Intel Atom® C3000 Processor Product Family

Specification Update

March 2024

Order Number: 336345-022US

Intel technologies may require enabled hardware, software or service activation.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Performance varies by use, configuration, and other factors. Learn more on the Performance Index site.

Your costs and results may vary.

"Conflict-free" refers to products, suppliers, supply chains, smelters, and refiners that, based on our due diligence, do not contain or source tantalum, tin, tungsten or gold (referred to as "conflict minerals" by the U.S. Securities and Exchange Commission) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or adjoining countries.

All product plans and roadmaps are subject to change without notice.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visiting the Intel Resource and Document Center.

Contents

Revision History

Date	Revision	Description
March 2024	022US	Added the following erratum: • System May Exhibit Unpredictable Behavior
December 2023	021US	Added the following erratum: Reading TCO_RLD Register Sets SMBus Host Status in Use Status Bit
March 2023	020US	Added the following erratum: • HSUART May Stop Functioning When DMA is Activated
June 2022	019US	Updated Table 27, "Component Marking Information" on page 34. Added the following erratum: • Processor May Violate SPI Flash Device Timing Requirements • Unexpected #PF, #GP, #UD, or Other Unpredictable System Behavior May Occur Updated the following errata: • Phase Lock loop (PLL) Feedback Circuit
May 2021	018US	Removed errata: DNV51.
March 2021	017US	Added the following erratum: • SoC PCIe LTSSM May Not Enter Detect Within 20 ms • Phase Lock loop (PLL) Feedback Circuit
June 2020	016US	Updated Table 27, "Component Marking Information" on page 34. Updated Specification Clarifications.
May 2020	015US	Updated Table 3, "Specification Clarifications" on page 11. Updated Table 27, "Component Marking Information" on page 34. Updated Specification Clarifications. Added the following erratum: • Potential Infinite SMI Loop • System Might Hang During AC Boot Cycle
January 2020	014US	Updated Specification Clarifications. Added the following erratum: PCIe Transmitter Preset May be Incorrect During 8.0 GT/s Equalization Configuration
November 2019	013US	Updated the following errata: • xHCI Host Controller Reset May Cause a System Hang Added the following erratum: • xHCI Short Packet Event Using Non-Event Data TRB
August 2019	012US	Added the following erratum: • Upstream PCIe Completion Packets With ECRC Errors May Hang Processor • Incorrect Bandwidth Calculations For LS or FS Devices Connected to USB 2.0 Hub • 10G Base-KR Slow Link up With Link Partners Issuing PRESET
November 2018	011US	Added the following errata: • PCIe Clock May go Inactive at The Same Time PERST# Goes Active • An Extra SMI May be Generated
September 2018	010US	Updated Table 27, "Component Marking Information" and added SKU 18. Added the following erratum: • eMMC Controller May Fail to Detect Error

Date	Revision	Description
August 2018	009US	Updated the following erratum: • Uncompressed SPI Images May Hang SPI Interface Removed the following erratum: • Incorrect Number of Enabled Cores Reported in MSR_CORE_THREAD_COUNT
June 2018	008US	Added the following erratum: • Uncompressed SPI Images May Hang SPI Interface
May 2018	007US	Added the following errata: • Intel® PT OVF Packet May Not be Followed by a FUP or TIP.PGE Packet • PCIe Link Capability Fields MLW And MLS For vRP Are Incorrect
April 2018	006US	Added the following errata: • Legacy SMBus Clock Violates Max SMBus 2.0 Specification Frequency
March 2018	005US	Updated Identification Information. Added the following errata: • Intel® Processor Trace Timing Packets May Not be Generated When Clock Modulation is Enabled • Processor Host Root Complex May Incorrectly Route Memory Accesses to Intel® Trace Hub
January 2018	004US	Added the following erratum: • NEWCENTURY_STS Cannot be Cleared
December 2017	003US	Added the following Specification Change: • Optional SMBALERT# Signal in SMB Controller - Legacy Added the following erratum: • Incorrect Number of Enabled Cores Reported in MSR_CORE_THREAD_COUNT
September 2017	002US	Updated the following erratum: • Performance Monitoring Event Branch Retired May Increment Twice For Near RET Imm16
August 2017	001US	• Initial 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® 64 and IA-32 Architectures Software Developer's Manual	325462 [1]
Intel® 64 and IA-32 Intel Architectures Optimization Reference Manual	248966 [1]
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	252046 [1]
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	D51397 [1]

Notes:
1. This document can be downloaded from http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html.

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® C3000 Processor 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, and documentation changes which apply to the Intel Atom® C3000 Processor 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.

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.

Table 1. Errata Summary Table (Sheet 1 of 3)

Errata Number/ HSD Number	Stepping	Status	Errata Title
	B1 (Production)		
DNV1.	X	No Fix	HECI Line Interrupt May Not be Generated
DNV2.	X	No Fix	xHCI Host Controller Reset May Cause a System Hang
DNV3.	X	No Fix	USB DBC-EXI is Not Enumerated Correctly
DNV4.	X	No Fix	Performance Monitoring Event Branch Retired May Increment Twice For Near RET Imm16
DNV5.	X	No Fix	NCSI_RXD Output Cannot be Tri-State to Meet NCSI Specification
DNV6.	X	No Fix	The X553 Ethernet Controller Transmitter Transition Time Does Not Conform to IEEE 802.3 Specification
DNV7.	X	No Fix	10 GBASE-KR Transmitter Does Not Fully Conform to Specification For Equalization
DNV8.	X	No Fix	Split Access to APIC-Access Page May Access Virtual-APIC Page
DNV9.	X	No Fix	PEBS Record EventingIP Field May be Incorrect After CS.Base Change
DNV10.	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
DNV11.	X	No Fix	SMRAM State-Save Area Above The 4 GB Boundary May Cause Unpredictable System Behavior
DNV12.	X	No Fix	POPCNT Instruction May Take Longer to Execute Than Expected
DNV13.	X	No Fix	APIC-Access VM Exit May Occur Instead of SMAP #PF
DNV14.	X	No Fix	Some Performance Counter Overflows May Not be Logged in IA32_PERF_GLOBAL_STATUS When FREEZE_PERFMON_ON_PMI is Enabled
DNV15.	X	No Fix	Performance Monitoring OFFCORE_RESPONSE1 Event May Improperly Count L2 Evictions
DNV16.	X	No Fix	Debug Exception May Not be Generated on Memory Read Spanning a Cacheline Boundary
DNV17.	X	No Fix	Intel® PT CR3 Filtering Compares Bits [11:5] of CR3 And IA32_RTIT_CR3_MATCH Outside of PAE Paging Mode
DNV18.	X	No Fix	Intel® PT OVF Packet May be Followed by TIP.PGD Packet
DNV19.	X	No Fix	Intel® PT OVF May be Followed by an Unexpected FUP Packet
DNV20.	X	No Fix	Performance Monitoring COREWB Offcore Response Event May Overcount
DNV21.	X	No Fix	FBSTP May Update FOP/FIP/FDP/FSW Before Exception or VM Exit
DNV22.	X	No Fix	PEBS Record May be Generated When Counters Frozen

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

Errata Number/ HSD Number	Stepping	Status	Errata Title
	B1 (Production)		
DNV23.	X	No Fix	IA32_PERF_GLOBAL_INUSE[62] May be Set
DNV24.	X	No Fix	xHCI Split-Transactions Error Counter Reset Issue
DNV25.	X	No Fix	Data Breakpoints May Not be Detected on Split Reads
DNV26.	X	No Fix	Intel® Trace Hub PTI Pattern Generator May Stop Working When Width is Changed While Enabled
DNV27.	X	No Fix	UART_IE_TXD Signal May be Low When IE Enters The Off State (Cloff)
DNV28.	X	No Fix	Intel® Trace Hub May Report Timeout Error Incorrectly
DNV29.	X	No Fix	Larger Than 32-Bit Writes to Intel® Trace Hub CSR_MTB_BAR May Cause a System Hang
DNV30.	X	No Fix	Potential Partial Trace Data Loss in Intel® Trace Hub ODLA When Storing to Memory
DNV31.	X	No Fix	Intel® Trace Hub Pipeline Empty Bit For PTI May be Not Set
DNV32.	X	No Fix	Intel® Trace Hub TAP Data Registers Are Read-Once
DNV33.	X	No Fix	Performance Monitoring Event Branch Retired May Increment Twice For Near RET Imm16
DNV34.	X	No Fix	NEWCENTURY_STS Cannot be Cleared
DNV35.	X	No Fix	Intel® Processor Trace Timing Packets May Not be Generated When Clock Modulation is Enabled
DNV36.	X	No Fix	Processor Host Root Complex May Incorrectly Route Memory Accesses to Intel® Trace Hub
DNV37.	X	No Fix	Legacy SMBus Clock Violates Max SMBus 2.0 Specification Frequency
DNV38.	X	No Fix	Intel® PT OVF Packet May Not be Followed by a FUP or TIP.PGE Packet
DNV39.	X	No Fix	PCIe Link Capability Fields MLW And MLS For vRP Are Incorrect
DNV40.	X	No Fix	Uncompressed SPI Images May Hang SPI Interface
DNV41.	X	No Fix	eMMC Controller May Fail to Detect Error
DNV42.	X	No Fix	PCIe Clock May go Inactive at The Same Time PERST# Goes Active
DNV43.	X	No Fix	An Extra SMI May be Generated
DNV44.	X	No Fix	10G Base-KR Slow Link up With Link Partners Issuing PRESET

Table 1. Errata Summary Table (Sheet 3 of 3)

Errata Number/ HSD Number	Stepping	Status	Errata Title
	B1 (Production)		
DNV45.	X	No Fix	Incorrect Bandwidth Calculations For LS or FS Devices Connected to USB 2.0 Hub
DNV46.	X	No Fix	Upstream PCIe Completion Packets With ECRC Errors May Hang Processor
DNV47.	X	No Fix	xHCI Short Packet Event Using Non-Event Data TRB
DNV48.	X	No Fix	PCIe Transmitter Preset May be Incorrect During 8.0 GT/s Equalization Configuration
DNV49.	X	No Fix	Potential Infinite SMI Loop
DNV50.	X	No Fix	System Might Hang During AC Boot Cycle
DNV51.			Removed
DNV52.	X	No Fix	Phase Lock loop (PLL) Feedback Circuit
DNV53.	X	No Fix	Processor May Violate SPI Flash Device Timing Requirements
DNV54.	X	No Fix	Unexpected #PF, #GP, #UD, or Other Unpredictable System Behavior May Occur
DNV55.	X	No Fix	HSUART May Stop Functioning When DMA is Activated
DNV56.	X	No Fix	Reading TCO_RLD Register Sets SMBus Host Status in Use Status Bit
DNV57.	X	No Fix	System May Exhibit Unpredictable Behavior

Table 2. Specification Changes

Number	Specification Change
1.	Optional SMBALERT# Signal in SMB Controller - Legacy

Table 3. Specification Clarifications

Number	Specification Clarification
1.	X553 Ethernet Controller Device ID and MAC Address Cannot Be Changed
2.	LAN Interface Signals Cannot Be Programed When LEK Is Running
3.	GPIO Input Pulse Width To Trigger the Interrupt

Table 4. Documentation Changes

Number	Documentation Change
NA	None to report at this time.

§

Identification Information

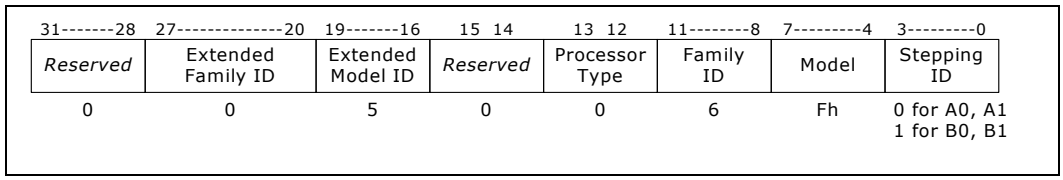
Component Identification Using Programming Interface

The CPU Identification (CPUID) instruction returns processor identification and feature information to the EAX, EBX, ECX, and EDX registers, as determined by input entered in EAX (and in some cases, ECX as well).

Details of the instruction can be found in the Instruction Set Reference portion of the *Intel® 64 and IA-32 Architectures Software Developer's Manual*.

When CPUID executes with EAX set to 01h, the SoC version information is returned in EAX. See Figure 1, "Version Information Returned by CPUID in EAX".

Figure 1. Version Information Returned by CPUID in EAX



Note: Once the SoC product is launched, the *Intel® 64 and IA-32 Architectures Software Developer's Manual* will refer to the SoC as having "DisplayFamily_DisplayModel" as 06_5FH.

Leaves 0 through 15h provides Basic CPUID Information.

Leaves 80000000h through 80000008h provide Extended CPUID Information.

Table 5, "CPUID Leaf 0h" through Table 25, "Extended CPUID Leaf 80000008h" contain descriptions of the leaves and sub-leaves.

CPUID Leaf 0 — Basic CPUID Information

Table 5. CPUID Leaf 0h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
0	n/a	EAX	[31:0]	Maximum CPUID input value in EAX that is recognized by the SoC for its Basic CPUID Information.	Normally 0x15. *See bit 22 (BOOT_NT4) of MSR 1A0h, IA32_MISC_ENABLE.*	Leaf 15h is the final leaf for SoC Basic CPUID Features
		EBX	[31:0]	Intel identification, ASCII encoded "uneG"	0x756E6547	"Genu"
		ECX	[31:0]	Intel identification, ASCII encoded "letn"	0x6C65746E	"ntel"
		EDX	[31:0]	Intel identification, ASCII encoded "Ieni"	0x49656E69	"ineI"

CPUID Leaf 1 — Version and Feature Information

Table 6. CPUID Leaf 1h, Output EAX and EBX

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
1	n/a	EAX	[3:0]	Stepping ID	Varies by product release	A0 Stepping = 0 A1 Stepping = 0 B0 Stepping = 1
			[7:4]	Model	0xF	0xF
			[11:8]	Family ID	6	6
			[13:12]	Processor Type	0	Original OEM Processor
			[15:14]	(Reserved)	0	
			[19:16]	Extended Model ID	5	5
			[27:20]	Extended Family ID	0	
		EBX	[7:0]	Brand Index	0	Brand String Method used rather than Brand Index Method
			[15:8]	CLFLUSH line size	8	64 bytes
			[23:16]	Maximum number of addressable IDs for logical processors in this package	0x20	32 IDs Max
			[31:24]	APIC ID assigned during power up	Varies	

Table 7. CPUID Leaf 1h, Output ECX (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
1	n/a	ECX	0	**SSE3** - Intel® Streaming SIMD Extensions 3 (Intel® SSE3)	1	Supported
			1	**PCLMULDQ** - PCLMULDQ instruction	1	Supported
			2	**DTES64** - 64-bit DS Area	1	Supported
			3	MONITOR/MWAIT feature supported	Varies	Depends on value of bit 18 in IA_MISC_ENABLE (MSR 1A0h)
			4	**DS_CPL** - CPL Qualified Debug Store	1	Supported
			5	**VMX** - Virtual Machine Extensions	1	Supported
			6	**SMX** - Safer Mode Extensions	0	Not Supported
			7	**EIST** - Intel Enhanced SpeedStep® Technology	1	Supported
			8	**TM2** - Intel® Thermal Monitor 2	1	Supported
			9	**SSSE3** - Supplemental Streaming SIMD Extensions 3	1	Supported
			10	**CNXT-ID** - L1 Context ID	0	Not Supported
			11	Privacy MSR	1	Supported
			12	FMA - Intel® Fast Memory Access (Intel® FMA) extensions using YMM state	0	Not Supported
			13	**CMPXCHG16B/CX16** - Compare and Exchange Bytes features	1	Supported
			14	**xTPR Update Control** - Allow changing bit 23 of IA32_MISC_ENABLE (MSR 1A0h)	1	Supported
			15	**PDCM** - PerfMon and Debug Capability, altering IA32_PERF_CAPABILITIES (MSR 345h)	1	Supported
			16	(Reserved)	0	
			17	**PCID** - Process-Context Identifiers	0	Not Supported
			18	**DCA** - Ability to prefetch data from memory-mapped device	0	Not Supported
			19	**SSE4.1** - Intel® Streaming SIMD Extensions 4.1	1	Supported
			20	**SSE4.2** - Intel® Streaming SIMD Extensions 4.2	1	Supported
			21	**x2APIC** - Extended Interrupt Mode	1	Supported
			22	**MOVBE** - MOVBE instruction	1	Supported
			23	**POPCNT** - POPCNT instruction	1	Supported
			24	TSC-Deadline	1	Supported
			25	**AESNI** - AESNI instruction	1	Supported
			26	**XSAVE** - XSAVE/XRSTOR extended states, XSETBV/XGETBV instructions, and XCRO	1	Supported

Table 7. CPUID Leaf 1h, Output ECX (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
1	n/a	ECX	27	**OSXSAVE** - A value of 1 indicates the OS has set CR4.OSXSAVE	Varies	
			28	**AVX** - AVX instruction extensions.	0	Not Supported
			29	**F16C/IVBNI** - 16-bit floating-point conversion instructions	0	Not Supported
			30	**RDRAND** - RDRAND instruction	1	Supported
			31	(Reserved)	0	

Table 8. CPUID Leaf 1h, Output EDX (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
1	n/a	EDX	0	**FPU** - Floating Point Unit on Chip	1	Supported
			1	**VME** - Virtual 8086 Mode Enhancements	1	Supported
			2	**DE** - Debugging Extensions	1	Supported
			3	**PSE** - Page Size Extension	1	Supported
			4	**TSC** - Time Stamp Counter	1	Supported
			5	**MSR** - Model Specific Registers RDMSR & WRMSR Instructions	1	Supported
			6	**PAE** - Physical Address Extension	1	Supported
			7	**MCE** - Machine Check Exception	1	Supported
			8	**CX8** - CMPXCHG8B Instruction	1	Supported
			9	**APIC** - APIC On-Chip	Varies	1 if bit 11 of IA32_APIC_BASE (MSR 1Bh) is set
			10	(Reserved)	0	
			11	**SEP** - SYSTENTER & SYSEXIT Instructions	1	Supported
			12	**MTRR** - Memory Type Range Registers	1	Supported
			13	**PGE** - Page Global Bit	1	Supported
			14	**MCA** - Machine Check Architecture	1	Supported
			15	**CMOV** - Conditional Move Instruction	1	Supported
			16	**PAT** - Page Attribute Table	1	Supported
			17	**PSE-36** - 36-bit Page Size Extension	1	Supported. Physical addresses may be up to 39 bits
			18	**PSN** - Processor Serial Number	0	Not Supported
			19	**CLFSH** - CLFLUSH Instruction	1	Supported
			20	(Reserved)	0	
			21	**DS** - Debug Store	1	Supported
			22	**ACPI** - Software Controlled Clock Facilities	1	Supported

Table 8. CPUID Leaf 1h, Output EDX (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
1	n/a	EDX	23	**MMX** - Intel MMX™ technology	1	Supported
			24	**FXSR** - FXSAVE and FXRSTOR Instructions	1	Supported
			25	**SSE** - Intel® Streaming SIMD Extensions	1	Supported
			26	**SSE2** - Intel® Streaming SIMD Extensions 2	1	Supported
			27	**SS** - Self Snoop	1	Supported
			28	**HTT** - Max APIC IDs reserved field is Valid. See CPUID, Leaf 1, EBX[23:16]	1	Supported
			29	**TM** - Intel® Thermal Monitor	1	Supported
			30	(Reserved)	0	
			31	**PBE** - Pending Break-Enable	1	Supported

CPUID Leaf 2 — Cache and TLB Information

Table 9. CPUID Leaf 2h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
2	n/a	EAX	[7:0]	Loop value - Number of times CPUID leaf 2 must be executed to retrieve complete information about caches and TLBs.	0x01	One time
			[15:8]	Micro Translation Lookaside Buffer (uTLB) Descriptor	0xA0	4K pages, fully associative, 32 entries
			[23:16]	Data Translation Lookaside Buffer (DTLB) Descriptor	0x64	4K pages, 4-way, 512 entries
			[30:24]	Instruction Translation Lookaside Buffer (ITLB) Descriptor	0x61	4K pages, fully associative, 48 entries
			[31]	Valid bit	0	Bits [30:0] are valid
		EBX	[7:0]	Large-Page DTLB Descriptor	0xC2	2M and 4M pages, 4-way, 16 entries
			[15:8]	General	0xFF	CPUID leaf 2 does not report cache descriptor information. Use CPUID leaf 4 instead
			[31:16]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 3— Reserved

The 96-bit processor serial number is not supported. For CPUID with EAX = 3, the results in EAX, EBX, ECX and EDS are reserved and zeros are returned.

CPUID Leaf 4— Deterministic Cache Parameters

CPUID leaf 4 has three sub-leaves.

Table 10. CPUID Leaf 4h (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
4	0	EAX	[4:0]	Cache Type	0x1	Data Cache
			[7:5]	Cache Level	0x1	Level 1 (L1)
			8	Self Initializing Cache?	1	Yes
			9	Fully Associative?	0	No
			[13:10]	(Reserved)	0	
			[25:14]	Max number of addressable IDs for logical processors sharing this cache	0	Max number is 1
			[31:26]	Max number of addressable IDs for processor cores in the SoC physical package (minus 1)	0xF	Max number is 16
		EBX	[11:0]	System Coherency Line Size (minus 1)	0x3F	64
			[21:12]	Physical Line Partitions	0	1 partition
			[31:22]	Ways (minus 1)	5	6 Ways
		ECX	[31:0]	Sets (minus 1)	0x3F	64 Sets
		EDX	0	Write-back Invalidate/Invalidate	1	WBINVD/INVD is not guaranteed to act upon lower level caches of non-originating threads sharing this cache.
			1	Cache Inclusiveness	0	Cache is not inclusive of lower cache levels
			2	Complex Cache Indexing	1	Complex Cache Indexing supported
			[31:3]	(Reserved)	0	
	1	EAX	[4:0]	Cache Type	0x2	Instruction Cache
			[7:5]	Cache Level	0x1	Level 1 (L1)
			8	Self Initializing Cache?	1	Yes
			9	Fully Associative?	0	No
			[13:10]	(Reserved)	0	
			[25:14]	Max number of addressable IDs for logical processors sharing this cache	0	Max number is 1
			[31:26]	Max number of addressable IDs for processor cores in the SoC physical package (minus 1)	0xF	Max number is 16
		EBX	[11:0]	System Coherency Line Size (minus 1)	0x3F	64
			[21:12]	Physical Line Partitions	0	1 partition
			[31:22]	Ways (minus 1)	7	8 Ways
		ECX	[31:0]	Sets (minus 1)	0x3F	64 Sets

Table 10. CPUID Leaf 4h (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
4	1	EDX	0	Write-back Invalidate/Invalidate	1	WBINVD/INVD is not guaranteed to act upon lower level caches of non-originating threads sharing this cache.
			1	Cache Inclusiveness	0	Cache is not inclusive of lower cache levels
			2	Complex Cache Indexing	1	Complex Cache Indexing supported
			[31:3]	(Reserved)	0	
	2	EAX	[4:0]	Cache Type	0x3	Unified Cache
			[7:5]	Cache Level	0x2	Level 2 (L2)
			8	Self Initializing Cache?	1	Yes
			9	Fully Associative?	0	No
			[13:10]	(Reserved)	0	
			[25:14]	Maximum number of addressable IDs for logical processors sharing this cache (minus 1)	0x3	Max number is 4
			[31:26]	Maximum number of addressable IDs for processor cores in the SoC physical package (minus 1)	0xF	Max number is 16
		EBX	[11:0]	System Coherency Line Size (minus 1)	0x3F	64
			[21:12]	Physical Line Partitions	0	1 partition
			[31:22]	Ways	0xF	16 Ways
		ECX	[31:0]	Sets (minus 1)	0x7FF	2048 Sets
		EDX	0	Write-back Invalidate/Invalidate	1	WBINVD/INVD is not guaranteed to act upon lower level caches of non-originating threads sharing this cache.
			1	Cache Inclusiveness	0	Cache is not inclusive of lower cache levels
			2	Complex Cache Indexing	0	Direct mapped cache
			[31:3]	(Reserved)	0	
	3+	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 5— MONITOR/MWAIT

Except for EDX[31:0], values shown in Table 11, "CPUID Leaf 5h" are valid only when MONITOR/MWAIT instructions are enabled.

Table 11. CPUID Leaf 5h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
5	n/a	EAX	[15:0]	Smallest monitor-line size in bytes	0x40 this can vary depending on filter size	64 bytes or the filter size, whichever is smaller
			[31:16]	(Reserved)	0	
		EBX	[15:0]	Largest monitor-line size in bytes	0x40 this can vary depending on filter size	64 bytes or the filter size, whichever is smaller
			[31:16]	(Reserved)	0	
		ECX	0	Enumeration of MONITOR-WAIT extensions	1	Supported
			1	Supports treating interrupts as break-event for MWAIT, even when interrupts disabled	1	Supported
			[31:2]	(Reserved)	0	
		EDX	[3:0]	Number of MWAIT C0 sub-states supported	0	0
			[7:4]	Number of MWAIT C1 sub-states supported	2	2
			[11:8]	Number of MWAIT C2 sub-states supported	0	0
			[15:12]	Number of MWAIT C3 sub-states supported	2	2
			[19:16]	Number of MWAIT C4 sub-states supported	4	4
			[23:20]	Number of MWAIT C5 sub-states supported	2	2
			[27:24]	Number of MWAIT C6 sub-states supported	0	0
			[31:28]	Number of MWAIT C7 sub-states supported	0	0

CPUID Leaf 6— Digital Thermometer and Power Management

Table 12. CPUID Leaf 6h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
6	n/a	EAX	0	Digital Thermal Sensor (DTS) support	1	Supported
			1	Intel® Turbo Boost Technology	0 or 1	Support varies by product SKU. BIOS can also disable this technology
			2	**ARAT -** APIC-Timer-always-running feature	1	Supported
			3	(Reserved)	0	
			4	**PLN** - Power limit notification controls support	0	Not Supported
			5	**ECMD** - Clock modulation duty cycle extension support	0	Not Supported
			6	**PTM** - Package thermal management support	0	Not Supported
			[31:7]	(Reserved)	0	
		EBX	[3:0]	Number of Interrupt Thresholds in Digital Thermal Sensor (DTS)	2	2 thresholds
			[31:4]	(Reserved)	0	
		ECX	0	Hardware Coordination Feedback Capability	1	Supported. IA32_MPERF (MSR E7h) and IA32_APERF (MSR E8h) are present
			[2:1]	(Reserved)	0	
			3	Performance-Energy BIAS Preference support	0	Not Supported IA32_ENERGY_PERFORMANCE_BIAS (MSR 1B0h) is not available
			[31:4]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 7— Extended feature Flags

The output shown in Table 13, "CPUID Leaf 7h" depends on the ECX input value.

Table 13. CPUID Leaf 7h (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
7	0	EAX	[31:0]	Maximum supported sub-leaf for CPUID leaf 7	0	Only sub-leaf 0
		EBX	0	**FSGSBASE** - Support for RDFSBASE/RDGSBASE/ WRFSBASE/WRGSBASE	1	Supported
			1	Support for IA32_TSC_ADJUST (MSR 3Bh)	1	Supported
			2	**SGX** - Support for Secure Enclaves (SE) and Intel® Software Guard Extensions (Intel® SGX)	0	Not Supported
			3	**BMI1** - Bit Manipulation Set 1	0	Not Supported
			4	HLE	0	Not Supported
			5	**AVX2** - Intel® Advanced Vector Extensions 2 (Intel® AVX2)	0	Not Supported
			6	(Reserved)	0	
			7	**SMEP** - Supervisor-Mode Execution Prevention	1	Supported
			8	**BMI2** - Bit Manipulation Set 2	0	Not Supported
			9	**ERMS** - Support for Enhanced REP MOV/STOSB	1	Supported
			10	**INVPCID** - Support for INVPCID instruction	0	Not Supported
			11	**RTM** - HLE+/RTM	0	Not Supported
			12	Support for Platform Quality of Service Monitoring (PQM) capability	0	Not Supported
			13	FPU CS and FPU DS Deprecation	1	The processor depreciates FPU CS and FPU DS values and these fields are 0000h
			14	Intel® Memory Protection Extensions (Intel® MPX)	1	Supported
			15	Support for Platform Quality of Service Enforcement (PQE)	1	Supported
			16	**AVX512F** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512) Foundation instructions)	0	Not Supported
			17	**AVX512DQ** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			18	**RDSEED** - Read Random SEED instruction	1	Supported
			19	(Reserved)	0	
			20	**SMAP** - Supervisory Mode Access Protection and the LAC/STAC instructions	1	Supported

Table 13. CPUID Leaf 7h (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
7	0	EBX	21	**AVX512IFMA** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			22	**PCOMMIT** - Persistent Commit instruction	0	Not Supported
			23	**CLFLUSHOPT** - Flush a Cache Line Optimized instruction	1	Supported
			24	(Reserved)	0	
			25	Intel® Processor Trace (Intel® PT)	1	Supported
			26	**AVX512PF** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			27	**AVX512ER** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			28	**AVX512CD** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			29	**SHA** - Intel® Secure Hash Algorithm Extensions (Intel® SHA Extensions)	1	Supported
			30	**AVX512BW** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			31	**AVX512VL** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
		ECX	0	**PREFETCHWT1** - PREFETCHWT1 instruction	0	Not Supported
			1	**AVX512VBMI** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Not Supported
			[31:2]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
7	1+	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 8 — Reserved

CPUID leaf 8 is not supported and is reserved. Zeros are returned.

CPUID Leaf 9 — Direct Cache Access (DCA) Information

CPUID leaf 9 is not supported and is reserved. Zeros are returned.

CPUID Leaf Ah — Architectural Performance Monitoring

Table 14. CPUID Leaf Ah

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
A	n/a	EAX	[7:0]	Version ID of architectural performance monitoring	4	Version 4
			[15:8]	Number of general-purpose, performance monitoring counters per logical processor	4	4 counters
			[23:16]	Bit width of general-purpose, performance monitoring counter	0x30	48 bits
			[31:24]	Length of EBX bit vector to enumerate architectural events	7	7
		EBX	0	Core Cycle event unavailable	0	Core Cycle event is available
			1	Instruction Retired event unavailable	0	Instruction Retired event is available
			2	Reference Cycles event unavailable	0	Reference Cycles event is available
			3	Last-level cache (L2 Cache) reference event unavailable	0	Last-level cache (L2 Cache) reference event is available
			4	Last-level cache (L2 Cache) misses event unavailable	0	Last-level cache (L2 Cache) misses event is available
			5	Branch instruction retired event unavailable	0	Branch instruction retired event is available
			6	Branch mispredict retired event unavailable	0	Branch mispredict retired event is available
		ECX	[31:0]	(Reserved)	0	
		EDX	[4:0]	Number of fixed-function performance counters (if Version ID > 1)	3	3 counters
			[12:5]	Bit width of fixed-function performance counters (if Version ID > 1)	0x30	48 bits
			[31:13]	(Reserved)	0	

CPUID Leaf Bh — Extended Topology Enumeration

CPUID leaf Bh has two sub-leaves.

Table 15. CPUID Leaf Bh

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
B	0	EAX	[4:0]	Number of bits to shift right on x2APIC ID (EDX[31:0]) to get a unique topology ID of the next level type	1	Shift right 1 bit
			[31:5]	(Reserved)	0	
		EBX	[15:0]	Number of logical processors at this level type. The number reflects configuration as shipped by Intel	1	1 logical processor
			[31:16]	(Reserved)	0	
		ECX	[7:0]	Level Number - Same value as ECX input	0	Level 0
			[15:8]	Level Type	1	SMT level
			[31:16]	(Reserved)	0	
		EDX	[31:0]	x2APIC ID the current logical processor	Varies	
	1	EAX	[4:0]	Number of bits to shift right on x2APIC ID (EDX[31:0]) to get a unique topology ID of the next level type	5	Shift right 5 bits
			[31:5]	(Reserved)	0	
		EBX	[15:0]	Number of logical processors at this level type. The number reflects configuration as shipped by Intel	2, 4, 8, 0xB, or 0x10	2, 4, 8, 12, or 16 depending on product SKU
			[31:16]	(Reserved)	0	
		ECX	[7:0]	Level Number - Same value as ECX input	1	Level 1
			[15:8]	Level Type	2	Core level
			[31:16]	(Reserved)	-	0
		EDX	[31:0]	x2APIC ID the current logical processor	Varies	
	2+	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	Original ECX	2+	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf Ch — Reserved

CPUID leaf Ch is not supported and is reserved. Zeros are returned.

CPUID Leaf Dh — Intel® Memory Protection Extensions (Intel® MPX), XSAVE Feature

CPUID leaf Dh has six sub-leaves (0 through 4, and 8) and is shown in Table 16, "CPUID Leaf Dh". The other sub-leaves are reserved.

Table 16. CPUID Leaf Dh (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
D	0	EAX	0	**X87 State** - Legacy Floating Point (x87/MMX)	1	Legacy FP state can be managed by XSAVE
			1	**SSE State** - Intel® Streaming SIMD Extensions (Intel® SSE)	1	Intel® SSE state can be managed by XSAVE
			2	**AVX State** - Advanced Vector Extensions (Intel® AVX)	0	Intel® AVX state cannot be managed by XSAVE
			3	**BNDREGS State** - Intel® Memory Protection Extensions (Intel® MPX) BNDREGS	1	Intel® MPX Bound Registers (BNDREGS) can be managed by XSAVE
			4	**BNDCSR State** - Intel® Memory Protection Extensions (Intel® MPX) BNDCSR	1	Intel® MPX Bound Control and Status Register (BNDCSR) can be managed by XSAVE
			[7:5]	**AVX-512 State** - Intel® Advanced Vector Extensions 512 (Intel® AVX-512)	0	Intel® AVX-512 not supported and cannot can be managed by XSAVE
			8	**PT State** - Intel® Processor Trace (Intel® PT), used for IA32_XSS (MSR DA0h)	0	Intel® PT MSRs state cannot can be managed by XSAVE
			9	**PKRU State** - Protection-key feature's register PKRU	0	PKRU state cannot can be managed by XSAVE
			[31:10]	(Reserved)	0	
		EBX	[31:0]	Maximum size required for features enabled in XCR0	0x240	576 bytes
		ECX	[31:0]	Max size required by all processor supported features	0x440	1088 bytes
		EDX	[31:0]	(Reserved)	0	
	1	EAX	0	Availability of XSAVEOPT	1	Available
			1	Support of XSAVEC and compact extensions of legacy XSTROR	1	Supported
			2	Support of XGETBV Leaf 1	1	Supported
			3	Support of XSAVES and XRSTORS instructions, and IA32_XSS (MSR DA0h)	1	Supported
			[31:4]	(Reserved)	0	
		EBX	[31:0]	Maximum size required for features enabled in XCR0 | IA32_XSS (MSR DA0h)	0x240	576 bytes
		ECX	[7:0]	(Reserved)	0	
			8	**PT State** - Intel® Processor Trace (Intel® PT)	1	Corresponding bit in IA32_XSS (MSR DA0h) can be set
			[31:9]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

Table 16. CPUID Leaf Dh (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
D	2	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	3	EAX	[31:0]	Intel® Memory Protection Extensions (Intel® MPX) - Size of feature state-save area	0x40	64 bytes
		EBX	[31:0]	Intel® MPX - Offset of feature state-save area	0x3C0	960 bytes
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	4	EAX	[31:0]	Intel® MPX - Size of feature state-save area	0x40	64 bytes
		EBX	[31:0]	Intel® MPX - Offset of feature state-save area	0x400	1024 bytes
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	8	EAX	[31:0]	Intel® Processor Trace (Intel® PT) - Size of Intel® PT state-save area	0x80	128 bytes
		EBX	[31:0]	(Reserved)	0	
		ECX	0	Intel® PT - Supervisor State	1	Intel® PT is supported in IA32_XSS (MSR DA0h)
			[31:1]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	All other values of ECX	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf Eh — Reserved

CPUID leaf Eh is not supported and is reserved. Zeros are returned.

CPUID Leaf Fh — Platform and Cache Quality of Service (QoS)

CPUID leaf Fh, Platform QoS Monitoring Enumeration and Cache QoS Monitoring Capability, is not supported and is reserved. Zeros are returned.

CPUID Leaf 10h — Platform and Cache QoS Enforcement Enumeration

CPUID leaf 10h contains three sub-leaves and is show in Table 17, "CPUID Leaf 10h".

Table 17. CPUID Leaf 10h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
10	0	EAX	[31:0]	(Reserved)	0	
		EBX	0	(Reserved)	0	
			1	L3 Cache	0	SoC has no L3 Cache
			2	L2 Cache	1	Supports L2 Cache QoS Enforcement
			[31:3]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	1	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	
	2	EAX	[4:0]	Length of Masks (minus 1)	7	8
			[31:5]	(Reserved)	0	
		EBX	[31:0]	Bitmask	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[15:0]	Highest COS number supported for this ResID (minus 1)	3	4 is highest number
			[31:16]	(Reserved)	0	
	3+	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 11h — Reserved

CPUID leaf 11h is not supported and is reserved. Zeros are returned.

CPUID Leaf 12h — Reserved

CPUID leaf 12h is not supported and is reserved. Zeros are returned.

CPUID Leaf 13h — Reserved

CPUID leaf 13h is not supported and is reserved. Zeros are returned.

CPUID Leaf 14h — Intel® Processor Trace (Intel® PT) Enumeration

CPUID leaf 14h has two sub-leaves and is shown in Table 18, "CPUID Leaf 14h".

Table 18. CPUID Leaf 14h (Sheet 1 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
14	0	EAX	[31:0]	Maximum valid sub-leaf	1	Only sub-leaves 0 and 1 are valid
		EBX	0	CR3 Filtering Support	1	IA32_RTIT_CTL (MSR 570h) can be set to 1, and that IA32_RTIT_CR3_MATCH (MSR 572h) can be accessed
			1	Support for Cycle-Accurate Mode and Configurable PSB	1	Supported
			2	Support for IP filtering, TraceStop filtering, and MTC timing packet	1	Supported
			3	Support for Processor Trace MSRs preserved across warm reset	1	Supported
			[31:4]	(Reserved)	0	
		ECX	0	Support of ToPA Output scheme	1	Supported. Tracing can be enabled with the ToPA bit of IA32_RTIT_CTL (MSR 570h)
			1	ToPA Tables Support Multiple Output Regions	1	Supported
			2	Support of Single-Range Output scheme	1	Supported
			3	Support of output to Trace Transport subsystem	0	Not Supported
			[30:2]	(Reserved)	0	
			31	Support of IP payloads contain LIP	1	Generated packets which contain IP payloads contain LIP values, which include the CS base component
		EDX	[31:0]	(Reserved)	0	
	1	EAX	[1:0]	Number of configurable Address Ranges for filtering supported	2	2 ranges
			[15:2]	(Reserved)	0	
			[31:16]	Bitmap of supported MTC Period encodings	0x249	0x249
		EBX	[15:0]	Bitmap of supported Cycle Threshold Value encodings	0xFFFF	0xFFFF
			[31:16]	Bitmap of supported configurable PSB Frequency encodings	0x003F	0x003F
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

Table 18. CPUID Leaf 14h (Sheet 2 of 2)

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
14	2+	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 15h — Time Stamp Counter (TSC) and Crystal Clock Ratio

CPUID leaf 15h is the last Basic CPUID leaf.

Table 19. Basic CPUID Leaf 15h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
15	n/a	EAX	[31:0]	Denominator of TSC/crystal clock ratio	3	3
		EBX	[31:0]	Numerator of TSC/crystal clock ratio	0xC0	192
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaves 16h through 7FFFFFFFh — Reserved

CPUID leaves 16h through 7FFFFFFFh are not supported and are reserved. Each of these leaves produces the same EAX, EBX, ECX, and EDS values as leaf 15h.

CPUID leaves greater than 80000000h are also reserved and produce the same EAX, EBX, ECX, and EDS values as leaf 15h.

CPUID Leaf 80000000h — Maximum EAX Value for CPUID Instruction

Table 20. Extended CPUID Leaf 80000000h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000000	n/a	EAX	[31:0]	Maximum input value in EAX for Extended Function CPUID information	0x80000008	0x80000008 is the maximum value
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 80000001h — Extended Feature Flags

Table 21. Extended CPUID Leaf 80000001h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000001	n/a	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	0	Availability of LAHF and SAHF instructions in 64-bit mode	1	Available
			5	Availability of LZCNT instruction	0	Not Available
			[7:1]	(Reserved)	0	
			8	Availability of PREFETCHW instruction	1	Available
			[31:9]	(Reserved)	0	
		EDX	[10:0]	(Reserved)	0	
			11	Availability of SYSCALL and SYSTRET instructions in 64-bit mode	1	Available
			[19:12]	(Reserved)	0	
			20	Availability of the Execute Disable Bit	Varies	1 indicates Available. Will be 1 whenever the NX_DISABLE bit of IA32_CR_MISC_ENABLES (MSR 1A0h) = 0
			[25:21]	(Reserved)	0	
			26	1 GB Pages	1	Enabled
			27	RDTSCP/IA32_TSC_AUX	1	1
			28	(Reserved)	0	
			29	Availability of Intel® 64 Architecture	1	Available
			[31:30]	(Reserved)	0	

CPUID Leaves 80000002h, 80000003h, and 80000004h— Intel Processor Brand String

Table 22. Extended CPUID Leaves 80000002h, 80000003h, and 80000004h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000002	n/a	EAX	[31:0]	Processor Brand String	65746E49	
		EBX	[31:0]		2952286C	
		ECX	[31:0]		6F744120	
		EDX	[31:0]		4D54286D	
80000003	n/a	EAX	[31:0]		50432029	
		EBX	[31:0]		33432055	
		ECX	[31:0]		20383538	
		EDX	[31:0]		2E322040	
80000004	n/a	EAX	[31:0]		48473030	
		EBX	[31:0]		7A	
		ECX	[31:0]		0	
		EDX	[31:0]		0	

CPUID Leaf 80000005h — Reserved

CPUID leaf 80000005h is not supported and is reserved. Zeros are returned.

CPUID Leaf 80000006h — Cache Parameters

Table 23. Extended CPUID Leaf 80000006h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000006	n/a	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[7:0]	Cache Line Size	0x40	64
			[15:12]	Associativity field	0x8	8
			[31:16]	Cache size in 1k units	0x800	2048 1k units (2MB)
		EDX	[31:0]	(Reserved)	0	

CPUID Leaf 80000007h — Advanced Power Management

Table 24. Extended CPUID Leaf 80000007h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000007	n/a	EAX	[31:0]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[7:0]	(Reserved)	0	
			8	Always Running TSC	1	Available
			[31:9]	(Reserved)	0	

CPUID Leaf 80000008h — Virtual/Physical Address Sizes

Table 25. Extended CPUID Leaf 80000008h

Leaf [EAX] (Hex)	Sub-leaf [ECX] (Hex)	CPUID Results	Bits	Meaning	Returned Value	What Value Indicates
80000008	n/a	EAX	[7:0]	Number of Physical Address Bits	0x27	39 bits
			[15:8]	Number of Linear Address Bits	0x30	48 bits
			[31:16]	(Reserved)	0	
		EBX	[31:0]	(Reserved)	0	
		ECX	[31:0]	(Reserved)	0	
		EDX	[31:0]	(Reserved)	0	

The BIOS is able to determine the silicon stepping of the entire SoC. This is accomplished by reading the 32-bit Manufacturer ID Register in configuration space, bus 0, device 0, function 0, offset F4h. The Bit 15:8 shows manufacturing ID which is processor ID. PCI Rev ID is located on bus0, device 31, function0, offset 08h bit [7:0].

Table 26 shows the information received when this register is read.

Table 26. SoC Stepping Information

Parameter	B1 SoC
Process ID	0Fh
PC Rev ID	11

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® C3000 Processor Product Family may be identified by the following component markings.

Table 27. Component Marking Information

SKU Name	S-Spec/Top Marking	Processor Number	Core Count	Speed (GHz)
SKU 0	SR3F3	C3955	16C	2.1
SKU 1	SR383	C3950	16C	1.7
SKU 2	SR387	C3850	12C	2.1
SKU 3	SR386	C3830	12C	1.9
SKU 4	SR385	C3750	8C	2.2
SKU 5	SR381	C3958	16C	2.0
SKU 6	SR38A	C3858	12C	2.0
SKU 7	SR389	C3758	8C	2.2
SKU 8	SR388	C3558	4C	2.2
SKU 9	SR3L7	C3538	4C	2.2
SKU 10	SR38B	C3338	2C	1.5
SKU 11	SR38C	C3808	12C	2.0
SKU 12	SR38F	C3708	8C	1.7
SKU 13	SR3JX	C3508	4C	1.6
SKU 14	SR38D	C3308	2C	1.6
SKU 18	SRCZL	C3336	2C	1.5
SKU 7R	SRH4F	C3758R	8C	2.4
SKU 8R	SRH4G	C3558R	4C	2.4
SKU 19	SRJQN	C3436L	4C	1.3
SKU 10R	SRH4E	C3338R	2C	1.8

Figure 2. Top Markings

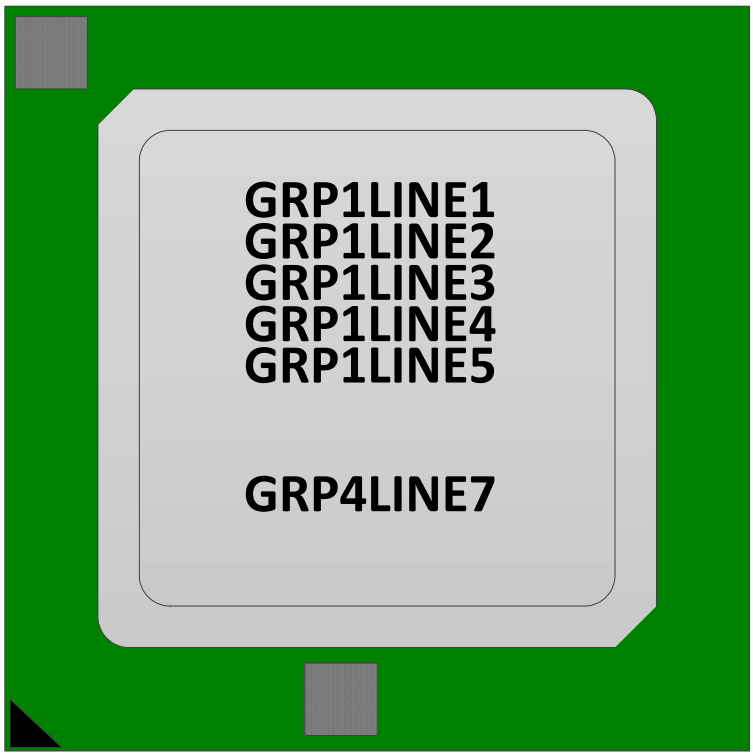


Table 28. Top Markings

Side	Group	Line	Text	Example
Top	1	1	\ (this is the Intel swirl)	
Top	1	2	INTEL CONFIDENTIAL	INTEL CONFIDENTIAL
Top	1	3	NA	NA
Top	1	4	"SPEC""SPEC#Q" "SPEED"GHZ	QJ3C 1.70GHZ
Top	1	5	{FPO} {e1}	FPO45678 e1
Top	4	7	Blank/Number	752RP488801939

§

Errata

DNV1. HECI Line Interrupt May Not be Generated

Problem: There are three different Host Embedded Controller Interface (HECI) interfaces used to communicate between Innovation Engine (IE)/Intel® Management Engine (Intel® ME) and the host CPU cores. Due to this erratum, if any HECI interfaces are configured to send different types of line interrupts (INTA, INTB, INTC, INTD, SMI, SCI and NMI), then interrupts may not be generated as expected.

Implication: An interrupt being missed may lead to the system hanging or experiencing other unexpected behavior. MSIs are not affected by this erratum.

Workaround: Software should configure all line interrupts to use the same type or use MSIs.

Status: No Fix.

DNV2. xHCI Host Controller Reset May Cause a System Hang

Problem: Within 1 ms of setting the Host Controller Reset bit (HCRST bit 1) of the USB Command Register (xHCI BAR + 80h), the xHCI host controller may fail to respond to register accesses.

Implication: The system may hang.

Workaround: None identified.

Note: Software must not make any accesses to the xHCI Host Controller registers for 1 ms after setting the HCRST bit 1 of the USB Command Register (xHCI BAR + 80h) and must add a 120 ms delay in between consecutive xHCI host controller resets.

Status: No Fix.

DNV3. USB DBC-EXI is Not Enumerated Correctly

Problem: USB DBC-EXI (Debug Capability External Interface) incorrectly returned non-zero indexes with zero length device descriptor strings.

Implication: Software may fail to enumerate the device when non-zero length device descriptor strings are returned with non-zero indexes.

Workaround: Software can ignore device descriptor strings that are zero length even if the index is non-zero.

Status: No Fix.

DNV4. Performance Monitoring Event Branch Retired May Increment Twice For Near RET Imm16

Problem: A Near RET imm16 instruction may increment performance monitoring event BR_INST_RETIRED.ALL_BRANCHES (Event C4H, UMask 00H) twice instead of once. This erratum does not occur if the UMask bits 3 (BR_INST_RETIRED.REMOVE_RET) and/or 7 (BR_INST_RETIRED.REMOVE_NOT_TAKEN_JCC) are set.

Implication: A performance monitoring counter counting the branch retired event may overcount. Software relying on the branch retired event incrementing deterministically may not function correctly.

Workaround: None identified. Software could have one counter count all branches other than not-taken JCC (UMask 7FH) and another counter count not-taken JCC (UMask 80) and sum them to produce the total count.

Status: No Fix.

DNV5. NCSI_RXD Output Cannot be Tri-State to Meet NCSI Specification

Problem: When a Network Controller Sideband Interface (NCSI) interface is de-selected, the NCSI receive Data NCSI_RXD[1:0] lines are constantly driven to “0” instead of entering tri-state mode.

Implication: This erratum prevents correct functionality of a shared-bus (multi-drop) NCSI topology. This issue does not affect point-to-point NCSI configuration design topology.

Workaround: None identified.

Status: No Fix.

DNV6. The X553 Ethernet Controller Transmitter Transition Time Does Not Conform to IEEE 802.3 Specification

Problem: The X553 transmitter may not meet IEEE* 802.3 clause 70 1000BASE-X specification for transition time compliance.

Implication: Compliance Testing may report specification violations. Intel has not observed any functional impact due to this errata. Intel has obtained a waiver.

Workaround: None identified.

Status: No Fix.

DNV7. 10 GBASE-KR Transmitter Does Not Fully Conform to Specification For Equalization

Problem: The processor's 10GBASE-KR transmitter does not conform to IEEE 802.3ap-2007 electrical specification.

- — Section 72.7.1.11 - For any coefficient update, the magnitudes of the changes in v1, v2, and v3 shall be within 5 mV of each other but processor's limit is 11 mV.
- — Table 72-8 - The pre-cursor equalization ratio (Rpre) is to be in range 0.95 - 1.05 with a coefficient status of c (1) disabled, c(0) maximum, and c(-1) disabled; the processor Rpre ratio is in the range 0.95 to 1.08 with the coefficient status listed.

Implication: Compliance testing may report specification violations. Intel has not observed any functional impact due to this erratum. Intel has obtained a waiver.

Workaround: None identified.

Status: No Fix.

DNV8. Split Access to APIC-Access Page May Access Virtual-APIC Page

Problem: A read from the APIC-access page that splits a cacheline boundary should cause an APIC-access VM exit. Due to this erratum, the processor may redirect such accesses to the virtual-APIC page without causing an APIC-access VM exit.

Implication: Guest software that attempts to access its APIC with a cacheline split may not be properly virtualized.

Workaround: None identified.

Status: No Fix.

DNV9. PEBS Record EventingIP Field May be Incorrect After CS.Base Change

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

Implication: Software attempting to identify the instruction that caused the PEBS event may report an 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: No Fix.

DNV10. 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: No Fix.

DNV11. SMRAM State-Save Area Above The 4 GB Boundary May Cause Unpredictable System Behavior

Problem: If BIOS uses the RSM instruction to load the SMBASE register with a value that would cause any part of the SMRAM state-save area to have an address above 4 GB, subsequent transitions into and out of SMM (system-management mode) might save and restore processor state from incorrect addresses.

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

Workaround: Ensure that the SMRAM state-save area is located entirely below the 4 GB address boundary.

Status: No Fix.

DNV12. POPCNT Instruction May Take Longer to Execute Than Expected

Problem: POPCNT instruction execution with a 32- or 64-bit operand may be delayed until previous non-dependent instructions have executed.

Implication: Software using the POPCNT instruction may experience lower performance than expected.

Workaround: None identified.

Status: No Fix.

DNV13. APIC-Access VM Exit May Occur Instead of SMAP #PF

Problem: A supervisor-mode data access through a user-mode page should cause a #PF if CR4.SMAP (Supervisor-Mode Access Prevention) is 1 and EFLAGS.AC is 0. Due to this erratum, a guest supervisor mode access to the APIC-access page may cause an APIC-access VM exit instead of a #PF due to SMAP.

Implication: A guest may miss an SMAP violation if it maps its APIC through a user-mode page. Intel has not observed this erratum with any commercially available software.

Workaround: Guest software should not map their APIC to a user mode page and attempt to access it from supervisor mode.

Status: No Fix.

DNV14. 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 Performance Monitoring Counters (PMCs) on a Performance Monitoring Interrupt (PMI) request by setting CTR_Frz bit 49 in IA32_PERF_GLOBAL_STATUS MSR (38EH). Due to this erratum, if FREEZE_PERFMON_ON_PMI is enabled, PMC overflows that occur within a few cycles of a PMI being pended may not be logged in IA32_PERF_GLOBAL_STATUS MSR.

Implication: A performance counter may overflow but not set the overflow bit in IA32_PERF_GLOBAL_STATUS MSR.

Workaround: Re-enabling the PMCs in UA32_PERF_GLOBAL_CTRL will log the overflows that were not previously logged in IA32_GLOBAL_STATUS.

Status: No Fix.

DNV15. Performance Monitoring OFFCORE_RESPONSE1 Event May Improperly Count L2 Evictions

Problem: Due to this erratum, a performance monitoring counter configured to count OFFCORE_RESPONSE1 (Event B7H, Umask 02H) uses MSR_OFFCORE_RSP0.COREWB (MSR 1A6H, bit 3) instead of the expected MSR_OFFCORE_RSP1.COREWB (MSR 1A7H, bit 3).

Implication: A performance monitoring counter using the OFFCORE_RESPONSE1 event will not count L2 evictions as expected when the COREWB value is not the same in MSR_OFFCORE_RSP1 and in MSR_OFFCORE_RSP0.

Workaround: None identified.

Status: No Fix.

DNV16. Debug Exception May Not be Generated on Memory Read Spanning a Cacheline Boundary

Problem: A debug exception should be generated on a read which accesses an address specified by a breakpoint address register (DR0-DR3) and its LEN*n* field (in DR7) configured to monitor data reads. Due to this erratum, under complex microarchitectural conditions the processor may not trigger a debug exception on a memory read that spans a cacheline boundary.

Implication: When this erratum occurs, a debugger is not notified of a read that matches a data breakpoint.

Workaround: None identified.

Status: No Fix.

DNV17. Intel® PT CR3 Filtering Compares Bits [11:5] of CR3 And IA32_RTIT_CR3_MATCH Outside of PAE Paging Mode

Problem: CR3[11:5] are used to locate the page-directory-pointer table only in PAE paging mode. When using Intel® Processor Trace (Intel® PT), those bits of CR3 are compared to IA32_RTIT_CR3_MATCH (MSR 572H) when IA32_RTIT_CTL.CR3Filter (MSR 570H bit 7) is set, independent of paging mode.

Implication: Any value written to the ignored CR3[11:5] bits which can only be non-zero outside of PAE paging mode must also be written to IA32_RTIT_CR3_MATCH[11:5] in order to result in a CR3 filtering match.

Workaround: None identified.

Status: No Fix.

DNV18. Intel® PT OVF Packet May be Followed by TIP.PGD Packet

Problem: If the Intel® Processor Trace (Intel® PT) encounters an internal buffer overflow and generates an OVF (Overflow) packet just as IA32_RTIT_CTL (MSR 570H) bit 0 (TraceEn) is cleared, or during a far transfer that causes IA32_RTIT_STATUS.ContextEn[1] (MSR 571H) to be cleared, the OVF may be followed by a TIP.PGD (Target Instruction Pointer - Packet Generation Disable) packet.

Implication: The Intel PT decoder may not expect a TIP.PGD to follow an OVF which could cause a decoder error.

Workaround: The Intel PT decoder should ignore a TIP.PGD that immediately follows OVF.

Status: No Fix.

DNV19. Intel® PT OVF May be Followed by an Unexpected FUP Packet

Problem: Certain Intel® Processor Trace (Intel® PT) packets, including FUPs (Flow Update Packets), should be issued only between TIP.PGE (Target IP Packet - Packet Generation Enable) and TIP.PGD (Target IP Packet - Packet Generation Disable) packets. When outside a TIP.PGE/TIP.PGD pair, as a result of IA32_RTIT_STATUS.FilterEn[0] (MSR 571H) being cleared, an OVF (Overflow) packet may be unexpectedly followed by a FUP.

Implication: The Intel PT decoder may incorrectly assume that tracing is enabled and resume decoding from the FUP IP.

Workaround: The Intel PT decoder may opt to scan ahead for other packets to confirm whether PacketEn is set.

Status: No Fix.

DNV20. Performance Monitoring COREWB Offcore Response Event May Overcount

Problem: An L2 eviction may affect the OFFCORE_RSP0 or OFFCORE_RSP1 performance monitoring events if it is configured to count COREWB occurrences or average offcore request latency even if the eviction was caused by an access made by a different core sharing the L2 cache.

Implication: The offcore response events may overcount when configured to count COREWB occurrence.

Workaround: None identified.

Status: No Fix.

DNV21. FBSTP May Update FOP/FIP/FDP/FSW Before Exception or VM Exit

Problem: Due to this erratum, a FBSTP whose memory access causes an exception (for example, #PF or #GP) or VM exit (for example, EPT violation), may unexpectedly update FOP, FIP, FDP, FSW.IE or FSW.PE. FSW.ES is not affected by this erratum.

Implication: An x87 exception handler that executes an FBSTP but relies on the FP exception state being unchanged after taking a memory exception may not behave as expected. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: No Fix.

DNV22. PEBS Record May be Generated When Counters Frozen

Problem: When Performance Monitoring counters are frozen due to IA32_PERF_GLOBAL_STATUS.CTR_Frz MSR (38EH, bit 59) being set, a Processor Event Based Sampling (PEBS) record may still be generated for counter 0 when the event specified by IA32_PERFEVTSEL0 MSR (186H) occurs.

Implication: An unexpected PEBS record may cause performance analysis software to behave unexpectedly.

Workaround: None identified.

Status: No Fix.

DNV23. IA32_PERF_GLOBAL_INUSE[62] May be Set

Problem: IA32_PERF_GLOBAL_INUSE MSR (392H) bit 62 is reserved. However, due to this erratum, it may sometimes be read as 1.

Implication: A read of IA32_PERF_GLOBAL_INUSE MSR may see bit 62 set in the result.

Workaround: None identified.

Status: No Fix.

DNV24. xHCI Split-Transactions Error Counter Reset Issue

Problem: The xHCI controller may not reset its split transaction error counter if a high-speed USB hub propagates a malformed bit from a low-speed or full-speed USB device exhibiting non-USB specification compliant signal quality.

Implication: Device dependent. Full speed and low speed devices behind the hub may be re-enumerated and may cause a device to not function as expected.

Workaround: None identified.

Status: No Fix.

DNV25. Data Breakpoints May Not be Detected on Split Reads

Problem: A debug exception should be generated on a read which accesses an address specified by a breakpoint address register and its LENn field configured to monitor data reads. Due to this erratum, under complex microarchitectural conditions the processor may not trigger a debug exception on a cacheline split memory read.

Implication: A debugger may not be notified when a read occurs that should match a data breakpoint if the read splits a cacheline.

Workaround: None identified.

Status: No Fix.

DNV26. Intel® Trace Hub PTI Pattern Generator May Stop Working When Width is Changed While Enabled

Problem: Intel® Trace Hub (Intel® TH) Parallel Trace Interface (PTI) pattern generator feature is used to test the connectivity between PTI port and trace capture hardware. Due to this erratum, once enabled the pattern generator may hang if the width is decreased.

Implication: Intel TH's pattern generator feature stops working when users decrease the width.

Workaround: Intel TH's PTI pattern generator width should be reconfigured only after an Intel TH soft reset. Intel TH soft reset can be done by setting NPKDSC.FLR bit to '1'.

Status: No Fix.

DNV27. UART_IE_TXD Signal May be Low When IE Enters The Off State (Cloff)

Problem: If Innovation Engine (IE) owns the IE UART pins and has them configured in UART mode when the IE enters the off state (Cloff) the UART_IE_TXD signal is driven low when it should be driven high.

Implication: Due to this erratum, the UART connected to the IE UART might interpret UART_IE_TXD low as a continue stream of "0"s.

Workaround: The IE needs to program the UART_IE_TXD pin as a GPO (General Purpose Output) driving "1" before entering Cloff. When existing Cloff IE needs to put UART_IE_TXD back into UART mode. Refer to the *Innovation Engine Developers Guide*, document ID558866 for more information.

Status: No Fix.

DNV28. Intel® Trace Hub May Report Timeout Error Incorrectly

Problem: Intel® Trace Hub (Intel® TH) can incorrectly report a timeout error in the NPKDSC (Device 4,5,6; Function 0; Offset 80h) register when the ICTOT (Inbound CCB Timeout Timer) and ISTOT (Inbound Switch Timeout Timer) are programmed from 0 to any non-zero value.

Implication: The user may observe a timeout error when none has occurred. Intel has not observed this erratum in commercially available software.

Workaround: None identified.

Status: No Fix.

DNV29. Larger Than 32-Bit Writes to Intel® Trace Hub CSR_MTB_BAR May Cause a System Hang

Problem: Intel® Trace Hub (Intel® TH) fails to fully receive or respond to writes larger than 32-bits to CSR_MTB_BAR (BAR0) MMIO region. This may lead to a system hang.

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

Workaround: None identified.

Status: No Fix.

DNV30. Potential Partial Trace Data Loss in Intel® Trace Hub ODLA When Storing to Memory

Problem: When On-Die Logic Analyzer (ODLA) is configured to trace to memory, under complex microarchitectural conditions, the trace may lose a timestamp.

Implication: Some ODLA trace data may be lost. This erratum does not affect other trace data sources. Typically lost trace data will be displayed as "OVERFLOW." Subsequent timestamps will allow the trace decoder to resume tracing. Intel has not observed this erratum in commercially available software.

Workaround: None identified. For a particular workload, changing the memory buffer size or disabling deep compression may eliminate the microarchitectural condition that caused the erratum.

Status: No Fix.

DNV31. Intel® Trace Hub Pipeline Empty Bit For PTI May be Not Set

Problem: If the Parallel Trace Interface (PTI) Port P2NULL bit in the GTHOPT0 register (CSR_MTB_BAR; Offset 0; bit 19) is set during tracing, and subsequently cleared (during tracing or after tracing is completed), the PLE (Pipeline Empty) bit (GTHSTAT register; Offset 0xD4; bit 2) may not be set to 1 even when the pipeline is empty.

Implication: Software may loop continuously waiting for Intel Trace Hub PTI PLE bit to be set.

Workaround: If P2NULL must be set during tracing, then termination of tracing must involve these additional steps: When pipeline empty is not set within a microsecond of terminating tracing, sending a FLAG packet may enable PTI PLE bit to be set. If the PTI PLE bit is not set after the FLAG packet is sent, software should repeat the sending a FLAG packet and checking the PLE bit up to two more times.

Status: No Fix.

DNV32. Intel® Trace Hub TAP Data Registers Are Read-Once

Problem: Each Intel Trace Hub TAP DR (Data Register) stores data shifted-in on the TDI pin into the DR on a TAP read operation.

Implication: Intel Trace Hub TAP DRs can be read only once. Subsequent DR reads will deliver unexpected data.

Workaround: None identified. Do not perform repeated reads.

Status: No Fix.

DNV33. Performance Monitoring Event Branch Retired May Increment Twice For Near RET Imm16

Problem: A Near RET imm16 instruction may increment performance monitoring event BR_INST_RETIRED.ALL_BRANCHES (Event C4H, UMask 00H) twice instead of once. This erratum does not occur if the UMask bits 3 (BR_INST_RETIRED.REMOVE_RET) and/or 7 (BR_INST_RETIRED.REMOVE_NOT_TAKEN_JCC) are set.

Implication: A performance monitoring counter counting the branch retired event may overcount. Software relying on the branch retired event incrementing deterministically may not function correctly.

Workaround: None identified. Software could have one counter count all branches other than not-taken JCC (UMask 7FH) and another counter count not-taken JCC (UMask 80) and sum them to produce the total count.

Status: No Fix.

DNV34. NEWCENTURY_STS Cannot be Cleared

Problem: The NEWCENTURY_STS bit in TCO1_STS register (TCOBASE + 4h, bit7) cannot be cleared by software writing a "1" back to the bit position. If the bit is written again the system may hang.

Implication: When this erratum occurs, the system may hang. The failure only can be seen when the Year byte rolls over from 99 to 00.

Workaround: None Identified.

Status: No Fix.

DNV35. Intel® Processor Trace Timing Packets May Not be Generated When Clock Modulation is Enabled

Problem: Intel® Processor Trace (Intel® PT) timing packets TSC (Timestamp), TMA (TSC/MTC Align), and CBR (Core:Bus Ratio) should be generated when the clocks resume when TM1 duty cycling is active or Clock Modulation is enabled (IA32_CLOCK_MODULATION MSR 0x19A bits 4:0). Due to this erratum when clock modulation is enabled, these packets may not be generated in certain microarchitectural conditions.

Implication: Due to this erratum, the debugger may be unable to properly track wall-clock time in portions of the trace.

Workaround: Disable clock modulation when Intel Processor Trace is in use to partially work around this erratum. Note that clock modulation due to TM1 cannot be mitigated. TM1 should not be active in properly thermally managed systems.

Status: No Fix.

DNV36. Processor Host Root Complex May Incorrectly Route Memory Accesses to Intel® Trace Hub

Problem: The Intel® Trace Hub RTIT_BAR (B0:D31:F7 offset 20h) is reported as a 2 KB memory range. Due to this erratum, the processor Host Root Complex will forward addresses from RTIT_BAR to RTIT_BAR +4MB -1 to Intel Trace Hub.

Implication: Devices assigned within the RTIT_BAR to RTIT_BAR + 4 MB -1 space may not function correctly.

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

Status: No Fix.

DNV37. Legacy SMBus Clock Violates Max SMBus 2.0 Specification Frequency

Problem: The legacy SMBus clock violates the SMBus Specification 2.0 max. 100 kHz speed.

Implication: No functional failures have been observed do to this erratum.

Workaround: None Identified.

Status: No Fix.

DNV38. Intel® PT OVF Packet May Not be Followed by a FUP or TIP.PGE Packet

Problem: If Intel® Processor Trace (Intel® PT) encounters an internal buffer overflow and generates an OVF (Overflow) packet, in some rare cases that packet may not be immediately followed by the expected Flow Update Packet (FUP) or TIP.PGE (Target IP - Packet Generation Enabled) packet.

Implication: An Intel PT decoder may encounter a Taken Not Taken (TNT), Target IP (TIP), or other control flow packet immediately following an OVF packet.

Workaround: An Intel PT decoder should scan ahead to the next FUP, TIP, or TIP.PGE packet following the OVF to determine the current IP.

Status: No Fix.

DNV39. PCIe Link Capability Fields MLW And MLS For vRP Are Incorrect

Problem: The Virtual Root Port (vRP) (Bus:0; Devices:6,22,23; Function:0) register LINKCAP (Offset 0x4Ch) fields Maximum Link Width (MLW) (bits [9:4]) and Maximum Link Speed (MLS) (bits [3:0]) indicate support for a x1 PCIe link and 2.5 GT/s Link Speed only. The processor's on-die link is a x8 link operating at 8.0 GT/s (MLW = 0x08 and MLS = 0x3, respectively).

Implication: The processor's on-die PCIe link will function as a x8, 8.0 GT/s link, regardless of the values in LINKCAP register. Software that relies upon the contents of LINKCAP may not operate as expected.

Workaround: None Identified.

Status: No Fix.

DNV40. Uncompressed SPI Images May Hang SPI Interface

Problem: When Innovation Engine (IE) firmware images are configured to be read in compressed mode, if an uncompressed image is read, the Serial Peripheral Interface (SPI) controller will hang.

Implication: When this erratum occurs, the SPI controller hangs and the platform will fail to boot.

Workaround: None identified. Firmware should read from SPI BAR1 MMIO address space directly.

Status: No Fix.

DNV41. eMMC Controller May Fail to Detect Error

Problem: The eMMC controller may fail to detect a CRC error if a bit error occurs on the DATA3 signal during read operations when in eMMC HS400 or DDR50 mode. CRC detection on other DATA signals is not impacted.

Implication: The controller will not flag the CRC error to the driver or application, which could result in data integrity issues. Bit errors on eMMC DATA signals are not expected on platforms that follow Intel recommended design guidelines and tuning processes.

Workaround: None identified. To mitigate the issue, eMMC HS200 or SDR50 mode can be used instead of HS400 or DDR50.

Status: No Fix.

DNV42. PCIe Clock May go Inactive at The Same Time PERST# Goes Active

Problem: When the PERST# is driven from SoC output PLTRST_N, the processor PCIe Clock might stop at the same time as PERST# is asserted when turning off the system. The PCIe 3.0 specification requires the PCIe clock to go inactive after PERST# goes active.

Implication: When this erratum occurs, the PCIe clock goes inactive at the same time PERST# goes active. No functional failure has been observed due to this erratum.

Workaround: None Identified.

Status: No Fix.

DNV43. An Extra SMI May be Generated

Problem: Two System Management Interrupts (SMIs) may be observed when only one is expected.

Implication: When this erratum occurs, the second SMI may not have any sources set.

Workaround: None Identified.

Status: No Fix.

DNV44. 10G Base-KR Slow Link up With Link Partners Issuing PRESET

Problem: During the IEEE 802.3 Clause 72 10GBASE-KR training sequence, approximately 45 ms after link training has commenced, the X553 transmitted signal reverts back to its INITIALIZE setting. During this time, no INITIALIZE request was issued by the link partner, thus violating IEEE 802.3 Clause 72, Section 72.6.10.2.5 “Coefficient Update Process.” After the reversion back to INITIALIZE coefficients, further link training requests are responded to correctly.

Implication: Due to this erratum, if a partner issues a TxFFE coefficient request, link establishment may take a long time to link, link establishment may fail, or link may be established with non-optimal trained coefficients. This behavior is more prominent to a link partner who issues a PRESET request at the beginning of 10GBASE-KR link training.

Workaround: Link partners which issue a PRESET request at the beginning of 10GBASE-KR link training, should configure the 10GBASE-KR INITIALIZE coefficients to the same value as the PRESET coefficients. Contact your Intel representative to obtain more information.

Status: No Fix.

DNV45. Incorrect Bandwidth Calculations For LS or FS Devices Connected to USB 2.0 Hub

Problem: Incorrect bandwidth computation for low speed or full speed periodic endpoints behind USB 2.0 high speed hubs connected to xHCI controller.

Implication: Due to this erratum, LS or FS periodic endpoints may not function or be enumerated as expected.

Workaround: None identified.

Status: No Fix.

DNV46. Upstream PCIe Completion Packets With ECRC Errors May Hang Processor

Problem: If the processor receives a completion packet that contains an ECRC error, the packet will be dropped instead of receiving a NAK.

Implication: When this erratum occurs, the processor will hang with an Internal Timer Error (MCi_STATUS.MCACOD = 400H) and ECRCE (bit 19) on PCI Configuration register, ERRUNCSTS (Bus:0; Device: 9-12, 14-17; Function: 0; Offset 105h) will be set to 1. Intel has only observed this erratum in a synthetic test environment.

Workaround: None identified.

Status: No Fix.

DNV47. xHCI Short Packet Event Using Non-Event Data TRB

Problem: The xHCI may generate an unexpected short packet event for the last transfer's Transfer Request Block (TRB) when using Non-Event Data TRB with multiple TRBs.

Implication: Transfer may fail due to the packet size error.

Note: This issue has only been observed in an synthetic environment. No known implication has been identified with commercial software.

Workaround: None identified. Intel recommends software to use Data Event TRBs for short packet completion.

Status: No Fix.

DNV48. PCIe Transmitter Preset May be Incorrect During 8.0 GT/s Equalization Configuration

Problem: The PCIe transmitter should use the preset value specified in the Lane Equalization Control register (LANEEQCTL, Bus 0, Device 9-12/14-17, Function 0, Offsets 0x20c, 0x0210, 0x0214, 0x0218, bits [3:0]). However, due to this erratum, during equalization Phase 1 and Phase 2, the transmitter will instead use the equalization default value (EQEVALCTL, Bus 0, Device 9, Function 0, Offset 00000bd0, bits [27:24]). The processor will correctly use negotiated Tx presets during Phase 3 of equalization and during normal (post-equalization) 8.0 GT/s operation.

Implication: The intended equalization preset value will not be used in Equalization Phase1 and Phase2, potentially leading to high bit error rates and an inability to train the PCIe link to 8.0 GT/s.

Workaround: To work around this erratum, it is possible for the software to configure the equalization default value (EQEVALCTL) to the same value as in Lane Equalization Control (LANEEQCTL) prior to enabling the port.

Status: No Fix.

DNV49. Potential Infinite SMI Loop

Problem: If a warm or cold reset occurs after an Integrated Error Handler (IEH) System Management Interrupt (SMI) is signaled, but before the IEH SMI is cleared, an infinite SMI loop may occur after the reset.

Implication: An infinite SMI loop may occur after a warm or cold reset until a G3 power cycle occurs.

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

Status: No Fix.

DNV50. System Might Hang During AC Boot Cycle

Problem: When a global reset happens while a message is in progress from the Punit to trace hub, the trace hub can be left in an undefined state even if the trace hub is disabled.

Implication: An undefined state can result in a system hang during a global reset.

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

Status: No Fix.

DNV51. Removed

DNV52. Phase Lock loop (PLL) Feedback Circuit

Problem: The USBPCIe PLL has an independent feedback circuit. A feedback circuit timing marginality may result in a momentary jitter excursion in the corresponding PLL circuitry and downstream circuitry.

Implication: If the USBPCIe PLL loses lock, USB 3.2/PCIe/CLKOUT_PCIE interfaces may experience errors, including correctable errors, interface downtrains, or hangs.

Workaround: A software workaround has been identified for this erratum and may be available in a software update.

Status: No Fix.

DNV53. Processor May Violate SPI Flash Device Timing Requirements

Problem: The processor's SPI controller may violate the "Suspend In-Progress Program Max Latency" time configured in DWORD 12 in the flash device's Serial Flash Discoverable Parameter (SFDP) table.

Implication: Due to this erratum, the processor may violate the flash device's timing requirements, which may lead to unpredictable system behavior.

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

Status: No Fix.

DNV54. Unexpected #PF, #GP, #UD, or Other Unpredictable System Behavior May Occur

Problem: Under complex micro-architectural conditions, the processor may execute incorrect instruction bytes, leading to #PF, #GP, #UD, or other unpredictable system behavior.

Implication: Due to this erratum, the system may exhibit unpredictable behavior, including unexpected Undefined Opcode (#UD), Page Fault (#PF), or General Protection (#GP) exceptions.

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

Status: No Fix.

DNV55. HSUART May Stop Functioning When DMA is Activated

Problem: The High-Speed Universal Asynchronous Receiver/Transmitter (HSUART) may stop functioning when the HSUART DMA is active ([MEMBA] Offset 84h, C4h bits = 0, and the HSUART is receiving/transmitting information.

Implication: When this erratum occurs, the HSUART will stop receiving/transmitting information and may cause a Reorder Buffer (ROB) Timeout Error Machine Check Exception (Machine Check bank 0 [MSR 401h] with IA32_MC0_STATUS.MCACOD_ROB = 1 [bit 10).

Workaround: None identified. Software should not activate the HSUART DMA.

Status: No Fix.

DNV56. Reading TCO_RLD Register Sets SMBus Host Status in Use Status Bit

Problem: When software reads the TCO_RLD (TCOBASE Offset 0), hardware sets the In Use Status (Host Status; SMBMAR Offset 0 or SBA Offset 0; bit 6) in the SMBus controller D31:F4.

Implication: Due to this erratum, the SMBus controller may appear to be in use, causing software to not be able to use the SMBus controller.

Workaround: None identified.

Status: No Fix.

DNV57. System May Exhibit Unpredictable Behavior

Problem: Under complex microarchitectural conditions, the processor may hang or exhibit an unpredictable system behavior.

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

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

Status: No Fix.

§

Specification Changes

1. Optional SMBALERT# Signal in SMB Controller - Legacy

The optional SMBALERT# signal (SMB_LEG_ALRT_N) is wake event when the system is in S4 or S5 (soft off) power state.

§

Specification Clarifications

1. X553 Ethernet Controller Device ID and MAC Address Cannot Be Changed

To consider product quality and reliability, after implemented with "Recovery Mode in Intel(R) Ethernet Devices/Adapters" in Ethernet FW v2.00, the device cannot be changed with Device ID fields (VID, DID, SVID and SSID) and MAC address fields after the original factory programming.

If the customer would like to change the Device ID or MAC address before production, the only way is re-flash the BIOS/IFWI.

2. LAN Interface Signals Cannot Be Programed When LEK Is Running

With LAN controllers enabled, the LAN Enablement Kit (LEK) will load and take ownership of the LAN interface signals LANx_PORTx_SDPx, LANx_Portx_LEDx, NCSI_x and LAN_MDC. Due to the shared signals being used as GPIO signals or other functions signals, both LAN LEK and the BIOS may configure the signals after power on resulting in a conflict. If the LAN is enabled in the platform, the above signals are owned by the LAN controller(s), then no other software (spsFITc, BIOS, or OS) should program the signal registers to change the signals' functions.

3. GPIO Input Pulse Width To Trigger the Interrupt

When the GPIO signals are used as input to trigger the interrupt, the input pulse width has to be minimum ~170 ns to result in no interrupt loss.

§

Documentation Changes

There are no documentation changes at this time.

§