

# Intel Xeon 4214 processor

---



<b>Artikel</b>	110557
<b>Herstellernummer</b>	BX806954214
<b>EAN</b>	0735858415613
Intel	

## **Intel® Turbo-Boost-Technik**

Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

## **Intel® vPro™ Plattformqualifizierung**

Intel® vPro™-Technik ist eine Zusammenstellung von Sicherheits- und Verwaltungsfunktionen, die in den Prozessor integriert sind und vier kritische Bereiche in der IT-Sicherheit handhaben: 1) Bedrohungsverwaltung, darunter Schutz vor Rootkits, Viren und Malware, 2) Schutz von Identitäten und Website-Zugriffspunkten, 3) Schutz von vertraulichen persönlichen und geschäftlichen Daten, 4) Remote- und lokale Überwachung, Korrektur und Reparatur von PCs und Workstations.

## **Intel® Hyper-Threading-Technik**

Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

## **Intel® Virtualisierungstechnik (VT-x)**

Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

## **Intel® Directed-I/O-Virtualisierungstechnik (VT-d)**

Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

## **Intel® VT-x mit Extended Page Tables (EPT)**

Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

## **Intel® TSX-NI**

Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

## **Intel® 64**

In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.<sup>1</sup> Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

## **Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

## **Erweiterungen des Befehlssatzes**

Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

## **Anzahl der AVX-512 FMA-Einheiten**

Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

## **Erweiterte Intel SpeedStep® Technologie**

Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

## **Intel® Speed Shift Technology**

Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

# **Zusammenfassung**

---

## **Intel® Turbo-Boost-Technik**

Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

## **Intel® vPro™ Plattformqualifizierung**

Intel® vPro™-Technik ist eine Zusammenstellung von Sicherheits- und Verwaltungsfunktionen, die in den Prozessor integriert sind und vier kritische Bereiche in der IT-Sicherheit handhaben: 1) Bedrohungsverwaltung, darunter Schutz vor Rootkits, Viren und Malware, 2) Schutz von Identitäten und Website-Zugriffspunkten, 3) Schutz von vertraulichen persönlichen und geschäftlichen Daten, 4) Remote- und lokale Überwachung, Korrektur und Reparatur von PCs und Workstations.

## **Intel® Hyper-Threading-Technik**

Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

## **Intel® Virtualisierungstechnik (VT-x)**

Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie

bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

### **Intel® Directed-I/O-Virtualisierungstechnik (VT-d)**

Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

### **Intel® VT-x mit Extended Page Tables (EPT)**

Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

### **Intel® TSX-NI**

Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

### **Intel® 64**

In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.<sup>1</sup> Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

### **Befehlssatz**

Ein Befehlssatz bezeichnet den Satz grundlegender Befehle und Anweisungen, die ein Mikroprozessor versteht und ausführen kann. Der angezeigte Wert gibt an, mit welchem Intel Befehlssatz dieser Prozessor kompatibel ist.

### **Erweiterungen des Befehlssatzes**

Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

### **Anzahl der AVX-512 FMA-Einheiten**

Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

### **Erweiterte Intel SpeedStep® Technologie**

Die Erweiterte Intel SpeedStep® Technologie ist eine fortschrittliche Funktionalität für die auf Mobilgeräten benötigte Kombination von hoher Leistung bei einem möglichst niedrigen Energieverbrauch. Die herkömmliche Intel SpeedStep® Technologie schaltet die Spannung und die Frequenz je nach Prozessorauslastung gleichzeitig zwischen hohen und niedrigen Werten um. Die Erweiterte Intel SpeedStep® Technologie baut auf dieser Architektur auf und nutzt Designstrategien wie Trennung zwischen Spannungs- und Frequenzänderungen sowie Taktpartitionierung und Wiederherstellung.

### **Intel® Speed Shift Technology**

Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

Intel Xeon 4214, Intel® Xeon Silver, LGA 3647 (Socket P), 14 nm, Intel, 2,2 GHz, 64-Bit

Intel Xeon 4214. Prozessorfamilie: Intel® Xeon Silver, Prozessorsockel: LGA 3647 (Socket P), Prozessor Lithografie: 14 nm. Speicherkanäle: Hexa-Kanal, Maximaler interner Speicher, vom Prozessor unterstützt: 1,02 TB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM. Marktsegment: Server, Unterstützte Befehlssätze: SSE4.2, AVX, AVX 2.0, AVX-512, Skalierbarkeit: 2S. Verpackungsart: Einzelhandels-Box. Prozessor-Paketgröße: 76mm x 56.5mm

## Merkmale

### Betriebsbedingungen

Tcase	77 °C
-------	-------

### Gewicht und Abmessungen

Prozessor-Paketgröße	76mm x 56.5mm
----------------------	---------------

### Logistikdaten

Warentarifnummer (HS)	85423119
-----------------------	----------

### Sonstige Funktionen

RAM-Speicher maximal	1 TB
----------------------	------

### Verpackungsdaten

Verpackungsart	Einzelhandels-Box
----------------	-------------------

### Grafik

Eingebaute Grafikkadapler	Nein
Separater Grafikkadapler	Nein
On-Board	Nicht verfügbar
Grafikkadaplermodell	
Dediziertes	Nicht verfügbar
Grafikkadaplermodell	

### Speicher

Maximaler interner Speicher, vom	1,02 TB
Prozessor unterstützt	
Speichertypen, vom Prozessor	DDR4-SDRAM
unterstützt	
Speichertaktraten, vom	2400 MHz
Prozessor unterstützt	
Speicherkanäle	Hexa-Kanal
ECC	Ja

### Technische Details

Startdatum	Q2'19
Produkttyp	Processor
Status	Launched
Unterstützte Arbeitsspeicher	DDR4-SDRAM
Speichergeschwindigkeit (max.)	2400 MHz
Anzahl der UPI-Links	2
Instandhaltungszustand	Baseline Servicing

### Merkmale

Execute Disable Bit	Ja
Marktsegment	Server
Maximale Anzahl der PCI-Express-Lanes	48
PCI-Express-Slots-Version	3.0
Unterstützte Befehlssätze	SSE4.2, AVX, AVX 2.0, AVX-512
Skalierbarkeit	2S
Eingebettete Optionen verfügbar	Ja
PCI Express CEM Revision	3.0
Exportkontroll-	5A992C
Klassifizierungsnummer (ECCN)	
Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS)	G077159

### Prozessor

Prozessorhersteller	Intel
Prozessorgeneration	Skalierbare Intel® Xeon® der 2. Generation
Prozessor	4214
Grundfrequenz des Prozessors	2,2 GHz
Prozessorfamilie	Intel® Xeon Silver
Anzahl Prozessorkerne	12
Prozessorsockel	LGA 3647 (Socket P)
Komponente für	Server/Arbeitsstation
Prozessor Lithografie	14 nm
Prozessor-Threads	24
Prozessorbetriebsmodi	64-Bit
Prozessor Boost-Frequenz	3,2 GHz
Prozessor-Cache	16,5 MB
Thermal Design Power (TDP)	85 W
Box	Ja
Kühler enthalten	Ja
Prozessor Codename	Cascade Lake

## Prozessor Besonderheiten

Intel® Hyper-Threading-Technik (Intel® HT Technology)	Ja
Intel® Turbo-Boost-Technologie	2.0
Intel® AES New Instructions (Intel® AES-NI)	Ja
Verbesserte Intel SpeedStep Technologie	Ja
Intel® Trusted-Execution-Technik	Ja
Intel®-Speed-Shift-Technologie	Ja
Intel® Transactional Synchronization Extensions	Ja
Intel® VT-x mit Extended Page Tables (EPT)	Ja
Intel® TSX-NI	Ja
Intel® 64	Ja
Intel® Virtualization Technologie (VT-X)	Ja
Intel® Virtualisierungstechnik für direkte I/O (VT-d)	Ja
Intel Turbo Boost Max Technology 3.0	Nein
AVX-512 Abgesicherte Multiply-Add (FMA) Einheiten	1
Intel® Deep Learning Boost (Intel® DL Boost)	Ja
Intel® Speed Select-Technologie - Leistungsprofil (Intel® SST-PP)	Nein
Intel® Resource Director Technology (Intel® RDT)	Ja
Intel® Volume Management Device (VMD)	Ja
Intel® Run Sure Technology	Nein
Modusbasierte Execute Control (MBE)	Ja
Intel® Optane™ DC Persistent Memory unterstützt	Nein
Intel® vPro™ Platform Eligibility	Ja
Intel Speed Select Technology (SST)	Nein
Intel® Speed Select Technology -Base Frequency (Intel® SST-BF)	-Nein
Intel® Optane™ DC Persistent Memory-Technologie	Nein

Preisänderungen und Irrtümer vorbehalten. Alle Produkte solange der Vorrat reicht.