

# **Processor Programming Reference (PPR) for AMD Family 1Ah Model 11h, Revision B0 Processors Volume 7 of 7**

# Legal Notices

© 2022-2024 Advanced Micro Devices, Inc. All rights reserved.

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of these materials, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of these materials, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by these materials. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

## Trademarks:

AMD, the AMD Arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc.

AGESA is a trademark of Advanced Micro Devices, Inc.

AMD Virtualization is a trademark of Advanced Micro Devices, Inc.

AMD-V is a trademark of Advanced Micro Devices, Inc.

Adobe is a registered trademark of Adobe.

Arm is a registered trademark of Arm Limited.

CXL is a trademark of Compute Express Link Consortium, Inc.

EPYC is a trademark of Advanced Micro Devices, Inc.

Infinity Fabric is a trademark of Advanced Micro Devices, Inc.

Linux is a registered trademark of Linus Torvalds.

MIPI I3C is a registered trademark of MIPI Alliance.

Microsoft is a registered trademark of Microsoft Corporation.

PCI Express is a registered trademark of PCI-SIG Corporation.

PCIe is a registered trademark of PCI-SIG Corporation.

SoundWire is a registered trademark of MIPI Alliance, Inc.

Windows is a registered trademark of Microsoft Corporation.

Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

Reverse engineering or disassembly is prohibited.

USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG ACTUAL OR DE FACTO VIDEO AND/OR AUDIO STANDARDS IS EXPRESSLY PROHIBITED WITHOUT ALL NECESSARY LICENSES UNDER APPLICABLE PATENTS. SUCH LICENSES MAY BE ACQUIRED FROM VARIOUS THIRD PARTIES INCLUDING, BUT NOT LIMITED TO, IN THE MPEG PATENT PORTFOLIO, WHICH LICENSE IS AVAILABLE FROM MPEG LA, L.L.C., 6312 S. FIDDLERS GREEN CIRCLE, SUITE 400E, GREENWOOD VILLAGE, COLORADO 80111.

# List of Chapters

Volume 1:

- 1**     [Overview](#)
- 2**     [Core Complex \(CCX\)](#)

Volume 2:

- 3**     [Reliability, Availability, and Serviceability \(RAS\) Features](#)

Volume 3:

- 4**     [System Management Unit \(SMU\)](#)

Volume 4:

- 5**     [Advanced Platform Management Link \(APML\)](#)
- 6**     [SB Temperature Sensor Interface \(SB-TSI\)](#)
- 7**     [Host System Management Port \(HSMP\)](#)
- 8**     [Data Fabric \(DF\)](#)
- 9**     [Unified Memory Controller \(UMC\)](#)

Volume 5:

- 10**    [Northbridge IO \(NBIO\)](#)

Volume 6:

- 11**    [Fusion Controller Hub \(FCH\)](#)

Volume 7:

- 12**    **Reserved**

**List of Namespaces**

**List of Definitions**

# Table of Contents

**12      Reserved**

# List of Figures

# List of Tables

**12 Reserved**

This chapter is intentionally left blank.

## List of Namespaces

Namespace	Heading(s)
Core::X86::Apic	2.1.13.2.2 [ <a href="#">Local APIC Registers</a> ]
Core::X86::Cpuid	2.1.14.1 [ <a href="#">CPUID Instruction Functions</a> ]
Core::X86::Msr	2.1.15.1 [ <a href="#">MSRs - MSR0000_xxxx</a> ] 2.1.15.2 [ <a href="#">MSRs - MSRC000_xxxx</a> ] 2.1.15.3 [ <a href="#">MSRs - MSRC001_0xxx</a> ] 2.1.15.4 [ <a href="#">MSRs - MSRC001_1xxx</a> ]
Core::X86::Pmc::Core	2.1.16.4 [ <a href="#">Large Increment per Cycle Events</a> ] 2.1.16.5.1 [ <a href="#">Floating-Point (FP) Events</a> ] 2.1.16.5.2 [ <a href="#">Load/Store (LS) Events</a> ] 2.1.16.5.3 [ <a href="#">Instruction Cache (IC) and Branch Prediction (BP) Events</a> ] 2.1.16.5.4 [ <a href="#">DE Events</a> ] 2.1.16.5.5 [ <a href="#">EX (SC) Events</a> ]
Core::X86::Pmc::L2	2.1.16.5.6 [ <a href="#">L2 Cache Events</a> ]
Core::X86::Pmc::L3	2.1.16.6.1 [ <a href="#">L3 Cache PMC Events</a> ]
Core::X86::Smm	2.1.13.1.6 [ <a href="#">System Management State</a> ]
DF	8.4.1 [ <a href="#">Function 4 Registers</a> ] 8.4.2 [ <a href="#">Function 7 Registers</a> ]
FCH::AOAC	11.3.7 [ <a href="#">Always On Always Connected (AOAC) Registers</a> ]
FCH::GPIO	11.3.10.2 [ <a href="#">GPIO Registers</a> ]
FCH::IO	11.3.1.1 [ <a href="#">Registers</a> ]
FCH::IOAPIC	11.3.2.1 [ <a href="#">IOAPIC Registers</a> ]
FCH::IOMUX	11.3.10.1.1 [ <a href="#">IOMUX Functional Table</a> ]
FCH::ITF::ESPI	11.3.8.2 [ <a href="#">eSPI Registers</a> ]
FCH::LPCHOSTSPIR EG	11.3.8.1.2 [ <a href="#">Serial Peripheral Interface (SPI) Registers</a> ]
FCH::MISC	11.3.9.1 [ <a href="#">Miscellaneous (MISC) Registers</a> ]
FCH::MISC2	11.3.9.2 [ <a href="#">Miscellaneous (MISC2) Registers</a> ]
FCH::PM	11.3.9.3 [ <a href="#">Power Management (PM) Registers and Standard ACPI Registers</a> ]
FCH::PM::RTCEXT	11.3.9.4 [ <a href="#">RTC External Registers</a> ]
FCH::RMTGPIO	11.3.10.3 [ <a href="#">REMOTE GPIO</a> ]



	<a href="#">and IOMUX Registers</a> ]
FCH::SMI	11.3.3 [ <a href="#">SMI Registers</a> ]
FCH::TMR::ACDC	11.3.6 [ <a href="#">Wake Alarm Device (AcDcTimer) Registers</a> ]
FCH::TMR::HPET	11.3.4 [ <a href="#">High Precision Event Timer (HPET) Registers</a> ]
FCH::TMR::WDT	11.3.5 [ <a href="#">Watchdog Timer (WDT) Registers</a> ]
IO	2.1.9 [ <a href="#">PCI Configuration Legacy Access</a> ]
IOHC	10.2.2.1 [ <a href="#">IOHC Registers</a> ]
L3::L3CRB	2.2.1 [ <a href="#">L3 MSR Registers</a> ]
L3::L3CT	2.2.2 [ <a href="#">L3 Clocks and Test (CT) MSR Registers.</a> ]
MCA::CS	3.2.5.8 [ <a href="#">CS</a> ]
MCA::DE	3.2.5.4 [ <a href="#">DE</a> ]
MCA::EX	3.2.5.5 [ <a href="#">EX</a> ]
MCA::FP	3.2.5.6 [ <a href="#">FP</a> ]
MCA::IF	3.2.5.2 [ <a href="#">IF</a> ]
MCA::KPX::GMI	3.2.5.17 [ <a href="#">KPX GMI</a> ]
MCA::KPX::SERDES	3.2.5.16 [ <a href="#">KPX SERDES</a> ]
MCA::L2	3.2.5.3 [ <a href="#">L2</a> ]
MCA::L3	3.2.5.7 [ <a href="#">L3</a> ]
MCA::LS	3.2.5.1 [ <a href="#">LS</a> ]
MCA::MP5	3.2.5.13 [ <a href="#">MP5</a> ]
MCA::MPDMA	3.2.5.24 [ <a href="#">MPDMA</a> ]
MCA::NBIF	3.2.5.20 [ <a href="#">NBIF</a> ]
MCA::NBIO	3.2.5.14 [ <a href="#">NBIO</a> ]
MCA::PCIE	3.2.5.15 [ <a href="#">PCIE</a> ]
MCA::PCS::GMI	3.2.5.18 [ <a href="#">PCS GMI</a> ]
MCA::PCS::XGMI	3.2.5.19 [ <a href="#">PCS XGMI</a> ]
MCA::PIE	3.2.5.9 [ <a href="#">PIE</a> ]
MCA::PSP	3.2.5.11 [ <a href="#">PSP</a> ]
MCA::SATA	3.2.5.23 [ <a href="#">SATA</a> ]
MCA::SHUB	3.2.5.21 [ <a href="#">SHUB</a> ]
MCA::SMU	3.2.5.12 [ <a href="#">SMU</a> ]
MCA::UMC	3.2.5.10 [ <a href="#">UMC</a> ]
MCA::USB	3.2.5.22 [ <a href="#">USB</a> ]
SBRMI	5.6 [ <a href="#">SB-RMI Registers</a> ]
SBTSI	6.4 [ <a href="#">SB-TSI Registers</a> ]
SMU::THM	4.4.1 [ <a href="#">Registers</a> ]
UMC	9.3.1 [ <a href="#">Controller Registers</a> ]
UMC::PMC	9.2.1 [ <a href="#">UMC Performance Monitor Events</a> ]

## List of Definitions

**ABS:** [ABS](#)(integer expression): Remove sign from signed value.

**AGESA™:** AMD Generic Encapsulated Software Architecture.

**AP:** Application [Processor](#).

**APML:** Advanced Platform Management Link.

**ARA:** Alert response address.

**ARP:** Address Resolution Protocol

**ASP:** AMD Secure Processor. Provides run time security services.

**BAR:** The [BAR](#), or base address register, physical register mnemonic format is of the form PREFIXxZZZ. PREFIX is an all capital letter name that connotes the BAR to which the offset is added to get the physical address of the operation. ZZZ is the offset.

**BCD:** Binary Coded Decimal number format.

**BCS:** Base Configuration Space.

**BIST:** Built-In Self-Test. Hardware within the processor that generates test patterns and verifies that they are stored correctly (in the case of memories) or received without error (in the case of links).

**BMC:** Base management controller.

**Boot VID:** Boot Voltage ID. This is the VDD and VDDNB voltage level that the processor requests from the external voltage regulator during the initial phase of the cold boot sequence.

**BSC:** Boot strap core. Core 0 of the [BSP](#).

**BSP:** Boot strap processor.

**C-states:** These are ACPI defined core power states. C0 is operational. All other [C-states](#) are low-power states in which the processor is not executing code. See [docACPI](#).

**Canonical-address:** An address in which the state of the most-significant implemented bit is duplicated in all the remaining higher-order bits, up to bit[63].

**CCC:** Common Command Code for I3C

**CCD:** Core Complex Die.

**CCX:** Core Complex where more than one core shares L3 resources.

**CEIL:** [CEIL](#)(real expression): Rounds real number up to nearest integer.

**CMP:** Specifies the core number.

**COF:** Current operating frequency of a given clock domain.

**Cold reset:** PWROK is de-asserted and RESET\_L is asserted.

**Configurable:** Indicates that the access type is configurable as described by the documentation.

**Controller or I3C Controller:** The device that initiates and terminates all communication and drives the clock, SCL.

**CoreCOF:** Core current operating frequency in MHz.  $\text{CoreCOF} = \text{Core}::\text{X86}::\text{Msr}::\text{PStateDef}[\text{CpuFid}[11:0]] * 5\text{MHz}$ .

**COUNT:** [COUNT](#)(integer expression): Returns the number of binary 1's in the integer.

**CpuCoreNum:** Specifies the core number.

**CPUID:** The [CPUID](#), or x86 processor identification state, physical register mnemonic format is of the form CPUID FnXXXX\_XXXX\_EiX[\_xYYY], where XXXX\_XXXX is the hex value in the EAX and YYY is the hex value in ECX.

**Decode Error:** This is a PCI-defined term that is applied to transactions on other than PCI buses. It indicates that the transaction is terminated without affecting the intended target; Reads return all 1s; Writes are discarded; the decode error code is returned in the response, if applicable; decode error bits are set if applicable.

**DE:** Data Fabric, also known as AMD Infinity Fabric™, is a technology introduced by AMD that enables high-speed and efficient communication between different components within a system.

**DID:** Divisor Identifier. Specifies the post-PLL divisor used to reduce the [COF](#).

**docACPI:** Advanced Configuration and Power Interface (ACPI) Specification; <http://www.acpi.info>.

**docAPM1:** AMD64 Architecture Programmer's Manual Volume 1: Application Programming, Publication No. 24592.

**docAPM2:** AMD64 Architecture Programmer's Manual Volume 2: System Programming, Publication No. 24593.

**docAPM3:** AMD64 Architecture Programmer's Manual Volume 3: Instruction-Set Reference, Publication No. 24594.

**docAPM4:** AMD64 Architecture Programmer's Manual Volume 4: 128-Bit and 256-Bit Media Instructions, Publication No. 26568.

**docAPM5:** AMD64 Architecture Programmer's Manual Volume 5: 64-Bit Media and x87 Floating-Point Instructions, Publication No. 26569.

**docI3C:** MIPI I3C® Specification; <http://www.mipi.org>.

**docJEDEC:** JEDEC Standards; <http://www.jedec.org>.

**docPCIe:** PCI Express® Specification; <http://www.pcisig.com>.

**docPCIlb:** PCI Local Bus Specification; <http://www.pcisig.com>.

**docRevG:** Revision Guide for AMD Family 1Ah Models 10-1Fh Processors, Publication No. 58730.

**docSEV:** Secure Encrypted Visualization API Specification, Publication No. 55766.

**docSMB:** System Management Bus ([SMBus](#)) Specification; <http://www.smbus.org>.

**Doubleword:** A 32-bit value.

**DW:** [Doubleword](#).

**EC:** Embedded Controller.

**ECS:** Extended Configuration Space.

**ENTDAA:** Enter Dynamic Address Assignment [CCC](#) for I3C

**Error-on-read:** Error occurs on read.

**Error-on-write:** Error occurs on write.

**Error-on-write-0:** Error occurs on bitwise write of 0.

**Error-on-write-1:** Error occurs on bitwise write of 1.

**FCH:** The integrated platform subsystem that contains the IO interfaces and bridges them to the system BIOS. Previously included in the Southbridge.

**FID:** Frequency Identifier. Specifies the PLL frequency multiplier for a given clock domain.

**FLOOR:** [FLOOR](#)(integer expression): Rounds real number down to nearest integer.

**GT/s:** Giga-Transfers per second.

**HSMP:** Host System Management Port

**HWPF:** Hardware Prefetcher.

**IBS:** Instruction based sampling.

**IFCM:** Isochronous flow-control mode, as defined in the link specification.

**Inaccessible:** Not readable or writable (e.g., Hide ? [Inaccessible](#) : Read-Write).

**IO configuration:** Access to configuration space through IO ports CF8h and CFCh.

**IOD:** I/O Die.

**IOHC:** IOHUB Core; the I/O crossbar.

**IOMMU:** I/O Memory Management Unit.

**IORR:** IO range register.

**KBC:** Keyboard Controller.

**L1 cache:** The level 1 caches (instruction cache and the data cache).

**L2 cache:** The level 2 caches.

**Linear (virtual) address:** The address generated by a core after the segment is applied.

**LINT:** Local interrupt.

**Logical address:** The address generated by a core before the segment is applied.

**logical mnemonic:** The register mnemonic format that describes the register functionally, what namespace to which the register belongs, a name for the register that connotes its function, and optionally, named parameters that indicate the different function of each instance (e.g., Link::Phy::PciDevVendIDF3). See 1.4.3.1 [[Logical Mnemonic](#)].

**LRU:** Least recently used.

**LVT:** Local vector table. A collection of APIC registers that define interrupts for local events (e.g., APIC[530:500] [Extended Interrupt [3:0] Local Vector Table]).

**Macro-op:** The front-end of the pipeline breaks instructions into macro-ops and transfers (dispatches) them to the back-end of the pipeline for scheduling and execution. See Software Optimization Guide.

**MAX:** [MAX](#)(integer expression list): Picks maximum integer or real value of comma separated list.

**MB:** Megabyte; 1024 KB.

**MCA:** Machine Check Architecture.

**MCAX:** Machine Check Architecture eXtensions.

**MDC:** Mega Data Center

**MergeEvent:** A [PMC](#) event that is capable of counter increments greater than 15, thus requiring merging a pair of even/odd performance monitors.

**Micro-op:** Processor schedulers break down macro-ops into sequences of even simpler instructions called micro-ops, each of which specifies a single primitive operation. See Software Optimization Guide.

**MIN:** [MIN](#)(integer expression list): Picks minimum integer or real value of comma separated list.

**MMIO:** Memory-Mapped Input-Output range. This is physical address space that is mapped to the IO functions such as the IO links or [MMIO](#)

[configuration](#).

**MMIO configuration:** Access to configuration space through memory space.

**MP1:** Power Management Microprocessor (also see [PMFW](#)).

**MP5:** System and Power Management Microprocessor for the [CCD](#).

**MPB:** Microcode patch block.

**MSR:** The [MSR](#), or x86 model specific register, physical register mnemonic format is of the form MSRXXXX\_XXXX, where XXXX\_XXXX is the hexadecimal MSR number. This space is accessed through x86 defined RDMSR and WRMSR instructions.

**MTRR:** Memory-type range register. The MTRRs specify the type of memory associated with various memory ranges.

**NBC:**  $NBC = (CPUID Fn00000001\_EBX[LocalApicId[3:0]] == 0)$ . Node Base Core. The lowest numbered core in the node.

**NTA:** Non-Temporal Access.

**NTB:** Non-transparent bridge. A device that links the memory space of two separate systems together. The processor implements a [NTB](#) that connects two systems together using the [PCIe®](#) interface.

**ODTS:** On die temperature sensing. UMC could be configured to manage DIMM thermals via command throttling and appropriate refresh rate based on temperature range reported by inband MR4 reading from DRAM devices.

**OOB:** Out of Band interface, typically referring to [APML](#) as opposed to In Band interface which refers to [HSMF](#)

**Operational frequency:** The frequency at which the processor operates.

**OW:** Octword. An 128-bit value.

**P-state:** Performance state.

**PCICFG:** The [PCICFG](#), or PCI defined configuration space, physical register mnemonic format is of the form DXFYxZZZ. Bus 0 is implied, X specifies the hexadecimal device number (this may be 1 or 2 digits). Y specifies the function number. ZZZ specifies the hexadecimal byte address (this may be 2 or 3 digits). Example: D18F2x40 specifies the register at bus 0, device 18h, function 2, and address 40h. If the mnemonic starts with B, then the [physical mnemonic](#) format is BWWDXYFYxZZZ where WW specifies the hexadecimal bus number (1 or 2 hex digits) or "XX" implying that the bus is relocatable. Example: BXXD00F6x40 specifies that the bus is relocatable, B0AD00F2x000 specifies that the bus is 0Ah.

**PCIe®:** PCI Express.

**PCS:** Physical Coding Sublayer.

**PEC:** Packet Error Checking or Packet Error Code.

**physical mnemonic:** The register mnemonic that is formed based on the physical address used to access the register (e.g., D18F3x00). See 1.4.3.2 [[Physical Mnemonic](#)].

**PMC:** The PMC, or x86 performance monitor counter, physical register mnemonic format is any of the forms {PMCxXXX, L2IPMCxXXX, NBPMMCxXXX}, where XXX is the performance monitor select.

**PMFW:** Power Management firmware. The main functionality of PMFW is to execute power management algorithms to control clock frequencies and voltages in the SOC to manage power, current and thermal infrastructure limits.

**POR:** Power on reset.

**POW:** [POW](#)(base, exponent): [POW](#)(x,y) returns the value x to the power of y.

**PPIN:** Protected Processor Inventory Number.

**Processor:** System on Chip (SoC) covered by this PPR. See 1.8 [[Processor Overview](#)].

**PSP:** AMD Platform Security Processor (legacy term). Replaced by AMD Secure Processor (see [ASP](#)).

**PTE:** Page table entry.

**QW:** Quadword. A 64-bit value.

**RAS:** Reliability, availability and serviceability (industry term). See 3.1 [[Machine Check Architecture](#)].

**REFCLK:** Reference clock. Refers to the clock frequency (100 MHz) or the clock period (10 ns) depending on the context used.

**register instance parameter specifier:** A [register instance parameter specifier](#) is of the form [\\_register parameter name](#)[[register parameter value list](#)] (e.g., The register instance parameter specifier [\\_dct\[1:0\]](#) has a [register parameter name](#) of [dct](#) (The DCT PHY instance name) and a register parameter value list of "1:0" or 2 instances of DCT PHY).

**register instance specifier:** The [register instance specifier](#) exists when there is more than one instance for a register. The register instance specifier consists of one or more register instance parameter specifier (e.g., The register instance specifier [\\_dct\[1:0\]\\_chiplet\[BCST,3:0\]\\_pad\[BCST,11:0\]](#) consists of 3 register instance parameter specifiers, [\\_dct\[1:0\]](#),

[\\_chiplet\[BCST,3:0\]](#), and [\\_pad\[BCST,11:0\]](#)).

**register name:** A name that connotes the function of the register.

**register namespace:** A namespace for which the [register name](#) must be unique. A [register namespace](#) indicates to which IP it belongs and an IP may have multiple namespaces. A namespace is a string that supports a list of "::-" separated names. The convention is for the list of names to be hierarchical, with the most significant name first and the least significant name last (e.g., Link::Phy::Rx is the RX component in the Link PHY).

**register parameter name:** A register parameter name is the name of the number of instances at some level of the logical hierarchy (e.g., The register parameter name [dct](#) specifies how many instances of the DCT PHY exist).

**register parameter value list:** The register parameter value list is the logical name for each instance of the register parameter name (e.g., For [\\_dct\[1:0\]](#), there are 2 DCT PHY instances, with the logical names 0 and 1, but it should be noted that the logical names 0 and 1 can correspond to physical values other than 0 and 1). It is the purpose of the AddressMappingTable to map these register parameter values to physical address values for the register.

**Reserved-write-as-0:** Reads are undefined. Must always write 0.

**Reserved-write-as-1:** Reads are undefined. Must always write 1.

**ROUND:** [ROUND](#)(real expression): Rounds to the nearest integer; halfway rounds away from zero.

**RTS:** Remote temperature sensor, typical examples are ADM1032, LM99, MAX6657, EMC1002.

**SB-RMI:** Remote Management interface.

**SB-TSI:** Sideband Internal Temperature Sensor Interface. See [APML](#).

**SBI:** Sideband interface.

**SDR:** Single Data Rate

**SDU:** Scan Dump Utility

**SETDASA:** Set Dynamic Address from Static Address CCC for I3C

**Shutdown:** A state in which the affected core waits for either INIT, RESET, or NMI. When shutdown state is entered, a shutdown special cycle is sent on the IO links.

**SMBus:** System Management Bus

**SMI:** System management interrupt.

**SMM:** System Management Mode.

**SMN:** System Management Network

**SMT:** Simultaneous multithreading. See Core::X86::CpuId::CoreId[ThreadsPerCore].

**Speculative event:** A performance monitor event counter that counts all occurrences of the event even if the event occurs during speculative code execution.

**SSC:** Spread Spectrum Clocking.

**SVM:** Secure virtual machine.

**Target or I3C target:** The target cannot initiate I3C communication and cannot drive the clock but can drive the data signal SDA and the alert signal ALERT\_L.

**Tcd:** Processor temperature control value.

**TDC:** Thermal Design Current.

**TDP:** Thermal Design Power. A power consumption parameter that is used in conjunction with thermal specifications to design appropriate cooling solutions for the processor.

**Thread:** One architectural context for instruction execution.

**TOM2:** Top of extended Memory.

**TSI:** Temperature sensor interface.

**TSM:** Temperature sensor macro.

**TSOD:** Temperature sensor mounted on DIMM PCB.

**UMI:** Unified Media Interface. The link between the processor and the [FCH](#).

**UNIT:** [UNIT](#)(register field reference): Input operand is a register field reference that contains a valid values table that defines a value with a unit (e.g., clocks, ns, ms, etc.). This function takes the value in the register field and returns the value associated with the unit (e.g., If the field had a valid value definition where 1010b was defined as 5 ns). Then if the field had the value of 1010b, then [UNIT\(\)](#) would return the value 5.

**Unpredictable:** The behavior of both reads and writes is unpredictable.

**VID:** Voltage level identifier.

**VMPL:** Virtual Machine Privilege Level.

**Volatile:** Indicates that a register field value may be modified by hardware, firmware, or microcode when fetching the first instruction and/or might have read or write side effects. No read may depend on the results of a previous read and no write may be omitted based on the value of a previous read or write. Not volatile indicates that software may service a read from the results of a previous read and that a write may be dropped if it's value matches the value previously read or written.

**Warm reset:** RESET\_L is asserted only (while PWROK stays high).

**WDT:** Watchdog timer. A timer that detects activity and triggers an error if a specified period of time expires without the activity.

**WRIG:** Writes Ignored.

**Write-0-only:** Writing a 0 clears to a 0; Writing a 1 has no effect. If not associated with Read, then reads are undefined.

**Write-1-only:** Writing a 1 sets to a 1; Writing a 0 has no effect. If not associated with Read, then reads are undefined.

**Write-1-to-clear:** Writing a 1 clears to a 0; Writing a 0 has no effect. If not associated with Read, then reads are undefined.

**Write-once:** Capable of being written once; all subsequent writes have no effect. If not associated with Read, then reads are undefined.

**X2APICEN:** x2 APIC is enabled. X2APICEN =

(Core::X86::Msr::APIC\_BAR[ApicEn] &&

Core::X86::Msr::APIC\_BAR[x2ApicEn]).

**XBAR:** Cross bar; command packet switch.

**xGMI:** A high-bandwidth, low-latency interconnect link between two processors (CPU sockets).