Intel® Core™ X-Series Processor Families

Datasheet – Volume 1 of 2

Supporting Intel® Core™ X-Series Processor Families – i7-7740X, i7-7800X, i7-7820X, i9-7900X, i9-7920X

January 2018

Document Number: 335899-004

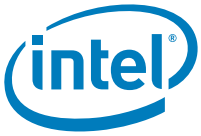
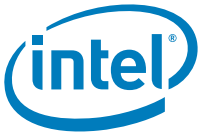
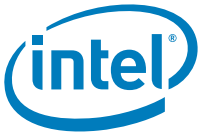


Table of Contents



Figures

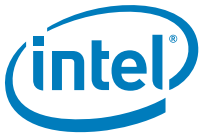
Tables



Revision History

Revision Number	Description	Date
001	• Initial release	May 2017
002	• Updated Section 1.3.1, “System Memory Support” • Updated Section 1.3.2, “PCI Express*” • Updated Section 1.4.1, “Processor Package and Core States” • Updated Section 1.4.2, “System States Support”	June 2017
003	• Updated Section 1.1 “Processor Feature Details”	June 2017
004	• Updated Chapter 1 “Introduction” • Updated Table 5.12	January 2018

§ §



1 Introduction

The Intel® Core™ X-Series processor families are the next generation of 64-bit, multi-core processors built on 14-nm process technology. Based on the low power / high performance processor microarchitecture, the processor is designed for a platform consisting of a processor and Platform Controller Hub (PCH). The X-Series processor is used with the Intel® X299 Chipset PCH.

The processor supports up to 46 bits of physical address space and 48 bits of virtual address space. The processor features up to 44 lanes of PCI Express* 3.0 links capable of 8.0 GT/s, and 4 lanes of DMI/PCI Express* 3.0. It features an Integrated Memory Controller (IMC) that supports 4 channels of DDR4 memory.

The integrated memory controller (IMC) and integrated I/O (IIO) are on a single silicon die. This single-die solution is known as a monolithic processor.

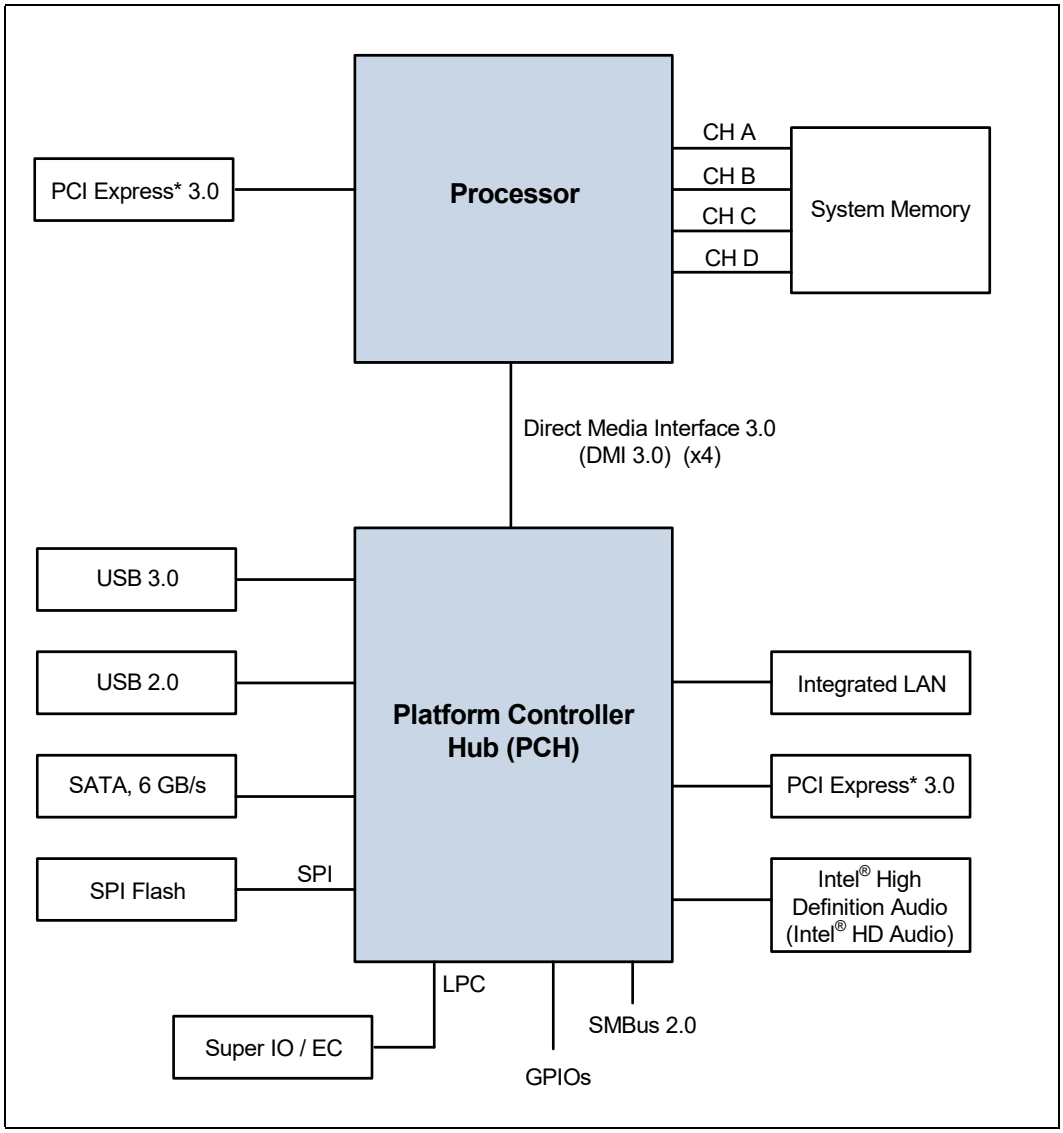
This document covers the following Intel® Core™ X-Series processor families:

- i7-7740X, i7-7800X, i7-7820X, i9-7900X, i9-7920X

Note: Throughout this document, the Intel® Core™ X-Series processor families may be referred to as "processor". The Intel® X299 Chipset PCH may be referred to as the "PCH".

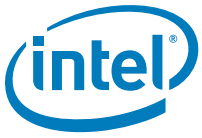
Note: Some processor features are not available on all processor SKUs.

Figure 1-1. Platform Block Diagram Example



1.1 Processor Feature Details

- Up to 10 execution cores
- Each core supports two threads (Intel® Hyper-Threading Technology)
- 32 KB instruction and 32 KB data first-level cache (L1) for each core
- 1.0 MB private instruction/data mid-level cache (MLC) for each core
- 1.375 MB shared Low-Level Cache (LLC) per core (non-inclusive)



1.2 Supported Technologies

- Intel® Virtualization Technology (Intel® VT)
- Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)
- Intel® Virtualization Technology (Intel® VT) Processor Extensions
- Intel® 64 Architecture
- Intel® Streaming SIMD Extensions 4.2 (Intel® SSE4.2)
- Intel® Advanced Vector Extensions 2.0 (Intel® AVX2)
- Intel® AVX Floating Point Bit Depth Conversion (Float 16)
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Execute Disable Bit
- Intel® Turbo Boost Technology
- Enhanced Intel® SpeedStep® Technology

1.3 Interfaces

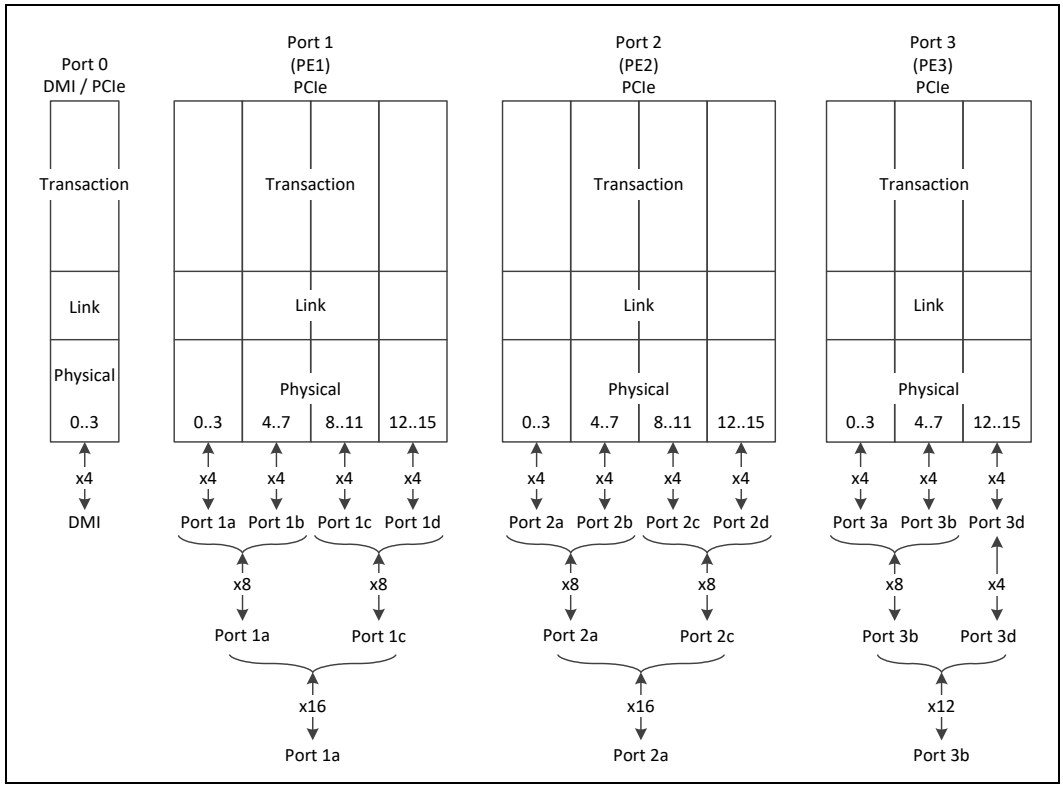
1.3.1 System Memory Support

- Supports four DDR4 channels
- Unbuffered DDR4 DIMMs supported
- Independent channel mode or lockstep mode
- Data burst length of eight cycles for all memory organization modes
- Memory DDR4 data transfer rates of 1600 MT/s, 1866 MT/s, 2133 MT/s, 2400 MT/s, and 2666 MT/s (1 DPC)
- 64-bit wide channels
- DDR4 standard I/O Voltage of 1.2 V
- 4Gb and 8Gb DDR4 DRAM technologies supported for these devices:
  - UDIMM x8
- Up to 2 ranks supported per memory channel
- Open with adaptive idle page close timer or closed page policy
- Per channel memory test and initialization engine can initialize DRAM to all logical zeros or a predefined test pattern
- Minimum memory configuration: independent channel support with 1 DIMM populated
- Command launch modes of 1n/2n
- Improved Thermal Throttling
- Memory thermal monitoring support for DIMM temperature using two memory signals, MEM_HOT_C{01/23}_N

1.3.2 PCI Express*

- The PCI Express* port(s) are fully-compliant with the *PCI Express* Base Specification*, Revision 3.0 (PCIe 3.0)
- Support for PCI Express* 3.0 (8.0 GT/s), 2.0 (5.0 GT/s), and 1.0 (2.5 GT/s)
- Up to 44 lanes of PCI Express* interconnect for general purpose PCI Express* devices at PCIe* 3.0 speeds that are configurable for up to 10 independent ports
  - Intel® Core™ i9-7900X processor supports 44 lanes
  - Intel® Core™ i7-7800X processor supports 28 lanes
- Negotiating down to narrower widths is supported. See Figure 1-2.
  - x16 port (Port 1 and Port 2) may negotiate down to x8, x4, x2, or x1
  - x12 port (Port 3) may negotiate down to x8, x4, x2, or x1
- Address Translation Services (ATS) 1.0 support
- Hierarchical PCI-compliant configuration mechanism for downstream devices
- Traditional PCI style traffic (asynchronous snooped, PCI ordering)
- PCI Express* extended configuration space. The first 256 bytes of configuration space aliases directly to the PCI compatibility configuration space. The remaining portion of the fixed 4-KB block of memory-mapped space above that (starting at 100h) is known as extended configuration space.
- PCI Express* Enhanced Access Mechanism – accessing the device configuration space in a flat memory mapped fashion
- Automatic discovery, negotiation, and training of link out of reset
- Supports receiving and decoding 64 bits of address from PCI Express*
  - Memory transactions received from PCI Express* that go above the top of physical address space (when Intel VT-d is enabled, the check would be against the translated Host Physical Address (HPA)) are reported as errors by the processor.
  - Outbound access to PCI Express* will always have address bits 63:46 cleared
- Re-issues Configuration cycles that have been previously completed with the Configuration Retry status
- Power Management Event (PME) functions
- Message Signaled Interrupt (MSI and MSI-X) messages
- Degraded Mode support and Lane Reversal support
- Static lane numbering reversal and polarity inversion support
- Support for PCIe* 3.0 atomic operation, PCIe* 3.0 optional extension on atomic read-modify-write mechanism

Figure 1-2. PCI Express* Lane Partitioning and Direct Media Interface Gen 3 (DMI3)



1.3.3 Direct Media Interface

- Chip-to-chip interface to the PCH
- The DMI3 port supports x4 link width and only operates in a x4 mode when in DMI3
- Operates at PCI Express* 1.0, 2.0, 3.0 speeds
- Transparent to software
- Processor and peer-to-peer writes and reads with 64-bit address support
- APIC and Message Signaled Interrupt (MSI) support. Will send Intel-defined "End of Interrupt" broadcast message when initiated by the processor.
- System Management Interrupt (SMI), SCI, and SERR error indication
- Static lane numbering reversal support
- Supports DMI virtual channels VC0, VC1, VCm, and VCp

1.3.4 Platform Environment Control Interface (PECI)

The PECI is a one-wire interface that provides a communication channel between a PECI client (the processor) and a PECI master (the PCH).

- Supports operation at up to 2 Mbps data transfers
- Link layer improvements to support additional services and higher efficiency over PECI 2.0 generation

- Services include processor thermal and estimated power information, control functions for power limiting, P-state and T-state control, and access for Machine Check Architecture registers and PCI configuration space (both within the processor package and downstream devices)
- Single domain (Domain 0) is supported

1.4 Power Management Support

1.4.1 Processor Package and Core States

- Advance Configuration and Power Interface (ACPI) C-states as implemented by the following processor C-states:
  - Package: PC0, PC1/PC1E, PC2, PC3, PC6 (Package C7 is not supported)
  - Core: CC0, CC1, CC1E, CC3, CC6
- Enhanced Intel SpeedStep Technology

1.4.2 System States Support

- S0, S3, S4, S5

1.4.3 Memory Controller

- Multiple CKE power-down modes
- Multiple self-refresh modes
- Memory thermal monitoring using MEM_HOT_C01_N and MEM_HOT_C23_N signals

1.4.4 PCI Express*

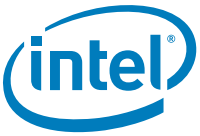
- L1 ASPM power management capability; L0s is not supported

1.5 Thermal Management Support

- Digital Thermal Sensor with multiple on-die temperature zones
- Adaptive Thermal Monitor
- THERMTRIP_N and PROCHOT_N signal support
- On-Demand mode clock modulation
- Fan speed control with DTS
- Two integrated SMBus masters for accessing thermal data from DIMMs
- New Memory Thermal Throttling features using MEM_HOT_C{01/23}_N signals

1.6 Package Summary

The processor socket type is noted as LGA2066. The processor package is a 52.5 x 45 mm FC-LGA package.



1.7 Terminology

Table 1-1. Terminology (Sheet 1 of 3)

Term	Description
ASPM	Active State Power Management
Cbo	Caching Agent (also referred to as CA). It is a term used for the internal logic providing ring interface to LLC and Core. The Cbo is a functional unit in the processor.
DDR4	Fourth generation Double Data Rate SDRAM memory technology.
DMA	Direct Memory Access
DMI3	Direct Media Interface Gen2 operating at PCI Express 3.0 speed.
DSB	Data Stream Buffer. Part of the processor core architecture.
DTLB	Data Translation Look-aside Buffer. Part of the processor core architecture.
DTS	Digital Thermal Sensor
Enhanced Intel SpeedStep® Technology	Allows the operating system to reduce power consumption when performance is not needed.
Execute Disable Bit	The Execute Disable bit allows memory to be marked as executable or non-executable, when combined with a supporting operating system. If code attempts to run in non-executable memory the processor raises an error to the operating system. This feature can prevent some classes of viruses or worms that exploit buffer overrun vulnerabilities and can thus help improve the overall security of the system. See the *Intel® 64 and IA-32 Architectures Software Developer's Manuals* for more detailed information.
Functional Operation	Refers to the normal operating conditions in which all processor specifications, including DC, AC, system bus, signal quality, mechanical, and thermal, are satisfied.
GSSE	Extension of the SSE/SSE2 (Streaming SIMD Extensions) floating point instruction set to 256b operands.
HA	Home Agent (HA)
ICU	Instruction Cache Unit. Part of the processor core architecture.
IFU	Instruction Fetch Unit. Part of the processor core.
IIO	The Integrated I/O Controller. An I/O controller that is integrated in the processor die.
IMC	The Integrated Memory Controller. A Memory Controller that is integrated in the processor die.
Integrated Heat Spreader (IHS)	A component of the processor package used to enhance the thermal performance of the package. Component thermal solutions interface with the processor at the IHS surface.
Intel® 64 Technology	64-bit memory extensions to the IA-32 architecture. Further details on Intel 64 architecture and programming model can be found at http://developer.intel.com/technology/intel64/.
Intel® Core™ i7 processor family for LGA2011-v3 Socket processor	Intel's 22-nm process based product. The processor supports Efficient Performance High-End Desktop platforms
Intel® ME	Intel® Management Engine
Intel® Turbo Boost Technology	A feature that opportunistically enables the processor to run a faster frequency. This results in increased performance of both single and multi-threaded applications.
Intel® TXT	Intel® Trusted Execution Technology
Intel® Virtualization Technology (Intel® VT)	Processor Virtualization which when used in conjunction with Virtual Machine Monitor software enables multiple, robust independent software environments inside a single platform.

Table 1-1. Terminology (Sheet 2 of 3)

Term	Description
Intel® VT-d	Intel® Virtualization Technology (Intel® VT) for Directed I/O. Intel VT-d is a hardware assist, under system software (Virtual Machine Manager or operating system) control, for enabling I/O device Virtualization. Intel VT-d also brings robust security by providing protection from errant DMAs by using DMA remapping, a key feature of Intel VT-d.
IOV	I/O Virtualization
IQ	Instruction Queue. Part of the core architecture.
IVR	Integrated Voltage Regulation (IVR): The processor supports several integrated voltage regulators.
Jitter	Any timing variation of a transition edge or edges from the defined Unit Interval (UI).
LGA2011-v3 Socket	The 2011-v3 land FC-LGA package mates with the system board through this surface mount, 2011-v3 contact socket.
LLC	Last Level Cache
LRDIMM	Load Reduced Dual In-line Memory Module
LRU	Least Recently Used. A term used in conjunction with cache allocation policy.
MESIF	Modified/Exclusive/Shared/Invalid/Forwarded. States used in conjunction with cache coherency
MLC	Mid Level Cache
NCTF	Non-Critical to Function: NCTF locations are typically redundant ground or non-critical reserved, so the loss of the solder joint continuity at end of life conditions will not affect the overall product functionality.
PCH	Platform Controller Hub. The next generation chipset with centralized platform capabilities including the main I/O interfaces along with display connectivity, audio features, power management, manageability, security and storage features.
PCI Express* 2.0	PCI Express Generation 2.0
PCI Express* 3.0	The third generation PCI Express specification that operates at twice the speed of PCI Express 2.0 (8 Gb/s); PCI Express 3.0 is completely backward compatible with PCI Express 1.0 and 2.0.
PECI	Platform Environment Control Interface
Processor	Includes the 64-bit cores, uncore, I/Os, and package
Processor Core	The term "processor core" refers to Si die itself which can contain multiple execution cores. Each execution core has an instruction cache, data cache, and 256-KB L2 cache. All execution cores share the L3 cache.
Rank	A unit of DRAM corresponding four to eight devices in parallel. These devices are usually, but not always, mounted on a single side of a DDR4 DIMM.
RDIMM	Registered Dual In-line Memory Module
RTID	Request Transaction IDs are credits issued by the Cbo to track outstanding transaction, and the RTIDs allocated to a Cbo are topology dependent.
SCI	System Control Interrupt. Used in ACPI protocol.
SKU	Stock Keeping Unit (SKU) is a subset of a processor type with specific features, electrical, power and thermal specifications. Not all features are supported on all SKUs. A SKU is based on specific use condition assumption.
SMBus	System Management Bus. A two-wire interface through which simple system and power management related devices can communicate with the rest of the system.
SSE	Intel® Streaming SIMD Extensions (Intel® SSE)
STD	Suspend-to-Disk

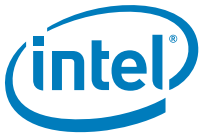


Table 1-1. Terminology (Sheet 3 of 3)

Term	Description
Storage Conditions	A non-operational state. The processor may be installed in a platform, in a tray, or loose. Processors may be sealed in packaging or exposed to free air. Under these conditions, processor landings should not be connected to any supply voltages, have any I/Os biased or receive any clocks. Upon exposure to "free air" (that is, unsealed packaging or a device removed from packaging material) the processor must be handled in accordance with moisture sensitivity labeling (MSL) as indicated on the packaging material.
STR	Suspend-to-RAM
SVID	Serial Voltage Identification
TAC	Thermal Averaging Constant
TCC	Thermal Control Circuit
TDP	Thermal Design Power
TLP	Transaction Layer Packet
TSOD	Temperature Sensor On DIMM
UDIMM	Unbuffered Dual In-line Memory Module
Uncore	The portion of the processor comprising the shared LLC cache, IMC, HA, PCU, Ubox, and IIO link interface.
Unit Interval	Signaling convention that is binary and unidirectional. In this binary signaling, one bit is sent for every edge of the forwarded clock, whether it be a rising edge or a falling edge. If a number of edges are collected at instances t_1, t_2, t_n,...., t_k then the UI at instance "n" is defined as: $UI_n = t_n - t_{n-1}$
V_{CCD}	DDR power rail
V_{CCIN}	Primary voltage input to the voltage regulators integrated into the processor.
V_{CCIO_IN}	IO voltage supply input
VSS	Processor ground
x1	Refers to a Link or Port with one Physical Lane
x16	Refers to a Link or Port with sixteen Physical Lanes
x4	Refers to a Link or Port with four Physical Lanes
x8	Refers to a Link or Port with eight Physical Lanes

1.8 Related Documents

Refer to the following documents for additional information.

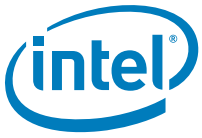
Table 1-2. Related Documents (Sheet 1 of 2)

Document	Document Number/ Location
Intel® Core™ X-Series Processor Family Datasheet, Volume 2 of 2	335900
Intel® Core™ X-Series Processor Family Specification Update	335901
Advanced Configuration and Power Interface Specification 4.0	http://www.acpi.info/
PCI Local Bus Specification 3.0	http://www.pcisig.com/
PCI Express Base Specification, Revision 3.0	http://www.pcisig.com/
PCI Express Base Specification, Revision 2.1	
PCI Express Base Specification, Revision 1.1	

Table 1-2. Related Documents (Sheet 2 of 2)

Document	Document Number/ Location
PCIe Gen 3 Connector High Speed Electrical Test Procedure*	325028-001 / http://www.intel.com/content/www/us/en/io/pci-express/pci-express-architecture-devnet-resources.html
Connector Model Quality Assessment Methodology	326123-002 / http://www.intel.com/content/www/us/en/architecture-and-technology/intel-connector-model-paper.html
DDR4 SDRAM Specification and Register Specification	http://www.jedec.org/
Intel® 64 and IA-32 Architectures Software Developer's Manuals • *Volume 1: Basic Architecture* • *Volume 2A: Instruction Set Reference, A-M* • *Volume 2B: Instruction Set Reference, N-Z* • *Volume 3A: System Programming Guide* • *Volume 3B: System Programming Guide* *Intel® 64 and IA-32 Architectures Optimization Reference Manual*	325462 / http://www.intel.com/products/processor/manuals/index.htm
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/vt-directed-io-spec.html

§ §



2 Interfaces

This chapter describes the functional behaviors supported by the processor. Topics covered include:

- System Memory Interface
- PCI Express* Interface
- Direct Media Interface 3 (DMI3) / PCI Express* Interface
- Platform Environment Control Interface (PECI)

2.1 System Memory Interface

2.1.1 System Memory Technology Support

The Integrated Memory Controller (IMC) supports DDR4 protocols with four independent 64-bit memory channels and supports 1 unbuffered DIMM per channel.

2.1.2 System Memory Timing Support

The IMC supports the following DDR4 Speed Bin, CAS Write Latency (CWL), and command signal mode timings on the main memory interface:

- t_{CL} = CAS Latency
- t_{RCD} = Activate Command to READ or WRITE Command delay
- t_{RP} = PRECHARGE Command Period
- CWL = CAS Write Latency
- Command Signal modes = 1n indicates a new command may be issued every clock and 2n indicates a new command may be issued every 2 clocks. Command launch mode programming depends on the transfer rate and memory configuration.

2.2 PCI Express* Interface

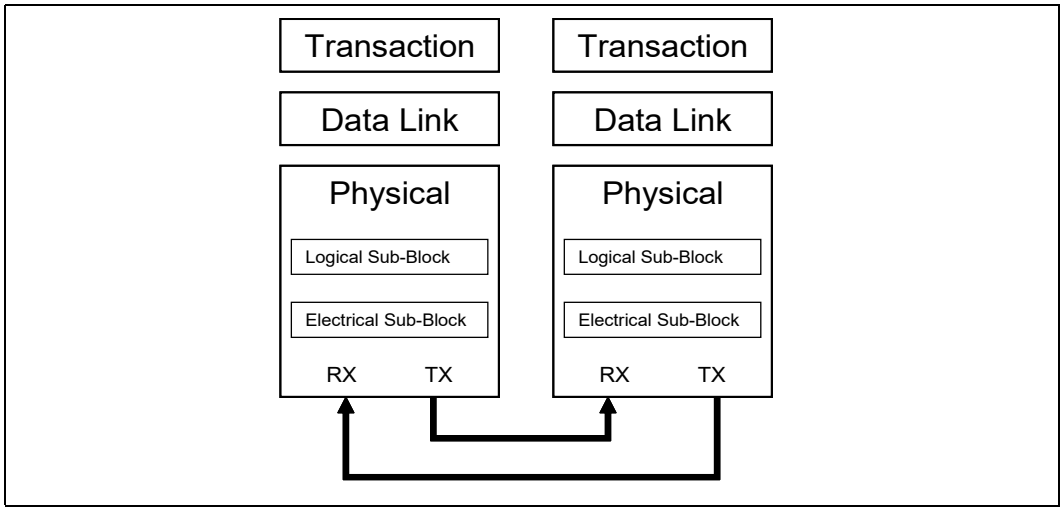
This section describes the PCI Express* 3.0 interface capabilities of the processor. See the *PCI Express* Base Specification* for details of PCI Express* 3.0.

2.2.1 PCI Express* Architecture

Compatibility with the PCI addressing model is maintained to ensure that all existing applications and drivers operate unchanged. The PCI Express* configuration uses standard mechanisms as defined in the PCI Plug-and-Play specification.

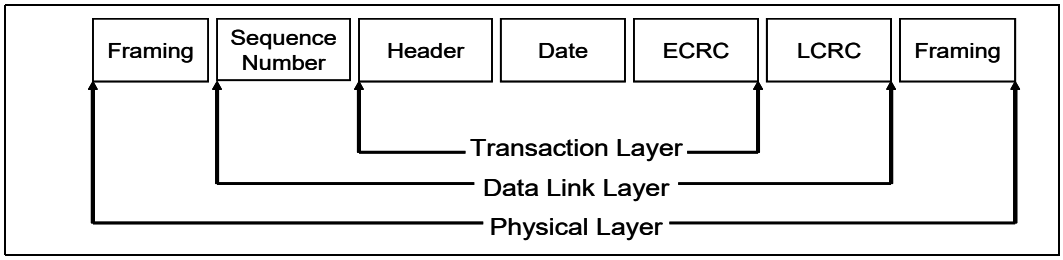
The PCI Express* architecture is specified in three layers – Transaction Layer, Data Link Layer, and Physical Layer. The partitioning in the component is not necessarily along these same boundaries. Refer to the following figure for the PCI Express* Layering Diagram.

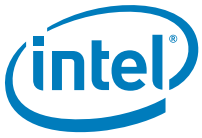
Figure 2-1. PCI Express* Layering Diagram



PCI Express* uses packets to communicate information between components. Packets are formed in the Transaction and Data Link Layers to carry the information from the transmitting component to the receiving component. As the transmitted packets flow through the other layers, the packets are extended with additional information necessary to handle packets at those layers. At the receiving side, the reverse process occurs and packets get transformed from their Physical Layer representation to the Data Link Layer representation and finally (for Transaction Layer Packets) to the form that can be processed by the Transaction Layer of the receiving device.

Figure 2-2. Packet Flow through the Layers





2.2.1.1 Transaction Layer

The upper layer of the PCI Express* architecture is the Transaction Layer. The Transaction Layer's primary responsibility is the assembly and disassembly of Transaction Layer Packets (TLPs). TLPs are used to communicate transactions, such as read and write, as well as certain types of events. The Transaction Layer also manages flow control of TLPs.

2.2.1.2 Data Link Layer

The middle layer in the PCI Express* stack, the Data Link Layer, serves as an intermediate stage between the Transaction Layer and the Physical Layer. Responsibilities of Data Link Layer include link management, error detection, and error correction.

The transmission side of the Data Link Layer accepts TLPs assembled by the Transaction Layer, calculates and applies data protection code and TLP sequence number, and submits them to Physical Layer for transmission across the Link. The receiving Data Link Layer is responsible for checking the integrity of received TLPs and for submitting them to the Transaction Layer for further processing. On detection of TLP error(s), this layer is responsible for requesting retransmission of TLPs until information is correctly received, or the Link is determined to have failed. The Data Link Layer also generates and consumes packets that are used for Link management functions.

2.2.1.3 Physical Layer

The Physical Layer includes all circuitry for interface operation, including driver and input buffers, parallel-to-serial and serial-to-parallel conversion, PLL(s), and impedance matching circuitry. It also includes logical functions related to interface initialization and maintenance. The Physical Layer exchanges data with the Data Link Layer in an implementation-specific format, and is responsible for converting this to an appropriate serialized format and transmitting it across the PCI Express* Link at a frequency and width compatible with the remote device.

2.2.2 PCI Express* Configuration Mechanism

The PCI Express* link is mapped through a PCI-to-PCI bridge structure.

PCI Express* extends the configuration space to 4096 bytes per-device/function, as compared to 256 bytes allowed by the Conventional PCI Specification. PCI Express* configuration space is divided into a PCI-compatible region (which consists of the first 256 bytes of a logical device's configuration space) and an extended PCI Express* region (which consists of the remaining configuration space). The PCI-compatible region can be accessed using either the mechanisms defined in the PCI specification or using the enhanced PCI Express* configuration access mechanism described in the PCI Express* Enhanced Configuration Mechanism section.

The PCI Express* Host Bridge is required to translate the memory-mapped PCI Express* configuration space accesses from the host processor to PCI Express* configuration cycles. To maintain compatibility with PCI configuration addressing mechanisms, it is recommended that system software access the enhanced configuration space using 32-bit operations (32-bit aligned) only.

See the *PCI Express* Base Specification* for details of both the PCI-compatible and PCI Express* Enhanced configuration mechanisms and transaction rules.

2.3 Direct Media Interface 3 (DMI3) / PCI Express* Interface

Direct Media Interface 3 (DMI3) connects the processor to the Platform Controller Hub (PCH). DMI3 is similar to a four-lane PCI Express* supporting a speed of 8 GT/s per lane.

Note: Only DMI3 x4 configuration is supported.

2.3.1 DMI3 Error Flow

DMI3 can only generate SERR in response to errors, never SCI, SMI, MSI, PCI INT, or GPE. Any DMI3 related SERR activity is associated with Device 0.

2.3.2 Processor / PCH Compatibility Assumptions

The processor is compatible with the PCH and is not compatible with any previous Intel Memory Controller Hub (MCH) and Integrated Controller Hub (ICH) products.

2.3.3 DMI3 Link Down

The DMI3 link going down is a fatal, unrecoverable error. If the DMI3 data link goes to data link down, after the link was up, then the DMI3 link hangs the system by not allowing the link to retrain to prevent data corruption. This is controlled by the PCH.

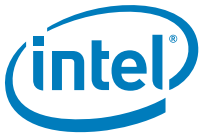
Downstream transactions that had been successfully transmitted across the link prior to the link going down may be processed as normal. No completions from downstream, non-posted transactions are returned upstream over the DMI3 link after a link down event.

2.4 Platform Environment Control Interface (PECI)

The Platform Environment Control Interface (PECI) uses a single wire for self-clocking and data transfer. The bus requires no additional control lines. The physical layer is a self-clocked one-wire bus that begins each bit with a driven, rising edge from an idle level near zero volts. The duration of the signal driven high depends on whether the bit value is a logic ‘0’ or logic ‘1’. PECI also includes variable data transfer rate established with every message. In this way, it is highly flexible even though underlying logic is simple.

The interface design was optimized for interfacing to Intel processor and chipset components in both single processor and multiple processor environments. The single wire interface provides low board routing overhead for the multiple load connections in the congested routing area near the processor and chipset components. Bus speed, error checking, and low protocol overhead provides adequate link bandwidth and reliability to transfer critical device operating conditions and configuration information.

§ §



3 Technologies

This chapter covers the following technologies:

- Intel® Virtualization Technology (Intel® VT)
- Security Technologies
- Intel® Hyper-Threading Technology (Intel® HT Technology)
- Intel® Turbo Boost Technology
- Enhanced Intel® SpeedStep® Technology
- Intel® Advanced Vector Extensions (Intel® AVX)

3.1 Intel® Virtualization Technology (Intel® VT)

Intel® Virtualization Technology (Intel® VT) makes a single system appear as multiple independent systems to software. This allows multiple, independent operating systems to run simultaneously on a single system. Intel VT comprises technology components to support virtualization of platforms based on Intel architecture microprocessors and chipsets.

- **Intel® Virtualization Technology (Intel® VT) for Intel® 64 and IA-32 Intel® Architecture (Intel® VT-x)** adds hardware support in the processor to improve the virtualization performance and robustness. Intel VT-x specifications and functional descriptions are included in the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B and is available at http://www.intel.com/products/processor/manuals/index.htm
- **Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)** adds processor and uncore implementations to support and improve I/O virtualization performance and robustness. The Intel VT-d specification and other Intel VT documents can be referenced at http://www.intel.com/technology/virtualization/index.htm

3.1.1 Intel® VT-x Objectives

Intel VT-x provides hardware acceleration for virtualization of IA platforms. Virtual Machine Monitor (VMM) can use Intel VT-x features to provide improved reliable virtualized platforms. By using Intel VT-x, a VMM is:

- **Robust:** VMMs no longer need to use para-virtualization or binary translation. This means that off-the-shelf operating systems and applications can be run without any special steps.
- **Enhanced:** Intel VT enables VMMs to run 64-bit guest operating systems on IA x86 processors.
- **More reliable:** Due to the hardware support, VMMs can now be smaller, less complex, and more efficient. This improves reliability and availability and reduces the potential for software conflicts.
- **More secure:** The use of hardware transitions in the VMM strengthens the isolation of VMs and further prevents corruption of one VM from affecting others on the same system.

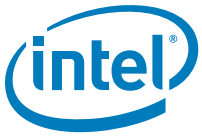
3.1.2 Intel® VT-x Features

The processor core supports the following Intel VT-x features:

- Extended Page Tables (EPT)
  - hardware assisted page table virtualization.
  - eliminates VM exits from guest operating system to the VMM for shadow page-table maintenance.
- Virtual Processor IDs (VPID)
  - Ability to assign a VM ID to tag processor core hardware structures (such as, TLBs).
  - This avoids flushes on VM transitions to give a lower-cost VM transition time and an overall reduction in virtualization overhead.
- Guest Preemption Timer
  - Mechanism for a VMM to preempt the execution of a guest operating system after an amount of time specified by the VMM. The VMM sets a timer value before entering a guest.
  - The feature aids VMM developers in flexibility and Quality of Service (QoS) guarantees.
- Descriptor-Table Exiting
  - Descriptor-table exiting allows a VMM to protect a guest operating system from internal (malicious software based) attack by preventing relocation of key system data structures like IDT (interrupt descriptor table), GDT (global descriptor table), LDT (local descriptor table), and TSS (task segment selector).
  - A VMM using this feature can intercept (by a VM exit) attempts to relocate these data structures and prevent them from being tampered by malicious software.
- Pause Loop Exiting (PLE)
  - PLE aims to improve virtualization performance and enhance the scaling of virtual machines with multiple virtual processors
  - PLE attempts to detect lock-holder preemption in a VM and helps the VMM to make better scheduling decisions

3.1.3 Intel® VT-d Objectives

The key Intel VT-d objectives are domain-based isolation and hardware-based virtualization. A domain can be abstractly defined as an isolated environment in a platform to which a subset of host physical memory is allocated. Virtualization allows for the creation of one or more partitions on a single system. This could be multiple partitions in the same operating system, or there can be multiple operating system instances running on the same system – offering benefits such as system consolidation, legacy migration, activity partitioning, or security.



3.1.3.1 Intel® VT-d Features Supported

The processor supports the following Intel VT-d features:

- Root entry, context entry, and default context
- Support for 4-K page sizes only
- Support for register-based fault recording only (for single entry only) and support for MSI interrupts for faults
  - — Support for fault collapsing based on Requester ID
- Support for both leaf and non-leaf caching
- Support for boot protection of default page table
  - — Support for non-caching of invalid page table entries
- Support for hardware based flushing of translated but pending writes and pending reads upon IOTLB invalidation
- Support for page-selective IOTLB invalidation
- Support for ARI (Alternative Requester ID – a PCI SIG ECR for increasing the function number count in a PCIe* device) to support I/O Virtualization (IOV) devices
- Improved invalidation architecture
- End point caching support (ATS)
- Interrupt remapping

3.1.4 Intel® Virtualization Technology Processor Extensions

The processor supports the following Intel VT processor extension features:

- Large Intel VT-d Pages
  - — Adds 2MB and 1GB page sizes to Intel VT-d implementations
  - — Matches current support for Extended Page Tables (EPT)
  - — Ability to share processor EPT page-table (with super-pages) with Intel VT-d
  - — Benefits:
    - Less memory foot-print for I/O page-tables when using super-pages
    - Potential for improved performance – due to shorter page-walks, allows hardware optimization for IOTLB
- Transition latency reductions expected to improve virtualization performance without the need for VMM enabling. This reduces the VMM overheads further and increase virtualization performance.

3.2 Security Technologies

3.2.1 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) Instructions

These instructions enable fast and secure data encryption and decryption, using the Advanced Encryption Standard (Intel AES-NI) which is defined by FIPS Publication number 197. Since Intel AES-NI is the dominant block cipher, and it is deployed in various protocols, the new instructions will be valuable for a wide range of applications.

The architecture consists of six instructions that offer full hardware support for Intel AES-NI. Four instructions support the Intel AES-NI encryption and decryption, and the other two instructions support the Intel AES-NI key expansion. Together, they offer a significant increase in performance compared to pure software implementations.

The Intel AES-NI instructions have the flexibility to support all three standard Intel AES-NI key lengths, all standard modes of operation, and even some nonstandard or future variants.

Beyond improving performance, the Intel AES-NI instructions provide important security benefits. Since the instructions run in data-independent time and do not use lookup tables, the instructions help in eliminating the major timing and cache-based attacks that threaten table-based software implementations of Intel AES-NI. In addition, these instructions make AES simple to implement, with reduced code size. This helps reducing the risk of inadvertent introduction of security flaws, such as difficult-to-detect side channel leaks.

3.2.2 Execute Disable Bit

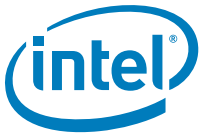
The Intel Execute Disable Bit functionality can help prevent certain classes of malicious buffer overflow attacks when combined with a supporting operating system.

- Allows the processor to classify areas in memory by where application code can execute and where it cannot.
- When a malicious worm attempts to insert code in the buffer, the processor disables code execution, preventing damage and worm propagation.

3.3 Intel® Hyper-Threading Technology (Intel® HT Technology)

The processor supports Intel® Hyper-Threading Technology (Intel® HT Technology) that allows an execution core to function as two logical processors. While some execution resources such as caches, execution units, and buses are shared, each logical processor has its own architectural state with its own set of general-purpose registers and control registers. This feature must be enabled using the BIOS and requires operating system support.

For more information on Intel Hyper-Threading Technology, see http://www.intel.com/products/ht/hyperthreading_more.htm.



3.4 Intel® Turbo Boost Max Technology 3.0

Intel Turbo Boost Technology is a feature that allows the processor to opportunistically and automatically run faster than its rated operating frequency if it is operating below power, temperature, and current limits. The result is increased performance in multi-threaded and single threaded workloads. It should be enabled in the BIOS for the processor to operate with maximum performance.

Processors with Intel Turbo Boost Max Technology 3.0 feature contain at least one processor core whose maximum turbo frequency is higher than the others. To realize the higher performance benefit of such a core, targeted applications must run **on that core**. The processor core with the higher frequency may vary from one processor to another. BIOS calls to the mailbox interface is used to identify the core with the higher performance.

3.4.1 Intel® Turbo Boost Operating Frequency

The processor's rated frequency assumes that all execution cores are running an application at the thermal design power (TDP). However, under typical operation, not all cores are active. Therefore, most applications are consuming less than the TDP at the rated frequency. To take advantage of the available TDP headroom, the active cores can increase their operating frequency.

To determine the highest performance frequency amongst active cores, the processor takes the following into consideration:

- number of cores operating in the C0 state
- estimated current consumption
- estimated power consumption
- die temperature

Any of these factors can affect the maximum frequency for a given workload. If the power, current, or thermal limit is reached, the processor will automatically reduce the frequency to stay with its TDP limit.

Note: Intel Turbo Boost Technology is only active if the operating system is requesting the P0 state.

3.5 Enhanced Intel® SpeedStep® Technology

The processor supports Enhanced Intel SpeedStep® Technology as an advanced means of enabling very high performance while also meeting the power-conservation needs of the platform.

Enhanced Intel SpeedStep Technology builds upon that architecture using design strategies that include the following:

- **Separation between Voltage and Frequency Changes**. By stepping voltage up and down in small increments separately from frequency changes, the processor is able to reduce periods of system unavailability that occur during frequency change. Thus, the system is able to transition between voltage and frequency states more often, providing improved power/performance balance.
- **Clock Partitioning and Recovery**. The bus clock continues running during state transition, even when the core clock and Phase-Locked Loop are stopped, which

allows logic to remain active. The core clock can also restart more quickly under Enhanced Intel SpeedStep Technology.

3.6 Intel® Advanced Vector Extensions (Intel® AVX)

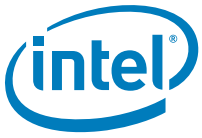
Intel Advanced Vector Extensions (Intel AVX) is a new 256-bit vector SIMD extension of Intel Architecture. The introduction of Intel AVX started with the 2nd Generation Intel® Core™ processor family. Intel AVX accelerates the trend of parallel computation in general purpose applications like image, video and audio processing, engineering applications (such as 3D modeling and analysis), scientific simulation, and financial analysts.

Intel AVX is a comprehensive ISA extension of the Intel 64 Architecture. The main elements of Intel AVX are:

- Support for wider vector data (up to 256-bit) for floating-point computation
- Efficient instruction encoding scheme that supports 3 operand syntax and headroom for future extensions
- Flexibility in programming environment, ranging from branch handling to relaxed memory alignment requirements
- New data manipulation and arithmetic compute primitives, including broadcast, permute, fused-multiply-add, and so on
- Floating point bit depth conversion (Float 16)
    - A group of 4 instructions that accelerate data conversion between 16-bit floating point format to 32-bit and vice versa.
    - This benefits image processing and graphical applications allowing compression of data so less memory and bandwidth is required.

The key advantages of Intel AVX are:

- **Performance** – Intel AVX can accelerate application performance using data parallelism and scalable hardware infrastructure across existing and new application domains:
    - 256-bit vector data sets can be processed up to twice the throughput of 128-bit data sets
    - Application performance can scale up with the number of hardware threads and number of cores
    - Application domain can scale out with advanced platform interconnect fabrics
- **Power Efficiency** – Intel AVX is extremely power efficient. Incremental power is insignificant when the instructions are unused or scarcely used. Combined with the high performance that it can deliver, applications that lend themselves heavily to using Intel AVX can be much more energy efficient and realize a higher performance-per-watt.
- **Extensibility** – Intel AVX has built-in extensibility for the future vector extensions:
    - Operating System context management for vector-widths beyond 256 bits is streamlined
    - Efficient instruction encoding allows unlimited functional enhancements:
        - Vector width support beyond 256 bits
        - 256-bit Vector Integer processing
        - Additional computational and/or data manipulation primitives



- **Compatibility** – Intel AVX is backward compatible with previous ISA extensions including Intel SSE4:
  - Existing Intel SSE applications/library can:
    - Run unmodified and benefit from processor enhancements
    - Recompile existing Intel® SSE intrinsic using compilers that generate Intel AVX code
    - Inter-operate with library ported to Intel AVX
  - Applications compiled with Intel AVX can inter-operate with existing Intel SSE libraries.

§ §

4 Signal Descriptions

This chapter describes the signals. They are arranged in functional groups according to their associated interface or category.

4.1 System Memory Interface

Table 4-1. Memory Channel DDR0, DDR1, DDR2, DDR3, DDR4, DDR5

Signal Name	Description
DDR{5:0}_ACT_N	Activate. When asserted, indicates MA[16:14] are command signals (RAS_N, CAS_N, WE_N).
DDR{5:0}_ALERT_N	Parity Error detected by the DIMM (one for each channel).
DDR{5:0}_BA[1:0]	Bank Address. Defines which bank is the destination for the current Activate, Read, Write, or Precharge command.
DDR{5:0}_BG[1:0]	Bank Group: Defines which bank group is the destination for the current Active, Read, Write or Precharge command. BG0 also determines which mode register is to be accessed during a MRS cycle.
DDR{5:0}_CID[2]	3DS DRAM Chip ID signal
DDR{5:0}_CKE[3:0]	Clock Enable.
DDR{5:0}_CLK_DN[3:0] DDR{5:0}_CLK_DP[3:0]	Differential clocks to the DIMM. All command and control signals are valid on the rising edge of clock.
DDR{5:0}_CS_N[7:0]	Chip Select. Each signal selects one rank as the target of the command and address. CS_N[7:6] are multiplexed with CID[4:3], respectively. CS_N[3:2] are multiplexed with CID[1:0], respectively.
DDR{5:0}_DQ[63:0]	Data Bus. DDR4 Data bits.
DDR{5:0}_DQS_DP[17:0] DDR{5:0}_DQS_DN[17:0]	Data strobes. Differential pair, Data Strobe. Differential strobes latch data for each DRAM. Different numbers of strobes are used depending on whether the connected DRAMs are x4,x8. Driven with edges in center of data, receive edges are aligned with data edges.
DDR{5:0}_MA[17:0]	Memory Address. Selects the Row address for Reads and writes, and the column address for activates. Also used to set values for DRAM configuration registers. MA[16], MA[15], and MA[14] are multi-function and multiplexed with RAS_N, CAS_N, and WE_N, respectively. **Note:** MA[17] is not used on X-Series Processor It is reserved for future processor implementations. The pin still requires to be routed appropriately on the board to support future drop-in compatibility.
DDR{5:0}_PAR	Even parity across Address and Command.
DDR{5:0}_ODT[3:0]	On Die Termination. Enables DRAM on die termination during Data Write or Data Read transactions.
Note: Channels DDR2 and DDR5 are reserved on the HEDT Intel X-Series processor.	

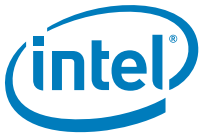


Table 4-2. Memory Channel Miscellaneous

Signal Name	Description
DDR {012,345}_RESET_N	System memory reset: Reset signal from processor to DRAM devices on the DIMMs. DDR012_RESET_N is used for memory channels 0, 1 and 2 while DDR345_RESET_N is used for memory channels 3, 4 and 5.
DDR{012,345}_SPDSCL	SMBus clock for the dedicated interface to the serial presence detect (SPD) and thermal sensors (TSoD) on the DIMMs. DDR_SCL_C012 is used for memory channels 0, 1 and 2 while DDR_SCL_C345 is used for memory channels 3, 4 and 5.
DDR{012,345}_SPDSDA	SMBus data for the dedicated interface to the serial presence detect (SPD) and thermal sensors (TSoD) on the DIMMs. DDR_SDA_C012 is used for memory channels 0, 1 and 2 while DDR_SDA_C345 is used for memory channels 3, 4 and 5.
DDR{5:0}_CAVREF	DIMM Command address VREF signal
DDR{012,345}_DRAM_PWR_OK	Power good for VCCD rail used by the DRAM. This is an input signal used to indicate the VCCD power supply is stable for memory channels 0, 1, 2 and channels 3, 4, 5.
DDR{012,345}_RCOMP[2:0]	DDR Compensation resistance control

4.2 PCI Express* Based Interface Signals

Note: PCI Express* Ports 1, 2 and 3 Signals are receive and transmit differential pairs.

Table 4-3. PCI Express Signals

Signal Name	Description
PE{3:1}_RX_DN/DP[15:0]	PCIe Receive Data Input
PE{3:1}_TX_DN/DP[15:0]	PCIe Transmit Data Output

Table 4-4. PCI Express Miscellaneous Signals

Signal Name	Description
PE_HP_SCL	PCI Express Hot-Plug SMBus Clock: Provides PCI Express* hot-plug support via a dedicated SMBus interface. Requires an external general purpose input/output (GPIO) expansion device on the platform.
PE_HP_SDA	PCI Express Hot-Plug SMBus Data: Provides PCI Express* hot-plug support via a dedicated SMBus interface. Requires an external general purpose input/output (GPIO) expansion device on the platform.

4.3 Direct Media Interface 3 (DMI3) Signals

Table 4-5. DMI3 Signals

Signal Name	Description
DMI_RX_DN/DP[3:0]	DMI3 Receive Data Input
DMI_TX_DN/DP[3:0]	DMI3 Transmit Data Output

4.4 PECI Signal

Table 4-6. PECI Signal

Signal Name	Description
PECI	PECI (Platform Environment Control Interface) is the serial sideband interface to the processor and is used primarily for thermal, power and error management.

4.5 System Reference Clock Signals

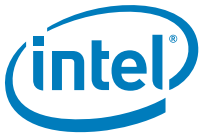
Table 4-7. System Reference Clock (BCLK{0/1/2}) Signals

Signal Name	Description
BCLK{0,1,2}_DN/DP	Reference Clock Differential input. These pins provide the required reference inputs to various PLLs inside the processor, such as PCIe. BCLK0, BCLK1 and BCLK2 run at 100 MHz from the same clock source.

4.6 JTAG and TAP Signals

Table 4-8. JTAG and TAP Signals

Signal Name	Description
BPM_N[7:0]	Breakpoint and Performance Monitor Signals: I/O signals from the processor that indicate the status of breakpoints and programmable counters used for monitoring processor performance. These are 100 MHz signals.
PRDY_N	Probe Mode Ready is a processor output used by debug tools to determine processor debug readiness.
PREQ_N	Probe Mode Request is used by debug tools to request debug operation of the processor.
TCK	TCK (Test Clock) provides the clock input for the processor Test Bus (also known as the Test Access Port).
TDI	TDI (Test Data In) transfers serial test data into the processor. TDI provides the serial input needed for JTAG specification support.
TDO	TDO (Test Data Out) transfers serial test data out of the processor. TDO provides the serial output needed for JTAG specification support.
TMS	TMS (Test Mode Select) is a JTAG specification support signal used by debug tools.
TRST_N	TRST_N (Test Reset) resets the Test Access Port (TAP) logic. TRST_N must be driven low during power on Reset.



4.7 Serial VID Interface (SVID) Signals

Table 4-9. SVID Signals

Signal Name	Description
SVIDALERT_N [1:0]	Serial VID alert.
SVIDCLK [1:0]	Serial VID clock.
SVIDDATA [1:0]	Serial VID data out.

4.8 Processor Asynchronous Sideband and Miscellaneous Signals

Table 4-10. Processor Asynchronous Sideband Signals (Sheet 1 of 2)

Signal Name	Description
CATERR_N	Indicates that the system has experienced a fatal or catastrophic error and cannot continue to operate. The processor will assert CATERR_N for unrecoverable machine check errors and other internal unrecoverable errors. It is expected that every processor in the system will wire-OR CATERR_N for all processors. Since this is an I/O land, external agents are allowed to assert this land which will cause the processor to take a machine check exception. The CATERR_N signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD. On Skylake, CATERR_N is used for signaling the following types of errors: • Legacy MCERR's, CATERR_N is asserted for 16 BCLKs.
ERROR_N[2:0]	Error status signals for integrated I/O (IIO) unit: 0 = Hardware correctable error (no operating system or firmware action necessary) 1 = Non-fatal error (operating system or firmware action required to contain and recover) 2 = Fatal error (system reset likely required to recover)
MEM_HOT_C{012/345}_N	Memory throttle control. Signals external BMC-less controller that DIMM is exceeding temperature limit and needs to increase to maximum fan speed. MEM_HOT_C012_N and MEM_HOT_C345_N signals have two modes of operation - input and output mode. Input mode is externally asserted and is used to detect external events such as VR_HOT# from the memory voltage regulator and causes the processor to throttle the appropriate memory channels. Output mode is asserted by the processor known as level mode. In level mode, the output indicates that a particular branch of memory subsystem is hot. MEM_HOT_C012_N is used for memory channels 0,1 & 2 while MEM_HOT_C345_N is used for memory channels 3, 4 & 5.
MSMI_N	Machine Check Exception (MCE) is signaled using this pin when eMCA2 is enabled. The MSMI_N signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD
PMSYNC	Power Management Sync. A sideband signal to communicate power management status from the Platform Controller Hub (PCH) to the processor.
PMSYNC_CLK	24 MHz SE Clock used for PCH PMSYNC.
PROCHOT_N	PROCHOT_N will go active when the processor temperature monitoring sensor detects that the processor has reached its maximum safe operating temperature. This indicates that the processor Thermal Control Circuit has been activated, if enabled. This signal can also be driven to the processor to activate the Thermal Control Circuit. This signal is sampled after PWRGOOD assertion.

Table 4-10. Processor Asynchronous Sideband Signals (Sheet 2 of 2)

Signal Name	Description
PWRGOOD	PWRGOOD is a processor input. The processor requires this signal to be a clean indication that all processor clocks and power supplies are stable and within their specifications. "Clean" implies that the signal will remain low (capable of sinking leakage current), without glitches, from the time that the power supplies are turned on until they come within specification. The signal must then transition monotonically to a high state. PWRGOOD can be driven inactive at any time, but clocks and power must again be stable before a subsequent rising edge of PWRGOOD. PWRGOOD transitions from inactive to active when all supplies except VCCIN are stable. The signal must be supplied to the processor; it is used to protect internal circuits against voltage sequencing issues. It should be driven high throughout boundary scan operation.
RESET_N	Global reset signal. Asserting the RESET_N signal resets the processor to a known state and invalidates its internal caches without writing back any of their contents. Note that some PLL, error states are not affected by reset and only PWRGOOD forces them to a known state.
THERMTRIP_N	Assertion of THERMTRIP_N (Thermal Trip) indicates one of two possible critical over-temperature conditions: One, the processor junction temperature has reached a level beyond which permanent silicon damage may occur and Two, the system memory interface has exceeded a critical temperature limit set by BIOS. Measurement of the processor junction temperature is accomplished through multiple internal thermal sensors that are monitored by the Digital Thermal Sensor (DTS). Simultaneously, the Power Control Unit (PCU) monitors external memory temperatures using the dedicated SMBus interface to the DIMMs. If any of the DIMMs exceed the BIOS defined limits, the PCU will signal THERMTRIP_N to prevent damage to the DIMMs. Once activated, the processor will stop all execution and shut down all PLLs. To further protect the processor, its core voltage (V_{CCIN}), V_{CCD}, V_{CCIO}, V_{CCIO} supplies must be removed following the assertion of THERMTRIP_N. Once activated, THERMTRIP_N remains latched until RESET_N is asserted. While the assertion of the RESET_N signal may de-assert THERMTRIP_N, if the processor's junction temperature remains at or above the trip level, THERMTRIP_N will again be asserted after RESET_N is de-asserted. This signal can also be asserted if the system memory interface has exceeded a critical temperature limit set by BIOS. The THERMTRIP_N signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD

Table 4-11. Miscellaneous Signals (Sheet 1 of 3)

Signal Name	Description
BIST_ENABLE	BIST Enable Strap. Input which allows the platform to enable or disable built-in self test (BIST) on the processor. This signal is pulled up on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
BMCINIT	BMC Initialization Strap. Indicates whether Processor Boot Mode should be used. Used in combination with FRMAGENT and SOCKET_ID inputs. 0 = Service Processor Boot Mode Disabled. Example boot modes: Local PCH (this processor hosts a legacy PCH with firmware behind it) 1 = Service Processor Boot Mode Enabled. In this mode of operation, the processor performs the absolute minimum internal configuration and then waits for the Service Processor to complete its initialization. The socket boots after receiving a "GO" handshake signal via a firmware scratchpad register. This signal is pulled down on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
DEBUG_EN_N	This pin is used to force debug to be enabled when the ITP is connected to the main board. This allows debug to occur beginning from cold boot.
DMIMODE_OVERRIDE	BMCINIT, DMIMODE_OVERRIDE, FRMAGENT, and LEGACY_SKT, whether local or remote, whether the boot PCH is attached, whether the socket is legacy and whether port0 is DMI or PCIe.

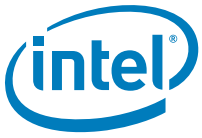


Table 4-11. Miscellaneous Signals (Sheet 2 of 3)

Signal Name	Description
EAR_N	External Alignment of Reset, used to bring the processor up into a deterministic state. This signal is pulled up on the die, refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
FIVR_FAULT	Indicates an internal error has occurred with the integrated voltage regulator. The FIVR_FAULT signal can be sampled any time after 1.5 ms after the assertion of PWRGOOD. FIVR_FAULT must be qualified by THERMTRIP_N assertion.
FRMAGENT	Bootable Firmware Agent Strap. This input configuration strap used in combination with SOCKET_ID to determine whether the socket is a legacy socket, bootable firmware agent is present, and DMI links are used in PCIe* mode (instead of DMI3 mode). The firmware flash ROM is located behind the local PCH attached to the processor via the DMI3 interface.This signal is pulled down on the die, refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
PM_FAST_WAKE_N	Power Management Fast Wake. Enables quick package C3 - C6 exits of all sockets. Asserted if any socket detects a break from package C3 - C6 state requiring all sockets to exit the low power state to service a snoop, memory access, or interrupt. Expected to be wired-OR among all processor sockets within the platform.
PROC_ID [1:0]	This output can be used by the platform to determine if the installed processor is an X-Series processor. There is no connection to the processor silicon for this signal. The processor package grounds or floats the pin to set '0' or '1', respectively. 00: X-Series Processor 01: Future processor 10: Future processor 11: Future processor
RSVD	RESERVED. All signals that are RSVD must be left unconnected on the board.
SAFE_MODE_BOOT	Safe Mode Boot Strap. SAFE_MODE_BOOT allows the processor to wake up safely by disabling all clock gating. This allows BIOS to load registers or patches if required. This signal is sampled after PWRGOOD assertion. The signal is pulled down on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
SKTOCC_N	SKTOCC_N (Socket Occupied) is used to indicate that a processor is present. This is pulled to ground on the processor package; there is no connection to the processor silicon for this signal.
SOCKET_ID[2:0]	SOCKET_IDStrap. Socket identification configuration straps for establishing the PECI address. This signal is used in combination with FRMAGENT to determine whether the socket is a legacy socket, bootable firmware agent is present, and DMI links are used in PCIe* mode (instead of DMI3 mode). Each processor socket consumes one Node ID, and there are 128 Home Agent tracker entries. This signal is pulled down on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
TEST[15:1]	TEST[14:13], TEST[2:1]] must be individually connected to an appropriate power source or ground through a resistor for proper processor operation.
TXT_AGENT	Intel® Trusted Execution Technology (Intel® TXT) Agent Strap. 0 = Default. The socket is not the Intel® TXT Agent. 1 = The socket is the Intel® TXT Agent. The legacy socket (identified by SOCKET_ID[1:0] = 00b) with Intel® TXT Agent should always set the TXT_AGENT to 1b. This signal is pulled down on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.

Table 4-11. Miscellaneous Signals (Sheet 3 of 3)

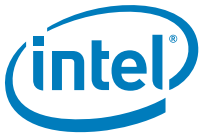
Signal Name	Description
TXT_PLTEN	Intel® Trusted Execution Technology (Intel® TXT) Platform Enable Strap. 0 = The platform is not Intel® TXT enabled. All sockets should be set to zero. Scalable DP (sDP) platforms should choose this setting if the Node Controller does not support Intel® TXT. 1 = Default. The platform is Intel® TXT enabled. All sockets should be set to one. In a non-Scalable DP platform this is the default. When this is set, Intel® TXT functionality requires the user to explicitly enable Intel® TXT via BIOS setup. This signal is pulled up on the die. Refer to Table 5-7, "Signals with On-Die Weak PU/PD" for details.
PROCDIS_N	PROCDIS_N assert initiates FRB and tri-states the processor.
PWR_DEBUG_N	This is a debug signal for power debug using Intel® ITP on the processor.
SOCKET_ID2	Asynchronous to other clocks in the processor.

4.9 Processor Power and Ground Supplies

Table 4-12. Power and Ground Signals

Signal Name	Description
V_{CCIN}	1.8 V - 1.55 V input to the Integrated Voltage Regulator (IVR) for the processor cores, lowest level caches (LLC), ring interface, PLL, IO, and home agent. It is provided by a VR 13.0 compliant motherboard voltage regulator (MBVR) for each CPU socket. The output voltage of this MBVR is controlled by the processor, using the serial voltage ID (SVID) bus.
VCCIN_SENSE VSS_VCCIN_SENSE	VCCIN_SENSE and VSS_VCCIN_SENSE are remote sense signals for V_{CCIN} MBVR13.0 and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification.
VCCIO_SENSE VSS_VCCIO_SENSE	VCCIO_SENSE and VSS_VCCIO_SENSE are remote sense signals for VCCIO and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification.
VCCSA_SENSE VSS_VCCSA_SENSE	VCCSA_SENSE and VSS_VCCSA_SENSE are remote sense signals, and are used by the voltage regulator to ensure accurate voltage regulation. These signals must be connected to the voltage regulator feedback circuit, which insures the output voltage remains within specification.
VCCIO	0.95 V - 1.0 V power supply for the processor IO.
VCCINPMAX	Pmax detect VCCIN supply through board R2 thermistor for VCCIN loadline temperature compensation
VCCSA	1.05 V - 0.55 V supply for IIO
VSENSEPMAX	Pmax detect circuit output voltage
V_{CCD_012} V_{CCD_345}	1.2 V - 1.05 V power supply for the processor system memory interface.
V_{SS}	Processor ground return.
V_{CCIO}	IO voltage supply input.

§



5 Electrical Specifications

This chapter describes processor signaling and DC specifications. References to various interfaces (memory, PCIe* PECI, and so forth) are also described.

5.1 Integrated Voltage Regulation

The platform voltage regulator is integrated into the processor. Due to this integration, the processor has one main voltage rail (V_{CCIN}) and a voltage rail for the memory interface (V_{CCD012}, V_{CCD345} - one for each memory channel pair). The V_{CCIN} voltage rail will supply the integrated voltage regulators which in turn will regulate to the appropriate voltages for the cores, cache, and system agents. This integration allows the processor to better control on-die voltages to optimize for both performance and power savings. The processor V_{CCIN} rail will remain a VID -based voltage with a loadline similar to the core voltage rail (called V_{CC}) in previous processors. In addition to the above, the processor has voltage rails VCCIO for IO, VCCSA for the System Agent, and VCC33 for PIROM.

5.2 Processor Signaling

The processor includes 2066 lands, which utilize various signaling technologies. Signals are grouped by electrical characteristics and buffer type into various signal groups. These include DDR4 (Reference Clock, Command, Control, and Data), PCI Express*, DMI3, Platform Environmental Control Interface (PECI), System Reference Clock, SMBus, JTAG and Test Access Port (TAP), SVID Interface, Processor Asynchronous Sideband, Miscellaneous, and Power/ Other signals. See Table 5-6 for details.

Intel strongly recommends performing analog simulations of all interfaces.

5.2.1 System Memory Interface Signal Groups

The system memory interface utilizes DDR4 technology, which consists of numerous signal groups. These include: Reference Clocks, Command Signals, Control Signals, and Data Signals. Each group consists of numerous signals, which may utilize various signaling technologies. See Table 5-6 for further details.

Throughout this chapter the system memory interface may be referred to as DDR4.

5.2.2 PCI Express* Signals

The PCI Express Signal Group consists of PCI Express* ports 1, 2, and 3, and PCI Express miscellaneous signals. See Table 5-6 for further details.

5.2.3 DMI3/PCI Express* Signals

The Direct Media Interface Gen 3(DMI3) sends and receives packets and/or commands to the PCH. The DMI3 is an extension of the standard PCI Express Specification. The DMI3/PCI Express Signals consist of DMI3 receive and transmit input/output signals and a control signal to select DMI3 or PCIe* 3.0 operation for port 0. See Table 5-6 for further details.

5.2.4 Platform Environmental Control Interface (PECI)

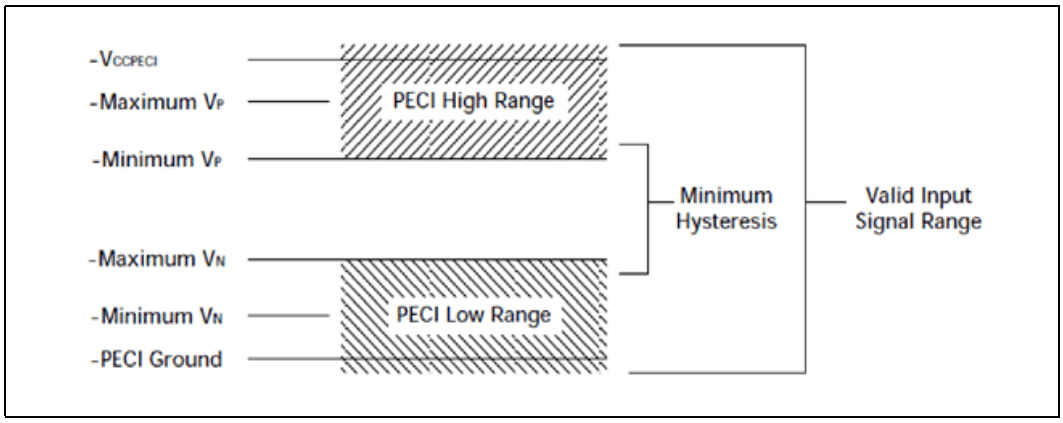
PECI is an Intel proprietary interface that provides a communication channel between Intel processors and chipset components to external system management logic and thermal monitoring devices. The processor contains a Digital Thermal Sensor (DTS) that reports a relative die temperature as an offset from Thermal Control Circuit (TCC) activation temperature. Temperature sensors located throughout the die are implemented as analog-to-digital converters calibrated at the factory. PECI provides an interface for external devices to read processor temperature, perform processor manageability functions, and manage processor interface tuning and diagnostics.

The PECI interface operates at a nominal voltage. The set of DC electrical specifications shown in Section 5.5.2.2 is used with devices normally operating from a PECI interface supply.

5.2.4.1 Input Device Hysteresis

The PECI client and host input buffers must use a Schmitt-triggered input design for improved noise immunity. Refer to the following image and Section 5.5.2.2.

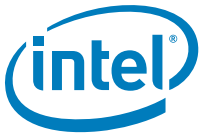
Figure 5-1. Input Device Hysteresis



5.2.5 System Reference Clocks (BCLK{0/1/2}_DP, BCLK{0/1/2}_DN)

The processor Core, processor Uncore, PCI Express*, and DDR4 memory interface frequencies are generated from BCLK{0/1/2}_DP and BCLK{0/1/2}_DN signals. The processor maximum core frequency and DDR memory frequency are set during manufacturing. It is possible to override the processor core frequency setting using software. This permits operation at lower core frequencies than the factory set maximum core frequency.

The processor core frequency is configured during reset by using values stored within the device during manufacturing. The stored value sets the lowest core multiplier at which the particular processor can operate. If higher speeds are desired, the appropriate ratio can be configured using the IA32_PERF_CTL MSR (MSR 199h); Bits [14:0].



Clock multiplying within the processor is provided by the internal phase locked loop (PLL), which requires a constant frequency BCLK{0/1/2}_DP, BCLK{0/1/2}_DN input, with exceptions for spread spectrum clocking. DC specifications for the BCLK{0/1/2}_DP, BCLK{0/1/2}_DN inputs are provided in Section 5.5.2.7.

5.2.6 JTAG and Test Access Port (TAP) Signals

Due to the voltage levels supported by other components in the JTAG and Test Access Port (TAP) logic, Intel recommends the processor be first in the TAP chain, followed by any other components within the system. A translation buffer should be used to connect to the rest of the chain unless one of the other components is capable of accepting an input of the appropriate voltage. Two copies of each signal may be required with each driving a different voltage level.

5.2.7 Processor Sideband Signals

The processor includes asynchronous sideband signals that provide asynchronous input, output or I/O signals between the processor and the platform or Platform Controller Hub. Details can be found in Table 5-6, "Signal Groups".

All Processor Asynchronous Sideband input signals are required to be asserted/ de-asserted for a defined number of BCLKs in order for the processor to recognize the proper signal state, these are outlined in Section 5.5.2.7, "Processor Asynchronous Sideband DC Specifications".

5.2.8 Power, Ground and Sense Signals

Processors also include various other signals including power/ground and sense points. Details can be found in Table 5-6, "Signal Groups".

5.2.8.1 Power and Ground Lands

All V_{CCD}, V_{CCIN}, and V_{CCSA}, and V_{CC33} lands must be connected to their respective processor power planes, while all V_{SS} lands must be connected to the system ground plane.

For clean on-chip power distribution, processors include lands for all required voltage supplies. These are listed in the following table.

Table 5-1. Power and Ground Lands

Power and Ground Lands	Comments
V_{CCIN}	Each V_{CCIN} land must be supplied with the voltage determined by the SVID Bus signals. VR 13.0 defines the voltage level associated with each core SVID pattern.
V_{CCD012} V_{CCD345}	Each V_{CCD} land is connected to a switchable 1.20 V supply, provide power to the processor DDR4 interface. V_{CCD} is also controlled by the SVID Bus. V_{CCD} is the generic term for V_{CCD012} and V_{CCD345}..
V_{CCSA}	IO voltage supply input
V_{CC33}	Power supply for PIROM.
V_{SS}	Ground
V_{CCIO}	IO voltage supply input

5.2.8.2 Decoupling Guidelines

Due to its large number of transistors and high internal clock speeds, the processor is capable of generating large current swings between low and full power states. This may cause voltages on power planes to sag below their minimum values if bulk decoupling is not adequate. Large electrolytic bulk capacitors (CBULK), help maintain the output voltage during current transients, for example coming out of an idle condition. Care must be taken in the baseboard design to ensure that the voltages provided to the processor remain within the specifications listed in Table 5-11, “Voltage Specification”. Failure to do so can result in timing violations or reduced lifetime of the processor.

5.2.8.3 Voltage Identification (VID)

The Voltage Identification (VID) specification for the VCCIN, VSA, voltage is defined by the VR13.0 PWM. The reference voltage or the VID setting is set using the SVID communication bus between the processor and the voltage regulator controller chip. The VID settings are the nominal voltages to be delivered to the processor's lands. The VR 13.0 Reference Code Voltage Identification Table specifies the reference voltage level corresponding to the VID value transmitted over serial VID. The VID codes will change due to temperature and/or current load changes in order to minimize the power and to maximize the performance of the part. The specifications are set so that a voltage regulator can operate with all supported frequencies.

Individual processor VID values may be calibrated during manufacturing such that two processor units with the same core frequency may have different default VID settings.

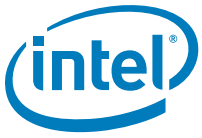
The processor uses voltage identification signals to support automatic selection of a power supply voltage. If the processor socket is empty (SKTOCC_N high), or a “not supported” response is received from the SVID bus, then the voltage regulation circuit cannot supply the voltage that is requested, the voltage regulator must disable itself or not power on. Vout MAX register (30h) is programmed by the processor to set the maximum supported VID code and if the programmed VID code is higher than the VID supported by the VR, then VR will respond with a “not supported” acknowledgment.

5.2.8.4 SVID Commands

The processor provides the ability to operate while transitioning to a new VID setting and its associated processor voltage rail. This is represented by a DC shift. It should be noted that a low-to-high or high-to-low voltage state change may result in as many VID transitions as necessary to reach the target voltage. Transitions above the maximum specified VID are not supported. The processor supports the following VR commands:

- SetVID_Fast (25 mV/µs for VCCIN, 10mV for VSA,VCCIO)
- SetVID_Slow is 1/4 of SetVID_Fast
- SetVID_Decay (downward voltage only and it's a function of the output capacitance's time constant) commands. The VR 13.0 Reference Code Voltage Identification Table includes SVID step sizes and DC shift ranges. Minimum and maximum voltages must be maintained as shown in Table 5-11. This is a CSR configuration option.

The VRM or EVRD utilized must be capable of regulating its output to the value defined by the new VID.



Power source characteristics must be guaranteed to be stable whenever the supply to the voltage regulator is stable.

5.2.8.5 SetWP Working Point Command

The SetWP is a command that invokes a look up table for VID set points. During the initial power on phase the CPU will program the WPx registers (WP0=3Ah..WP7=41h) on a per rail address basis. When use with the AllCall address, SetWP acts as a group command that moves all voltage rails on the bus to new voltages in the look up table index. The SetWP command can also be used with an individual VR rail address and that rail moves to the voltage in the loop up table index. Each VR domain address has registers WP0-WPx (3Ah..41h) which stores the VID code for that domain's work points.

The Work Point command is encoded to support up to 8 VID targets, slew rate for the command, and alert function. The PWM should use its auto power state or auto-phase shedding functions to select appropriate # phases, CCM/DCM operation, and so forth. based on output load current after the SetWP command target has been reached.

Typical SetWP usage will be:

1. Processor writes VID codes to WP registers WP0 (3Ah) -WP4 (3Dh) in each VR domain. Normally done during SVID enumeration phase of system boot.
2. If a WP0-7 register is not programmed by the CPU, the VR stays at its present VID setting when it receives a SetWP (WPn) command.
3. Processor sends SetWP (WPn) command to one of the AllCall addresses 0Eh or 0Fh. See PWM guideline for more information on AllCall address mapping.
4. Voltage rails change VID to their corresponding VID code stored in their WPx register
5. CPU polls each VR addresses reading stutus1 to clear the alerts from the VRs
6. SVID error handling

WP0 = State 0, programed by master

WP1 = State 1, programmed by master

WP2 = State 2, programmed by master

WP3 = State 3, programmed by master

WP4 = State 4, programmed by master

…

WP7 = State 7

5.2.8.6 SetVID Fast Command

The SetVID_Fast command contains the target VID in the payload byte. The range of voltage is defined in the VID table. The VR should ramp to the new VID setting with a fast slew rate as defined in the slew rate data register. It is minimum of 25 mV/µs for V_{CCIN} and 10 mV/µs for other rails, depending on the amount of decoupling capacitance.

The SetVID_Fast command is preemptive. The VR interrupts its current processes and moves to the new VID. The SetVID_Fast command operates on 1 VR address at a time. This command is used in the processor for package C6 fast exit.

5.2.8.7 SetVID Slow

The SetVID_Slow command contains the target VID in the payload byte. The range of voltage is defined in the VID table. The VR should ramp to the new VID setting with a "slow" slew rate as defined in the slow slew rate data register. The SetVID_Slow is nominally 4x slower than the SetVID_Fast slew rate.

The SetVID_Slow command is preemptive, the VR interrupts its current processes and moves to the new VID. This is the instruction used for normal P-state voltage change. This command is used in the processor for the Intel Enhanced SpeedStep Technology transitions.

5.2.8.8 SetVID Decay

The SetVID_Decay command is the slowest of the DVID transitions. It is only used for VID down transitions. The VR does not control the slew rate, the output voltage declines with the output load current only.

The SetVID_Decay command is preemptive, the VR interrupts its current processes and moves to the new VID. This command is used in the processor for package C6 entry, allowing capacitor discharge by the leakage, thus saving energy.This command is only used in VID down direction in the processor package C6 entry.

5.2.8.9 SVID Voltage Rail Addressing

The processor addresses 4 different voltage rail control segments within VR13.0 (V_{CCIN}, V_{CCD}, V_{CCSA}, and V_{CCIO}). The SVID data packet contains a 4-bit addressing code.

Table 5-2. SVID Address Usage Bus 1

PWM Address (HEX)	Protocol ID	Processor
00	04H(10 mV VID)	V_{CCIN}
01	07H(5 mV VID)	V_{CCSA}
02	07H(5 mV VID)	V_{CCIO}
03	N/A	Reserved for optional rail
04		Reserved for optional rail
05		Reserved for optional rail

Notes:
1. Check with VR vendors for determining the physical address assignment method for their controllers.
2. VR addressing is assigned on a per voltage rail basis.
3. Dual VR controllers will have two addresses with the lowest order address, always being the higher phase count.
4. For future platform flexibility, the VR controller should include an address offset, as shown with +1 not used.

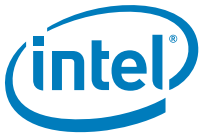


Table 5-3. SVID Address Usage Bus 2

PWM Address (HEX)	Protocol ID	Processor
00	04H(10mV VID) or 07H(5mV VID)	V_{CCD012}
01		NA
02	04H(10mV VID) or 07H(5mV VID)	V_{CCD345}
03		NA

Notes:
1. Check with VR vendors for determining the physical address assignment method for their controllers.
2. VR addressing is assigned on a per voltage rail basis.
3. Dual VR controllers will have two addresses with the lowest order address, always being the higher phase count.

Table 5-4. VR13.0 Reference Code Voltage Identification (VID) Table (Sheet 1 of 2)

HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN
00	0.00	20	0.81	40	1.13	60	1.45	80	1.77	A0	2.09	C0	2.41	E0	2.73
01	0.50	21	0.82	41	1.14	61	1.46	81	1.78	A1	2.10	C1	2.42	E1	2.74
02	0.51	22	0.83	42	1.15	62	1.47	82	1.79	A2	2.11	C2	2.43	E2	2.75
03	0.52	23	0.84	43	1.16	63	1.48	83	1.80	A3	2.12	C3	2.44	E3	2.76
04	0.53	24	0.85	44	1.17	64	1.49	84	1.81	A4	2.13	C4	2.45	E4	2.77
05	0.54	25	0.86	45	1.18	65	1.50	85	1.82	A5	2.14	C5	2.46	E5	2.78
06	0.55	26	0.87	46	1.19	66	1.51	86	1.83	A6	2.15	C6	2.47	E6	2.79
07	0.56	27	0.88	47	1.20	67	1.52	87	1.84	A7	2.16	C7	2.48	E7	2.80
08	0.57	28	0.89	48	1.21	68	1.53	88	1.85	A8	2.17	C8	2.49	E8	2.81
09	0.58	29	0.90	49	1.22	69	1.54	89	1.86	A9	2.18	C9	2.50	E9	2.82
0A	0.59	2A	0.91	4A	1.23	6A	1.55	8A	1.87	AA	2.19	CA	2.51	EA	2.83
0B	0.60	2B	0.92	4B	1.24	6B	1.56	8B	1.88	AB	2.20	CB	2.52	EB	2.84
0C	0.61	2C	0.93	4C	1.25	6C	1.57	8C	1.89	AC	2.21	CC	2.53	EC	2.85
0D	0.62	2D	0.94	4D	1.26	6D	1.58	8D	1.90	AD	2.22	CD	2.54	ED	2.86
0E	0.63	2E	0.95	4E	1.27	6E	1.59	8E	1.91	AE	2.23	CE	2.55	EE	2.87
0F	0.64	2F	0.96	4F	1.28	6F	1.60	8F	1.92	AF	2.24	CF	2.56	EF	2.88
10	0.65	30	0.97	50	1.29	70	1.61	90	1.93	B0	2.25	D0	2.57	F0	2.89
11	0.66	31	0.98	51	1.30	71	1.62	91	1.94	B1	2.26	D1	2.58	F1	2.90
12	0.67	32	0.98	52	1.31	72	1.63	92	1.95	B2	2.27	D2	2.59	F2	2.91
13	0.68	33	1.00	53	1.32	73	1.64	93	1.96	B3	2.28	D3	2.60	F3	2.92
14	0.69	34	1.01	54	1.33	74	1.65	94	1.97	B4	2.29	D4	2.61	F4	2.93
15	0.70	35	1.02	55	1.34	75	1.66	95	1.98	B5	2.30	D5	2.62	F5	2.94
16	0.71	36	1.03	56	1.35	76	1.67	96	1.99	B6	2.31	D6	2.63	F6	2.95
17	0.72	37	1.04	57	1.36	77	1.68	97	2.00	B7	2.32	D7	2.64	F7	2.96
18	0.73	38	1.05	58	1.37	78	1.69	98	2.01	B8	2.33	D8	2.65	F8	2.97
19	0.74	39	1.06	59	1.38	79	1.70	99	2.02	B9	2.34	D9	2.66	F9	2.98
1A	0.75	3A	1.07	5A	1.39	7A	1.71	9A	2.03	BA	2.35	DA	2.67	FA	2.99
1B	0.76	3B	1.08	5B	1.40	7B	1.72	9B	2.04	BB	2.36	DB	2.68	FB	3.00
1C	0.77	3C	1.09	5C	1.41	7C	1.73	9C	2.05	BC	2.37	DC	2.69	FC	3.01
1D	0.78	3D	1.10	5D	1.42	7D	1.74	9D	2.06	BD	2.38	DD	2.70	FD	3.02

Table 5-4. VR13.0 Reference Code Voltage Identification (VID) Table (Sheet 2 of 2)

HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN	HEX	VCCIN
1E	0.79	3E	1.11	5E	1.43	7E	1.75	9E	2.07	BE	2.39	DE	2.71	FE	3.03
1F	0.80	3F	1.12	5F	1.44	7F	1.76	9F	2.08	BF	2.40	DF	2.72	FF	3.04

Notes:
1. 00h = Off State
2. VID Range HEX 65-97 are not used by the processor
3. VCCD can use Protocol ID of 10 mV or 5 mV.
4. VCCD can use VID Table 5-4.

5.2.9 Reserved or Unused Signals

All Reserved (RSVD) signals must not be connected. Connection of these signals to V_{CCIN}, V_{CCD}, V_{SS}, or to any other signal (including each other) can result in component malfunction or incompatibility with future processors.

For reliable operation, always connect unused inputs or bi-directional signals to an appropriate signal level. Unused active high inputs should be connected through a resistor to ground (V_{SS}). Unused outputs maybe left unconnected; however, this may interfere with some Test Access Port (TAP) functions, complicate debug probing, and prevent boundary scan testing. A resistor must be used when tying bi-directional signals to power or ground. When tying any signal to power or ground, a resistor will also allow for system testability.

5.3 Signal Group Summary

Signals are grouped by buffer type and similar characteristics as listed in the following table. The buffer type indicates which signaling technology and specifications apply to the signals.

Table 5-5. Signal Description Buffer Types

Signal	Description
Analog	Analog reference or output. May be used as a threshold voltage or for buffer compensation
Asynchronous	Signal has no timing relationship with any system reference clock.
CMOS	CMOS Output buffers: 1.05 V tolerant / CMOS Input buffers
DDR4	CMOS Output buffers 1.2 V tolerant
DMI3	Direct Media Interface Gen 3 signals. These signals are compatible with PCI Express* 3.0 Signaling Environment AC Specifications.
Open Drain	Open Drain buffers: 1.05 V tolerant
PCI Express*	PCI Express interface signals. These signals are compatible with PCI Express 3.0 Signaling Environment AC Specifications and are AC coupled. The buffers are not 3.3–V tolerant. Refer to the PCIe specification.
Reference	Voltage reference signal.
SSTL	Source Series Terminated Logic (JEDEC SSTL_15)
Note: Qualifier for a buffer type.	

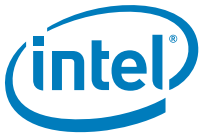


Table 5-6. Signal Groups (Sheet 1 of 2)

Differential/Single Ended	Buffer Type	Signal
DDR4 Reference Clocks		
Differential	SSTL Output	DDR{0/1/2/3/4/5}_CLK_D[N/P] [3:0]
DDR4 Command Signals		
Single-ended	SSTL Output	DDR{0/1/2/3/4/5}_ACT_N DDR{0/1/2/3/4/5}_BA[1:0] DDR{0/1/2/3/4/5}_BG[1:0] DDR{0/1/2/3/4/5}_MA[17:0] DDR{0/1/2/3/4/5}_PAR
DDR4 Control Signals		
Single-ended	SSTL Output	DDR{0/1/2/3/4/5}_CS_N[7:0] DDR{0/1/2/3/4/5}_CID[2] DDR{0/1/2/3/4/5}_ODT[3:0] DDR{0/1/2/3/4/5}_CKE[3:0]
DDR4 Data Signals		
Differential	SSTL Input/Output	DDR{0/1/2/3/4/5}_DQS_D[N/P] [17:0]
Single-ended	SSTL Input/Output	DDR{0/1/2/3/4/5}_DQ[63:0] DDR{0/1/2/3/4/5}_ECC[7:0]
DDR4 Miscellaneous Signals		
Single-ended	SSTL Input	DDR{0/1/2/3/4/5}_ALERT_N
	CMOS Input **Note:** Input voltage from platform cannot exceed 1.2 V max.	DDR{012,345}_DRAM_PWR_OK
	CMOS 1.2 V Output	DDR{012,345}_RESET_N
	Open Drain Output / CMOS Input	DDR[012,345]_SPDSCL DDR[012,345]_SPDSDA
	DC Output	DDR{5:0}_CAVREF
	DDR Compensation resistance control	DDR{012,345}_RCOMP[2:0]
PCI Express* Port 1, 2, & 3 Signals		
Differential	PCI Express* Input	PE{3:1}_RX_DN/DP[15:0]
Differential	PCI Express* Output	PE{3:1}_TX_DN/DP[15:0]
PCI Express* Miscellaneous Signals		
Single-ended	Open Drain Output	PE_HP_SCL
	Open Drain Output /CMOS Input	PE_HP_SDA
DMI3/PCI Express* Signals		
Differential	DMI3 Input	DMI3_RX_D[N/P][3:0]
	DMI3 Output	DMI3_TX_D[N/P][3:0]
Single-ended	DMI Miscellaneous	DMIMODE_OVERRIDE
Platform Environmental Control Interface (PECI)		
Single-ended	PECI Input/Output	PECI

Table 5-6. Signal Groups (Sheet 2 of 2)

Differential/Single Ended	Buffer Type	Signal
System Reference Clock (BCLK{0/1/2})		
Differential	CMOS 1.05 V Input	BCLK{0/1/2}_D[N/P]
JTAG & TAP Signals		
Single ended	CMOS Input	TCK,TDI,TMS,TRST_N,PREQ_N
	Open Drain Output /CMOS Input	BPM_N[7:0]
	Open Drain Output	TDO, PRDY_N
Serial VID Interface (SVID) Signals		
Single ended	CMOS Input	SVIDALERT_N[1:0]
	Open Drain Output / CMOS Input	SVIDDATA [1:0]
	Open Drain Output	SVIDCLK [1:0]
Processor Asynchronous Sideband Signals		
Single ended	CMOS Input	BIST_ENABLE, BMCINIT, DEBUG_EN_N
		FRMAGENT, PWRGOOD, PMSYNC RESET_N, SAFE_MODE_BOOT, SOCKET_ID[1:0], TXT_AGENT TXT_PLTEN
	CMOS Output	FIVR_FAULT
	Open Drain Output / CMOS Input	CATERR_N, MEM_HOT_C01_N, MEM_HOT_C23_N, MSMI_N, PM_FAST_WAKE_N, PROCHOT_N
	Open Drain Output	ERROR_N[2:0], THERMTRIP_N
Miscellaneous Signals		
	CMOS Input	EAR_N,LEGACY_SKT,NMI,PMSYNCPMSY NC_CLK,PROCDIS_N, PWR_DEBUG_N,SOCKET_ID2
	Open Drain Output / CMOS Input	TSC_SYNC
	Not connected to Silicon	SKTOCC_N,PKGID[2:0], PROC_ID[1:0]
Power/Other Signals		
	Power / Ground	V_{CCIN}, V_{CCD_012}, V_{CCD_345}, V_{CCIO}, V_{CC33}, V_{CC33}, V_{SS}
	Sense Points	VCCIN_SENSE, VCCIO_SENSE, VCCSA_SENSE, VSS_VCCIN_SENSE, VSS_VCCIO_SENSE, VSS_VCCSA_SENSE, VCCIN_PMAX, VSENSEPMAX

Notes:
1. Refer to Chapter 4, "Signal Descriptions" for signal description details.
2. DDR{0/1/2/3/4/5} refers to DDR4 Channel 0, DDR4 Channel 1, DDR4 Channel 2, DDR4 Channel 3, DDR4 Channel 4 and DDR4 Channel 5.

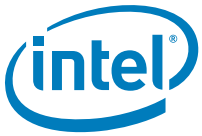


Table 5-7. Signals with On-Die Weak PU/PD

Signal Name	Pull Up/Pull Down	Rail	Value	Units	Notes
BIST_ENABLE	Pull Up	V_{CCIO}	3K-8K	Ω	
BMCINIT	Pull Down	VSS	3K-8K	Ω	
DEBUG_EN_N	Pull Up	V_{CCIO}	3K-8K	Ω	
DMIMODE_OVERRIDE	Pull Up	V_{CCIO}	3K-8K	Ω	
EAR_N	Pull Up	V_{CCIO}	3K-8K	Ω	
FRMAGENT	Pull Down	VSS	3K-8K	Ω	
LEGACY_SKT	Pull Down	VSS	3K-8K	Ω	
MSMI_N	Pull Up	V_{CCIO}	3K-8K	Ω	
NMI	Pull Down	VSS	3K-8K	Ω	
PM_FAST_WAKE_N	Pull Up	V_{CCIO}	3K-8K	Ω	
PROCDIS_N	Pull Up	V_{CCIO}	3K-8K	Ω	
SAFE_MODE_BOOT	Pull Down	VSS	3K-8K	Ω	
SOCKET_ID[2:0]	Pull Down	VSS	3K-8K	Ω	
TCK	Pull Down	VSS	3K-8K	Ω	
TDI	Pull Up	V_{CCIO}	3K-8K	Ω	
TMS	Pull Up	V_{CCIO}	3K-8K	Ω	
TRST_N	Pull Up	V_{CCIO}	3K-8K	Ω	
TXT_AGENT	Pull Down	VSS	3K-8K	Ω	
TXT_PLTEN	Pull Up	V_{CCIO}	3K-8K	Ω	

5.3.1 Power-On Configuration (POC) Options

Several configuration options can be configured by hardware. The processor samples its hardware configuration at reset, on the active-to-inactive transition of RESET_N, or upon assertion of PWRGOOD (inactive-to-active transition). For specifics on these options, see the following table.

The sampled information configures the processor for subsequent operation. These configuration options cannot be changed except by another reset transition of the latching signal (RESET_N or PWRGOOD).

Table 5-8. Power-On Configuration Option Lands (Sheet 1 of 2)

Configuration Option	Land Name	Notes
Output tri state	PROCDIS_N	1
Execute BIST (Built-In Self Test)	BIST_ENABLE	2
Enable Service Processor Boot Mode	BMCINIT	3
Power-up Sequence Halt	EAR_N	3
Enable Intel® Trusted Execution Technology (Intel® TXT) Platform	TXT_PLTEN	3
Enable Bootable Firmware Agent	FRMAGENT	3

Table 5-8. Power-On Configuration Option Lands (Sheet 2 of 2)

Configuration Option	Land Name	Notes
Enable Intel Trusted Execution Technology (Intel TXT) Agent	TXT_AGENT	3
Enable Safe Mode Boot	SAFE_MODE_BOOT	3
Configure Socket ID	SOCKET_ID[1:0]	3
Enable legacy socket boot	LEGACY_SKT	3

Notes:
1. Output tri-state option enables Fault Resilient Booting (FRB), for FRB details, see the Fault Resilient Booting (FRB) Section. The signal used to latch PROCDIS_N for enabling FRB mode is RESET_N.
2. BIST_ENABLE is sampled at RESET_N de-assertion
3. This signal is sampled after PWRGOOD assertion.

5.4 Absolute Maximum and Minimum Ratings

The following table specifies absolute maximum and minimum ratings. At conditions outside functional operation condition limits, but within absolute maximum and minimum ratings, neither functionality nor long-term reliability can be expected. If a device is returned to conditions within functional operation limits after having been subjected to conditions outside these limits, but within the absolute maximum and minimum ratings, the device may be functional, but with its lifetime degraded depending on exposure to conditions exceeding the functional operation condition limits.

Although the processor contains protective circuitry to resist damage from Electro-Static Discharge (ESD), precautions should always be taken to avoid high static voltages or electric fields.

Table 5-9. Processor Absolute Minimum and Maximum Ratings

Symbol	Parameter	Min	Max	Unit
V_{CCIN}	Processor input voltage with respect to Vss	-0.3	2.15	V
V_{CCD}	Processor IO supply voltage for DDR4 (standard voltage) with respect to V_{SS}	-0.3	1.35	V
V_{CCIO}	IO voltage supply input with respect to V_{SS}	-0.3	1.35	V
V_{CCSA}	IO voltage supply input with respect to V_{SS}	-0.3	1.35	V

Notes:
1. For functional operation, all processor electrical, signal quality, mechanical, and thermal specifications must be satisfied.
2. Excessive Overshoot or undershoot on any signal will likely result in permanent damage to the processor.

5.4.1 Storage Conditions Specifications

Environmental storage condition limits define the temperature and relative humidity limits to which the device is exposed to while being stored in a Moisture Barrier Bag. The specified storage conditions are for component level prior to board attach (see notes in the following table for post board attach limits).

The following table specifies absolute maximum and minimum storage temperature limits which represent the maximum or minimum device condition beyond which damage, latent or otherwise, may occur. The table also specifies sustained storage temperature, relative humidity, and time-duration limits. These limits specify the

maximum or minimum device storage conditions for a sustained period of time. At conditions outside sustained limits, but within absolute maximum and minimum ratings, quality and reliability may be affected.

Table 5-10. Storage Condition Ratings

Symbol	Parameter	Min	Max	Unit
$T_{absolute\ storage}$	The minimum/maximum device storage temperature beyond which damage (latent or otherwise) may occur when subjected to for any length of time.	-25	125	°C
$T_{sustained\ storage}$	The minimum/maximum device storage temperature for a sustained period of time.	-5	40	°C
$T_{short\ term\ storage}$	The ambient storage temperature (in shipping media) for a short period of time.	-20	85	°C
$RH_{sustained\ storage}$	The maximum device storage relative humidity for a sustained period of time.Unopened bag, includes 6 months storage time by customer.	60% @ 24		°C
$Time_{short\ term\ storage}$	A short period of time (in shipping media).	0	72	hours

Notes:
1. Storage conditions are applicable to storage environments only. In this scenario, the processor must not receive a clock, and no lands can be connected to a voltage bias. Storage within these limits will not affect the long-term reliability of the device. For functional operation, please refer to the processor case temperature specifications.
2. These ratings apply to the Intel component and do not include the tray or packaging.
3. Failure to adhere to this specification can affect the long-term reliability of the processor.
4. Non-operating storage limits post board attach: Storage condition limits for the component once attached to the application board are not specified. Intel does not conduct component level certification assessments post board attach given the multitude of attach methods, socket types and board types used by customers. Provided as general guidance only, Intel board products are specified and certified to meet the following temperature and humidity limits (Non-Operating Temperature Limit: -40 °C to 70 °C and Humidity: 50% to 90%, non condensing with a maximum wet bulb of 28 °C).
5. Device storage temperature qualification methods follow JEDEC High and Low Temperature Storage Life Standards: *JESD22-A119* (low temperature) and *JESD22-A103* (high temperature).

5.5 DC Specifications

DC specifications are defined at the processor pads, unless otherwise noted. DC specifications are only valid while meeting specifications for case temperature, clock frequency, and input voltages. Care should be taken to read all notes associated with each specification.

5.5.1 Voltage and Current Specifications

Table 5-11. Voltage Specification (Sheet 1 of 2)

Symbols	Parameter	Voltage Plane	Min	Nom	Max	Unit	Notes[1]
V_{CCIN}	Input to Integrated Voltage Regulator	VCCIN	= VID - Rll*Iout-0.022V	= VID - Rll*Iout	= VID - Rll*Iout+0.022V	V	2, 3, 4, 5, 8, 12
V_{CCIN} VID Range		VCCIN	1.60	1.80	1.83	V	2, 3, 4, 5, 8, 12
V_{VID_STEP} (V_{CCIN})	VID step size during a transition	VCCIN	—	10.0	—	mV	6
V_{VID_STEP} (V_{CCD})	VID step size during a transition	—	5	—	10	mV	

Table 5-11. Voltage Specification (Sheet 2 of 2)

Symbols	Parameter	Voltage Plane	Min	Nom	Max	Unit	Notes[1]
V_{CCD} (V_{CCD_012}, V_{CCD_345})	I/O Voltage for DDR4 (Standard Voltage)	VCCD	1.17	1.2	1.26	V	7, 9, 10, 11
V_{CCSA}	Power supply for IIO	—	0.5	—	1.1	V	
V_{CCIO}	IO voltage supply input		0.937	1.00	1.057	V	
V_{CC33}	Power supply for PIROM		3.14	3.3	3.47	V	

Notes:
1. Unless otherwise noted, all specifications in this table apply to all processors.
2. These voltages are targets only. A variable voltage source should exist on systems in the event that a different voltage is required.
3. The VCCIN voltage specification requirements are measured across the remote sense pin pairs (VCCIN_SENSE and VSS_VCCIN_SENSE) on the processor package. Voltage measurement should be taken with a DC to 100 MHz bandwidth oscilloscope limit (or DC to 20 MHz for older model oscilloscopes), using a 1.5 pF maximum probe capacitance, and 1 Mohm minimum impedance. The maximum length of the ground wire on the probe should be less than 5 mm to ensure external noise from the system is not coupled in the scope probe.
4. Refer to VCCIN Static and Transient Tolerance Processor and corresponding Figure 5-2, "VCCIN Static and Transient Tolerance Load Lines 1.0 mOHM" on page 50. The processor should not be subjected to any static VCCIN level that exceeds the VCCIN_MAX associated with any particular current. Failure to adhere to this specification can shorten processor lifetime.
5. ICCIN_MAX is specified at the relative VCC_MAX point on the VCCIN load line. The processor is capable of drawing ICCIN_MAX for up to 2 ms.
6. This specification represents the VCCIN reduction or VCCIN increase due to each VID transition. For Voltage Identification (VID), see Table 5-4, "VR13.0 Reference Code Voltage Identification (VID) Table".
7. Baseboard bandwidth is limited to 20 MHz.
8. N/A
9. DC + AC + Ripple = Tolerance
10. VCCD tolerance at processor pins. Required in order to meet +/-5% tolerance at processor die.
11. The VCCD012, VCCD345 voltage specification requirements are measured across vias on the platform. Choose VCCD012 or VCCD345 vias close to the socket and measure with a DC to 100 MHz bandwidth oscilloscope limit (or DC to 20 MHz for older model oscilloscopes), using 1.5 pF maximum probe capacitance, and 1M ohm minimum impedance. The maximum length of the ground wire on the probe should be less than 5 mm to ensure external noise from the system is not coupled in the scope probe.
12. VCCIN has a Vboot setting of 1.7 V and is not included in the PWRGOOD indication.

Table 5-12. Current (ICCIN_MAX and ICCIN_TDC) Specification

TDP (W)	140	165
VCCIN ICCMAX (A)	200	205
VCCSA ICCMAX (A)	15	15
VCCIO ICCMAX (A)	12	12
VCCD ICCMAX (A)	6	6
VCCIN TDC (A)	77	89
VCCSA TDC (A)	14	14
VCCIO TDC (A)	11	11
VCCD TDC (A)	4	4
Pmax Package (W)	308	363

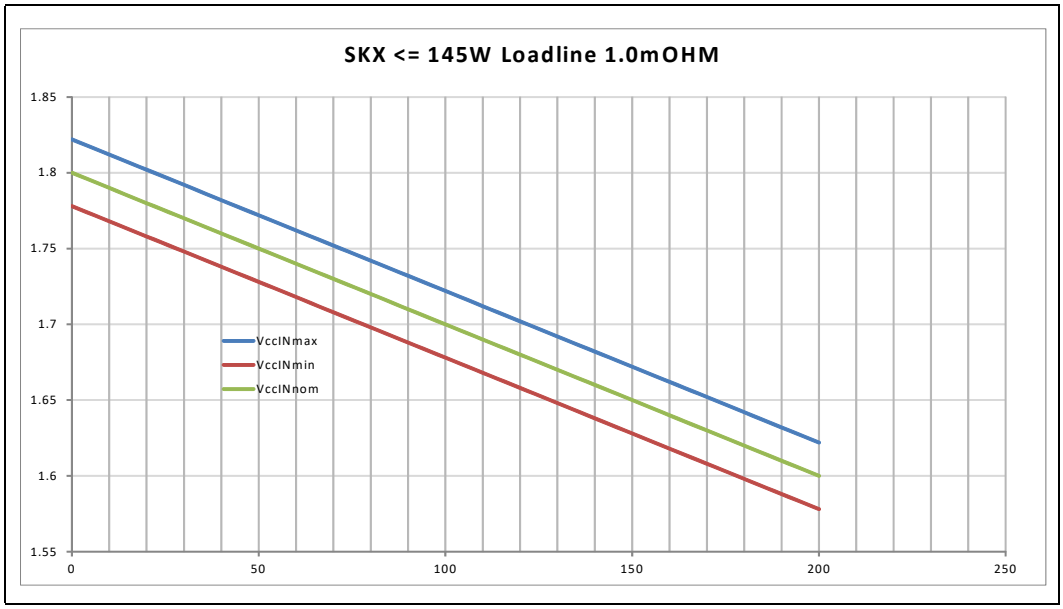
Notes:
1. Unless otherwise noted, all specifications in this table apply to all processors.
2. N/A
3. I_{CCIN_TDC} (Thermal Design Current) is the sustained (DC equivalent) current that the processor is capable of drawing indefinitely and should be used for the voltage regulator thermal assessment. The voltage regulator is responsible for monitoring its temperature and asserting the necessary signal to inform the processor of a thermal excursion.
4. Minimum V_{CCIN} and maximum I_{CCIN} are specified at the maximum processor case temperature (T_{CASE}). ICCIN_MAX is specified at the relative VCCIN_MAX point on the VCCIN load line. The processor is capable of drawing ICCIN_MAX for up to 2 ms.

Table 5-13. V_{CCIN} Static and Transient Tolerance for 1.0LL

I_{CCIN} (A)	V_{CCIN_Max} (V)	V_{CCIN_Nom} (V)	V_{CCIN_Min} (V)	Notes
0	VID +0.022	VID -0.000	VID -0.022	
10	VID +0.012	VID -0.010	VID -0.032	
20	VID +0.002	VID -0.020	VID -0.042	
30	VID -0.008	VID -0.030	VID -0.052	
40	VID -0.018	VID -0.040	VID -0.062	
50	VID -0.028	VID -0.050	VID -0.072	
60	VID -0.038	VID -0.060	VID -0.082	
70	VID -0.048	VID -0.070	VID -0.092	
80	VID -0.058	VID -0.080	VID -0.102	
90	VID -0.068	VID -0.090	VID -0.112	
100	VID -0.078	VID -0.100	VID -0.122	
110	VID -0.088	VID -0.110	VID -0.132	
120	VID -0.098	VID -0.120	VID -0.142	
130	VID -0.108	VID -0.130	VID -0.152	
140	VID -0.118	VID -0.140	VID -0.162	
150	VID -0.128	VID -0.150	VID -0.172	
160	VID -0.138	VID -0.160	VID -0.182	
170	VID -0.148	VID -0.170	VID -0.192	
180	VID -0.158	VID -0.180	VID -0.202	
190	VID -0.168	VID -0.190	VID -0.212	
200	VID -0.178	VID -0.200	VID -0.222	
210	VID -0.188	VID -0.210	VID -0.232	
220	VID -0.198	VID -0.220	VID -0.242	
230	VID - 0.208	VID - 0.230	VID - 0.252	

Notes:
1. The V_{CCIN_MIN} and V_{CCIN_MAX} loadlines represent static and transient limits.
2. This table is intended to aid in reading discrete points on graph in Figure 5-2, "VCCIN Static and Transient Tolerance Load Lines 1.0 mOHM" on page 50.
3. The loadlines specify voltage limits at the die measured at the V_{CCIN_SENSE} and $V_{SS\_VCCIN\_SENSE}$ lands. Voltage regulation feedback for voltage regulator circuits must also be taken from processor V_{CCIN_SENSE} and $V_{SS\_VCCIN\_SENSE}$ lands.
4. The Adaptive Loadline Positioning slope is 1.00 mΩ (mohm) with ±22mV TOB (Tolerance of Band).

Figure 5-2. VCCIN Static and Transient Tolerance Load Lines 1.0 mOHM



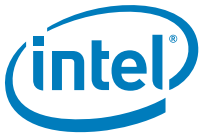
5.5.2 Signal DC Specifications

For additional specifications, refer to Section 1.8, "Related Documents."

5.5.2.1 DDR4 Signal DC Specifications

For the next table, use Signal Group Table 5-6, "Signal Groups" to identify which signals belong to each group.

Symbol	Parameter	Min	Nom	Max	Units	Notes[1]
I_{IL}	Input Leakage Current	-1.4	—	+1.4	mA	9
Data Signals						
R_{ON}	DDR4 Data Buffer On Resistance	25.5	30	34.5	ohm	6
Data ODT	On-Die Termination for Data Signals	42.5	50	57.5	ohm	8
Reference Clock and Command Signals						
V_{OL}	Output Low Voltage	—	$(V_{CCD} / 2)* (R_{ON} / (R_{ON} + R_{VTT\_TERM}))$	—	V	2, 7
V_{OH}	Output High Voltage	—	$V_{CCD} - ((V_{CCD} / 2)* (R_{ON} / (R_{ON} + R_{VTT\_TERM})))$	—	V	2, 5, 7
Data Signals						
V_{OL}	Output Low Voltage	—	$Vol=(Ron / (Ron + R_{VDD\_TERM})) *V_{CCD}$	—	V	10
V_{OH}	Output High Voltage	—	V_{CCD}	—	V	



Symbol	Parameter	Min	Nom	Max	Units	Notes[1]
Reference Clock Signal						
R_{ON}	DDR4 Clock Buffer On Resistance	25.5	30	34.5	ohm	6
Command Signals						
R_{ON}	DDR4 Command Buffer On Resistance	15.3	18	20.7	ohm	6, 11
R_{ON}	DDR4 Reset Buffer On Resistance	76.5	90	103.5	ohm	6
$V_{OL\_CMOS1.2V}$	Output Low Voltage, Signals DDR_RESET_C{01/23}_N	—	—	$0.2*V_{CCD}$	V	1, 2
$V_{OH\_CMOS1.2V}$	Output High Voltage, Signals DDR_RESET_C{01/23}_N	$0.9*V_{CCD}$	—	—	V	1, 2
Control Signals						
R_{ON}	DDR4 Control Buffer On Resistance	25.5	30	34.5	ohm	6
DDR4 Miscellaneous Signals						
DRAM_PWR_OK_C{01/23}						
V_{IL}	Input Low Voltage	—	0.3*VCCD	—	mV	2, 3
V_{IH}	Input High Voltage	—	0.7*VCCD	—	mV	2, 4, 5
ALERT_N						
V_{IL}	Input Low Voltage	Vref-90	—	Vref - 70	mV	3
V_{IH}	Input High Voltage	Vref+70	—	Vref+90	mV	4
ODT	On Die Termination	36	45	54	ohms	

Notes:
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. The voltage rail V_{CCD} which will be set to 1.2 V nominal depending on the voltage of all DIMMs connected to the processor.
3. V_{IL} is the maximum voltage level at a receiving agent that will be interpreted as a logical low value.
4. V_{IH} is the minimum voltage level at a receiving agent that will be interpreted as a logical high value.
5. V_{IH} and V_{OH} may experience excursions above V_{CCD}. However, input signal drivers must comply with the signal quality specifications.
6. This is the pull down driver resistance. Reset drive does not have a termination.
7. R_{VTT_TERM} is the termination on the DIMM and not controlled by the processor. Please refer to the applicable DIMM datasheet.
8. The minimum and maximum values for these signals are programmable by BIOS to one of the pairs.
9. Input leakage current is specified for all DDR4 signals.
10. Vol = Ron * [VCCD/(Ron + Rtt_Eff)], where Rtt_Eff is the effective pull-up resistance of all DIMMs in the system, including ODTs and series resistors on the DIMMs.
11. This Ron value is only for UDIMM, otherwise the Ron Value is 30 ohm.

5.5.2.2 PECI DC Specifications

Symbol	Definition and Conditions	Min	Max	Units	Figure	Notes[1]
V_{In}	Input Voltage Range	-0.15	0.15 + V_{CCIO}	V		1
$V_{Hysteresis}$	Hysteresis	$0.1*V_{CCIO}$	—	V		
V_N	Negative-edge threshold voltage	$0.275*V_{CCIO}$	$0.500*V_{CCIO}$	V	Figure 5-1	2
V_P	Positive-edge threshold voltage	$0.550*V_{CCIO}$	$0.725*V_{CCIO}$	V	Figure 5-1	2
I_{Source}	Pullup Resistance (V_{OH} = $0.75*V_{CCIO}$)	-6.00	—	mA		
I_{Leak+}	High impedance state leakage to V_{CCIO} (V_{leak} = V_{OL})	±50	±200	µA		3, 4

Symbol	Definition and Conditions	Min	Max	Units	Figure	Notes[1]
R_{ON}	High impedance leakage to GND (V_{leak} = V_{OH})	41	11	Ω		
C_{Bus}	Bus capacitance per node	—	10	pF		5
V_{Noise}	Signal noise immunity above 300 MHz	0.100*V_{CCIO}	—	V_{p-p}		
	Output Edge Rate (50 ohm to V_{SS}, between V_{IL} and V_{IH})	5	15	V/ns		

Notes:
1. The input voltage range specifies an overshoot/undershoot that applies only to the PECI data signal and not to the V_{TT} reference itself.
2. It is expected that the PECI driver will take into account, the variance in the receiver input thresholds and consequently, be able to drive its output within safe limits (-0.150 V to 0.275*V_{CCIO} for the low level and 0.725*V_{CCIO} to V_{CCIO}+0.150 V for the high level).
3. V_{CCIO} nominal levels will vary between processor families. All PECI devices will operate at the V_{CCIO} level determined by the processor installed in the system.
4. The leakage specification applies to powered devices on the PECI bus.
5. Excessive capacitive loading on the PECI line may slow down the signal rise/fall times and consequently limit the maximum bit rate at which the interface can operate.

5.5.2.3 System Reference Clock (BCLK{0/1/2}) DC Specifications

Symbol	Parameter	Signal	Min	Max	Unit	Figure	Notes[1]
$V_{BCLK\_diff\_ih}$	Differential Input High Voltage	Differential	0.150	N/A	V	Figure 5-3	9
$V_{BCLK\_diff\_il}$	Differential Input Low Voltage	Differential	—	-0.150	V	Figure 5-3	9
V_{cross} (abs)	Absolute Crossing Point	Single Ended	0.250	0.550	V	Figure 5-4 and Figure 5-5	2, 4, 7, 9
V_{cross} (rel)	Relative Crossing Point	Single Ended	0.250 + 0.5*(VHavg - 0.700)	0.550 + 0.5*(V_{Havg} - 0.700)	V	Figure 5-4	3, 4, 5, 9
ΔV_{cross}	Range of Crossing Points	Single Ended	N/A	0.140	V	Figure 5-6	6, 9
V_{TH}	Threshold Voltage	Single Ended	Vcross - 0.1	Vcross + 0.1	V		9
I_{IL}	Input Leakage Current	N/A	—	1.50	mA		8, 9
C_{pad}	Pad Capacitance	N/A	1.90	1.72	pF		9

Notes:
1. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
2. Crossing Voltage is defined as the instantaneous voltage value when the rising edge of BCLK{0/1}_DN is equal to the falling edge of BCLK{0/1}_DP.
3. V_{Havg} is the statistical average of the VH measured by the oscilloscope.
4. The crossing point must meet the absolute and relative crossing point specifications simultaneously.
5. V_{Havg} can be measured directly using “Vtop” on Agilent* and “High” on Tektronix oscilloscopes.
6. V_{CROSS} is defined as the total variation of all crossing voltages as defined in Note 3.
7. The rising edge of BCLK{0/1}_DN is equal to the falling edge of BCLK{0/1}_DP.
8. For Vin between 0 and Vih.
9. Specifications can be validated at the pin.

Figure 5-3. BCLK{0/1/2} Differential Clock Measurement Point for Ringback

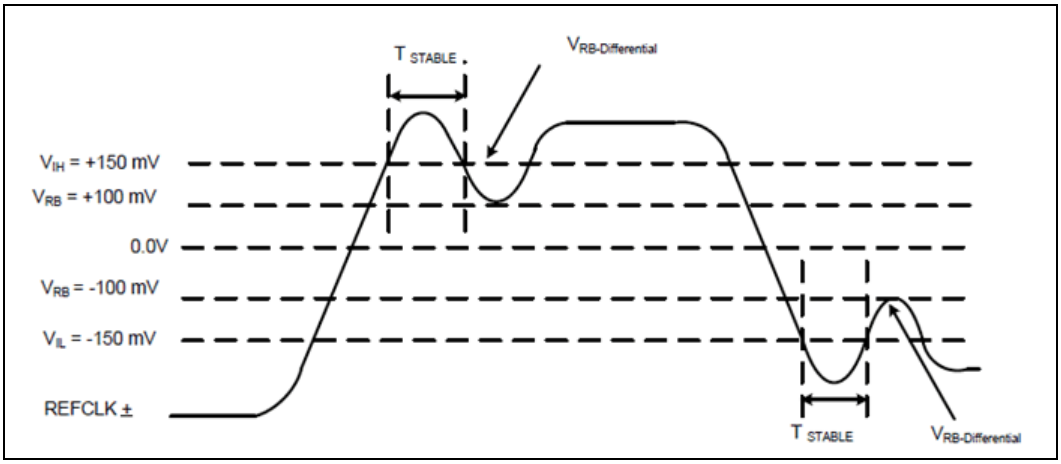


Figure 5-4. BCLK{0/1/2} Differential Clock Crosspoint Specification

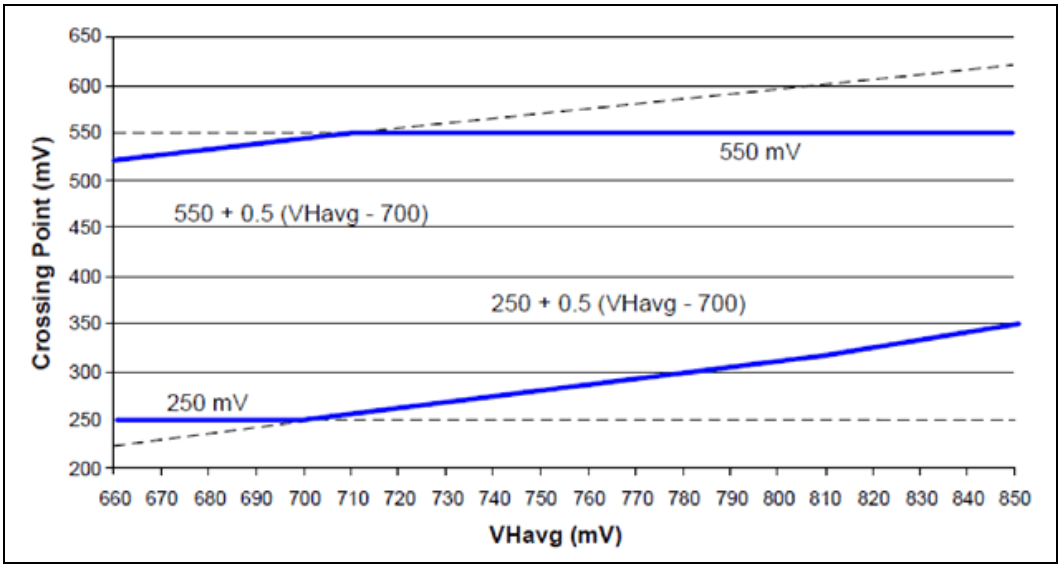


Figure 5-5. BCLK{0/1/2} Single Ended Clock Measurement Points for Absolute Cross Point and Swing

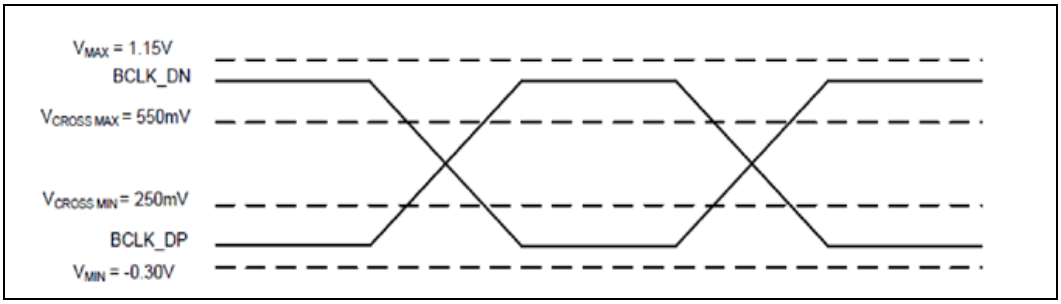
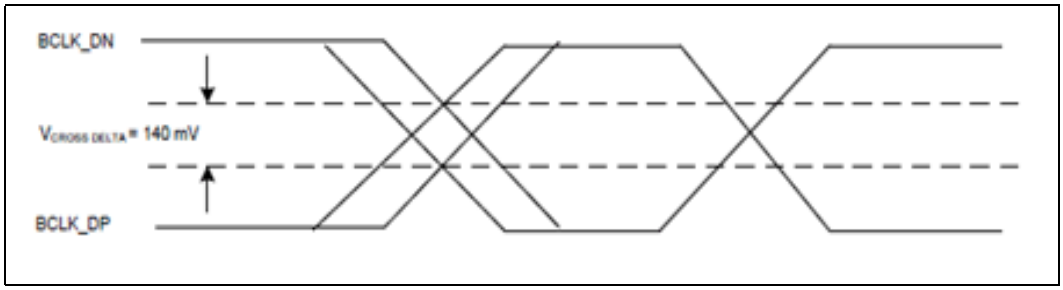


Figure 5-6. BCLK{0/1/2} Single Ended Clock Measure Points for Delta Cross Point



5.5.2.4 SMBus DC Specifications

Symbol	Parameter	Min	Max	Units	Notes
V_{IL}	Input Low Voltage	—	0.3*V_{CCIO}	V	
V_{IH}	Input High Voltage	0.7*V_{CCIO}	—	V	
$V_{Hysteresis}$	Hysteresis	0.1*V_{CCIO}	—	V	
V_{OL}	Output Low Voltage	—	0.2*V_{CCIO}	V	1
R_{ON}	Buffer On Resistance	14	4	Ω	
I_L	Leakage Current Signals	±50	±200	µA	
	Output Edge Rate (50 ohm to V_{CCIO}, between V_{IL} and V_{IH})	1.13	5	V/ns	1

Note:
1. Value obtained through test bench with 50 ohm pull up to V_{CCIO}.

5.5.2.5 JTAG and TAP Signals DC Specifications

Symbol	Parameter	Min	Max	Units	Notes
V_{IL}	Input Low Voltage	—	0.3*V_{CCIO}	V	
V_{IH}	Input High Voltage	0.7*V_{CCIO}	—	V	
V_{OL}	Output Low Voltage	—	0.2*V_{CCIO}	V	
$V_{Hysteresis}$	Hysteresis	0.1*V_{CCIO}	—		
SR	Input Slew Rate: TCK0, TCK1, BPM_N[7:0],TDI	0.05	—	V/ns	2
R_{ON}	Buffer On Resistance Signals BPM_N[7:0], TDO	14	4	Ω	
I_{IL}	Input Leakage Current Signals	±50	±200	µA	
SR	Output Edge Rate (50 ohm to V_{CCIO}) Signal: BPM_N[7:0], PRDY_N, TDO	1.13	5	V/ns	1

Notes:
1. These are measured between V_{IL} and V_{IH}.
2. The signal edge rate must be met or the signal must transition monotonically to the asserted state.

5.5.2.6 Serial VID Interface (SVID) DC Specifications

Symbol	Parameter	Min	Nom	Max	Units	Notes
V_{CCIO}	CPU I/O Voltage	V_{CCIO} - 5%	1.0	V_{CCIO} + 5%	V	1
V_{IL}	Input Low Voltage Signals SVIDDATA, SVIDALERT_N	—	—	0.3*V_{CCIO}	V	1
V_{IH}	Input High Voltage Signals SVIDDATA, SVIDALERT_N	0.7*V_{CCIO}	—	—	V	1
V_{OL}	Output Low Voltage Signals: SVIDCLK, SVIDDATA	—	—	0.2*V_{CCIO}	V	1, 6
$V_{Hysteresis}$	Hysteresis	0.1*V_{CCIO}	—	—	V	1
R_{ON}	Buffer On Resistance Signals SVIDCLK, SVIDDATA	14	—	4	Ω	2
I_{IL}	Input Leakage Current	±50	—	±200	µA	3, 4
	Input Edge Rate Signal: SVIDALERT_N	0.05	—	—	V/ns	5
	Output Edge Rate	1.13	—	5	V/ns	5, 6

Notes:
1. V_{CCIO} refers to instantaneous V_{CCIO}.
2. Measured at 0.31*V_{CCIO}.
3. Vin between 0V and V_{CCIO} (applies to SVIDDATA and SVIDALERT_N only).
4. N/A
5. These are measured between V_{IL} and V_{IH}.
6. Value obtained through test bench with 50 ohms pull-up to V_{CCIO}.

5.5.2.7 Processor Asynchronous Sideband DC Specifications

Symbol	Parameter	Min	Max	Units	Notes
CMOS input buffers					
V_{IL}	Input Low Voltage	—	0.3*V_{CCIO}	V	1, 2, 4
V_{IH}	Input High Voltage	0.7*V_{CCIO}	—	V	1, 2, 4
$V_{Hysteresis}$	Hysteresis Signals	0.1*V_{CCIO}	—	V	1,2, 4
SR_1	Input Slew Rate	0.005	—	V/ns	
SR_2	Input Slew Rate: PMSYNC	0.05	—	V/ns	
Open Drain Output buffers					
I_L	Input Leakage Current	±50	±200	µA	1, 2, 4
R_{ON}	Buffer On Resistance	14	4	Ω	1, 2, 4
SR	Output Edge Rate	1.13	5	V/ns	3, 5

Notes:
1. This table applies to the processor sideband and miscellaneous signals specified in Table 5-6, "Signal Groups".
2. Unless otherwise noted, all specifications in this table apply to all processor frequencies.
3. These are measured between V_{IL} and V_{IH}.
4. In the case of bidirectional signals they use either a CMOS output /CMOS input buffer or they use Open Drain / CMOS input buffer.
5. VOL level for open drain buffers may be obtained with the Buffer ON Resistance and the external 50 ohm pull-up to VCCIO.

5.5.2.8 Miscellaneous Signals DC Specifications

Symbol	Parameter	Min	Nominal	Max	Units	Notes
SKTOCC_N Signal						
$V_{O\_ABS\_MAX}$	Output Absolute Max Voltage	—	3.30	3.50	V	
I_{OMAX}	Output Max Current	—	—	1	mA	

§