3 Breaks The Boundary Scan Chain

Problem: The boundary scan chain is not functional if soft straps are configured to disable SATA 2 and/or SATA 3.

Implication: When this erratum occurs, boundary scan testing will give erroneous results.

Workaround: SATA 2 Disable and SATA 3 Disable soft straps must be 0 when boundary scan is used.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR47. VM Exits During Execution of INTn in Virtual-8086 Mode with Virtual-Mode Extensions May Save RFLAGS Incorrectly

Problem: An APIC-access VM exit or a VM exit due to an EPT (Extended Page Table) violation or an EPT misconfiguration that occurs during execution of the INTn instruction in virtual-8086 mode (EFLAGS.VM = 1) with virtual-mode extensions (CR4.VME = 1) may save an incorrect value for RFLAGS in the guest-state area of the VMCS.

Implication: This erratum may cause a virtual-machine monitor to handle the VM exit incorrectly, may cause a subsequent VM entry to fail, or may cause incorrect operation of guest software.

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

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR48. Clearing IA32_MC0_CTL[5] May Prevent Machine Check Notification

Problem: Clearing bit 5 of a logical processor's IA32_MC0_CTL MSR (400H) may incorrectly block notifying other logical processors of any local machine check.

Implication: The system may not react as expected to a machine check exception when IA32_MC0_CTL[5] is 0.

Workaround: None identified.

Status: For the steppings affected, see Table 1, "Errata Summary Table" on page 9.

AVR49. USB 2.0 Device May Not be Detected at System Power-On

Problem: Certain internal conditions may cause one or more USB ports to fail at system power-on.

Implication: When this erratum occurs, a USB device attached to the affected port will not function. In addition, the OS may report problems with the USB port.

Workaround: An updated (January 2018) BIOS code change has been identified and may be implemented as workaround for this erratum.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR50. LPC Clock Control Using the LPC_CLKRUN# May Not Behave As Expected

Problem: The LPC_CLKRUN# pin should be an input/open drain output signal as stated for the CLKRUN# signal in Section 2 of the Intel Low Pin Count (LPC) Interface Specification, Revision 1.1. Due to this erratum, if the signal is configured to be an output signal, the buffer may drive an active high level.

Implication: The SoC may prevent a peripheral device from successfully requesting the LPC clock.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR51. PMI May be Pended When PMI LVT Mask Bit Set

Problem: If a performance counter overflow or PEBS (Precise Event Based Sampling) record generation is unable to trigger a PMI (Performance Monitoring Interrupt) due to the PMI LVT (Local Vector Table) entry’s mask bit being set, the PMI should be dropped. Due to this erratum, the PMI may instead be pended and may be taken after the PMI LVT entry mask bit is cleared.

Implication: An unexpected PMI may occur.

Workaround: None identified

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR52. Performance Monitoring Counter Overflows May Not be Reflected in IA32_PERF_GLOBAL_STATUS

Problem: When an overflow indication in IA32_PERF_GLOBAL_STATUS MSR (38EH) is cleared via either the logging of a PEBS (Precise Event Based Sampling) record or an MSR write to IA32_PERF_GLOBAL_OVF_CTRL MSR (390H), a simultaneous counter overflow may not set its corresponding overflow bit.

Implication: When this erratum occurs, a counter overflow will not be logged in IA32_PERF_GLOBAL_STATUS, although it may still pend a Performance Monitoring Interrupt.

Workaround: None identified.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR53. Malformed IPv6 Extension Headers May Result in LAN Device Hang

Problem: Certain malformed IPv6 extension headers are not processed correctly.

Implication: Due to this erratum, the LAN device may behave unpredictably.

Workaround: Intel® Ethernet Software release version 20.2 and above contains a workaround for this erratum.

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

AVR54. System May Experience Inability to Boot or May Cease Operation

Problem: The SoC LPC_CLKOUT0 and/or LPC_CLKOUT1 signals (Low Pin Count bus clock outputs) may stop functioning.

Implication: If the LPC clock(s) stop functioning the system will no longer be able to boot.

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

Status: For the steppings affected, see Table 1, “Errata Summary Table” on page 9.

§ §

Specification Changes

1. LPC Interface Signals

All of the LPC interface signals (Table 10) are defined as muxed with GPIO signals. This implies that if the LPC interface is not used in your design these signals can be GPIO signals. This specification change removes the muxed support of GPIO signals for all LPC signals except LPC_CLKOUT1. These signals must be left in their default (LPC) state and not de-selected via software to be GPIO pins. Bits [26:21] and bits [29:28] in register SC_USE_SEL should not be set to 1.

Table 10. LPC Interface Signals

Signal Affected	Pin Number
LPC_AD0/GPIOS_21	AG54
LPC_AD1/GPIOS_22	AM53
LPC_AD2/GPIOS_23	AL53
LPC_AD3/GPIOS_24	AG59
LPC_FRAMEB/GPIOS_25	AH56
LPC_CLKOUT0/GPIOS_26	AG51
LPC_CLKRUNB/GPIOS_28	AH48
ILB_SERIRQ/GPIOS_29	AT50

Notes:
1. LPC_CLKOUT1 signal can be selected as GPIOS_27 via software but Intel has not validated this mode.

§ §

Specification Clarifications

1. Top Swap Feature

Due to Errata #40 "Top Swap Mechanism May Become Incorrectly configured" the Top Swap capability is de-featured. Affected documents are:

- Intel Atom® Processor C2000 Product Family for Microserver Datasheet.

2. The GbE NCSI_CLK_OUT (P50) is not functional

The NCSI_CLK_OUT function was not implemented in the product design and should not have been included in the product documentation. The NC-SI clock output is optional per the NC-SI specification.

As a result an external source for the NC-SI clock input is required for the NC-SI interface, if it is used.

3. Power Down Sequence Guidance

It is recommended to use the Power Down Sequence documented in the Platform Design Guide (PDG). The power down sequence documented in the Datasheet is calling ramp down of rail VCCSRAM at an incorrect instance.

4. ILB_SERIRQ Signal Pin

A platform pull-up resistor is required as stated in the following document:

- Intel Atom® Processor C2000 Product Family for Microserver Datasheet.

The Datasheet signal definition and the PDG are missing the following text:

"If your system does not use SERIRQ and BIOS puts SERIRQ in Quiet-Mode, then the weak external pull up resistor is not required. All other cases must implement an external pull-up resistor, 8.2k to 10k, tied to 3.3V."

§ §

Documentation Changes

1. PCIe Peer-to-peer transactions are not supported in the C2000 Product Family.

The following documentation has been published removing references to Peer-to-peer:

- Intel Atom® Processor C2000 Product Family for Microserver Datasheet.

§ §